PSR

2020 Payment Security Report

verizon

About the cover

In many organizations, data protection and compliance responsibilities ultimately fall on the shoulders of the Chief Information Security Officer (CISO).

At a time of increasing complexity, many CISOs must wrestle with organizational data security proficiency constraints and inadequate leadership support when designing and executing data protection strategies. They often feel overwhelmed by the speed and scope of their responsibilities, and find that introducing more technologies is not the answer.

The cover design hints at the solution: an aerial view of a bridge surrounded by seven trapdoors. The bridge represents a solid, direct path to compliance that provides safe passage during a time of growing data security challenges.

Data compromises are not necessarily inevitable. They can be prevented, but that requires more than conventional thinking. CISOs need to strategize to build sound data security programs that can also adapt when the waters rise. In this report, we identify how to address the top seven data protection management traps that impede sound data security.

That way when shift happens, your organization won't get trapped in a breach.

Table of contents

01

02

03

04

Verizon has published the Payment Security Report (PSR) since 2010, when we presented the industry with a first-ever study on the actual value and performance of the Payment Card Industry Data Security Standard (PCI DSS). The first and only report of its kind, the PSR provides an in-depth perspective on the regulatory landscape of the payment card industry (PCI). A decade after the first edition, it remains the most anticipated report within the industry that directly addresses the challenges of protecting payment data and meeting compliance requirements.

With every edition, the PSR reveals groundbreaking insights that help shape the industry's understanding of data protection successes and failures, as well as previously undervalued or unknown cause-and-effect factors.

This report is available online at verizon.com/paymentsecurityreport

10
— Years —

What our readers are telling us:

Verizon's 2019 Payment Security Report—Not Just for PCI

"If you are responsible for cybersecurity or data protection in your organization, stop what you are doing and read this report. Actually, first, go patch your servers and applications, and then read this report. Much like Verizon's Data Breach Investigations Report (DBIR), the Payment Security Report (PSR) is a must-read for security professionals. ... The compliance statistics are informative and show some alarming trends about how well companies are protecting payment card data. Those trends should cause any CISO to look closely at how their organization is handling data protection—and not just for payment cards. ... When I downloaded the PSR, I expected the usual treasure trove of data Verizon usually provides. What delighted me, however, was the report provided a very accessible way to improve security and compliance posture. ... Reading the Verizon report is a good start, but the real value comes from implementing the recommendations. This will ensure greater data protection as well as help with audit compliance."

—Anthony Israel-Davis, Tripwire

Anthony Israel-Davis, "Verizon's 2019 Payment Security Report—Not Just for PCI," The State of Security Blog, Tripwire Inc., Dec 3, 2019.

https://www.tripwire.com/state-of-security/regulatory-compliance/verizons-2019-payment-report/

Verizon Payment Security Report history

In this report, we distill a range of security and compliance subjects into valuable insights to help CISOs and others break down complex thinking into digestible bits. We explore various tools, tactics and methods applied by numerous organizations and take a look at why some companies accomplish so much more than others in their efforts to achieve sustainable and effective data security. We distinguish between approaches that separate busy security teams from productive security teams, the different ways decisions are made that impact how strategies are formed, and which goals are embraced. For example, why are technology solutions prioritized while the maturity development of capabilities and processes are ignored? How can leaders adapt, innovate and evolve during challenging times to improve their control environment posture and security cultures? The recommendations included in this report should have an immediate, positive impact. We explain the top security pitfalls and present solutions to equip CISOs with approaches to take with data security compliance challenges.

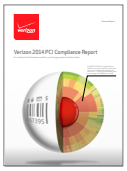
2010: Complexity and uncertainty

An exploration of the complexity of PCI security, the growing pains of PCI compliance and the need to evolve toward a process-driven approach for compliance

2011: Dealing with evolution

A review of the changing compliance requirements, with insights into the importance of sound decision-making and how organizations can position themselves for success

2014: Simplifying complexity



A review of the value of compliance, the impact of PCI DSS changes, the need for sustainability and how to improve scope reduction and compliance program management

2015: Achieving sustainability

A focused look at improving the sustainability of compliance, and a review of the state of scope reduction and payment security

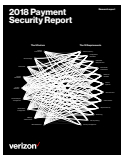
2016: Developing proficiency

Developing data security proficiency, skills and experience, and applying a structured approach to compliance management

2017: Establishing internal control

The importance of establishing and maintaining an internal control environment and a holistic approach, including security control life-cycle management

2018: Sustainable control effectiveness



Introduction of five practical models to achieve sustainable control effectiveness across your control environment, including the 9 Factors of Control Effectiveness and Sustainability, and the Constraints of Organizational Proficiency

2019: Evaluating program performance

Achieving high-performance security programs with sustainable and effective controls in a predictable manner, and addressing constraints that prevent continuous improvement of process and capability maturity

Executive summary

While data security is a complex problem, it doesn't need to be complicated. A subject or entity is complex when it consists of multiple parts. It only becomes complicated when you are unable to distinguish between the parts and their relations to each other. The individual elements to build and maintain a successful data security program and their interrelationships are known. In this report, we explore the essential elements needed to successfully construct and cross the compliance bridge without falling prey to the impact of external, environmental shifts during challenging times.

Too few organizational leaders, C-suite executives and others understand the underlying reasons for their company's lack of sustainability and control effectiveness. For this reason, we devoted this issue of the PSR to revisiting the challenges CISOs face in designing, implementing and executing a sound data security compliance program and in leveraging the power of strategic thinking.

Threats to payment card data continue to increase and impact the payment security landscape in numerous—and increasingly insidious—ways. The negative disruption from payment security data breaches can have a temporary or lasting impact on an organization's sales and company stock price and reputation.

With the potential for such severe repercussions, it's an enigma why compliance sustainability continues to atrophy, as seen in our most-recently compiled Verizon data.

Fewer and fewer organizations are demonstrating the ability to keep a minimum baseline of security controls in place. In 2019, from the total population of organizations assessed on PCI DSS compliance, only 27.9% of organizations achieved 100% compliance during their interim compliance validation.[1] This is a further 8.8 percentage-point (pp) drop from the year before, when only 36.7% of organizations demonstrated full compliance.

In 2019, from the total population of organizations assessed on PCI DSS compliance, only 27.9% of organizations achieved 100% compliance during their interim compliance validation.[1]

In previous editions of the PSR, we reviewed in detail the concepts of control effectiveness and sustainability. We introduced the 9-5-4 Compliance Program Performance Evaluation Framework (the 9 Factors of Control Effectiveness and Sustainability, the 5 Constraints of Organizational Proficiency and the 4 Lines of Assurance), valuable tools to help implement, maintain and measure control effectiveness. In the 2019 PSR, we reviewed how organizations can address constraints and develop data security compliance management proficiencies to become more efficient. We also discussed the application of metrics and maturity models for improving the sustainability and effectiveness of the control environment. What next steps should your organization take?

> "One would think that, with the introduction of advanced security technology, increased regulatory focus, and incentives for business to invest in the protection of information, security incidents would be rare. However, the truth is that even with the advances being made, security incidents still happen. Private information is still compromised. Internal incidents and fraud are reported all too frequently. Why is information security not improving in leaps and bounds? One answer is that information security professionals continue to find themselves reacting to issues within the enterprise rather than taking a proactive stance. This constant firefighting leaves little time for innovation, strategic thinking and planning. Security professionals revert to applying controls to problems as they arise, often with an overreliance on technology. This is often accompanied by a lack of historical data, so problems continue to occur, even though they have been 'fixed' at some previous point...
>
> "Additionally, many enterprise cultures have not accepted information security, and information security managers continue to struggle to demonstrate value. When information risk management is not integrated into the business, organisational silos can reduce opportunities for strategic solutions. A holistic risk-based approach to managing information assets must be implemented."[2]
>
> —Rolf M. von Roessing, The Business Model for Information Security, ISACA, 2010

1 For details about the data set, see the Methodology section on page 114.
2 Rolf M. von Roessing, The Business Model for Information Security, ISACA, 2010. https://www.isaca.org/bookstore/it-governance-and-business-management/wbmis1

This report addresses the underlying reasons for why organizations are struggling to keep their PCI data security controls in place. Data security is a complex problem, and managing data security compliance can be a quagmire. Broad generalizations do not take into account the complexity leading to failures. With a nearly 10 pp annual drop in full compliance, we need to reach an inflection point.

It is essential for organizations across the payment card industry to hone in on specifics and apply precision to definitions, objectives and the critical components of compliance performance management.

Control environment: the actions, policies, values and management styles that influence and set the tone of the day-to-day activities of an organization; a reflection of its values; the atmosphere in which people conduct their activities and carry out their control responsibilities

“It is an immutable law in business that words are words, explanations are explanations, promises are promises, but only performance is reality.”[3]

—Harold S. Geneen, former president of International Telephone and Telegraph Corporation

3 Harold S. Geneen. www.quoteland.com/author/Harold-S-Geneen-Quotes/4725/

The compliance landscape

Introduction

Many organizations lack the resources (capacity, capabilities and competence) as well as commitment from business leaders (communication and culture) to support data security and compliance initiatives. Various reasons exist for why organizations don't succeed in addressing such neglect. The reasons given are often superficial and speculative: willful inattention, lack of resources, data security not being treated as a business priority, executive leadership's failure to support the CISO, the steering committee's inability to execute a sound data security compliance strategy, etc. While these reasons may be applicable in some cases, clarification of the root cause and primary contributing factors is essential before organizations select solutions to maximize the business value of data security and compliance.

The nature of poor data security performance

Poor performance on compliance assessments isn't a spontaneous act; rather, it's the outcome of a sequence of activities and events based on strategic planning – or lack thereof. Unless the security and compliance strategy, business models and operating models are improved, it's mostly symptoms that are addressed. A healthy control environment's system output depends on past and current inputs. It's a causal system. Data security is a process that requires long-term attention to strategic initiatives.

Achieving and maintaining a mature data security compliance program is very seldom solely the result of a standard formula. It is a continuously evolving process in which capabilities and processes are developed over time, where various adjustments (some micro, some macro) are made based on observations at points in time.

Seek clarification. Find the root cause. Select the best solutions. Avoid future problems. Maximize value.

You need motivated leadership willing to support a CISO and steering committee with the means (proficiency) to manage this process. However, this structure is not easy to achieve when the average tenure of a CISO is two years or less! Page 20 of this report delves into CISO challenges and how they contribute to the breakdown of sustainability in control environments.

2010 Full compliance: 22.0%

PCI DSS 1.1 and 1.2

Least compliant Key Requirements:
Requirement 11
Requirement 10
Requirement 03

2011 Full compliance: 21.0%

PCI DSS 1.2

Least compliant Key Requirements:
Requirement 11
Requirement 12
Requirement 03

2012 Full compliance: 11.1%

PCI DSS 2.0

Least compliant Key Requirements:
Requirement 11
Requirement 02
Requirement 10

2013 Full compliance: 20.0%

PCI DSS 2.0

Least compliant Key Requirements:
Requirement 11
Requirement 03
Requirement 10

2014 Full compliance: 37.1%

PCI DSS 3.0

Least compliant Key Requirements:
Requirement 11
Requirement 02
Requirement 06

2015 Full compliance: 48.4%

PCI DSS 3.0

Least compliant Key Requirements:
Requirement 11
Requirement 03
Requirement 06

Least compliant key industries:
Hospitality
Retail
Financial

2016 Full compliance: 55.4%

PCI DSS 3.1

Least compliant Key Requirements:
Requirement 11
Requirement 06
Requirement 12

Least compliant key industries:
Hospitality
Financial
Retail

2017 Full compliance: 52.5%

PCI DSS 3.1 and 3.2

Least compliant Key Requirements:
Requirement 11
Requirement 03
Requirement 06

Least compliant key industries:
Hospitality
Financial
Retail

2018 Full compliance: 36.7%

PCI DSS 3.2

Least compliant Key Requirements:
Requirement 11
Requirement 12
Requirement 10

Least compliant key industries:
Hospitality
Financial
IT services

2019 Full compliance: 27.9%

PCI DSS 3.2.1

Least compliant Key Requirements:
Requirement 11
Requirement 06
Requirement 12

Least compliant key industries:
Retail
Financial
Hospitality

In this report, we are rating control sustainability—the ability to keep controls in place—not the ability to achieve once-per-year compliance. The compliance downturn in 2019 isn't the result of changes to the PCI DSS requirements. A marked decrease in sustainability has been noted by the PSR for several years. There is a substantial drop in full compliance across the Americas region and a substantial increase in control gap, i.e., the percentage of controls found not in place. Asia-Pacific is the only region that improved its compliance from the year before. As before, security testing—Requirement 11—continues to be the requirement that organizations experience the most difficulty with keeping in place.

A note about compliance and control sustainability

"Compliance sustainability" is the ability of organizations to design, implement and maintain robust and resilient control environments that meet regulatory requirements over extended periods. PCI DSS compliance is evaluated through point-in-time validations during interim and final compliance assessments. It presents a reasonable determination of the sustainability of PCI DSS controls by identifying how many controls remained in place throughout the annual validation period, evaluating organizational competence and commitment toward early detection and correction of significant control performance deviations.

Data security is a 24/7, ongoing activity. For it to be effective, multiple layers must work together in a series of control systems that make up the control environment. Organizations cannot allow any significant weaknesses to be present in the environment and expect sensitive data to be effectively protected. All systems need to consistently meet their respective control objectives.

Drawing a distinction between general failures and the failure of control objectives is important. All organizations have experienced various forms of control failure throughout the year. Failures of individual controls at some point are largely inevitable—but they should be brief. Deviation from control standards should be rapidly detected and corrected. In addition, failure of one or more controls should, in general, not result in a collapse of the entire system, just as the failure of one system should not result in the complete failure of control objectives and of the entire environment.

This is the "defense in depth" principle: To maintain effective data security, control environments need sufficient robustness and resilience built in, even as temporary failures occur.

A bridge over shifting waters

As the Verizon PSR's most recent compliance findings show, decision makers need to apply deep, methodical and scientific practices to challenge and reverse the underlying problems causing data security compliance programs to fail in establishing sustainable control environments. Critical to combating this negative security trend is the CISO's role of strategizing and addressing constraints that hamper the achievement of objectives. As the world adapts to digital transformation and other disruptions, such as the coronavirus, control sustainability can only get more complicated—and important.

A suspension bridge—particularly, the Choluteca Bridge in Honduras—can serve as a powerful metaphor for information security practitioners who are using dated security practices, and are ignoring or oblivious to the need for preparing for and adapting to changing security conditions.

Built by the U.S. Army Corps of Engineers in the 1930s, the bridge is a critical transit point on the Pan-American Highway, the city of Choluteca and southern Honduras. Rebuilt from 1996 to 1998 with state-of-the-art engineering by a Japanese firm, it is said to rival the Golden Gate Bridge in San Francisco for its exceptional architecture and exemplary construction.

In the fall of 1998, Hurricane Mitch, a Category 5 storm, swept into Choluteca. Mitch destroyed more than 150 bridges in Honduras, but the Choluteca Bridge survived. As Mitch's winds died down, the bridge looked undamaged and ethereal. The highway on both sides had completely disappeared. Even more unimaginable was that the river had shifted course and no longer flowed under the bridge. A "bridge to nowhere," it looked like a photoshopped structure. When the wide Choluteca river swelled sixfold, the flooding carved a new channel through the surrounding earth. Some six years later, rebuilding efforts finally reconnected the bridge and highway, restoring its former purpose and leaving behind a fascinating metaphor.

Like the Choluteca Bridge, payment security can be well engineered. However, if it's maintained with a wash-rinse-repeat cycle of validation, an unexpected shift can render its defenses useless. Thoughtful, strategic consideration needs to be baked into processes, such as the steps recommended in the 9-5-4 Compliance Program Performance Evaluation Framework.[4] A solid compliance program requires agility, adaptation, innovation and higher levels of maturity to withstand threatening winds. If companies fail to include these components in their security frameworks, disruptions, shifts or novel attacks could leave them compromised. This metaphor is instructive for compliance specialists who know how important it is to be aware of the interdependencies between control systems and the control environment. For example, did the engineers plan broadly enough to include a soil test to determine the potential impact of the river changing course?

Now consider the recent example of the coronavirus pandemic. Businesses have invested in security models based on previous working practices, but how many are compatible with long-term shifts in work-from-home practices, which may become permanent for some workers? Bring-your-own-device (BYOD) and other mobile risks have skyrocketed since coronavirus drove a considerable percentage of the workforce to a home base (see Appendix A: "Evolving mobile security" on page 120). The security "bridges" were built to be robust and resilient for an office-based workforce, even when globally distributed. How adequate those bridges are now that the river has shifted to remote-based work patterns will only become clear over time. How organizational strategies can adapt to move or rebuild the bridge is also applicable to this situation.

Photo credit: Yuri Cortez, Getty Images

4 2019 Payment Security Report, Verizon, 2019. https://www.verizon.com/business/resources/reports/payment-security-report/

Shift happens. Sometimes really big shifts happen, such as digital transformation. For example, there's a race to secure cryptographic systems that will become easily crackable and outdated in 20 years because quantum computing will be millions of times faster than present computer technologies, according to the National Institute of Standards and Technology (NIST).[5]

History is full of radical shifts and ripple effects, such as those created by quantum computing and the ARPANET (see "Birth of the internet—A tectonic shift"). It's inevitable that shifts will continue to alter the way we do things, and digital transformation is likely to move the river multiple times. We are facing potential change at warp speed because of a predicted Fourth Industrial Revolution, which will advance the use of robotics, artificial intelligence (AI), the Internet of Things (IoT) and other technologies. The speed and scope of digital transformation are generating significant multi-industry change—such as collaborative technologies in the automobile industry—as well as significant accompanying risk.

Concurrently, mobile devices are taking a leading role in payment security. In 2016, the use of mobile devices for online payments surpassed in number the same use by computers, according to Statcounter.[6]

This trend is disconcerting for payment security, considering the comparative lack of protections on mobile devices.

Based on the payment security findings documented in this report, those risks are snowballing at a very rapid rate, and the momentum is exacerbated when CISOs fail to integrate mobile into their payment security plans.

What does this mean for payment security?

In a world that is changing so rapidly, we can hardly predict the future. Adaptation and innovation are increasingly important tools for managers weathering disruptive storms. CISOs must stay abreast of near-term changes and watch for pending storms while building and maintaining a solid compliance bridge. That means developing flexibility and adaptability to security needs while creating backup plans in case the river evolves or shifts unexpectedly.

Threat actors are devising new methods of disruption daily, such as the new mobile banking Trojan EventBot, which can bypass multifactor authentication to steal user data from financial applications. This is why it's critical to build strategic, unbreachable bridges founded on reliable, repeatable methodologies, such as the 9-5-4 Compliance Program Performance Evaluation Framework. These bridges also need to be adaptable so when a malicious actor creates a Category 5 threat, the bridge shifts when—and where—the river evolves.

Birth of the internet—A tectonic shift

1969 was the year of the U.S. moon landing. Lesser known is that in the same year, a major industrial revolution occurred. The very first message was sent on the Advanced Research Projects Agency Network (ARPANET), which eventually evolved into the internet. On October 29, 1969, UCLA professor Leonard Kleinrock and his student Charley Kline attempted to transmit the text "login" to the computer of another programmer, Bill Duvall, at Stanford Research Institute over the first two-node network on the ARPANET. After the letters "l" and "o" were sent, the system crashed, making the first message ever sent on the internet "lo." About an hour later, after recovering from the crash by rebuilding the operating system, the SDS Sigma 7 computer at UCLA successfully transmitted the text "login." [7]

Forward 11 years to 1980. While working in Geneva, Switzerland, as an independent contractor at CERN, Tim Berners-Lee proposed a project based on the concept of hypertext to facilitate sharing and updating information among researchers. He then released a publication proposing a system for managing information on the internet. Information within that publication would become the framework for the World Wide Web we know today, which has radically changed communication and countless other interactions, including virtually everything discussed in this report.

5 Sophie Bushwick, "New Encryption System Protects Data from Quantum Computers," Scientific American, Oct 8, 2019. https://www.scientificamerican.com/magazine/sa/2019/10-01/

6 "Mobile and tablet internet usage exceeds desktop for first time worldwide," StatCounter, Nov 1, 2016. https://gs.statcounter.com/press/mobile-and-tablet-internet-usage-exceeds-desktop-for-first-time-worldwide#

7 "The Computer History Museum, SRI International, and BBN Celebrate the 40th Anniversary of First ARPANET Transmission," Computer History Museum, Oct 27, 2009. https://computerhistory.org/press-releases/museum-celebrates-arpanet-anniversary/ Also see https://www.youtube.com/watch?v=7duyI0ZZ5BQ

Top 7 strategic data security management traps

Lack of data security sustainability and effectiveness is largely the result of poor business, strategic and operational architecture design and execution (see page 22 for elaboration on these traps). Addressing these impediments will not only build a strong compliance bridge but also a program that can adapt when necessary.

1 Inadequate leadership

As stated before, data security isn't an IT problem, nor is it one of knowledge. It's a problem of proficiency, where the collective leadership (CEOs, boards of directors, CIOs, CISOs and other executive decision makers) lack the skills, competency, experience and resources to operate effective and sustainable data security compliance management systems.

The first issue is the manner in which organizations approach compliance management and the objectives they prioritize for change. That change needs to be driven from the top—by the CISO, the CIO, the CEO and the board.

Organizations can benefit from reevaluating the role, position and scope of responsibilities of the CISO and their ability to execute sound security strategies. For starters, most CISOs may be incorrectly positioned in the organization—54% report to the CIO,[8] which is far from ideal, since they often lack the independence and authority to execute programs that are more strategic. Some 35% of CISOs are new in their role, due to the high churn rate. In many cases, the compromises they make during their first 100 days in office may haunt them for the rest of their tenure. We discuss this on page 20 in "The CISO hot seat" section of this report.

2 Failing to secure strategic support

A security strategy and plan includes a prioritized list of objectives with adequate backup for critical role resources. An essential and often missing ingredient for a successful data security strategy is a mutual collaboration, alignment and support between the organization's business objectives and priorities, and its security compliance objectives and priorities. Security strategy is seldom effective without support from a security business model (see Figure 1) and security operating model. What is missing in many organizations is the communication of the business model for security to the stakeholders. Many security strategies are not supported by a sound security business model that ties the design, strategy and operations to the core processes, which in turn tie the people, processes and technology together. CISOs need to get better at defining the business model to explain to the board how data security and compliance generate value for the organization. This helps to secure needed investments and resources for long-term sustainability. In addition, CISOs must know how to evaluate and improve the strength of security business and operating models. The development of this management skill should be prioritized across the payment security industry by organizations worldwide.

3 Lack of resourcing capabilities

CISOs struggle to get the resources they need to support security strategies. They struggle to address internal constraints. A desperate need exists to address the cybersecurity skills shortage, particularly in the fields of security management and strategic planning and execution. However, the lack of skilled resources isn't the main reason for poor data security sustainability. Developing organizational proficiencies—the skills and experience to address the six primary organizational constraints (capacity, capability, competence, commitment, communication, culture)—is another critical need. Those constraints are preventing organizations from developing the process and capability maturities needed to achieve the primary objective: a sustainable and effective control environment that operates with consistent performance and predictable outputs.

4 Falling short on sound strategic design

Effective data security compliance programs start with a sound strategy. With a poor strategy, whatever cascades down will likely be weak, too. If mature processes and capabilities are not clearly specified objectives in the strategic plan, it's unlikely there will be maturity of data security capabilities. What gets measured gets done. We have covered this important point in many previous PSR publications.

CISOs and business leaders don't agree on security strategies for many

8 Information Security Maturity Report 2019: Full Survey Results, ClubCISO, 2019. http://www2.company85.com/clubciso-report-2019

reasons, which compromises their ability to achieve support and turn it into meaningful deliverables.

The ultimate goal of PCI security compliance should be to develop and maintain a mature data security compliance program that results in sustainable and effective data security with continuous improvement in a consistent and predictable manner. CISOs and their executive teams need to be aware of and align on the most successful strategies others in their industry are using to overcome obstacles for achieving this goal. No need to reinvent the wheel, but it needs shaping to fit. Security strategy design and execution should be supported by industry-accepted security models and frameworks. Such frameworks are only truly effective when applied in alignment with an organization's operational and business objectives.

5 Deficient strategy execution

CISO priorities and solutions are far too technology focused. CISOs need to spend a lot more time on processes and strategy to achieve a balance between strategic planning and execution, and managing the day-to-day operational challenges (i.e., "firefighting"). The correct selection, application and adherence to supporting frameworks is the other major piece of the puzzle that organizations get wrong. Some CISOs continue to take shortcuts, many times out of a perceived necessity, and at other times because they don't know any better or simply because it's less challenging. They may have to make very difficult compromises on their strategy because funding isn't made available, budgets are cut or security projects and programs are rejected in preference for IT projects. Technology solutions may be sought because a personnel resourcing budget isn't available. While the business will approve a budget for a kit or tool (perceived as a one-off investment), it won't approve a budget for resources requiring an ongoing cost.

When security frameworks are selectively and partially followed, the value of those frameworks is diminished substantially. Taking such shortcuts is prevalent throughout the industry, and many organizations are fairly blatant and blasé about adhering to frameworks. It's essential that CISOs get the requirements of the control environment right first before they execute the program and related projects. Nearly all security incidents can be traced back to poor decisions made during the design and execution of the security strategy and the operational architecture of the control environment.

6 Low capability and process maturity with lack of continuous improvement

We've known for decades that organizations need to develop maturity for data security operations and performance to become consistent and outcomes to become predictable. PCI DSS, as a baseline compliance standard that establishes minimum levels of assurance, needs to evolve further. Many organizations demonstrate that moving beyond the baseline security standards to deliver enhanced sustainability and maturity—established by frameworks such as the PCI DSS—can be achieved with or without the use of additional standards and frameworks. The achievement of mature data security control environments is in reach of all organizations. What is needed is increased focus on maturing all core processes—instead of the widespread continued focus and over-reliance on technology.

7 Communication and culture constraints

How companies communicate about complex planning projects, such as a compliance program implementation, can impact the likelihood of a breach. Poor company communication can be a significant, underlying reason for why company data compliance is trending downward. CISOs and their teams struggle to communicate and collaborate with the executive team, hampered in part by limited interactions and relationships at the executive level.

Business leaders often fail to see the value of investing time and resources into understanding data security and compliance beyond its more traditional functions. They may remain comfortably involved in supporting other technology areas while believing that compliance with a baseline standard equals security. An important step in developing a broader security culture is having strong communications plans that clarify and justify risk and security in ways that catalyze employees to embrace them. Communication plans that don't directly align with business goals and vision seldom receive the support required to be effective and sustainable across the lifetime of the security strategy execution.

The CISO merry-go-round: Breaking the vicious cycle

Some of the greatest challenges CISOs face relate to securing investments for data security and compliance programs. Investments are needed to realize their security strategy and deliver continuous process and capability improvement. The effort required to secure these funds can result in CISO stress, overwork and tenures of two years or less. This can turn into a slippery slope. Security leaders unable to achieve effective and sustainable control environments leave an organization prematurely, likely breaking any momentum gained on the delivery of a data security management program. It plunges the next CISO into an environment where they, again, are forced to focus on realizing quick wins, which in most cases are technology focused—with projects that drive strategic objectives ending up on the back burner.

In this vicious cycle, organizations don't develop their core data security processes and capabilities and, in turn, can't address the six constraints of organizational proficiency.[9] They stay in a reactive mode, responding to events. The balance between strategy and operations can't be achieved. In this cycle, both the CISOs and their teams constantly fight fires, and the business leaders don't see a security investment return.

One way for CISOs to get off the merry-go-round and break the cycle is to implement and maintain a high-performance data security environment, which is comprised of five key elements.

Do not neglect the fundamental principles.

A majority of organizations are still ignoring the cornerstones of a successful data security compliance program. There is immense value in understanding these fundamental building blocks:

The seven data security principles

1. **Success is achieved by design, not luck**
2. **All controls must be effective, not just present**
3. **Controls have dependencies and function with control systems, not in isolation**
4. **For controls to be sustainable, their control environment must also be sustainable**
5. **Operating performance indicators should be measured and reported**
6. **The input, activity and output of all core processes must be consistent and predictable to support timely detection, prevention and correction of performance deviations**
7. **Continuous improvement must be made toward adequate process and capability maturity**

9 2019 Payment Security Report, Verizon, 2019. https://www.verizon.com/business/resources/reports/payment-security-report/

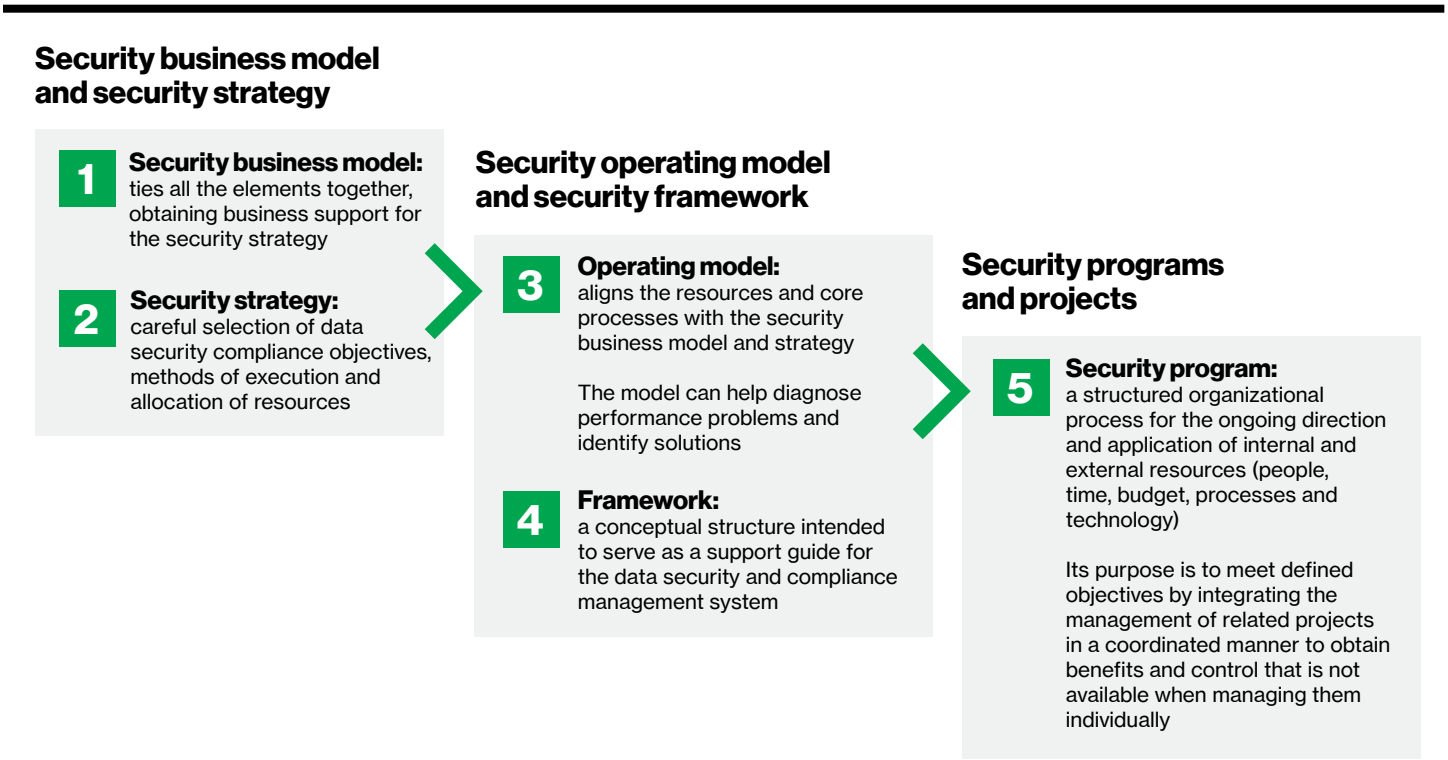


Figure 1. Aligning security business and operating models

Elements of a high-performance data security environment

The five elements that make up a high-performance data security compliance management environment are:

1. Security business model

An overarching model that ties all the elements together to obtain business support for security strategy. This model defines the objectives and how core processes are structured to deliver maximum value—and supports how the organization's frameworks and models are aligned.

See page 49 for more details on the Business Model for Information Security (BMIS) defined by ISACA.

2. Security strategy

The security business model is then translated into a strategy. The strategy is mainly concerned with determining the careful selection and prioritization of the security and compliance approach and objectives, and ultimately guides the allocation of scarce resources. The security strategy must be aligned with the business model. Today, only a small number of CISOs are successful in aligning the cybersecurity function with their organizational strategy.

3. Security operating model

The strategy is supported by the security operating model and concerned with the alignment of resources and processes. The operating model represents how value is created by an organization—and by whom within the organization. The operating model must be aligned with your strategy or there will be poor execution and an uphill battle to deliver results.

See page 51 for a discussion on the security operating model.

4. Security frameworks

CISOs are finding it difficult to align their security framework with the organization's mission. The correct selection and application of frameworks should move organizations away from being too technology focused.

Frameworks provide structure. They can be thought of as the skeletal system upon which the body of a sound program can be built. Generally, frameworks are operational in nature and provide a detailed description of how to implement, create or manage a program or process. Frameworks are typically principles-based and open to continuous improvement. As a result, frameworks usually rely on subsidiary standards to "make it happen." The BMIS addresses these challenges by offering a way for enterprises to synthesize the frameworks and standards they are utilizing, as well as a formal model they can follow to create a holistic information security program that does more for the enterprise than traditional approaches.[10]

See page 55 for a list of the top security frameworks.

Questions explored in this report

- **Why do most organizations worldwide demonstrate a low capability on compliance sustainability with the PCI DSS baseline set of controls?**
- **What are the main underlying reasons for organizations' inability to maintain sustainable control environments?**
- **What lies behind the challenges CISOs face?**
- **What are the crucial shortcomings in data security and compliance strategy that organizations should address?**
- **Why should there be less emphasis on technical aspects of security and more attention on the strategic transformation of security as a business control function?**

10 The Business Model for Information Security, ISACA, 2010. https://www.isaca.org/bookstore/it-governance-and-business-management/wbmis1

5. Security program and projects

The operating model is supported by the security program. The program delivers outcomes by managing a collection of projects where the achievement of long-term objectives can only be realized when it's collectively managed as a program. Organizations can incorporate the 9-5-4 Framework to evaluate program performance and to drive process and capability maturity. Program management benefits include improvement of performance among participating projects through integration, alignment of objectives, economies of scale and broad oversight.

For many organizations, a large part of the journey in PCI security and compliance is about moving from a disjointed set of activities to creating a formalized program. The question of strategy gets to the heart of what it takes to move a program forward. Instead of short-term projects with small, immediate goals, security must evolve into a long-term program with a mission, objectives and strategy that improve the security posture of the organization.[11] From a governance perspective, there are six major outcomes that the security program should work to achieve.[12] In its publication on information security governance, ISACA defined these outcomes as:

- Strategic alignment
- Risk management
- Value delivery
- Resource management
- Performance management
- Assurance process integration

The intent of a data security compliance management program is to design and execute a governance framework and maintain control over the program activities for extended periods of time. This provides the best possible chance to succeed in achieving the stated objectives with the available resources.

Key concepts: Data security compliance management operations

Understanding the elements of operating successful data security and compliance management systems is an important first step. A conceptual framework of operations can be described under the acronym "DIME":[13]

- **D**: Design and test controls
- **I**: Implement and integrate controls
- **M**: Monitor, measure and report control performance
- **E**: Evaluate and evolve control capability and process maturity

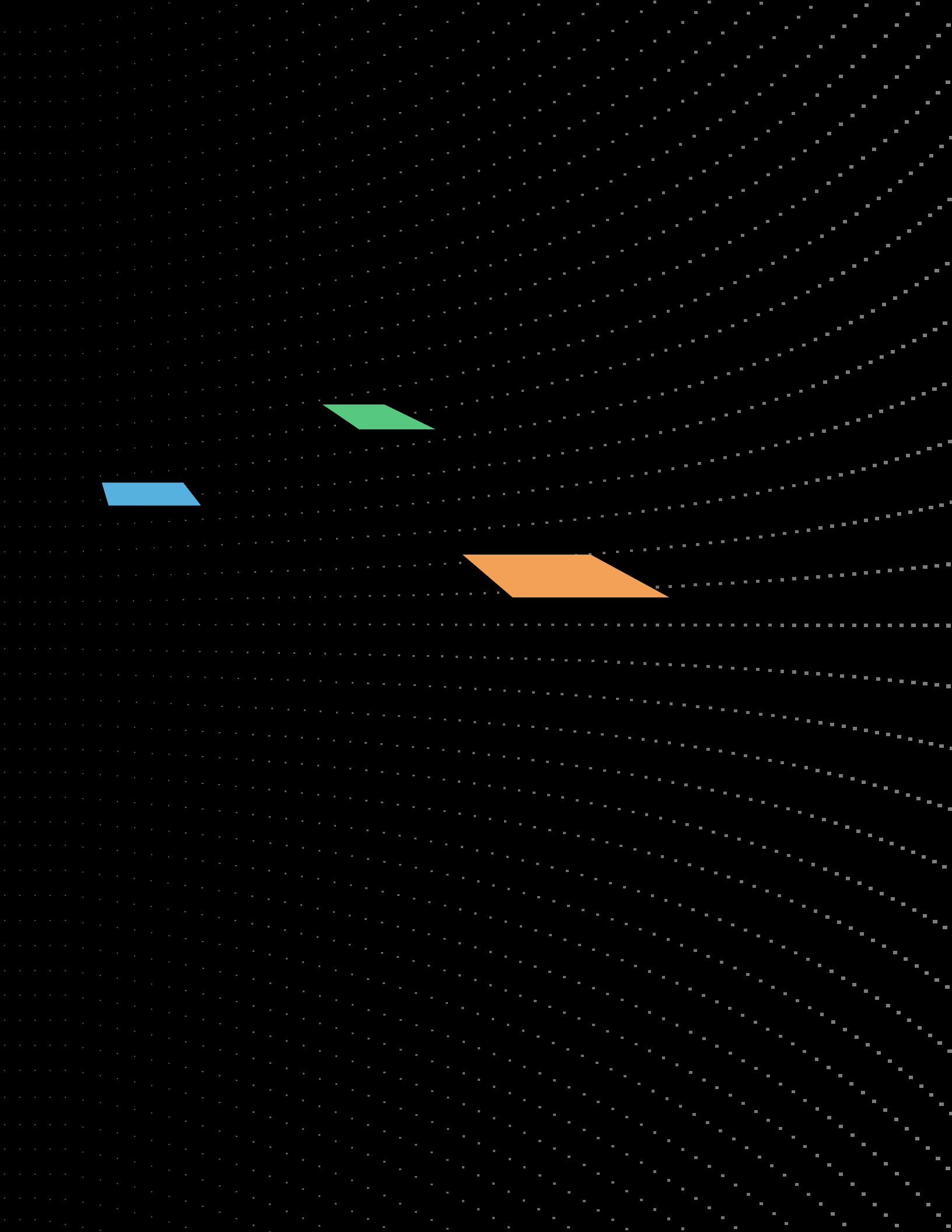
Throughout this report, when we refer to the "operation of controls" or the "operation of the control environment," all of these DIME activities are included under that umbrella.

11 2019 Payment Security Report, Verizon, 2019, pages 15 to 20. https://www.verizon.com/business/resources/reports/payment-security-report/

12 The Business Model for Information Security, ISACA, 2010. https://www.isaca.org/bookstore/it-governance-and-business-management/wbmis1
Also, Information Security Governance: Guidance for Information Security Managers, ISACA, 2008. https://www.isaca.org/bookstore/it-governance-and-business-management/w3itg
Also see Board Briefing on IT Governance, 2nd Edition, IT Governance Institute, 2003. https://www.oecd.org/site/ictworkshops/year/2006/37599342.pdf

13 John Mitchell, LHS Business Control, "Measuring Control Effectiveness—GRC 2.0—Breaking Down The Silos," ISACA Ireland Conference, Oct 3, 2014.

02 Commentary section



The CISO hot seat

Organizations are still grappling with many of the same risks that existed a decade ago, while struggling with new attacks as criminals alter their tactics. A quick look at the 2020 Verizon Data Breach Investigations Report[14] shows that financial gain remains a primary motivator for cybercrime and accounts for nearly 9 in 10 (86%) breaches. Within the retail industry, 99% of incidents were financially motivated, with payment data remaining the most-sought-after and lucrative commodity by threat actors. Web applications, rather than point-of-sale (POS) devices, are now the main vector for retail breaches. Within the financial and insurance industries, 30% of breaches were caused by web application attacks, primarily driven by external threat actors using stolen credentials to obtain access to sensitive data stored in the cloud.

The growing demand for CISOs in organizations around the world can be attributed to the burgeoning number of information security risks and targeted cyberattacks, breach disclosure laws becoming common internationally, and increasing media attention devoted to security breaches. If one person in the organization isn't formally held responsible for managing information security, then it's also harder to hold individuals across the organization responsible. That can lead to disaster.

While the role of the CISOs was formalized in the mid-1990s,[15] their presence is relatively new and has become somewhat standard in many organizations. Today, many organizations employ a CISO or director of information security—a senior leader responsible for information security and compliance, regardless of size or industry.

A Cyber Security Job Trends survey in 2016 that polled 435 senior-level technology professionals found that fewer than half (49%) said their companies employ a CSO/CISO solely responsible for security.[16] A more-recent 2019 Bitglass survey reported that 38% of the 2019 Fortune 500 organizations don't have a designated CISO. Of that 38%, only 16% have another executive listed as responsible for cybersecurity. The hospitality industry is the least likely to have an executive listed as responsible for cybersecurity strategy.[17] An interesting potential correlation is that the hospitality industry has among the lowest level of payment card data security sustainability when compared to other key industries, based on Verizon's PSR research over the past decade. Improvements are noted for this sector in this year's analysis.

Since the emergence of the job title in the late 1990s, the CISO role has become more complex—and demanding—by the day. CISOs and others in this position increasingly find traditional data security strategies and functions no longer adequate when dealing with the current expanding and dynamic risk environment.

The role of the CISO continues to expand.[18] The position requires a delicate balance of entrepreneurial understanding, business acumen and technical knowledge. CISOs manage a wide range of areas: security strategy, security architecture, security performance management, IT compliance management, IT risk management, threat management, identity and access management, and third-party security, among other responsibilities. At the same time, a CISO has to enable business while managing risk, ensuring that security does not become a roadblock for essential business functions. In many organizations, the CISO function lacks clearly defined lines of responsibility.

There is a wide range of functions that CISOs govern, manage and perform. For many organizations, it's challenging to make sense of this and decide on an appropriate approach for their business's mission.

Today's CISO leads an increasingly precarious life. Many are held responsible for something they can never provide 100% assurance on, i.e., 24/7, year-round security of sensitive data across the enterprise. Without layers of protective controls and the strategy to keep them in place, it may take only one missed vulnerability, insider or insecure process to result in a data compromise.

14 2020 Verizon Data Breach Investigations Report. https://enterprise.verizon.com/resources/reports/dbir/

15 Tom Field, "Steve Katz on Reinventing the CISO," Bank Info Security, Sep 5, 2019. https://www.bankinfosecurity.com/steve-katz-on-reinventing-ciso-a-13020

16 Ryan Corey, "Cybrary's 2016 Cyber Security Job Trends Report," Cybrary, Dec 16, 2015. https://www.cybrary.it/blog/2015/12/cybrarys-2016-cyber-security-job-trends-report/

17 "The Cloudfathers, an analysis of Cybersecurity in the Fortune 500," Bitglass, 2019. https://pages.bitglass.com/rs/418-ZAL-815/images/Bitglass_TheCloudfathers_Fortune500.pdf

18 See Appendix C: CISO responsibilities

CISO challenges

For many CISOs, the #1 pain point is likely dealing with complexity with a lack of visibility on risks, assets, organization changes, and legal and compliance requirements.

CISOs operate in a fast-moving environment dealing with numerous constraints: budgets, time, tools and lack of skilled workforce. Meanwhile, there are constant internal and external threats across the control environment. Consistently maintaining secure systems that store, process and transmit sensitive data is far from easy. Tracking and protecting financial and customer data across data centers, workstations, mobile devices and cloud infrastructure is a challenge in itself. Threat actors relentlessly attempt to find new ways to infiltrate networks and system components, and to harm the workplace via phishing scams, malware, ransomware or hacking attacks. In addition, they are often excluded from or misaligned on strategic business changes or choices, such as product decisions, mergers and acquisitions.

CISOs are expected to manage a broad set of stakeholders with increasingly diverse teams to handle different areas of concern. Most organizations manage a multivendor environment with between 20 and 70 different IT security products for monitoring and detection—sometimes from as many vendors! Two-thirds of organizations (66%) are actively consolidating their number of cybersecurity vendors, according to 2019 Enterprise Strategy Group (ESG) research.[19] There is progress on vendor consolidation: The Cisco 2020 CISO Benchmark Report[20] found that 85% of organizations are now using 20 vendors or fewer.[21]

Data security needs are growing more diverse by industry. CISOs need to spend time understanding the industry they're in and the strategic direction and business priorities of their organization. Yet many CISOs still spend much of their time firefighting or allocating precious time to conversations with business leaders who think cyber risk and data security are all technical problems or merely compliance exercises. Inadequate education at the senior executive level often results in business leaders failing to realize, or not adequately being informed, that the actual complexity of data security management lies not within software applications, but with vulnerabilities in the business management processes.

“For every complex problem, there is an answer that is clear, simple and wrong.”[22]

—H. L. Mencken, American journalist, cultural scholar and critic

Inadequate education at the senior executive level often results in business leaders failing to realize, or not adequately being informed, that the actual complexity of data security management lies not within software applications, but with vulnerabilities in the business management processes.

19 Jon Oltsik, “The Cybersecurity Technology Consolidation Conundrum,” Enterprise Strategy Group blogs, Mar 26, 2019. https://www.esg-global.com/blog/the-cybersecurity-technology-consolidation-conundrum

20 Cisco 2020 CISO Benchmark Report, Cisco, 2020. https://www.cisco.com/c/en/us/products/security/ciso-benchmark-report-2020.html

21 For further details, also see “Trap 3: Lack of resourcing capabilities” on page 32.

22 H.L. Mencken. https://en.wikiquote.org/wiki/H._L._Mencken

Trap 1

Inadequate leadership

“If you think technology can solve your security problems, then you don’t understand the problems and you don’t understand the technology.”[23]

—Bruce Schneier, public-interest technologist

CISO position and role

An organization’s data security and compliance success is often a function of the effectiveness of the CISO. A strong CISO can be instrumental and make the difference between a functional, robust data security program with a healthy control environment and one with constant chaos. The CISO’s position is often compromised by lack of sound business processes on the security team side, which negatively impacts the security and compliance program. This often leads to a diminished understanding of the value of security and compliance on the business side.

The responsibilities of CISOs vary by industry, size and how the organization is regulated. See Appendix C on page 134 for an infographic on the CISO’s roles and responsibilities. CISOs face significant challenges when their managers (CIOs, CEOs or board members) demand them to be short-term problem fixers without enabling them to be long-term role developers building and maturing security capabilities and processes. CISOs must avoid this IT trap where they get stuck in security operations focused on deploying and managing security technology solutions.

Being a CISO isn’t only about technical abilities and cybersecurity knowledge. A skilled CISO builds and operates a successful data security compliance program that continuously improves capability maturity while representing the organization with political astuteness. It requires a long-term sustainable role, fully integrated into the business to help the organization grow in alignment with information security risk compliance.

Traditionally, many CISOs were technologists by training and trade and typically had limited exposure to and knowledge of the overall business. Before rising to management positions, many CISOs held roles in network security architecture, developing software, maintaining physical appliances, threat detection and remediation, and compliance-related activities. When considering CISOs at most Fortune 100 companies, 59% came up through the IT and IT security ranks, and 40% hold a degree in business.[24]

CISOs who come from a technical background may be less likely to develop business metrics for reporting the performance of the data security compliance management program. These CISOs need to develop and maintain various program performance metrics to show the business risk of not designing and implementing a sustainable and effective control environment. The focus should not

23 Bruce Schneier, Secrets & Lies: Digital Security in a Networked World, John Wiley & Sons, 2000. https://www.schneier.com/books/secrets_and_lies/pref.html

24 Nate Lord, “The Anatomy of a CISO: A Breakdown of Today’s Top Security Leaders,” Digital Guardian, Dec 5, 2017. https://digitalguardian.com/blog/anatomy-ciso-breakdown-todays-top-security-leaders-infographic

be merely on demonstrating the importance of patching vulnerable applications, but also explaining to executives how missing patches put other critical application platforms and the business at risk, as one example. These conversations must be elevated to a strategic level. Ultimately, the CISO, as a C-suite position, is a job that requires a long-term view. That means developing a robust strategy, a security business model and an efficient operating model.

Business and strategy analysis is an important component of the job. CISOs must build threat models to define and prioritize what they need to protect, who it needs to be protected from and the way in which it will be protected. The manner in which data is protected must be defined, including the processes, policies, standards, people and technology required. In other words, the control environment must be defined in detail. This sounds simple, but it's a complex challenge. Both the IT infrastructure and compliance environment are expanding due to the growth of mobile computing, migration to the cloud, the IoT and other technologies.

The four faces of the CISO

CISOs continue to serve the vital functions of managing security technologies (technologist) and protecting enterprise assets (guardian). At the same time, they are increasingly expected to focus more on setting security strategy (strategist) and advising business leaders on security's importance (advisor).[25]

- **Technologist:** Assess and implement security technologies and standards to build organizational capabilities
- **Guardian:** Protect business assets by understanding the threat landscape and managing the effectiveness of the cyber-risk program
- **Strategist:** Drive business and cyber-risk strategy alignment, innovate and instigate transitional change to manage risk through valued investments
- **Advisor:** Integrate with the business to educate, advise and influence activities with cyber-risk implications

"Technology is dominated by two types of people: Those who understand what they do not manage and those who manage what they do not understand."[26]

—Archibald Putt, author (pseudonym)

25 Taryn Aguas and Khalid Kark, "The new CISO—Leading the strategic security organization," Deloitte Review, 2016. https://www2.deloitte.com/content/dam/insights/us/articles/ciso-next-generation-strategic-security-organization/DR19_TheNewCISO.pdf

26 Putt's Law and the Successful Technocrat: How to Win in the Information Age, Wiley-IEEE Press, 2006. https://en.wikipedia.org/wiki/Putt%27s_Law_and_the_Successful_Technocrat

Common data security mistakes

CISOs need to correct unproductive practices that don't help to promote and sustain effective data security, such as:

- **Lacking an effective security strategy:** Continuing to operate in a reactive mode
- **Not understanding the scope of their risks:** Operating with poor risk assessment and management practices
- **Viewing data protection as a technology problem:** Not managing data protection as an operational business process and cultural problem
- **Failing to get real buy-in from board members and senior business management:** Not communicating a compelling narrative about the need for security investment
- **Not knowing what to address first:** Inability to balance quick wins with long-term strategic initiatives
- **Being unaware of data and IT assets:** Operating with many blind spots; not knowing where data exists and its sensitivity level; failure to map data flow and stop shadow IT channels
- **Security functioning as an island:** Not addressing security as a cross-functional issue that affects other parts of the organization
- **Not testing their security:** Failing to test whether controls are effective and continuously testing for vulnerabilities (see page 65, Figure 4—PCI DSS Key Requirement trends—Security testing has the lowest compliance over the past 12 years)
- **Inadequate education of the workforces:** Having inadequate security awareness, training and education
- **Denying that they're a target:** Not believing they're at risk; thinking they are too insignificant to become a target

"Strategy is abstract by definition, but metrics give strategy form, allowing our minds to grasp it more readily."[27]

—Michael Harris and Bill Tayler, Harvard Business Review

27 Michael Harris and Bill Tayler, "Don't Let Metrics Undermine Your Business," Harvard Business Review, September–October 2019. https://hbr.org/2019/09/dont-let-metrics-undermine-your-business

Balancing between strategic and tactical execution

The CISO and the steering committee need to address these challenges on a strategic and tactical level. It requires balancing day-to-day data protection and compliance with long-term projects that ensure that the organization is well positioned to maintain an effective and sustainable control environment. Too much focus on detail means less time to look at the big picture and to think, plan and execute strategically. Just as it's easy for a CISO to spend all day poring over the minutiae of the information security program, it's possible to get locked into an endless series of strategy meetings. This is the opposite problem: The CISO is so focused on strategy that it's impossible to have a firm grasp of what's happening operationally, day to day.

Many CISOs tend to play a role in too many aspects of managing the control environment. This is especially likely when a CISO steps up from a task-based position. The shift to the CISO role is often a matter of transitioning from a tactical to strategic position. For CISOs that hope to assume a more strategic role, they need to tackle organizational issues such as a shortage of security talent (see page 32) to support operational and technical activities—a key issue that can keep them mired in minutiae.

How the performance of the control environment plays out in practice may depend more on the security strategy, security business model and operating model, and less on the size and structure of your organization. (See page 48 for more details on security business and operating models.)

In more than half of organizations (54%), the information security function reports to the CIO or CTO, according to the ClubCISO Information Security Maturity Report 2019.[28]

Authority and reporting

Organizational structure and reporting relationships matter. They have a direct bearing on the effectiveness of communication and how the organization is managed. The chain of command, who the CISO reports to (be it the CEO or the CIO), often reveals more about the maturity of the organization than it does about the effectiveness of the CISO.

It's beneficial for organizations to place the CISO/CSO in an organizational position with independence and oversight abilities where they can act as a business adviser for security functions and features. In general, CISOs are best positioned within the organization reporting to the CEO and board. However, CISOs reporting to the CIO is still the most common scenario in many industries.[29] This is not ideal. In many cases, it does not promote sufficient independence and objectivity for the CISO, and it potentially leads to the CISO's work being tightly controlled or restricted. A CISO-to-CIO reporting structure can introduce a conflict of interest. CIOs usually need to arbitrate operational issues alongside security performance capabilities. See page 35 on the importance of an independent budget.

This isn't a new situation. A 2015 survey conducted by the Georgia Institute of Technology found that only 22% of respondents work in an organization where the CISO reports directly to the CEO, while 40% still report to the CIO.[30] How has the positioning of the CISO evolved since then? Not much has changed. The 2019 State of the CIO survey, conducted by CIO.com, found that 23% of top security executives reported to the CEO, while nearly 45% reported to a CIO.[31]

Financial losses are 46% higher in organizations where the CISO reports to the CIO, according to a report from Pricewaterhouse Coopers. A CISO reporting to the Chief Risk Officer (CRO) or Chief Financial Officer (CFO) may have more independence, since they are removed from operational structures where there is conflict between operational delivery targets. In general, more CISOs may have made the shift in reporting to the CEO.[32]

However, this is not true for all industries. For example, a report from Carbon Black found 62% of CISOs at financial institutions still report to a CIO.[33]

And a survey from IDG reveals that security executives are more likely to report to the CEO at smaller companies with revenue less than $100 million a year.[34] In general, the CSO and CISO position are more prevalent in companies with more than 1,000 employees.

28 Information Security Maturity Report 2019, ClubCISO, 2019. http://www2.company85.com/clubciso-report-2019

29 Information Security Maturity Report 2019, ClubCISO, 2019. http://www2.company85.com/clubciso-report-2019

30 Jody R. Westby, Governance of Cybersecurity: 2015 Report, Georgia Tech Information Security Center, Oct 2015. www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/tech-briefs/governance-of-cybersecurity.pdf

31 Josh Fruhlinger, "Does it matter who the CISO reports to?" CSO/IDG, Apr 30, 2019. https://www.csoonline.com/article/3278020/does-it-matter-who-the-ciso-reports-to.html

32 PwC's 2018 Global State of Information Security Survey found that 40% of CISOs report to a CEO. Strengthening Digital Society Against Cyber Shocks: Key findings from The Global State of Information Security® Survey 2018, PwC, 2018. https://www.pwc.com.br/pt/global-state-of-information-security-survey-2018/pwc-2018-gsiss-strengthening-digital-society-against-cyber-shocks.pdf

33 Tom Kellermann (Carbon Black) and Bill Young (Optiv), "Modern Bank Heists: The Bank Robbery Shifts to Cyberspace," Carbon Black, Mar 2019. https://networksunlimited.africa/images/Promos/Other/documents/carbon-black-modern-bank-heists-report-march-2019.pdf

34 2019 State of the CIO, IDG, Jan 17, 2019. https://www.idg.com/tools-for-marketers/2019-state-of-the-cio/

Communicating in the boardroom

It's common for CISOs to become the focal point for all data and cybersecurity questions from the board of directors, shareholders, auditors, regulators and media. They also can become the scapegoat for overlooked vulnerabilities.[35]

Data protection, compliance and cyber risk are business issues that board members may find especially challenging to oversee. To make the conversation more relevant and relatable, CISOs can benefit from focusing their message on the following points:

- **Top data security risks:** Use compelling narratives to tell a story about the current risk assessment results and the corresponding mitigation controls and management actions, particularly as they relate to top current business challenges
- **Program maturity:** Explain your organization's maturity level in relation to the threat landscape and industry peers
- **Emerging threats:** Identify who is attacking the organization or its industry peers and review lessons learned. Explain news events and trends, such as the spread of ransomware or a high-profile data breach, and explain how they might impact your organization
- **Audit and regulatory concerns:** Give status updates on any open audit, assessment and regulatory issues
- **Public or private partnership:** Make a note of any industry group participation and collaborations with law enforcement or intelligence agencies

35 Taryn Aguas and Khalid Kark, "The new CISO—Leading the strategic security organization," Deloitte Review, 2016. https://www2.deloitte.com/content/dam/insights/us/articles/ciso-next-generation-strategic-security-organization/DR19_TheNewCISO.pdf

Trap 2

Failing to secure strategic support

The precarious CISO tenure

Professional opportunities are plentiful within the cybersecurity industry for those with the right skills and experience. However, CISOs don't have a long shelf life. The ClubCISO Information Security Maturity Report 2019 found that 35% of CISOs are new in their role.[36] There is such a high churn, the role is sometimes referred to as the "CISO musical chairs" or the "CISO carousel."

There are widely divergent estimates for how long the average CISO stays in the role. The average tenure of a CISO is estimated to be about two years. This isn't a recent development. Back in 2013, the Ponemon Institute suggested a 2.1-year average. In 2020, a study by Nominet reported that it's just over two years at 26 months.[37] A career as a virtual CISO is increasingly rather attractive. In a 2018 ESG ISSA study, 29% of respondents were serving as a virtual CISO for one or more organizations, 21% were actively pursuing it and 33% were open to becoming a virtual CISO sometime in the future.[38]

Constant changes in security leadership can be a significant contributing factor in the lack of security strategy performance, lowering data protection defenses and increasing the risk of data compromises. The tendency for CISOs to switch companies every few years seems to intensify the problem. Organizations are having a difficult time replacing CISOs. It can take between three and six-plus months to fill a position, and in some cases (10%), the position remains unfilled.[39] This loss of talent contributes significantly to or directly results in an inability to achieve goals. On average, it can take a new CISO about six months to get up to speed and assess the existing compliance and control environments and to formulate plans for change. The changes may be a substantial departure from the existing strategy, or changes to parts of the security program. Once the plans are approved, it may take three to five years to roll out and complete a strategy and program. We see security steering committees put together a five-year plan, get two or three years into executing it and then watch it disintegrate. Implementing security strategies requires years of investment. For medium-sized to large organizations, it's common for the implementation of basic security strategies to require at least three years. For large organizations, it can require as many as 10 years. Deep organizational change takes time.

When CISOs start out by building an elaborate three- to-five-year strategic security plan, changing jobs every two to three-and-a-half years does not allow them to see it through to fruition. This may be one reason why some CISOs opt to take on deliverables that they can complete in several months to demonstrate some tangible short-term results on security and compliance initiatives without the challenges associated with the management of executing long-term strategies.

36 Information Security Maturity Report 2019, ClubCISO, 2019. http://www2.company85.com/clubciso-report-2019

37 CISO Stress—Life Inside the Perimeter: One Year On, Nominet Cyber Security, 2020. https://media.nominetcyber.com/wp-content/uploads/2020/02/Nominet_The-CISO-Stress-Report_2020_V10.pdf

38 Jon Oltsik, "The Life and Times of Cybersecurity Professionals," Enterprise Strategy Group and Information Systems Security Association, Nov 2017. https://www.esg-global.com/hubfs/issa/ESG-ISSA-Research-Report-Life-of-Cybersecurity-Professionals-Nov-2017.pdf

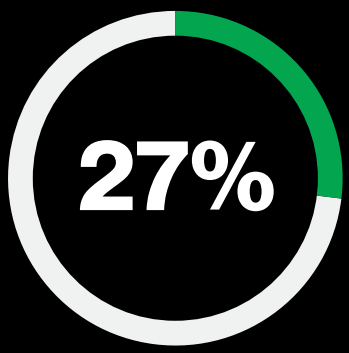
39 State of Cybersecurity: Implications for 2015, ISACA, 2015. https://www.rsaconference.com/about/press-releases/study-82-of-organizations-expect-a-cyberattack-yet

Why do CISOs change jobs so frequently?

Some 80% of Fortune 100 CISOs have held their current positions for less than five years, according to a study by Digital Guardian. Some 59% had a technical information security background when they started their careers; 13% had a programming and engineering background; only 8% had a business background.[40]

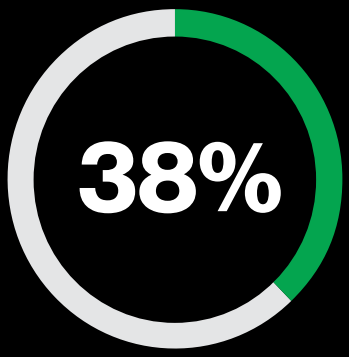
When ESG and the Information Systems Security Association (ISSA) sought to answer the question of why, in a survey of 343 cybersecurity professionals and ISSA members, they found that 36% change jobs when offered higher compensation packages from other organizations.[41]

Clearly, in a competitive industry, money matters to CISOs, but the study found that they also want to work for executives who are willing to fund, participate in and cheerlead cybersecurity efforts across the entire organization. When you look at the data beyond financial compensation, other patterns emerge:

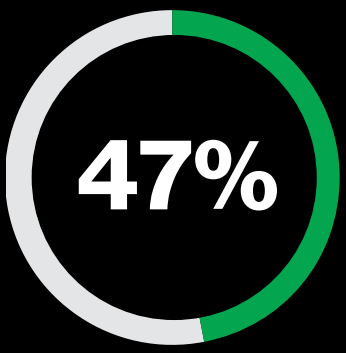


Twenty-seven percent of cybersecurity budgets are not commensurate with the organization's size and industry.

Thirty percent of CISOs weren't actively participating with executive managers or the board of directors.



Thirty-eight percent of organizations do not have a corporate culture that emphasizes cybersecurity.



Forty-seven percent of survey respondents rated their CISOs as "somewhat effective."

40 Nate Lord, "The Anatomy of a CISO: A Breakdown of Today's Top Security Leaders," Digital Guardian, Dec 5, 2017. https://digitalguardian.com/blog/anatomy-ciso-breakdown-todays-top-security-leaders-infographic

41 Jon Oltsik, Enterprise Strategy Group Senior Principal Analyst and Fellow, "The Life and Times of Cybersecurity Professionals," A Cooperative Research Project by Enterprise Strategy Group and the International Systems Security Association (ISSA), Enterprise Strategy Group (ESG) and International Systems Security Association (ISSA), 2020. https://www.issa.org/wp-content/uploads/2020/07/ESG-ISSA-Research-Report-Cybersecurity-Professionals-Jul-2020.pdf

Why do CISOs get fired?

CISOs may be dismissed for any number of reasons. Dismissals may be due to performance sand traps, such as not staying within budget, poor reporting, failing to align security operations with the board's business goals or being unprepared for a data compromise. Other reasons may include the perception of spreading fear, uncertainty and doubt (FUD) instead of intelligent business strategies. It's not uncommon for CISOs to shoulder the blame with security failures and neglected security technologies. Even inadequate maintenance and monitoring resulting in a systems issue may fall on the CISO's shoulders.

Tripwire conducted a survey at the 2017 Infosecurity Europe conference and found that 40% of respondents said CEOs should shoulder the blame for breaches; 21% suggested it should be CISOs; 14% said the CIO was responsible. "Accountability starts with the CEO, but information security is a shared responsibility across every function and level of an organization," said Tim Erlin, vice president of product management and strategy at Tripwire, in response to the findings. "Data breaches are a problem that the board-level executives need to be responsible for addressing, which means that the CISO must be involved in those board-level discussions. The board can't take meaningful, productive risk management action without that expertise in the room."[42]

However, making the CISO the party responsible for most security glitches and failures is logical. Technological innovation is their bailiwick, and they are frequently responsible for selecting the data security partners as well as a methodology to address security concerns.

Yet only 21% of IT security professionals believed the CISO should be held responsible, followed by the CEO, when a breach occurs, according to a 2017 Zettaset survey.[43]

It's all part of being in the CISO hot seat, which is hard to hold long term in the present security landscape. Even if company cybersecurity is properly budgeted with ample spending, one surprise cyberattack may be enough to unseat the CISO.

42 2017 Infosecurity Europe conference, Tripwire, 2017.

43 Ramona Carr, "Data Breach Accountability and Responsibility: Who Gets Blamed for Data Breaches?," Zettaset. https://www.zettaset.com/blog/data-breach-accountability-and-responsibility-who-gets-blamed-data-breaches

CISO stress

Today, CISO jobs frequently come with long working hours, lack of power on executive boards, diminishing hiring pools of trained professionals and budget constraints. It's a demanding combination of job hurdles. Add to that the constant stress of not having done enough to secure the organizational infrastructure against attacks from external and internal threat actors.

Internet and DNS security firm Nominet surveyed 800 CISOs and executives from companies in the U.S. and U.K. in November 2019, to probe the role stress plays for CISOs across the industry. While all C-level executives suffer from stress, CISOs and security leaders tend to feel the pressure more acutely, based on the findings of Nominet's CISO Stress Report—Life Inside the Perimeter: One Year On.[44]

Some 88% of CISOs in various industries consider themselves under moderate or high levels of stress, only a slight decrease from the 91% of CISOs who reported similar results in 2018, according to the report. That pressure also snowballs into the executives' work/life balance, with security leaders reporting that they are working an extra 10 hours a week over and above their contractual obligations. CISOs believe that the stress of their jobs had a negative effect on their mental health in 2019, and in some cases, also on their physical health and relationships, sometimes resulting in eventual burnout and even substance abuse, the study reported.

Many of the stressors are a combination of internal and external factors: expanding control environments to manage; external cyberattacks in the form of ransomware and data breaches; boardroom and other executive pressures to respond immediately to such incidents and answer tough questions, sometimes to the press and government entities. Some 74% of board members believe that their CISOs are moderately or tremendously stressed, the study also revealed. Of the CISOs surveyed, almost 90% worked more than 40 hours per week.

44 CISO Stress—Life Inside the Perimeter: One Year On, Nominet Cyber Security, 2020. https://media.nominetcyber.com/wp-content/uploads/2020/02/Nominet_The-CISO-Stress-Report_2020_V10.pdf

Trap 3

Lack of resourcing capabilities

The impact of a global information security skills shortage on data protection

Essential to a robust data security strategy is having the right people at every level to identify, build and staff the defense and response functions. That is, by many accounts, the area where organizations lack strength. The global skills shortage in the information security profession is overwhelming and a significant contributing factor to ineffective and unsustainable control environments. A logical conclusion is that the skills shortage will worsen as cyberthreats increase.

In addition, organizations are plagued by a lack of end-user security awareness while struggling to keep up with the growing cybersecurity workload. The shortage is about skills and experience, not just job vacancies. Many organizations lack both human capital capacity and advanced skills in several security areas.

Since most organizations are erroneously treating data security as a problem solved by technology alone, the number of security technology vendors has increased significantly to meet burgeoning need. Today, information security is mainly a product-based business, with at least 2,336 vendors of security products competing in the industry.[45] While some organizations manage to keep the number of security vendors to relatively few (less than 20), many manage 50 to 100 or more different point solutions from a mix of vendors. Small organizations are using on average between 15 and 20 tools; medium-sized businesses are using 50 to 60; and large organizations or enterprises are using over 130 tools on average.[46]

Meanwhile, organizations are expanding their use of technology as part of their business mission to protect sensitive data. While many organizations procure security technology, they let it languish due to lack of time or resources and fail to correctly configure and document security control design and maintenance procedures.

The skills shortage is in part driven by organizations not investing in training their existing employees to properly deploy and utilize the tech they purchase. This doesn't even touch on how overwhelmed understaffed departments are, so finding time to actually go through training is another hurdle. To address this, CISOs are engaging strategic partners for advisory services, with many organizations gravitating toward managed security services and cloud-based solutions, and transitioning to vendors that offer broad platforms.

The skills shortage also results in limited time to work with business units to align cybersecurity with business processes. The failure lies not so much within the security teams, but with the ability to gain and maintain support from across the organization.

45 For a handy reference to security vendors, see Security Yearbook 2020, IT-Harvest Press, 2020. https://www.security-yearbook.com/yearbook-2020/, which has details for 2,336 vendors of security products.

46 Brad Sowell, "RSA 2019: Most Organizations Use Too Many Cybersecurity Tools," BizTech Magazine, Mar 6, 2019. https://biztechmagazine.com/article/2019/03/rsa-2019-most-organizations-use-too-many-cybersecurity-tools

A Boston Consulting Group (BCG) analysis of the causes of data losses in 50 major breaches found that in the majority (72%) of cases, it was due to organizational, process and people failures. For example, malicious insiders, failure to fully implement purchased security products, social engineering, negligent insiders and physical loss. It is not the latest security technology that protects organizations against data breaches. Inadequate security technology played a key role in only 28% of critical breaches.[47]

This underscores, yet again, that more technology is not driving a solution for sustainable data protection.

By the numbers—trends and predictions

The number of unfilled information security positions now stands at 4.07 million professionals, up from 2.93 million from the previous year, according to the (ISC)² Cybersecurity Workforce Study. More than half (51%) of cybersecurity professionals believe their organization is at moderate or extreme risk due to staff shortages. Nearly two-thirds (65%) of responding organizations reported a shortage of cybersecurity staff. This includes 561,000 people in North America. The shortage of skilled workers in the industry in Europe has soared by more than 100% over the same period, from 142,000 to 291,000. The shortfall in Asia-Pacific is a staggering 2.6 million.[48]

The number of unfilled cybersecurity jobs globally is expected to be 3.5 million by 2021, an increase of 1 million positions since 2014, according to Cybersecurity Ventures.[49]

Over the eight-year period tracked, the number of unfilled cybersecurity jobs grew by 350%, from 1 million positions in 2013 to 3.5 million in 2021. Of the 3.5 million open cybersecurity positions expected by 2021, Cybersecurity Ventures estimates more than 2 million will be in the Asia-Pacific region, and nearly 400,000 will be in Europe.

ISACA's State of Cybersecurity 2020 report states:[50]

- Nearly two-thirds (62%) of respondents said their organization's cybersecurity teams are understaffed
- More than half (57%) have unfilled cybersecurity positions on their teams
- In the survey, 70% of respondents said fewer than half of cybersecurity applicants are well qualified
- Only 27% said recent university graduates in cybersecurity are ready for the challenges they will face in the field
- 66% said it's difficult to retain cybersecurity talent (an increase from last year)
- Of the candidates applying for these security positions, fewer than one in four are even qualified

A Boston Consulting Group (BCG) analysis of the causes of data losses in 50 major breaches found that in the majority (72%) of cases, it was due to organizational, process and people failures. For example, malicious insiders, failure to fully implement purchased security products, social engineering, negligent insiders and physical loss. It is not the latest security technology that protects organizations against data breaches. Inadequate security technology played a key role in only 28% of critical breaches.

47 Alex Asen, Walter Bohmayr, Stefan Deutscher, Marcial Gonzalez and David Mkrtchian, "Are You Spending Enough on Cybersecurity?" Boston Consulting Group, Feb 20, 2019. https://www.bcg.com/publications/2019/are-you-spending-enough-cybersecurity.aspx
See also, Walter Bohmayr and Alexander Türk, "Report from Davos: Board Oversight of Cyberresilience," World Economic Forum, Jan 19, 2017. https://www.bcg.com/publications/2017/technology-digital-report-davos-board-oversight-cyberresilience.aspx

48 Strategies for Building and Growing Strong Cybersecurity Teams. (ISC)² Cybersecurity Workforce Study, 2019, (ISC)², 2019. https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx

49 Steve Morgan, "Cybersecurity Talent Crunch to Create 3.5 Million Unfilled Jobs Globally by 2021," Cybersecurity Ventures, Oct 24, 2019. https://cybersecurityventures.com/jobs

50 State of Cybersecurity 2020, ISACA, 2020. https://www.isaca.org/go/state-of-cybersecurity-2020

The unknown resources buried in your "sandbox"

"In our experience, organizations rarely use all the security tools and features they have purchased. For example, a professional services company was planning to purchase a system that would allow it to test email attachments in a safe 'sandbox' environment before they could harm company computers. In the middle of the planning process, the company hired a new CISO, who discovered that the email security gateway the company already owned had an unutilized feature for sandboxing. Her staff enabled the feature and gained the functionality with minimal added cost or management complexity. Before embarking on ambitious investments or falling victim to the shiny-new-object attraction, it's paramount to verify that the capabilities you seek are not already in hand."[51]

— Alex Asen,
Boston Consulting Group

Important security product management tasks:

- **Conduct a thorough inventory of security tools**
- **Redundant tools should exist by design, not by chance**
- **Plan how security tools will be integrated into processes; if it requires new hiring, have a plan for that too**
- **Decommission old tools**

Areas of shortage

Nearly every position within cybersecurity is afflicted by workforce shortages. In addition to highly skilled technical staff, a desperate shortage exists of people who can design secure systems and develop secure software. This is not a new problem; it has existed for more than 10 years. In 2010, the U.S. had only about 1,000 security specialists with the skills and abilities to take on these roles, compared to the 10- to 30-fold need of 10,000 to 30,000 personnel, according to the 2010 CSIS report "A Human Capital Crisis in Cybersecurity."[52]

The information security training and education system is failing to prepare students for these roles. Employers find that graduates from many programs lack fundamental knowledge, practical experience and critical soft skills. The most acute skills shortages were seen in cloud security (33%), application security (32%), and security analysis and investigations (30%).[53]

Recruitment, compensation and retention

The cybersecurity unemployment rate was at 0% in 2019, where it has stagnated since 2011. Job applicants can find a new job in under two weeks and often have multiple job offers from which to choose. While a 0% unemployment rate sounds optimal for any industry, it creates a lot of challenges for organizations, including retention issues, salary inflation and subpar, underqualified candidates landing jobs that have little to no competition. Some 32% of organizations say it takes more than six months to fill security positions at their organization, according to ISACA's State of Cybersecurity 2019 Survey.[54]

Lack of skills and experience

Without exposure to information security practices, recent program graduates face a steep learning curve in the cybersecurity field. Employers often find cybersecurity graduates lacking in essential soft skills, such as teamwork, problem solving, communication and leadership. In ISACA's 2019 cybersecurity survey, only 24% of respondents think that recent university graduates in cybersecurity are well prepared for the cybersecurity challenges in their organization.

Some graduates are ill-prepared for the demands of the security workplace: In addition to lacking practical experience, they are often lacking in comprehension of the fundamentals of computing and information security. As a result, many graduates require extensive on-the-job training before they can productively contribute to executing the security strategy and programs.

What practical steps can organizations take to address the skills gap? In a 2018 survey by 451 Research, 62% of respondents simply replied that organizations should train existing staff with new skills.[55]

51 Alex Asen, "Are You Spending Enough on Cybersecurity?," BCG, Feb 20, 2019. https://www.bcg.com/publications/2019/are-you-spending-enough-cybersecurity.aspx

52 Karen Evans and Franklin Reeder, "A Human Capital Crisis in Cybersecurity," CSIS, Nov 15, 2010. https://www.csis.org/analysis/human-capital-crisis-cybersecurity

53 Jon Oltsik, Enterprise Strategy Group Senior Principal Analyst and Fellow, "The Life and Times of Cybersecurity Professionals," 2017, 2018. A Cooperative Research Project by Enterprise Strategy Group and the International Systems Security Association (ISSA), Enterprise Strategy Group (ESG) and International Systems Security Association (ISSA),
2017: https://2ll3s9303aos3ya6kr1rrsd7-wpengine.netdna-ssl.com/wp-content/uploads/2017/11/2017-ESG-ISSA-full-report.pdf
2018: https://2ll3s9303aos3ya6kr1rrsd7-wpengine.netdna-ssl.com/wp-content/uploads/2019/05/ESG-ISSA-2018-Survey-Results.pdf

54 State of Cybersecurity, 2019, ISACA, 2019. https://www.isaca.org/-/media/files/isacadp/project/isaca/why-isaca/surveys-and-reports/state-of-cybersecurity-2019-part-2_res_eng_0619

55 Jenny Dowd, "A Perpetual Problem," eSentire, Sept 10, 2019. https://www.esentire.com/blog/a-perpetual-problem

CISO spending

Are organizations maximizing the value of the technologies they are purchasing? When security tools are deployed out of the box without a thoughtful security plan, organizations are likely to run into configuration failure. The best metrics are a product's ability to lower risk and keep the organization in compliance.

The ongoing struggle for effective cybersecurity

The top three drivers for security spending are (1) security risks; (2) business needs; and (3) industry changes, according to Gartner.[56] A significant driver of the cybersecurity spending for digital transformation is the importance of regulatory and compliance standards. Recent regulatory changes, such as the EU's Global Data Protection Regulation (GDPR), has forced organizations to become more accountable.

In the 2019 PSR,[57] we discussed why some CISOs consistently command the budget and resources they need while others struggle to do so. Security budgets are often perceived as too small and dependent on the IT department. It's a constant subject of debate, and rightly so. The security budget has a large influence on how well a CISO can execute a security strategy and, frankly, how well they do their job and stay in it.

More CISOs are overseeing governance overlay functions of defining and establishing security policies (84%) while there is a slight decline in the number of CISOs directly controlling and allocating budgets for security projects (60%), according to the ISACA State of Cybersecurity 2019 report.[58] Obtaining a security budget independent from CIO and IT spending offers the CISO more power and execution ability, in addition to better oversight, more independence and more governance over data security and compliance. An independent budget can allow for security investments in the necessary process, people and architecture changes. Even on a very limited budget, organizations can still reduce risk by solving security and compliance problems with a "back to the basics" approach for security controls, focusing on critical systems that matter for data protection, adjusting the security architecture and baselining the control environment.

How companies are spending money on cybersecurity tools is a trending topic in boardrooms: CEOs are being asked to verify whether their security expenditures are effective and appropriate. Pouring money and resources into cybersecurity does not necessarily result in better security. So much depends on how it's done. Consider a recent finding by Mandiant that, on average, alerts occur in only 9% of attacks[59] (see page 38). Whether the security technology is up to the job is not the central question industry leaders should be asking. Rather, are organizations maximizing the value of the technologies they are purchasing? When security tools are deployed out of the box without a thoughtful security plan, organizations are likely to run into configuration failure.[60] The best metrics are a product's ability to lower risk and keep the organization in compliance.

56 "Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019," Gartner, Aug 15, 2018. https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019

57 2019 Payment Security Report, Verizon, 2019. https://www.verizon.com/business/resources/reports/payment-security-report/

58 State of Cybersecurity 2019, ISACA, 2019. https://www.isaca.org/-/media/files/isacadp/project/isaca/why-isaca/surveys-and-reports/state-of-cybersecurity-2019-part-2_res_eng_0619

59 Mandiant Security Effectiveness Report — Deep Dive into Cyber Reality, FireEye, May 2020. https://www.fireeye.com/current-threats/annual-threat-report/security-effectiveness-report.html

60 See an example of configuration failure on page 34 under "The unknown resources buried in your 'sandbox.' "

What does it take to win the support of the organization to invest in security?

Sixty percent of respondents to the annual ISACA State of Cybersecurity Survey indicated that they feel their cybersecurity budget is currently underfunded, with nearly 20% believing that their budgets are significantly underfunded. Almost 70% of respondents believe that their cybersecurity team is understaffed, with over 20% of respondents indicating that they perceive their enterprise as significantly understaffed.[61]

"It's part of the CISO's job to transition from unsupported to being fully supported, but that can only be done when the stage has been properly set within an organization," said Doug Graham, Chief Security Officer at Nuance Communications.[62]

A research report from the Institute of Applied Network Security (IANS) highlights three key findings: [63]

01 Successful CISOs have aligned their security strategies and programs to support the top three to five business initiative priorities of the CEO

02 Metrics are good, but a compelling narrative is what matters. Owning the narrative is the conversation that the CISO has with the executive team about how security is helping the organization grow and win in the marketplace

03 The ability to win support from the business side of the organization for security initiatives, and the additional budget needed, is a skill that can be learned and improved

61 State of Cybersecurity 2019, ISACA, 2019. https://www.isaca.org/-/media/files/isacadp/project/isaca/why-isaca/surveys-and-reports/state-of-cybersecurity-2019-part-2_res_eng_0619

62 "IANS Research Identifies Obstacles in Enterprise Security Budgeting to Help CISOs Win the Battle of the Budget and Manage Risk," Businesswire, Apr 11, 2018. https://www.businesswire.com/news/home/20180411005699/en/IANS-Research-Identifies-Obstacles-Enterprise-Security-Budgeting

63 "Winning the Battle of the Budget," IANS Research, Apr 2018. https://portal.iansresearch.com/content/3566/frp/winning-the-battle-of-the-budget

Where does cybersecurity rank in spending?

Cybersecurity was at the top of the list of transformative technology investments in 2019. In terms of high-priority technology investments, companies are spending nearly 35% of their budget on cybersecurity technologies. Only cloud technologies rank higher at 37%, according to a 2018–2019 survey by Altimeter Investments.[64] AI, Big Data and the IoT trailed behind. In 2019, security services spending overtook product spending in every spending bracket, according to Forrester.[65]

Digital transformation is driving organizations to continue to move to the cloud, with organizations already hosting 61% of their workloads and applications in multicloud environments, according to the Info-Tech Research Group 2020 Security Priorities Report, which included the top-ranked security priorities for 2020. Beginning in 2020, organizations project that 79% of their workloads and applications will move to the cloud, with 84% moving to the cloud in 2021. If the majority of organizations' operations are hosted in the cloud, including high-risk or sensitive data and applications, it makes sense that data security and cloud are a package deal. Forty-three percent of respondents reported that data security was a top priority for 2020, tying with cloud security and just beating out email security.[66]

Security spending is driven by security incidents.

One in four enterprises (1,000-plus employees) are increasing 2020 IT spending due to a recent security incident, according to a Spiceworks survey conducted in July 2019 across North America and Europe.[67]

The study also determined:

- About 44% of responding organizations said that they will increase their IT budgets in 2020
- Overall, those 2020 IT budget increases are mainly driven by the need to upgrade outdated IT infrastructure (64%), escalating security concerns (47%) and employee growth (47%)
- Security spending is 7% of the total IT budget spend
- The average length of the purchase journey is six months or less
- The average number of decision makers involved is three people for small organizations, six for medium and 12 for large enterprises

One interesting finding relating to the 2020 coronavirus pandemic is that it increased organizations' surface area, requiring CISOs to meet this challenge with further security investments. Nearly 70% of major organizations increased cybersecurity spending following the outbreak.[68]

Is most of the budget truly spent on security controls?

In 2019, around 38% of organizations said that they will increase their IT budgets. Security and compliance account for two spots on the list of the top five factors driving this growth, according to a survey by Spiceworks.[69] Overall, 2020 IT budget increases are mainly driven by the need to upgrade outdated IT infrastructure, followed by escalating security concerns and employee growth. For example, two-thirds of large enterprises (5,000-plus employees) plan to deploy 5G technology by 2021, the survey found.

The majority of IT spending is spent on upgrading outdated IT infrastructure, followed by increased priority on IT projects (56%) and security concerns (56%), according to the 2019 security spending outlook by Gartner.[70]

No doubt security is still largely (and incorrectly) perceived as a technology problem. The fact that some security budgets are taking an ever-larger portion of IT budgets reinforces this conclusion. This challenge is founded in two misunderstandings: that security problems are generally solved via technology, and more egregious, that security is linked to IT. It's fallacious to think that security problems are technology problems, although it's true that technology can help resolve security issues.

64 Brian Solis, "The State of Digital Transformation: 2018/2019 Edition," Altimeter, 2019. http://insights.prophet.com/the-state-of-digital-transformation-2018-2019

65 Jeff Pollard with Christopher McClean, Elsa Pikulik and Peggy Dostie, "Security Budgets 2019: The Year of Services Arrives," Forrester, Dec 17, 2018. https://www.forrester.com/report/Security+Budgets+2019+The+Year+Of+Services+Arrives/-/E-RES141372

66 2020 Security Priorities Report, Info-Tech Research Group, 2020. https://www.infotech.com/research/ss/2020-security-priorities-report

67 The 2020 State of IT, Spiceworks, 2020. https://www.spiceworks.com/marketing/state-of-it/report/

68 Jastra Ilic, "Almost 70% of Major Organisations to Increase Cybersecurity Spending Following Coronavirus Outbreak," LearnBonds, Jun 19, 2020. https://learnbonds.com/news/almost-70-of-major-organisations-to-increase-cybersecurity-spending-following-coronavirus-outbreak/

69 The 2020 State of IT, Spiceworks, 2020. https://www.spiceworks.com/marketing/state-of-it/report/

70 "A Look at Cyber-Security Spending in 2019: Where Budgets are Increasing and Why," ARIA Cybersecurity Solutions, Mar 21, 2019. https://blog.ariacybersecurity.com/blog/cyber-security-spending-2019-blog

How many organizations evaluate effectiveness of security spending?

Organizations often lack procedures for measuring the effectiveness of their security spending. CISOs who do implement procedures often prefer to evaluate a security service or product based on its ability to reduce risk and to remain in compliance with regulatory requirements. This is a shift in attitude, since historically, security spending was more motivated by operational and tactical considerations such as incident response, breach mitigation and IP protection, according to Gartner.[71]

How effective organizations are with their evaluation of security spending remains doubtful, since a majority of organizations don't have the capabilities and processes in place to effectively measure either their exposure to risk or the effectiveness of their controls for reducing that exposure.

Many organizations lack confidence in:

- Measuring how well their security strategy is working and where improvements are needed
- Determining and quantifying their data risk exposure with reasonable accuracy (relatively few organizations maintain reasonably mature risk management practices)
- Improving their capability to measure, report and improve the effectiveness of their security controls

Mandiant Security Effectiveness Report 2020: A deep dive into cyber reality

Organizations want reliable data that informs them of whether their security investments are delivering real value and protecting them from becoming the next major cyberattack headline. This report reveals that, while organizations continue to invest significant budget dollars in security controls and assume that this means assets are fully protected, the reality is that a majority of the tested attacks successfully infiltrated the organizations' production environments without their knowledge. The bulk of companies assume they are protected. The truth is that, more often than not, they are exposed:

- 91% of attacks did not generate an alert
- Only 9% of attacks received alerts, demonstrating that most organizations and their security teams do not have the visibility they need into serious threats, even when they use central security information and event management (SIEM); security orchestration, automation and response (SOAR); and analysis platforms
- 53% of attacks successfully infiltrated environments without detection
- 26% of attacks successfully infiltrated environments, with detection
- Exfiltration techniques and tactics were successful 67% of the time
- 68% of ransomware attacks were unnoticed
- 33% of attacks were prevented by security tools, which perform differently from one environment to the next
- The size of an organization generally did not correlate to security effectiveness

The tests consisted of real attacks, specific malicious behaviors, and actor-attributed techniques and tactics run in enterprise-level production environments representing 11 industries against 123 market-leading security technologies, including network, email, endpoint and cloud solutions.

Aggregated data for attack interactions

Total is greater than 100% because alerted is a subset of detected and attacks can be either or both detected and prevented.[72]

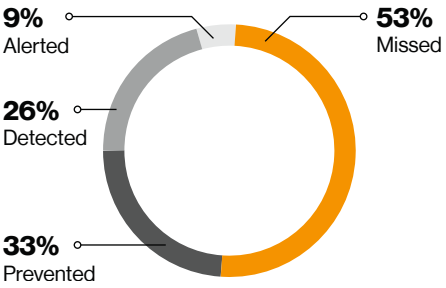


Figure 2. Attack interactions

71 "A Look at Cyber-Security Spending in 2019: Where Budgets are Increasing and Why," ARIA Cybersecurity Solutions, Mar 21, 2019. https://blog.ariacybersecurity.com/blog/cyber-security-spending-2019-blog

72 Mandiant Security Effectiveness Report 2020—Deep Dive into Cyber Reality, FireEye, May 2020. https://www.fireeye.com/current-threats/annual-threat-report/security-effectiveness-report.html

The lopsided CISO priorities

All organizations need to prioritize data protection objectives and activities. It's too expensive to protect all assets from all threats and vulnerabilities. Data cannot all be protected equally; companies must constantly prioritize and assess risks.

Risk management isn't static either. Threats come and go, increase, and decrease, as does a board's risk appetite. Data protection never has been just an IT challenge, solved with capital investments in security products and services. It's an investment that must be made every year to develop processes and a culture that demonstrates commitment to control effectiveness and continuous improvement. It requires attention to a complex and constantly evolving strategy that should be part of a company's entire business ecosystem.

Therefore, CISOs should be balancing their time with sufficient attention to developing initiatives of strategic and operational value. However, too many remain technology focused. CISOs are challenged to identify the components (data, devices, documents and processes) most valuable and critical to the organization and focus aggressively on them. They need to prioritize and categorize the risks they are facing. Using industry frameworks and standards to structure the data protection compliance program is only a start. Knowing what the exact critical decision points are for structuring security program objectives and priorities is just as essential—but we don't see this in practice.[73]

As mentioned earlier in the Choluteca Bridge metaphor, shift happens! CISO priorities for 2020 were upended when the coronavirus pandemic hit. Organizations worldwide experienced a situation overnight where 80% to 100% of their workforces began working remotely. Threat actors quickly adapted their attacks to target remote workers. CISOs suddenly had to deal with how to address foundational security issues. This included prioritization shifts to reconsider which assets became more vulnerable as a result. Managing a remote workforce also changed day-to-day operations. Some organizations failed to prepare for security updates to be distributed and verified efficiently, and to adapt overall security posture to the new circumstances—similar to how the Choluteca Bridge in Honduras was unable to deal with drastic change to its environment.

Most CISOs focus on cloud security management as a top priority to ensure that all users maintain secure access to the right resources. More organizations are implementing zero trust models (see "Mobile security" on page 123 for details on zero trust).

CISOs who embrace the DevSecOps concept so that cybersecurity is prioritized at the outset of any IT-related project make use of the agile framework for different purposes, focusing either on DevOps to prioritize delivery time or SecOps to prioritize security, to try to balance the two objectives.

In addition, user education remains a top priority to improve security awareness and install an intentional culture of data protection across the organization.

While these initiatives are important, it's clear that CISO priorities remain technology focused while they struggle to improve the visibility and communication of security risks, align

73 The role of decision-making and culture in data protection is a subject we will focus on within the next edition of the PSR.

better with the business, and make key performance indicators (KPIs) and relationships with stakeholders across the business more meaningful.

This list can be worrisome depending on the security maturity of organizations. For many, activities at the very top should include maintaining updated, documented data flows and network configurations; keeping accurate asset inventories at all times; and running effective risk assessments. We place these three items in this order based on the gaps that we see in the field: CISOs often do not know what data is traversing where on their networks, where it is stored or what their critical assets are. Without this information, they cannot make informed risk decisions, which then means they are funding the wrong security initiatives. They get caught flat-footed in a breach, oftentimes because they have asked for funds to be invested in the wrong places.

Organizations are clearly over-reliant on technology—as indicated in the "Mandiant Security Effectiveness Report" section on page 38—and don't offer the level of protection that most expect.

Sustainable and effective security is achieved through processes and culture. Tools need a process, and a process needs an audit and performance measurement. CISOs also need to balance their time to attend to the improvement of their security strategies and align their security business models and operating models to enable them to execute effectively.

The average security operations team receives over 11,000 alerts per day, and the vast majority must be manually processed, according to a Forrester Consulting thought leadership paper commissioned by Palo Alto Networks, "The State of 2020 Security Operations."[74]

Alert fatigue from the number of security products that generate alerts is also on the CISO's top 5 list of concerns.

Security operations teams can't keep up with the incoming volume of alerts. Only 47% of organizations noted that they can address most or all security alerts received in a day, according to "The State of 2020 Security Operations." Nearly 20% of alerts are manually reviewed/triaged by an analyst; almost a third are false positives; and 28% are outright ignored by analysts struggling to keep up with the workload. Only 17% of alerts are touched by automation, leaving security teams to rely on an average of 10 different categories of security tools when managing alerts.

Security operations teams are evaluated across five key metrics, on average, with the most popular being mean time to investigate, number of incidents handled, mean time to respond, threat score and number of alerts. Fewer than half of these teams meet these metrics most of the time; even fewer hit their key metrics all of the time.

This problem has existed for many years. Most organizations lack capacity and enough people to perform the reviews. In the 2018 edition of the same report, approximately 79% of survey respondents said the lack of qualified candidates leaves their mean time to respond for resolving incidents at an average 4.35 days. Three-quarters of respondents (75%) said they are fairly or very challenged by working with multiple security tools. Forty-two percent of participants said they don't have a system in place for measuring incident response metrics. It takes an average of eight months to train security analysts to be effective, only to have a quarter of those professionals switch to a new organization within two years.

74 "The State of 2020 Security Operations," Forrester Consulting on behalf of Palo Alto Networks, April 2020. https://www.paloaltonetworks.com/resources/research/forrester-the-2020-state-of-security

Trap 4

Falling short on sound strategic design

Strategy design challenges

Turning strategy into results

In addition to the budgeting process, the strategic planning process is the backbone for execution in organizations. That puts a high priority on developing a sound strategy for your security program. Fortunately, organizations have access to a clear and widely accepted definition of what strategy is, thanks to Michael Porter, renowned Bishop William Lawrence professor at Harvard Business School, who performed seminal work on strategy in the 1980s. Yet organizations often fail to turn such seminal advice into successful results when it comes to data protection and compliance strategy.

The reason is clear. When crafting security strategies, many CISOs create detailed road maps that specify who should do what, by when and with what resources. Unfortunately, Gantt charts seldom survive contact with reality. Crafting and executing an organization's data protection and compliance strategy can be extraordinarily difficult, particularly in organizations with low maturity in transformation and change management. It's no surprise that many try to oversimplify the process of security strategy design, alignment execution and management—or dilute it to match their level of competence.

Despite the obvious importance of good planning, design and execution, many organizations don't focus sufficiently on setting themselves up for success with the needed capabilities, processes and leadership for turning security strategies into results. Even members of security steering committees often lack a clear sense of how major priorities and initiatives fit together. When the objective is to maintain a control environment that is sustainable, with security control systems that are effective and control performance that produces predictable results that are tracked and reported, then the security strategy needs to support the achievement of these outcomes. Strategy execution is a long-term process with the continuous development of capabilities and processes that requires years of attention.

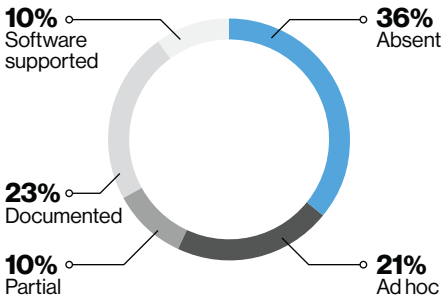
Pinpointing bad security strategies

The shortcomings of a bad security strategy are usually painfully obvious, at least in retrospect, and particularly in the aftermath of a data compromise. But seemingly good strategies—those promoted in several books, frameworks and standards published during the past decade—often fail, too. See Appendix D, "Suggested reading," for guidance on security strategy.

When that happens, it's often harder to pinpoint the reasons why organizations don't succeed in designing and executing security strategies that meet their objectives. Organizations must maintain a capability to correct deviations of control performance in a timely and predictable manner. This is why it's essential to explore and even delve deeply into the many pitfalls CISOs experience during strategy design, alignment and execution.

Security strategy maturity

The successful design, implementation, monitoring and evaluation (DIME)—followed by improvement—of corporate security strategies depends on several organizational processes and capabilities that need to be developed toward higher levels of maturity. A 2019 study on security maturity by Orange Cyberdefense (formerly SecureLink) found that security strategy in most organizations is absent or lacks maturity.[75] The study asked respondents: "Do you have an overall cybersecurity strategy of the business?"



Two-thirds of the responses indicated there is a cybersecurity strategy in place, but when looking closer, over half of these strategies aren't supported by processes, such as vulnerability management and a penetration testing process.

Figure 3. Use of cybersecurity strategy

75 The 2019 Security Maturity Report, Orange Cyberdefense (formerly SecureLink), 2019. https://securelink.net/campaign/sma/security-maturity-report-2019/

> **“There is a slightly odd notion in business today that things are moving so fast that strategy becomes an obsolete idea. That all you need is to be flexible and adaptable. Or as the current vocabulary puts it, ‘agile.’ This is a mistake. You cannot substitute agility for strategy. If you do not develop a strategy for your own, you become a part of someone else’s strategy. You, in fact, become reactive to external circumstances. The absence of strategy is fine, if you don’t care where you’re going.”[76]**
>
> **—Alvin Toffler, futurist**

The value of security steering committees

Steering committees need a lot of guidance on how to do strategic planning for data security and compliance management. In the 2019 PSR,[77] we reviewed the role and value of security steering committees. In payment security, steering committees play significant roles in the data protection and compliance priorities of organizations and manage the general course of operations. They help steer the position, course and even the distance traveled of security practices. By definition, they are a form of corporate governance made up of high-level executives, authorities and stakeholders who provide strategic oversight and guidance on the security strategy and program. They meet at key stages during the course of a project and influence strategic decisions. In short, a steering committee does exactly what its name suggests: steering projects, programs and organizations toward desired successful outcomes.

While their primary purpose in payment security is to direct data protection and compliance programs, steering committees also fill several other important roles, including:

- Giving input on issues concerning the development of a project or organization
- Providing insight on concerns related to the budget, marketing, hiring, etc.
- Determining what outcomes need to be realized through a project or undertaking
- Prioritizing steps and goals that need to be taken and realized in a project
- Helping to develop policies and procedures relevant to a project or operation
- Projecting potential risks and monitoring or eliminating them as required
- Setting timelines and monitoring progress
- Offering advice on business or project topics for which they have oversight

Security and compliance is primarily a control function.

An important side note: The primary function of the steering committee, and the security and compliance organization in general, is not to be a “business enabler.” This is an often-repeated cliché. Security and compliance is primarily a control function of the organization. The purpose of security and compliance teams is to measure actual performance and compare it with standards to identify any deviation, taking corrective action and communicating the results as input for continuous improvement. Security and compliance teams should not dilute their focus from this function due to being measured on and held responsible for enabling business initiatives.

76 Quoted from Bill Stackpole and Eric Oksendahl, Security Strategy: From Requirements to Reality, Auerbach Publications, Oct 13, 2010.
77 2019 Payment Security Report, Verizon, 2019. https://www.verizon.com/business/resources/reports/payment-security-report/

Strategy design failures

When defining an organization's security strategy, CISOs follow a common approach advocated by many publications. The steps typically consist of identifying a series of objectives (unfortunately, often heavily technology focused!) and translating them into a collection of projects, each with their activities and tasks. The projects, collectively wrapped into a program, are assigned project managers and overseen by a program manager (often the CISO) tasked with cascading the program activities down the hierarchy. The CISO and the steering committee provide guidance, identify and correct deviations, and measure progress. Unfortunately, many organizations fall prey to common myths about strategy—for example, believing that "strategy" is merely high-level planning that resides at the top of the organization, where a simple list of predefined goals are formulated by executives. This isn't what strategy is, or how a security strategy should be designed. Too many organizations remain stuck with an approach to strategy design and execution that doesn't work.

Incorrect placement of authority to execute

One of the first design failures of security strategies is the failure to designate responsibility, authority and capability to execute throughout the organization. Successful execution of a corporate security strategy isn't as simple as just putting the right people in place to get the right things done. It is vitally important to enable managers at all levels to first clearly understand and then be enabled to support the execution of the security strategy.

While concentrating authority and decision-making power at the top may boost performance in the short term, it degrades an organization's capacity to execute over the long run. Top-down execution of corporate security and compliance strategies has other downsides in addition to the risk of unraveling after the departure of a strong CISO. To understand why this happens, it helps to remember that effective execution in large, complex organizations emerges from a collaboration of perspectives, decisions and actions at all levels.

Managers that are the closest to the operations on the ground usually can respond the fastest. They are often positioned to make the best calls on data security and evaluate the course of action on security control standard deviations. When top executives insist on making the important calls themselves, they diminish middle management's decision-making skills, initiatives, efficiency and ownership of results.

To most employees, line managers, not senior executives, represent "management." Employees are unlikely to interact regularly with the C-suite and the board. Corporate culture is significantly influenced by how the line manager conducts daily business, negotiates challenging circumstances and manages personnel. However, execution needs to be generated from the middle, and oversight from the top is essential.

When top executives—the CEO, CIO and board members—fail to ensure that middle managers clearly understand the security strategy, the managers can be hamstrung in their efforts to translate overall company strategy into meaningful terms for their teams or units. In most cases, the executive teams must provide significantly more support.

The 7 basic components of strategy planning

In general, traditional strategy planning has seven basic components:

1. **Vision, mission and values: Alignment of the vision, mission and corporate values of the business with the vision, mission and corporate values of the security organization**
2. **Strategic objectives: Identification, evaluation and alignment between strategic objectives of the business and the security organization**
3. **Plan analysis: Analysis of the strategy plan, objectives, priorities and allocation of resources**
4. **Strategy formulation: Choosing the most appropriate courses of action, detailing the steps and processes needed to reach plan goals, and evaluating feedback and progress reports**
5. **Strategy implementation: Assignment of roles and responsibilities to execute the plan**
6. **Evaluation: Testing the efficiency and effectiveness of the strategy, and obtaining assurance that the strategic choices are properly implemented using control metrics**
7. **Capability and process maturity: Determining how close the strategic planning process is to being complete and capable of continual improvement (see the 2019 PSR, page 26, for more details on process and capability maturity)**

9 strategy checks

In his book on strategy, Jeroen Kraaijenbrink emphasizes several checks to find out whether your strategy fulfills basic criteria.[78] While there is an endless number of criteria that you can use to assess your security strategy, the following nine checks are particularly useful:

1. **Coherence: Do all elements match? Do they add up to a coherent strategy or not?**
2. **Efficiency: Are all elements used up to their maximum potential? Can they be better exploited?**
3. **Effectiveness: Does the strategy work? Are you achieving what you want and getting adequate performance?**
4. **Uniqueness: Is the strategy unique enough? Or can it be executed by many other organizations as well? (Note: This one is relevant for business, but not so much for cybersecurity.)**
5. **Flexibility: Is the strategy sufficiently flexible? Can it easily be adapted to changes if necessary?**
6. **Robustness: Can the strategy survive for a sufficiently long time? Is it resistant to changes in the environment?**
7. **Scalability: Is the strategy scalable? Can it grow easily without too much extra effort and investments?**
8. **Responsibility: Does the strategy comply with ethical and moral standards? Is what is being done right?**
9. **Pros and cons: Do the benefits, advantages and strengths of the strategy outweigh its cost, disadvantages and weakness?**

Prioritizing wrong objectives

While a defined security program and related projects are the general mechanisms to achieve strategic goals, many pitfalls exist. Foremost is prioritization. Most CISOs deal with a diverse set of stakeholders who want to "get projects done." The resources to deliver those projects are finite and in high demand. There are very seldom, if ever, enough resources to satisfy everyone's needs (see page 32 on lack of resources). When a CISO fails to properly prioritize and/or picks the wrong projects, the organizational performance on data protection, compliance and effectiveness suffer.

As in business strategy, information security strategy at its most basic level is a set of trade-offs and choices about where the organization can and must invest to achieve the best outcomes. Determining the priorities requires a combination of skills and sources, as well as active threat intelligence (such as the Verizon DBIR and other reports) to understand which information security and cyberthreat risks to prioritize, decide which controls will provide the best protection to support the robustness and resilience of the control environment, and tackle a range of other considerations. Every "yes" to any particular project requires a "no" to several others—while juggling budgetary constraints—to secure support for initiatives that will be proven successful and the best choices in the future.

Strategic planning, design and alignment should be conducted at least on an annual basis and revisited at least quarterly. Strategic planning is a process, not an event. There should be organizational reviews of the strategic planning inputs, adjustments, updated action plans and metrics throughout the year. Don't get stuck on calendar cycles; stay nimble and change course as needed.

4 Lines of Assurance

For more details on the collaboration needed across the organization, we reviewed the 4 Lines of Assurance model in the 2019 PSR[79] and how assurance comes directly from work units: the front-line staff, operational management and directors. In other words, those responsible for delivering specific objectives or processes.

The decisions and actions occur between the front-line staff, who need to be held individually responsible as the first line of assurance. The next line of assurance comes with the risk management and compliance functions that monitor the implementation of policies and procedures and serve as the management oversight over the first line. Then, internal auditing in the third line provides a level of objective, independent assurance, and also timely information to the board that the risk management and internal control framework is working as designed, with reasonable (not absolute) assurance of the overall effectiveness of governance, risk management and controls. The role of internal auditing is largely detection and correction, i.e., detecting control weaknesses or breakdowns and suggesting improvements or remedial action. Then, in the fourth line are the external auditors, regulators and other external bodies that provide assurance on the effectiveness of governance, risk management and internal controls. They should evaluate the manner in which the first first three lines of assurance achieve control objectives.

78 Jeroen Kraaijenbrink, The Strategy Handbook, Part 1: Strategy Generation, Effectual Strategy Press, page 114, 2015. https://www.amazon.com/Strategy-Handbook-Practical-Refreshing-Making/dp/9082344300/

79 Verizon 2019 Payment Security Report, page 12, 2019. https://www.verizon.com/business/resources/reports/payment-security-report/

A common strategy design pitfall occurs when CISOs and their steering committees start their strategic planning initiatives from the inside out. By starting internally, they prioritize activities and define strategic objectives to solve areas of data security and compliance that do not perform well. However, in most cases, these are only symptoms of larger issues in their control environment that need to be corrected. For example, by not solving issues in the 6 Cs—the 6 Constraints of Organizational Proficiency, namely capacity, capability, competence, commitment, communication and culture—across all lines of assurance (line staff, risk and compliance teams, internal audit, and external audit), the reasons for those constraints existing in the first place will likely remain unaddressed. They need to focus on the primary causes and contributors that prevent the achievement of strategic objectives, and not on treating the symptoms.

Failure to focus—taking on too many responsibilities

Limiting the number of commitments requires deprioritizing and then focusing all resources on a narrow remaining set of priorities. For example, organizations benefit substantially when their strategic objectives include the already-prioritized 9 Factors of Control Effectiveness and Sustainability Framework as a primary objective within their strategy and program. See Appendix B on page 124, specifically the updated PCI DSS compliance calendar.

It's not uncommon for executives to fail to grasp the potential impact of not making sound trade-offs. To successfully execute strategy, it's important to limit the number of strategic initiatives on which you focus. Avoid spreading resources—particularly people and time, but also budget—too thin. You need to build your security and compliance budget around your strategy and successfully communicate this to the stakeholders. Organizations that struggle to execute their strategy often demonstrate that they did not link their long-term business strategy with the annual financial budgets. The findings of a study by the Palladium Group revealed that fewer than half (40%) of organizations link their long-term business strategy with the annual financial budgets.[80] This does not promote the capability to successfully execute strategy, and almost guarantees a disconnect between commitments and the available capacity to deliver. The same may be true for security and compliance budgets.

This debilitating practice creates an unhealthy cultural detachment between commitments and resources. These organizations present a stark contrast to companies with successful execution strategies that limit the number of strategic initiatives they focus on. They start with strategy and then carefully build their budgets around a defined strategic plan.

Inadequate management and oversight

The biggest concern of all may be executive inattention. Once a plan is decided upon, often surprisingly little follow-through occurs to ensure its execution. Many security strategies fail simply because they don't get communicated to all of the people involved. While many organizations may have relatively effective processes for cascading security and compliance goals downward in the organization, more often the procedures for managing horizontal performance commitments across silos lack teeth. Various management options are available to address this problem, such as a centralized project-management office, service level agreements and cross-functional committees. Most organizations require an improved structure in their processes to coordinate activities across units.

In many organizations, lack of focus and oversight has become endemic. For example, when it comes to strategy, one study found that 70% of leaders review strategy only about one day a month. Some 85% of leadership teams discuss strategy less than an hour per month.[81]

In conclusion, CISOs will benefit from being reminded that sound data security strategy and program design adds value faster than it adds costs.

“Design adds value faster than it adds costs.”

—Joel Spolsky, web programmer, writer and creator of Trello

80 David P. Norton, “Strategy Execution, A Competency that Creates Competitive Advantage,” Palladium Group, 2007.

81 Ron Carucci, “Executives Fail to Execute Strategy Because They're Too Internally Focused,” Harvard Business Review, Nov 13, 2017. https://hbr.org/2017/11/executives-fail-to-execute-strategy-because-theyre-too-internally-focused

Trap 5

Deficient strategy execution

Why CISOs struggle to execute strategies

It's no secret: Most organizations struggle with strategy execution. According to McKinsey research, 70% of change efforts fall short of desired results.[82] Similarly, corporate security strategy execution can go wrong for a variety of reasons. One of the most significant challenges CISOs face is the failure to align a security and business strategy. Second to that is the challenge coordinating strategy across business units.

In many cases, low performance on strategic data protection and compliance objectives (such as sustainability and control effectiveness across the control environment) are not directly attributable to the poor performance of security and compliance teams (the first two lines of assurance). Instead, low performance stems from failed coordination to deliver with other teams in the organization.

Deciding you want a security strategy and program that effectively protects data in a consistent, repeatable manner with predictable results isn't the same as developing capabilities and resources that enable you to design, implement and maintain processes and controls that deliver on that strategy (aligning actions to your strategy).

Many organizations react too slowly. They cannot mitigate emerging security threats in time or react quickly but lose sight of their corporate security strategy. Organizations fail to allocate or reallocate funds to the right places quickly enough to be effective. The reallocation of people is even worse. It can be challenging for organizations to do a good job of shifting people across units to support strategic priorities—many resist the change to avoid disrupting other units.

Already-scarce security team resources often get trapped in unproductive uses. Very few organizations routinely track performance against a documented and maintained performance standard. Performance monitoring is only an annual affair at most companies, and often not well quantified.

Actions typically follow decisions. If your organization does not have the ability to make well-aligned decisions to improve data security and compliance, it will not be well positioned to take well-aligned actions either.

What is strategic alignment?

Research on strategic alignment began in the 1950s with Peter Drucker's work on management by objectives. The subject of best practices for achieving strategic alignment is generally well understood. In some managers' minds, strategy execution equals alignment. However, this isn't true.

Wikipedia defines "strategic alignment" as follows: "[T]he process and the result of linking an organization's structure and resources with its strategy and business environment (regulatory, physical, etc.). Strategic alignment enables higher performance by optimizing the contributions of people, processes and inputs to the realization of measurable objectives and, thus, minimizing waste and misdirection of effort and resources to unintended or unspecified purposes."[83]

Strategic alignment: The process of aligning an organization's structure, resources, decisions and actions with its strategy and business environment such that they support the achievement of strategic goals.

82 Boris Ewenstein, Wesley Smith and Ashvin Sologar, "Changing change management," McKinsey and Company, Jul 1, 2015. https://www.mckinsey.com/featured-insights/leadership/changing-change-management

83 "Strategic alignment," Wikipedia, https://en.wikipedia.org/wiki/Strategic_alignment

Align first, then execute!

Strategic alignment—the process and result of connecting your organization's structure and resources with your strategy and business environment—is one of the key differences between organizations that perform well and those that don't. Aligning data protection compliance activities to business and security strategies is what makes the difference. Just having a strategy isn't enough; by itself, it may have no real effect on the performance of your security program.

A lack of proper alignment between security operations and business strategy remains one of the most common mistakes. CISOs should measure what the business actually cares about. They need to clearly articulate why investing in sustainable and effective data protection and compliance matters to the business, how that is associated with specific business objectives, how they will lower risk, and to what degree and at what cost. Both the top leadership and the security team must share the same understanding of the organizational risk being assumed and the capability to mitigate it.

As a side note, during compliance validation assessments, Qualified Security Assessors (QSAs) evaluate the risk management policies, standards and reports. The risk assessment reports that are presented as evidence of compliance are often dissociated from the enterprise risk assessment processes. The risk assessments are conducted merely for the purpose of producing a risk report to meet PCI DSS compliance validation requirements; they are nearly useless as input for generic corporate risk mitigation and management.

The CISO should understand exactly how the security strategy is aligned with the organizational capabilities. Next, CISOs need to know how their security strategy is aligned with the long-term purpose of the data protection and compliance vision of the organization. Often, the organization has the best of intentions but is incapable of delivering on the strategy.

Many CISOs are managing risk for parts—but not all—of their organization because they don't have full visibility into their enterprise landscape. For example, many CISOs still struggle to maintain a full IT asset inventory and a complete list of all third-party suppliers and cloud applications used by employees and business units. Small to mid-size organizations often don't track risk metrics because they lack the money and expertise to implement such practices, while large companies sometimes don't because they're overwhelmed by the perceived complexity of such an undertaking.

In conclusion, for many organizations, it's essential to switch to a new model to achieve the goals and mission of their security strategy.

A foundational security strategy should be a carefully chosen response to a business environment, and factor in the exact condition, capabilities and constraints that exist within the control environment. Formulating and executing a security strategy requires a set of carefully crafted decisions about the direction the business should go in to achieve data protection and compliance objectives.

It requires clarity about how constraints will be dealt with, and sound strategic thinking to select the most appropriate security business models and operating models to support and enable sustainable execution of the strategy.

Next, we review the importance of making sound decisions about the adoption of security models and frameworks, and how those decisions can support the design of a security strategy and program.

Security models and frameworks

Organizations often struggle to gain a firm grasp on the critical elements of data protection compliance success. Many problems in data protection and compliance remain unsolved regardless of past actions taken by security teams. The cause-and-effect thinking method is not effectively applied for solving these problems. Organizations continue to remain overly reliant on technology to solve problems. CISOs are consumed with continuous firefighting, resulting in little time for innovation. The data protection problem-resolution strategies are attempts to address obvious symptoms without identifying underlying causes. This results in perceived quick wins, but long-term malaise.

As stated before, organizations across the payment security industry must move away from managing data protection and compliance as if it is solely an IT concern. The question is: "How?" How can a CISO steer an organization and develop a security culture that moves away from a technology focused approach that applies point-in-time corrections without providing lasting improvements in data protection? How can the organization develop data security and compliance to be understood as a quality improvement process in an organization, aiming at continuous improvement of organizational performance?

It makes no sense for CISOs to push harder and harder on familiar solutions, while fundamental problems persist. Data security should be managed as a set of related and interdependent systems—with a better understanding of the big picture. There are many variables to consider. Silos need to be avoided, as well as collaborative security relationships built and maintained across the organization. The strategic direction must be clear to all stakeholders.

In addition to developing a sound data protection strategy that is aligned with business objectives and receives continued support from the board and executive teams, CISOs must apply systemic security management. Organizations need to introduce a business model approach to reveal and manage the structures that underlie the complex data protection compliance ecosystem.

For many organizations, transforming how to develop the capability to design, implement and maintain PCI security compliance, and maintain a control environment that is sustainable and effective, will likely need to begin with revisiting all components, their security strategy, security business models

Common strategy concerns

Why is the success rate of strategy execution so incredibly low? The simple answer would be that successfully executing a good strategy is just exceptionally hard. But that is hardly a gratifying answer. There are many other efforts that are exceptionally hard, but we succeed at them nevertheless. Therefore, to start with, we need to have a good understanding of the problems that organizations face when executing their strategy. When we know these problems, we understand the underlying reasons why strategy execution fails, which helps us find the solutions.

In his book The Strategy Handbook, Part 2: Strategy Execution,[83] Jeroen Kraaijenbrink reveals how issues with strategy execution can be distilled down to about 21 concerns. Review this list and choose which ones best describe your organization's security implementation issues. Then take the challenge: Research and create a plan for how your organization needs to redesign to become more strategic and successful with compliance.

1. **Unclear communication**
2. **Poor or nonexistent communication**
3. **Lack of commitment**
4. **Insufficient or inadequate resources**
5. **Isolated and fragmented actions**
6. **Ambiguous or conflicting goals**
7. **No or unclear strategy**
8. **No clear priorities**
9. **Ambiguous responsibilities**
10. **Lack of performance information**
11. **Silo behavior and suboptimization**
12. **Wrong or ineffective culture**
13. **Resistance to change**
14. **Over-complexity**
15. **Insufficient management capabilities**
16. **Delay, plans are not met**
17. **Budget is exceeded**
18. **Lack of middle-management support**
19. **Strategy is not adapted to changes**
20. **Poor leadership**
21. **Bad strategy execution**

83 Jeroen Kraaijenbrink, The Strategy Handbook, Part 2: Strategy Execution, Effectual Strategy Press, 2018, page 13. https://www.amazon.com/gp/product/9082344335

and the operating model. In short, organizations will have a far better chance at succeeding with maintaining PCI security compliance when they have a well-defined security business and operating model that is aligned to the overall business strategy. For such transformations to succeed, leadership teams should examine and possibly substantially revise their existing security operating models.

Many organizations that go through their annual PCI security compliance validation cycles successfully do so with the help of one or more security frameworks (see page 55 for a list of the top frameworks).

Traditionally, most security frameworks focus on people (employees), process (controls that are in place to ensure security) and technology, without sufficient coverage of organizational design, strategy and the operations (the "how-to") for the strategy execution. Closer integration is needed between business and information security in order to align data protection compliance with the organization's objectives, culture, executive and line-management ownership, and accountability for implementing, monitoring and reporting on information security.

In addition to the use of security frameworks, many organizations still need to realize the value of security business models and operating models.

Business Model for Information Security (BMIS)

In general, a business model is a design for the successful operation of a business, and a description of the value that the business generates. The operating models represent how an organization creates value, and by whom within the organization—describing the way that an organization structures its core processes. Similarly, an organization should have a defined security business model (SBM) and security operating model (SOM). The CISO and steering committee should evaluate the organization's security operating model and ask if it is appropriately aligned with the security strategy. If the answer is no, the security team and others risk poor execution and an uphill battle to deliver results, which often impact the entity's compliance status.

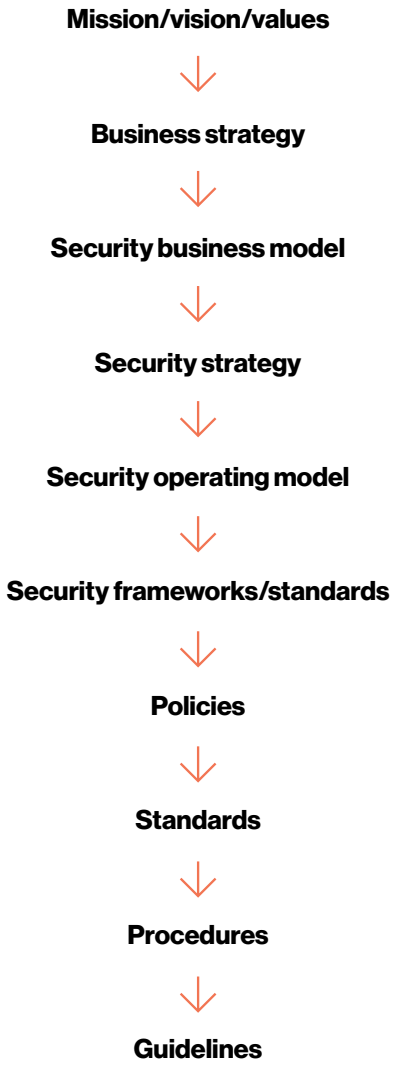
Models should be independent of any particular technology or technological changes over time. They should cover not only traditional information security but also privacy, physical security, risk management and compliance. For multinational organizations, security models ideally also should be applicable across geographies and regulatory and legal systems.

Creating an intentional security culture is a primary objective for the model, as applied to information security. The intentional information security culture focuses on the organization's governance needs, a type of culture with several important characteristics:

- Alignment of information security and business objectives, which help with management's understanding of security issues and secure senior management's commitment to data protection compliance initiatives
- Balance among the organization, people, process and technology
- A business model that will help guide planning prior to the implementation of technologies
- Allowance for the convergence of security strategies

"Any time you sincerely want to make a change, the first thing you must do is to raise your standards."[84]

—Anthony Robbins, motivational speaker



84 Anthony Robbins. https://www.tonyrobbins.com/tony-robbins-quotes/inspirational-quotes/

"The Business Model for Information Security (BMIS) fills a gap and addresses the security programme at the strategic or business level. The model allows security managers to gain a broad view of what is happening in the enterprise, enabling them to better treat information risk while assisting senior management in meeting its goals. By looking at the security programme from a systems perspective, BMIS provides a means for security professionals to consider areas that may not have been accounted for in existing standards. It is important to distinguish amongst models, standards and frameworks. While BMIS overcomes some of the known difficulties in information security, it is primarily a model that must be supported by additional standards and frameworks. An overarching security model such as BMIS must, therefore, be the foundation for all standards and frameworks applied in the information security arena. BMIS creates opportunities for the information security programme to establish itself as a solid business enabler by considering security's impact on the business."[85]

— The Business Model for Information Security

The Business Model for Information Security (BMIS), launched by ISACA in 2009, provides a comprehensive approach for managing information security while directly addressing business objectives. The model was based on the Systemic Security Management framework developed by the University of Southern California's Marshall School of Business Institute for Critical Information Infrastructure Protection. In 2008, ISACA acquired the rights to develop the model to help embed its concepts in information security practices globally. The BMIS exploits system thinking in order to structure the complex and dynamic field of information security. The model promotes a holistic, dynamic, business-oriented approach to information security, which includes considering the interactions within the system, understanding the hidden conceptual problems and finding the best possible solutions.

Elements of the BMIS

The model is made up of four elements: people, process, technology, and organizational strategy and design—a critical element. It has six dynamic interconnections; governing, culture, architecture, enabling and support, emergence, and human factors.[86]

1. **Organizational design and strategy:** This is very important. An organization is a network of people, assets and processes interacting with each other in defined roles and working toward a common goal. An enterprise's strategy specifies its business goals and the objectives to be achieved, as well as the values and missions to be pursued. Design defines how the organization implements its strategy. Processes, culture and architecture are important to determine the design.
2. **People:** The people element represents the human resources and the security issues that surround them. It defines who implements (through design) each part of the strategy. Externally, customers, suppliers, media, stakeholders and others can have a strong influence on the enterprise and need to be considered within the security posture.
3. **Process:** Process includes formal and informal mechanisms (large and small, simple and complex) to get things done and provides a vital link to all of the dynamic interconnections. Processes identify, measure, manage and control risk, availability, integrity and confidentiality. They also ensure accountability. They are derived from the strategy and implement the operational part of the organization element.
4. **Technology:** The technology element is composed of all of the tools, applications and infrastructures that makes processes more efficient. As an evolving element that experiences frequent changes, it has its own dynamic risks. Given the typical enterprise's dependence on technology, it constitutes a core part of the enterprise's infrastructure and a critical component in accomplishing its mission. Technology is often seen by the enterprise's management team as a way to resolve security threats and risks. While technical controls are helpful in mitigating some types of risks, technology should not be viewed as an information security solution.

85 "The Business Model for Information Security," ISACA, 2010. Also see Yulia Cherdantseva, "An Introduction to the Business Model for Information Security." https://users.cs.cf.ac.uk/Y.V.Cherdantseva/TutorialYear2-InfoSecBMIS.pdf

86 "Business Model for Information Security (BMIS)," CIO Wiki. https://cio-wiki.org/wiki/Business_Model_for_Information_Security_(BMIS)

Operating model introduction

Strategy is essentially deciding where you will allocate scarce resources on objectives that are prioritized. When people think of security strategy, most will focus on which environments (internal networks, cloud) to prioritize data protection initiatives, and which vendors and tools to deploy. However, equally important but often overlooked is the organization's security operating model (SOM)—the coordinated collection of security capabilities, organization structure, assets, people, technology, partnerships and governance used to effectively deliver the data security strategy.

Success comes from designing the best strategies and then executing these strategies to the right degree. Operational design follows strategy. The relationship also works the other way around. Improvement in your SOM can lead to positive changes to your security strategy, too. Therefore, a strategy and business model without an operating model are less likely to succeed in delivering the value expected of data security compliance programs. Organizations can unlock the value in their data security and compliance practices by aligning their SOM with their risk and security strategy to execute more effectively and deliver predictable results.

Business leaders should develop and maintain a clear sense of their strategic data security ambitions—where to play and how to win—and the models they wish to employ. The SOM is the operational design that makes it possible to deliver the security strategy, defining how the security initiatives are integrated and function. The SOM is responsible for the how, where and when, and is part of the execution life cycle of strategy.

Avoid a strategy without a clear operating model.

An operating model is the connective fiber between strategy and execution. It is one of the tools that a CISO and a steering committee should use to help them formulate and execute the security strategy. Typically, work on the SOM starts after the formulation of the strategic security plan. A documented operating model offers a structured visual representation of the combination of structures, processes, roles, skills, technologies and other assets that allow an organization to deliver on its strategy. It translates the strategic plan into actionable decisions and operating requirements. This can help to:

- Reveal areas where the strategic plan will be hard to implement
- Provide clarity on how work should get done by various teams and decision support
- Communicate the performance metrics that matter most
- Present an optimal organization structure with the desired number of operational layers in the organization and spans of control for managers

This also includes what capabilities—the processes, data, people and systems the security organization has to keep itself running—that need to be applied at the right time (when) and in the right place, in different locations (where).

Operating models compartmentalize the control environment to outline the working parts. They serve to instruct leaders and others to identify concerns with performance issues. Operating models also serve as a step-by-step check when changes are implemented.

Julie Choo, author of The Strategy Journey, mentioned, "I like to use the car analogy to describe the operating model as the engine of an organisation. In 2016, the fastest Formula One (F1) car, the Mercedes Silver Arrow, driven by Lewis Hamilton (arguably the fastest driver) did not win because of engine and reliability problems. Instead, the World Championship was won by his teammate Nico Rosberg, who had a better functioning engine that was able to last the distance of a whole season. Nico benefited from a slightly better operating model, and that's what led to his overall win. Nico had the processes, data, systems and the people (including himself)—the complete capability package—to win that World Championship. The mechanical failures that Lewis suffered, mostly not through fault of his own, were a result of failures somewhere within his operating model. It is clear Lewis also had some organisational problems within his management team, and we do not know what other issues lay behind the Mercedes garage or in Lewis' own mind. Put simply, he lost because his operating model package was inferior to Nico's."[87]

87 Julie Choo, "How to design a Target Operating Model (TOM) that delivers," Stratability Academy, Mar 2, 2017, update May 4, 2020. www.strategyjourney.com/target-operating-model-that-delivers/

The business organization should not be a passive recipient of services from the security organization; they are the reason the service exists and should actively participate in its design, implementation, evaluation, monitoring and maturity improvement.

Security efforts in many organizations are reactive, busy with activity and unable to answer the question, "Are we becoming more secure by improving the sustainability and effectiveness of our control environment?" For most organizations, the reality is that their security needs will always exceed their capacity. A more strategic approach is necessary.

Therefore, an operating model is similar to an interactive road map with regular changes. However, there are many maps within the map instructing on specific needs, such as software applications, decision-making, processes and other components integral to a well-designed plan.

Exploring a target security operating model

What is a target security operating model (TSOM)? In a nutshell, it's a future-state version of the operating model snapped at a specific point in time. The SOM can describe the way an organization protects data today—the "as is." It can also communicate the vision of how data will be protected in the future—the "to be." In this context, it is often referred to as the TSOM.

So if a TSOM doesn't exist, what is needed to achieve it? Transformation of the operating model itself. This requires a large effort in the form of a program of change.

Organizations typically design TSOMs to be delivered in phases, following the transformation of the security strategy, security business model, SOM (the existing one) and the TSOM. The phases should be executed in the right place at the right time, while having the agility to cater to unforeseen changes. Then the organization is in the position to successfully navigate its journey to achieve the beneficial outcomes of the TSOM.

Benefits of a defined SOM

A SOM enables an organization to focus on identifying risks, recommending risk responses and facilitating trade-off decisions related to these risks. The core of this model is a continuous improvement process, with collaboration across all lines of assurance (see page 44 for description of the 4 Lines of Assurance), designed to sustain the controls that protect the data and secure the organization.

An operating model covers six elements making up the acronym POLISM:[88]

- **Processes and activities:** The work that needs to be done
- **Organization and people:** The people doing the work and how they are organized
- **Locations, buildings and other assets:** The places where the work is done and the equipment in those places that's needed to support the work
- **Information:** The software applications and databases needed to support the work
- **Sourcing and partners:** Those outside the organization supporting the work
- **Management systems:** The planning and performance management of the work

Each element of the operating model needs to be designed to contribute to the success of the organization and facilitate sustainable control effectiveness across the control environment.

88 Andrew Campbell, Mikel Gutierrez and Mark Lancelott, Operating Model Canvas, Van Haren Publishing, 2017. www.operatingmodelcanvas.com

As we have mentioned several times in this report, security efforts in many organizations are focused almost exclusively on deploying and maintaining technologies, responding to a continuous stream of alerts, and meeting regulatory requirements. The result is a reactive security organization, busy with activity and unable to answer the question, "Are we becoming more secure by improving the sustainability and effectiveness of our control environment?"

For most organizations, the reality is that their security needs will always exceed their capacity. A more strategic approach is necessary.

A SOM enables this approach. It provides governance and oversight of security for the entire organization. It establishes priorities and provides direction to optimize security resource allocations. It communicates expectations and oversight of risks and efforts to address them.

The security organization should not own security risk decisions; the business does. The security organization is a control function that supports risk management. The business manager should indicate which security services, functions and risk mitigations are required similar to other functional specifications. The business organization should not be a passive recipient of services from the security organization; they are the reason the service exists and should actively participate in its design, implementation, evaluation, monitoring and maturity improvement.

The SOM can transition ownership of security risks. It also changes focus away from simply maintaining security controls for the sake of compliance with a regulatory standard to where it should be: the mitigation and management of security risks. Risk evaluation should form the basis for all security decision-making and performance management. The business is not only a recipient of the security and compliance services, but it is also instrumental in the collaboration, implementation and sustainability of the security program across the control environment.

Organizations that try to shortcut their way to a new operating model may find the design ineffective and the implementation lacking employee traction—or, worse, dilutive to value. The motivation to change a SOM may be slightly different across organizations, but they tend to converge around some combination of the following needs.

The right operating model:

- Should make it easier to identify and make important decisions quickly and effectively
- Clarifies decision-making—who gets involved in decisions and where "the buck stops" to improve the speed and quality of decision-making
- Helps the CISO break down silos to increase collaboration and improve results across the organization
- Presents clarity on responsibility assignments for data security and compliance activities, i.e., who does what, and how, to improve the speed of execution and eliminate uncertainty and redundancy
- Removes organizational layers and increases spans of control to reduce complexity, cost and "execution drag" on the security program
- Increases clarity around the results and security strategy and program performance metrics that matter most

Collaboratively developing the strategic plan and operating model plan with stakeholders is as important as the actual contents of the plan.

Monitoring the performance of your security business plan and SOM hinges on security metrics and reporting, oversight, and a series of management controls.

This is a process that should span all lines of assurance and involve multiple internal and external stakeholders. Without this crucial cross-functional alignment, security and compliance plans continue to be developed and maintained in silos.

Executive leadership and external stakeholders should be involved from the start of the process, and not merely included at the very end—which can lead to uninformed decisions, lack of organizational support and misalignment across the entire model. Collaboratively developing the strategic plan and operating model plan with stakeholders is as important as the actual contents of the plan.

Essential security strategy questions

Developing and maintaining a SOM will help answer questions such as:

Strategy assessment

- Is the data security compliance strategy aligned with the business and supported by the board?
- Is the strategy supported by a defined and effective security business model?
- Is the business model supported by a defined SOM?
- How do you gather input to define the TSOM—the "to be"?

Authority and power of execution

- Are the CISO and steering committee correctly positioned?
- Are the CISO's position, role and responsibilities correctly defined and understood?

Resource allocation

- Is security spending in the right places to support a sustainable and effective compliance and control environment?
- How can you have confidence that your resources are allocated appropriately across the organization?
- Are the right resources allocated to areas of greatest risk, in a timely manner?
- When the environment changes, how can you easily identify gaps, prioritize opportunities and shift your resources accordingly?

Process evaluation

- Are you proactively managing security and compliance risks or just reacting to them?

Top security control frameworks

Recognizing that data protection is not an IT issue, leadership should ensure that the enterprise develops, adopts and implements a security framework. It's common for organizations to adopt more than one framework in order to meet various required compliance initiatives.

Framework types

There are four main types of security frameworks:

1. Control frameworks, such as NIST 800-53; CIS Controls (CSCs), PCI DSS with a catalog set of baseline security controls
2. Program frameworks, such as ISO 27001; NIST CSF
3. Risk frameworks, such as NIST 800-39, 800-37, 800-30; ISO 27005; FAIR
4. Governance frameworks, such as ISO/IEC 27002, COBIT, COSO

The PCI DSS is a security control framework. It is not a program, risk or governance framework. The PCI SSC only recently (in July 2019) mapped PCI DSS to NIST CSF.

There are many options, and organizations are cautioned against framework overload.

- **Payment Card Industry Data Security Standard (PCI DSS):** A voluntary, nonlegislative, industry self-governance standard for the protection of payment card data
- **Control Objectives for Information and Related Technologies (COBIT):** An IT management framework to develop, organize and implement strategies around information management and governance
- **National Institute of Standards and Technology Cybersecurity Framework (NIST CSF):** Developed by the U.S. Department of Commerce to help mature cyber resiliency
- **NIST Risk Management Framework (NIST RMF):** A framework with over 900 controls covering details down to system-level settings
- **ISO 27000 Series:** A globally recognized framework for best-practice information security management
- **Center for Internet Security (CIS) Critical Security Controls (CSCs):** A highly practical and useful framework for every organization to use for both implementation and assessment
- **CIS Benchmarks:** Includes 100-plus configuration guidelines developed by a global community of cybersecurity experts
- **Security Controls Framework (SCF):** Cybersecurity and privacy control guidance to cover the strategic, operational and tactical needs of organizations
- **Committee of Sponsoring Organizations of the Treadway Commission (COSO)**: A collaborative initiative by five organizations focused on internal controls that goes far beyond cybersecurity
- **Cloud Security Alliance (CSA):** A framework tailored for implementing cloud security best practices
- **ISO 15048:** Also known as the Common Criteria, ISO 15048 was developed to facilitate a consistent universal model of evaluation of security products and systems, and guidelines for the specification of security targets (STs)
- **Information Technology Infrastructure Library (ITIL):** ITIL is a set of detailed practices for IT service management (ITSM) that focuses on aligning IT services with the needs of the business
- **Sherwood Applied Business Security Architecture (SABSA):** A proven security framework and methodology for enterprise security architecture and service management

Noteworthy legislation on data and security protection that is supported by frameworks:

- **General Data Protection Regulation (GDPR):** A data privacy framework for all companies operating in the European Union (EU)
- **HIPAA Security Rule (HSR):** Health Insurance Portability and Accountability Act of 1996 (HIPAA) proposed to protect consumers
- **Sarbanes-Oxley Act Section 404 (SOX 404):** Section 404 "Management Assessment of Internal Controls" is one of the most complicated, contested and expensive-to-implement of all the Sarbanes-Oxley Act, and is directly applicable to most information security professionals. Most of the time, COSO and COBIT are used as an implementation standard for SOX 404

Trap 6

Low capability and process maturity with lack of continuous improvement

Sixty percent of surveyed organizations do not apply capability and maturity models to measure PCI security program maturity.[89]

“Measurement is the first step that leads to control and eventually to improvement. If you can’t measure something, you can’t understand it. If you can’t understand it, you can’t control it. If you can’t control it, you can’t improve it.”[90]

—H. James Harrington, quality expert

Why do most organizations start out strong with PCI security compliance and then fail to sustain their success?

Two quotations from W. Edwards Deming, an American engineer, professor and author, come to mind:

“If you can’t describe what you are doing as a process, you don’t know what you’re doing.”[91]

“Manage the cause, not the result.”[92]

In short, the answer is: inadequate capability and business process management and control. These are two of the most essential ingredients required to help sustain data security and compliance programs. The business processes and capabilities are what hold all of the organization’s resources and assets together, from its people to technology and security vendors. It’s critical to invest in robust processes, capacity and capability management.

CISOs need to maintain a clear understanding of process and capability inefficiencies across the control environment and why they occur. Understanding how to rectify the inefficiencies will streamline processes that can then be improved continuously.

In the 2019 Payment Security Report, we discussed the importance of organizations devoting efforts and attention to developing the maturity of security processes and capabilities. If sound investments in security and compliance are to be made, assessing maturity is essential.

Few organizations attempt to design and implement a structured security and compliance maturity program. How do we know this? Well, it’s based on our own findings in our 2018 PSR survey,[93] industry experience and other reports.

Security maturity modeling is important as a self-assessment step: It creates a feedback loop that informs business practices and incorporates risk assessments. Maturity models should not deviate from business priorities and should always be aligned with the relevant industry and risks known within a particular sector. Designing, implementing and maintaining an effective security strategy and program requires a high degree of synchronization and collaboration.

89 Verizon global PCI customer 2018–2019 survey, 2019 Payment Security Report, page 7, Verizon 2019. https://www.verizon.com/business/resources/reports/payment-security-report/
90 H. James Harrington. https://en.wikipedia.org/wiki/Cost_of_poor_quality
91 W. Edwards Deming. https://www.goodreads.com/quotes/298857-if-you-can-t-describe-what-you-are-doing-as-a
92 The W. Edwards Deming Institute Blog. https://blog.deming.org/w-edwards-deming-quotes/large-list-of-quotes-by-w-edwards-deming/
93 2018 Payment Security Report, Verizon, 2018, page 20. https://www.verizon.com/business/resources/reports/payment-security-report/

To effectively protect the organization from common data security and compliance failures, CISOs, supported by the security steering committee, need to break through organizational silos to lay the foundation for the development of mature security practices. This will require time, dedication and a structured approach.

Understanding business process and capability

Before embarking on a project for continuous data protection and compliance improvement, it's important to have a clear understanding of the key elements—the processes and capabilities needed to achieve and sustain the organization's security objectives.

CISOs are trapped by low capability and process maturity with a lack of continuous improvement in their PCI security compliance environments. Given the general lack of skilled security resources (discussed in "Trap 3: Lack of resourcing capabilities" on page 32), many CISOs haven't taken on this task to identify and analyze processes and capabilities across the control environment. It is a complex but essential task.

The first obstacle that CISOs need to overcome to avoid Trap 6 is providing ample time and attention to understand all the processes within the control environment, which includes the PCI security compliance environment. A CISO must have an adequate understanding of the resources needed and relationships between the key process and capability components. This includes each of the 6 Cs—capacity, capability, competencies, commitment, communication and culture—and how each impacts the 9 Factors of Control Effectiveness and Sustainability across the 4 Lines of Assurance, i.e., the 9-5-4 Compliance Program Performance Evaluation Framework. If this is not done, CISOs will likely miss components and relationships that are essential for achieving an effective and sustainable control environment.

Next, CISOs must not only have clarity on where inefficiency occurs within the control environment, but also take the time to understand why it happens. Drilling down to the root of common inefficiencies and evaluating the best solution options can reduce the risk of the same mistakes being repeated time and time again. Benchmarking against a maturity model will help identify these inefficiencies.

Lack of collaboration and support

Without strong communication and collaboration from the top down (see "Trap 7: Communication and culture constraints" on page 60), slow adoption across the business can prevent the security team from achieving improved process maturity.

Security and compliance processes involve multiple teams (all 4 Lines of Assurance). In order to get everyone working more effectively, it's important to ensure that people across all lines of assurance are on board and understand the benefits of implementing process and capability

> **"Defining a maturity goal in line with your organization's risk appetite firmly places a stake in the ground, creating a focus point, a principle of attainment, which in turn establishes boundaries where you can identify the need to make minor improvements."[94]**
>
> **— 2019 Security Maturity Report, Orange Cyberdefense (formerly SecureLink)**

94 2019 Security Maturity Report, Orange Cyberdefense (formerly SecureLink), 2019. https://securelink.net/campaign/sma/security-maturity-report-2019/

"Organizations do their best when they focus their process improvements on a manageable number of process areas at a time. Therefore, the first improvements should focus on those processes that have the greatest potential impact should things go wrong. At more mature levels, you look beyond process definitions and work on the consistency of application and adherence, training, monitoring and evaluation. All this work converges toward automation and best practices."[95]

—2019 PSR

improvements, which requires making changes to the way that they work. Individuals and teams hold valuable operational knowledge, and the CISO needs their input to strengthen the insight fed back into strategic security planning.

Collaboration among CISOs is key to successful program building, within and across industries. Maturity models must be actionable and realistic, within themselves, to reduce costs and provide true benefit to the company. They are necessary, too, as a component of the cycle of (1) articulating an organization's business objectives, (2) performing risk assessments, (3) aligning policies and procedures with business objectives and risks, (4) benchmarking performance, (5) striving for greater organizational efficiency and (6) rearticulating or updating an organization's business objectives, etc.

CISOs should know, too, the limits of each step. For instance, a maturity-based approach is not a stand-in for a risk assessment. Each one is distinct and a key component to a strong security and compliance program. With continued low capability and process maturity and a lack of continuous improvement, an organization remains in an eddy, constantly repeating the lower three steps in the cycle. Breaking out of that smaller, restrictive current into the larger flow of a healthy, dynamic security and compliance program that continuously flows and improves requires customized maturity models that are focused on helping CISOs make and advocate for intelligent budget decisions.

To ensure that funds for security and compliance initiatives are spent judiciously, the return on investment in a maturity model must be quantifiable and overseen. Knowledge-sharing is also key to developing maturity models that drive a business to greater degrees of efficiency and profitability. While CISOs in the retail and hospitality sectors, for instance, are known for sharing knowledge of threats unique to their industry and technologies that can aid in overall security initiatives, these same groups should be leveraged to create a sense of what mature capabilities and processes look like. For example, retail and hospitality companies can benchmark themselves against realistic, cost-effective best practices. (Does this kind of exchange currently exist? And does any formal output exist?)

CISOs are called upon to lead this charge—to guide this river, if you will.

To facilitate smooth security and compliance operations, the CISO needs to ensure that process ownership and accountability spans teams and encourage effective collaboration when it comes to identifying and implementing process improvement opportunities. Essential to the process is securing buy-in and collaboration from across the business for continuous improvement that can be initiated and sustained. This should start with involved leadership (refer to "Trap 2: Failing to secure strategic support" on page 28).

Sound process design and execution help define an organization's security culture, mission and vision. That's why it's essential that the organization leadership team supports process management and enables the CISO and steering committee to effectively maintain governance across the control environment to ensure the adherence of critical security processes. This top-down approach to maturity development will help CISOs communicate the value of security process management to the entire organization and keep employees motivated to observe the security processes that apply to their roles.

95 2019 Payment Security Report, Verizon, 2019. https://www.verizon.com/business/resources/reports/payment-security-report/

Not taking a systemic approach to maturity development

As mentioned, a control environment includes a wide range of processes with a mix of critical business, security and compliance activities that, by their very nature, are complex. Organizations need advanced navigational aids and guidance on how to integrate the applications of maturity models and metrics into their compliance programs. Working toward a recognized maturity development framework can make maturity development of the control environment a lot easier. The CISO and steering committee can then apply proven practical techniques supported by a clear methodology to help ensure a standardized way of working to develop and manage security and compliance processes. For more details on this, revisit the discussion on the benefits of maturity models in the 2019 PSR.[96]

In the 2019 PSR, we discussed the need for organizations to devote effort and attention to developing the maturity of security processes and capabilities. A methodical and comprehensive maturity assessment is essential, assuming the necessary investments in security and compliance are made.

The security maturity of small organizations

In its 2019 annual security report,[97] Orange Cyberdefense (formerly SecureLink) saw that smaller companies (under 1,000 employees) are dealing with six times more incidents than larger ones. Is this reflected in their perceived maturity?

One might assume that the bigger a company is, the more mature it perceives itself. This holds until organizations get bigger than 10,000 employees, which is somewhat unexpected.

Organizations with a large workforce place greater emphasis on structure and work specialization. Work specialization determines how tasks are subdivided into separate jobs. The more an activity is broken down into small tasks, the more specialization is required by each individual employee. Small organizations have fewer people to divide tasks among, so the jobs in small organizations have a lower degree of work specialization than the jobs in large organizations.

Medium-sized organizations (1,001 to 10,000 employees) lead the way in overall maturity. The data shows this grouping to be the sweet spot. They have fully documented processes, with their people categorized as defined and their technology characterized as available.

Difference in security maturity by industry

The finance industry is the most mature vertical, according to the Orange Cyberdefense (formerly SecureLink) study. The study found that retail (likely due to “brick and mortar” retail) comes in last overall on cybersecurity maturity. The largest companies (over 10,000 employees) are remarkably critical of their own security maturity. They score lower than midsize and small organizations. Whether this is caused by greater self-awareness, separation of duties or missing the bigger picture over such a large organization is not known.

96 2019 Payment Security Report, Verizon, 2019, page 25. https://www.verizon.com/business/resources/reports/payment-security-report/
97 2019 Security Mature Report, Orange Cyberdefense (formerly SecureLink), 2019. https://securelink.net/campaign/sma/security-maturity-report-2019/

Trap 7

Communication and culture constraints

Which of these three assignments should be discussed most?

- Sign a multimillion-dollar contract for a nuclear reactor
- Create a proposal for an inexpensive bike shed for clerical staff
- Arrange for refreshments for a joint welfare committee

Tackling the elephant in the room

How organizations communicate about complex planning projects such as compliance program implementation can impact the robustness and resilience of the control environment, and perhaps also the likelihood of a security breach resulting in a data compromise. Poor company communications can be a significant, underlying reason for why company data security compliance is trending downward: The willingness and ability to wrestle with a company's evolving compliance concerns helps to build sound security strategies, business models and operating models.

Effective communication is needed from the watercooler chat to the boardroom meeting. When a CISO manages those communications, it's important to remember that human nature tends to focus on the most familiar, easier-to-grasp concerns while the elephant in the room is left to saunter in the side aisles. In general, people do not prefer tackling bigger, more complicated projects, partly because they often require complex, strategic thinking that includes foreseeing more serious outcomes because of the heightened degree of responsibility, work and monetary investment—and overall liability. Bottom line, it's more stressful.

In 1999, Danish software developer Poul-Henning Kamp promoted the term "bike shedding" to describe the tendency of planning committees or organizations to downplay the more important concerns and instead focus disproportionally on trivial issues.[98]

The term eventually spread throughout the software industry to describe trends in software development. Kamp based his theory on "Parkinson's Law of Triviality," which was coined in 1957 by C. Northcote Parkinson, who argued in his spoof of management that, when given the choice, the human mind tends to focus on unimportant details to avoid dealing with more crucial, costly and complex matters.[99]

As part of his argument, Parkinson included a fictionalized example of a committee with three assignments: Sign a multimillion-dollar contract for a nuclear reactor, create a proposal for an inexpensive bike shed for clerical staff and arrange for refreshments for a joint welfare committee. The contract for the reactor then takes the least amount of debate and time because it's too technical and costly. Completing a bike shed results in significantly more debate because the details and processes are more familiar to the committee members. The refreshments discussion requires the greatest amount of time because "every man there knows about coffee—what it is, how it should be made, where it should be bought—and whether indeed it should be bought at all. This item on the agenda will occupy the members for an hour and a quarter, and they will end by asking the secretary to procure further information, leaving the matter to be decided at the next meeting," he concludes. Most committees will spend a disproportional amount of time discussing the simpler

98 Poul-Henning Kamp, "The Bikeshed email," http://phk.freebsd.dk/sagas/bikeshed/
99 C. Northcote Parkinson, Parkinson's Law, BuccaneerBooks, 1996.

aspects of a project, such as building the staff bike shed, because it's easier to visualize such a simple structure as compared to an atomic reactor, he argues. The more complex and costly the project, the less willing a committee is to wrestle collectively with the details and challenges. In general, he purports the human mind tends to seek out the more comfortable, familiar territory.

For CISOs, it's important to remember that, even at the watercooler, complex conversations about data protection and compliance foster an educated and attuned culture. And how you convey the message is important. Strategies for making data protection effective and sustainable can be unfamiliar territory for CISOs with technical backgrounds. They may need to learn how to rephrase the conversation by avoiding technical jargon and learning how to communicate more broadly about strategy and other "tougher" stuff.

For details about the scope of PCI security program communication, see page 12 of the 2019 PSR.[100]

It's the CISO's responsibility to initiate those conversations in the boardroom, where cybersecurity avoidance and underinvestment is common. The problem is tied to the belief that security is merely a rote fortification process of firewalls, etc., that falls under the job description of security personnel who comply with security standards and frameworks. Effective communication breaks that mindset and helps board members, CIOs and CEOs understand their critical responsibilities and manage their company's unique, evolving security challenges. When managing these communications, a good CISO fosters productive coalitions that tackle the elephant in the room. They stay alert and attuned to when those conversations are veering off the path to the bike shed. That's the time to steer the conversation back on the main path, or the elephant could get stuck in the bike shed!

When promoting complex data protection strategies that their organization needs to invest in, a skilled CISO stays current and well educated about the resources and capabilities needed and how long it will take to achieve sustainable control effectiveness. They are familiar with the business metrics for the maturity of the program. They aren't afraid to incorporate feedback and ask throughout the organization: "How can I increase your interest in this important topic?"

Engaging participants through examples, analogies and/or stories is a great technique for aligning agendas. It fosters collaboration and helps to resonate with their experience, which is what you need when building a strategic data protection program.

"Successful CISOs craft their stories in language that business leaders understand. They frame their technical solution in how it will benefit the business. If the listener does not understand the story because of jargon, then he or she is unlikely to retell or spread it within the organization," according to "Winning the Battle of the Budget" by IANS Research.

"The impact of these narratives also depends on the credibility of the storyteller, or how the CISO is regarded across departments and at the executive level. CISOs need to craft long-arc and short-arc stories: CISOs who have mastered the art of driving the narrative tend to develop two classes of security stories. One type tells a multi-year story of integrating InfoSec into the fabric of the company. This long-arc narrative understands the business and articulates how InfoSec powers growth and profitability. The short-arc stories detail particular investments and how they improve risk posture. Importantly, these two classes of security stories are coherent and fit well together."[101]

—"Winning the Battle of the Budget," IANS Research

100 Payment Security Report, page 12, Verizon, 2019. https://www.verizon.com/business/resources/reports/payment-security-report/
101 "Winning the Battle of the Budget," IANS Research, Apr 2018. https://portal.iansresearch.com/content/3566/frp/winning-the-battle-of-the-budget

03 State of compliance

State of compliance

The state of PCI DSS compliance, 2020 (and 12 Key Requirements)

By Anne Turner, Sky Hackett and Dyana Pearson, Senior Consultants, Verizon PCI Security Practice

Ten years ago, Verizon published the first analysis of PCI DSS assessments. The report continues to provide valuable insights on the ability of organizations to meet the requirements of the standard and understand how effective programs are at sustaining compliance over time.

In the 2019 publication of this report, we introduced an extended dataset that incorporated assessment data compiled from other QSA companies. That dataset is further expanded in this year's report. This enhanced dataset provides a deeper understanding of the compliance landscape from 334 engagements performed across approximately 60 countries around the world.

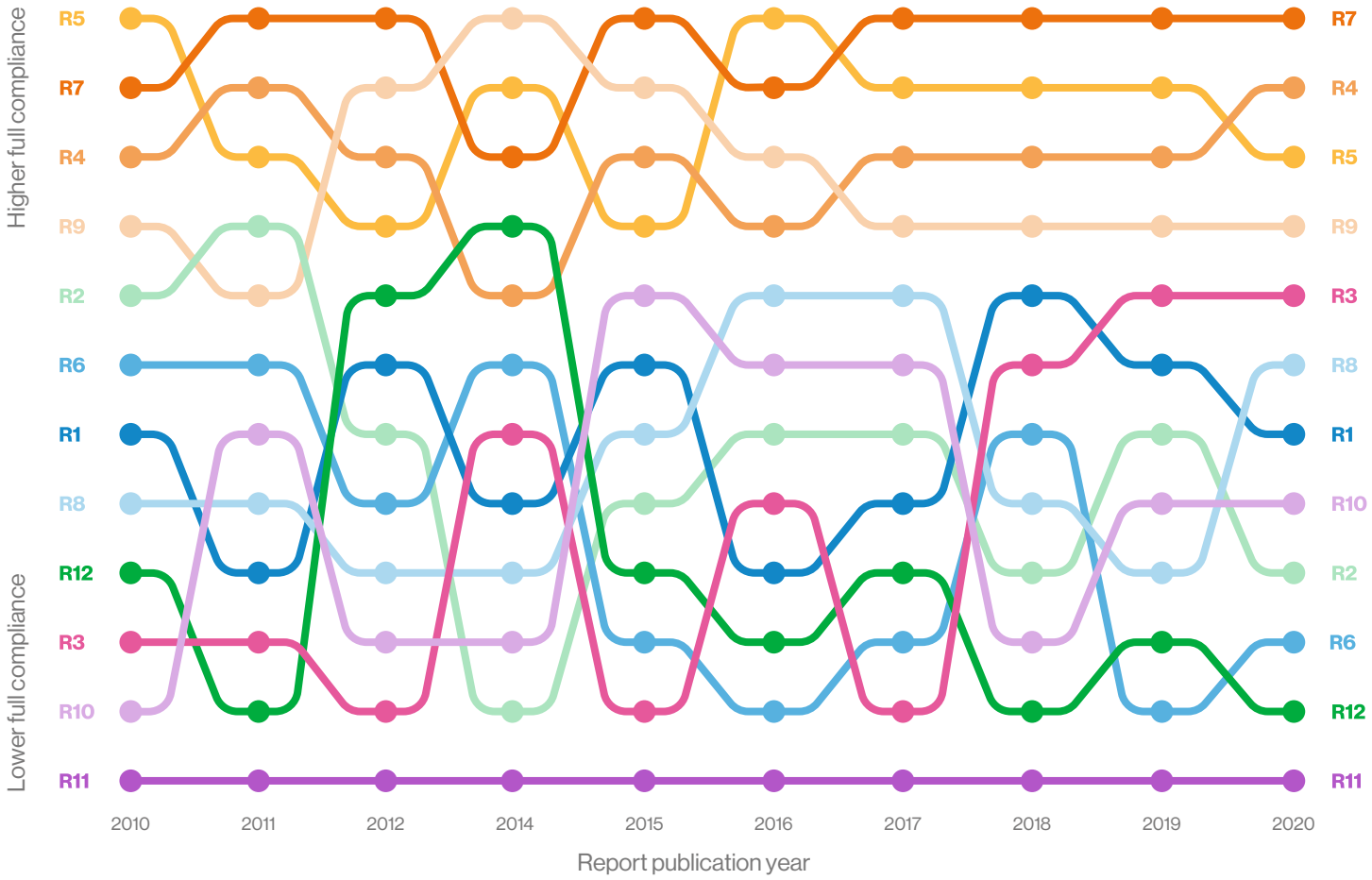
The data reported in this section is taken from Intital Reports on Compliance (IROCs). These are a snapshot of an organization's state of compliance at a point in time, prior to final assessment. These insightful interim reports capture lapses in controls that can occur as a result of poor compliance management practices or ineffective control design.

Historically, full compliance across all requirements increased year-on-year until 2016. Since that time, we consistently observed a marked reduction. In 2019, compliance fell to 27.9%, a drop of 8.8 percentage points (pp) from the previous year, and a huge 27.5 pp from 2016, when compliance peaked. The control gap, which measures how far organizations are from full compliance, remains relatively stable for the third year in a row with just a 0.6 pp increase in 2019 to 7.7%.

Year (report publication yr)	**2010**	**2018**	**2019**	**2020**
PCI requirement				
Requirement 1: Install and maintain a firewall configuration.	7	5	6	7
Requirement 2: Do not use vendor-supplied defaults.	5	8	7	9
Requirement 3: Protect stored cardholder data.	10	6	4	5
Requirement 4: Protect data in transit.	3	3	3	2
Requirement 5: Protect against malicious software.	1	2	1	3
Requirement 6: Develop and maintain secure systems.	5	7	11	10
Requirement 7: Restrict access.	2	1	1	1
Requirement 8: Authenticate access.	8	8	9	6
Requirement 9: Control physical access.	4	4	4	4
Requirement 10: Track and monitor access.	11	10	8	8
Requirement 11: Test security systems and processes.	12	12	12	12
Requirement 12: Security management	8	11	10	11

Table 1. Full compliance (ranking); Req 7 is the best performing and Req 11 the worst performing Key Requirements.

Figure 4. Full compliance (requirement order by rank)



Full compliance: Trends analysis

Requirement 7 remains the most well maintained, retaining the top-ranking requirement position for the fourth consecutive year. Requirement 5 was knocked into third place for full compliance by Requirement 4. Requirement 4 also reported the lowest control gap for this year, improving its position from a lowly eighth place in the previous year to first place.

At the other end of the rankings, Requirement 11 continues to occupy the bottom position for both full compliance and control gap, as it has done throughout the history of this report. Requirement 12 saw the largest drop in full compliance across all of the requirements in 2019, falling 7.7 pp and ranking 11th for full compliance overall. Requirement 5 reported the greatest increase in control gap at 3.8 pp and took 11th place in the control gap rankings.

Regionally, Asia-Pacific (APAC) outperforms both Europe, the Middle East and Africa (EMEA) and the Americas by some margin for both full compliance and control gap. In 2019, APAC reported 87% compliance across all requirements, while EMEA was at 40.5% and the Americas at just 8.5% full compliance at interim assessment. Compared to 2018 figures, this represents a drop in compliance for both the Americas (11.9 pp) and EMEA (7.9 pp), but an improvement for APAC of 17.4 pp.

Both EMEA and APAC successfully lowered the control gap across all requirements in 2019, with EMEA reporting a control gap of 3.9% and APAC just 0.2%. The Americas saw a widening control gap as compared to the previous year of 5.5 pp, to 11.1%.

The ability of APAC to maintain compliance year-on-year compared with the other regions is a continuing trend. It is disconcerting to compare this to the Americas, where we see a drastic reduction in overall compliance. It demonstrates clearly that sustainability can be achieved, but that some regions and sectors are doing things more effectively than others, and we need to pay attention to that trend and learn how to perform better.

IT services continues to maintain full compliance above other sectors, at 39.3%. Retail lags behind at 16.7% full compliance across all requirements, and saw a 19.7 pp drop in 2019 as compared to the previous year. However, it is finance that reports the largest control gap at 9.3% across all requirements, an increase of 1.8 pp since 2018. All other sectors report a slight-to-moderate contraction of control gap; in 2019, hospitality showed the most significant reduction of 5.5 pp, to 7.1%.

For clarity: A reduction in control gap is a positive outcome. The smaller the control gap is, the fewer controls are found to be not in place during validation, which narrows the noncompliance gap.

2019 PCI DSS validation dataset

PCI DSS version: 3.2.1

Number of engagements: 154

2019 PCI DSS results – interim validation

100% compliance (pass): 43 (27.9%)

<100% compliance (failed): 111 (72.0%)

The PCI DSS version 3.2.1 consists of 12 PCI DSS Key Requirements, 78 base requirements and over 400 test procedures.

We measure the performance of the four key industries on three metrics:

- Full compliance
- Control gap
- Use of compensating controls

Full compliance

The share of companies achieving 100% PCI DSS compliance at interim validation. All companies studied had passed a previous validation assessment, so this indicates how well they managed to sustain compliance.

Control gap

The number of failed controls divided by the total number of controls expected. This is an average figure that gives a measure of how far the assessed companies were from full compliance.

Compensating control

This percentage indicates how many companies used one or more compensating controls for the specified section of the DSS. It's not how many compensating controls were used.

Compliance trends: Control gap

Year (report publication yr)	**2010**	**2018**	**2019**	**2020**
PCI requirement				
Requirement 1: Install and maintain a firewall configuration.	5	3	4	7
Requirement 2: Do not use vendor-supplied defaults.	4	10	10	5
Requirement 3: Protect stored cardholder data.	2	11	2	3
Requirement 4: Protect data in transit.	7	7	8	1
Requirement 5: Protect against malicious software.	10	5	5	11
Requirement 6: Develop and maintain secure systems.	8	4	6	4
Requirement 7: Restrict access.	11	6	3	6
Requirement 8: Authenticate access.	6	8	7	8
Requirement 9: Control physical access.	12	1	1	2
Requirement 10: Track and monitor access.	3	9	9	10
Requirement 11: Test security systems and processes.	1	12	12	12
Requirement 12: Security management	9	2	11	9

Table 2. Control gap: Ranked from 1 (best) to 12 (worst) per PCI DSS Key Requirement.

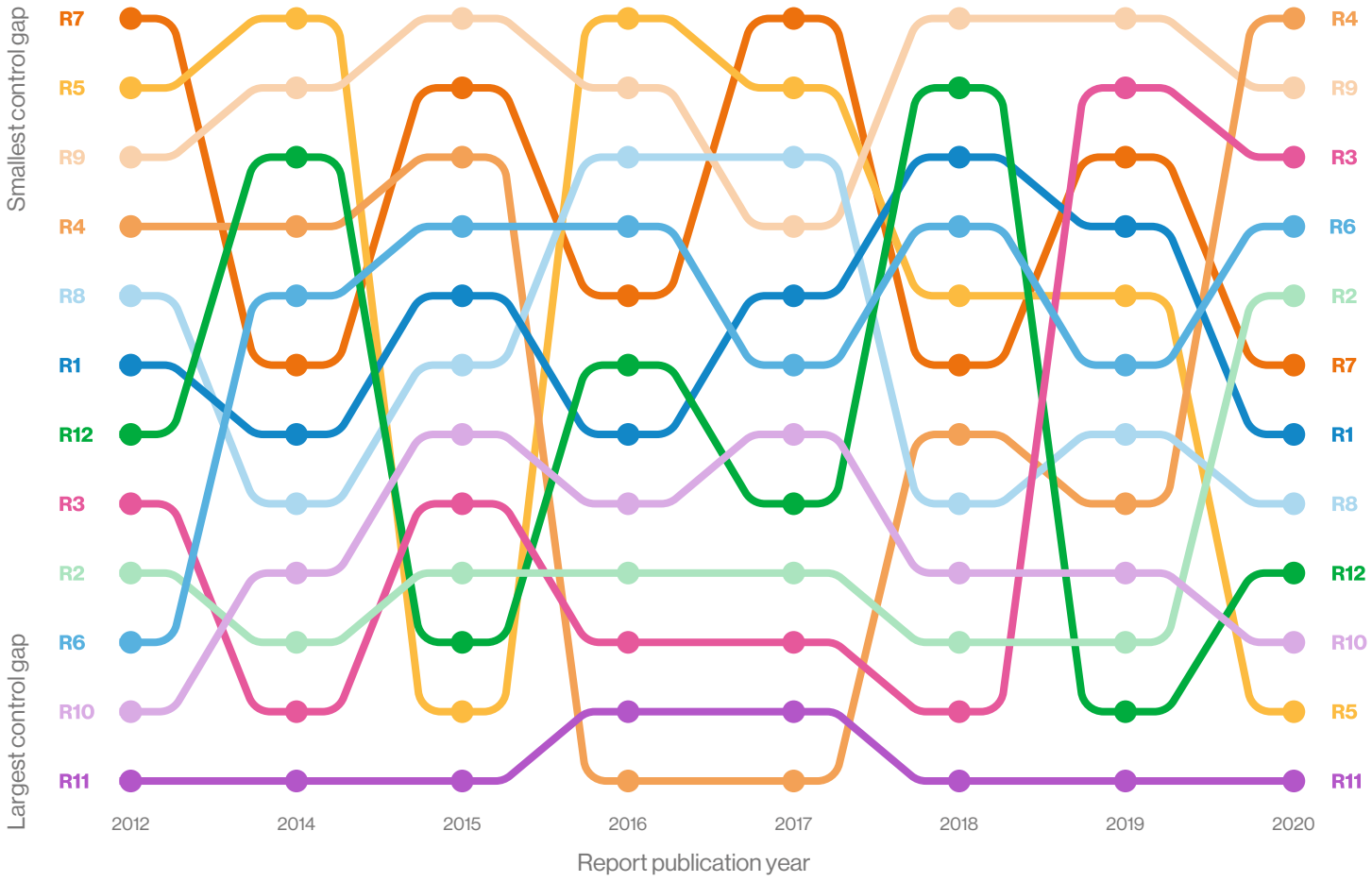


Figure 5. Control gap (requirement order by rank); Requirement 11 has the largest gap (bad), and Requirement 4 the smallest gap (good).

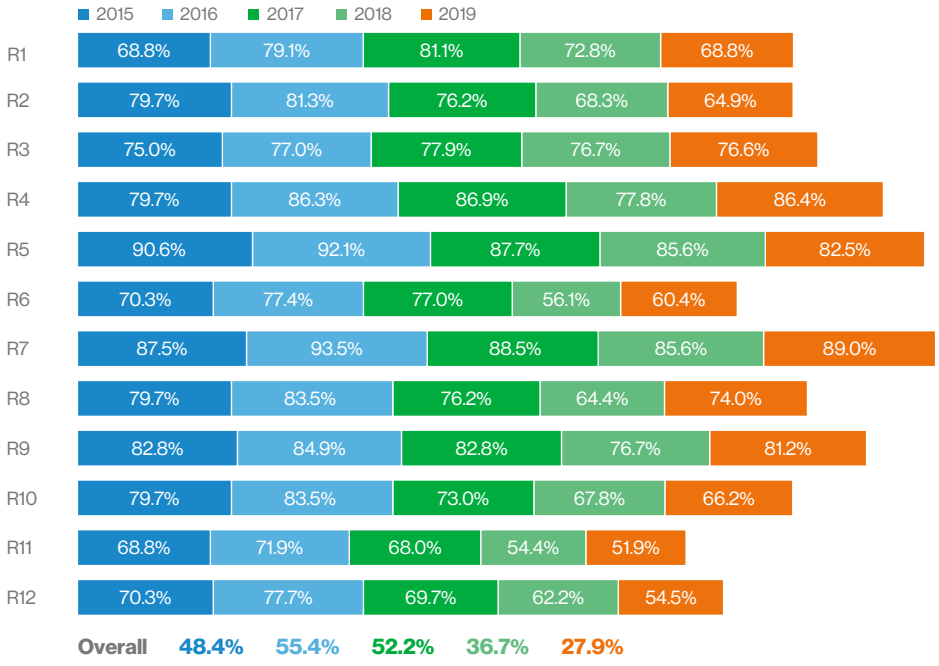
Five-year trends

Full compliance

Requirement 7 (Restrict access) has the strongest performance in terms of full compliance, followed by Requirement 5 (Protect against malicious software).

Requirement 11 (Test security systems and processes) is clearly the weakest performer, followed by Requirement 12 (Security policies and management), and Requirement 6 (Develop and maintain secure systems).

Figure 6. Full compliance



Control gap

The control gap graph clearly indicates the extent to which organizations are struggling to maintain the security controls under Requirement 11 (Test security systems and processes). It is a concern that the control gap increased for three years in a row.

Other key requirements with high control gaps are Requirement 2 (Do not use vendor-supplied defaults) and Requirement 4 (Protect data in transit). It is evident that the control gap on Requirement 4 improved substantially, from a very high 13.0% in 2015 to the lowest gap of 3.8% in 2019.

Figure 7. Control gap

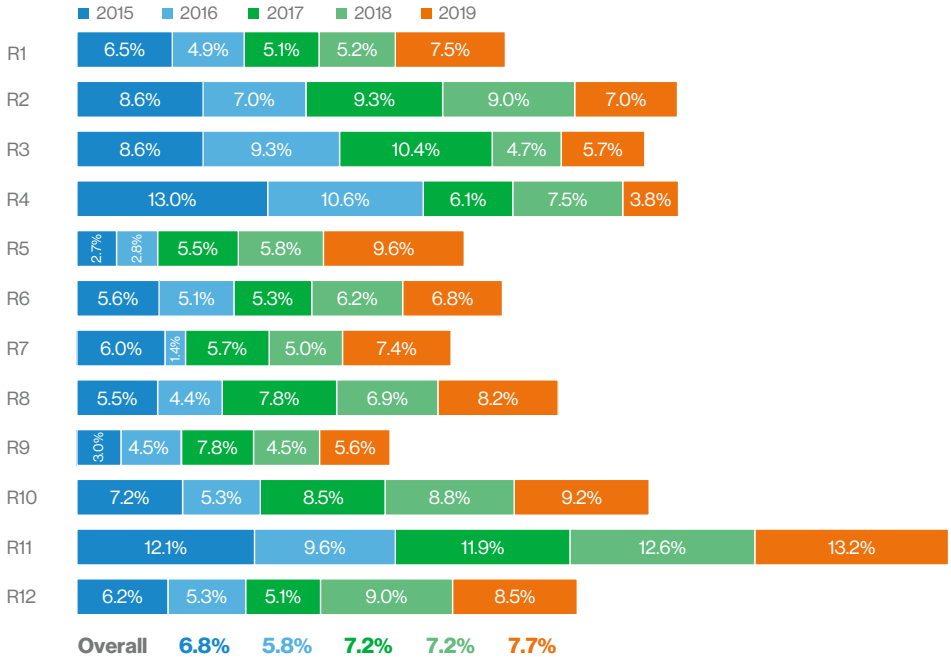
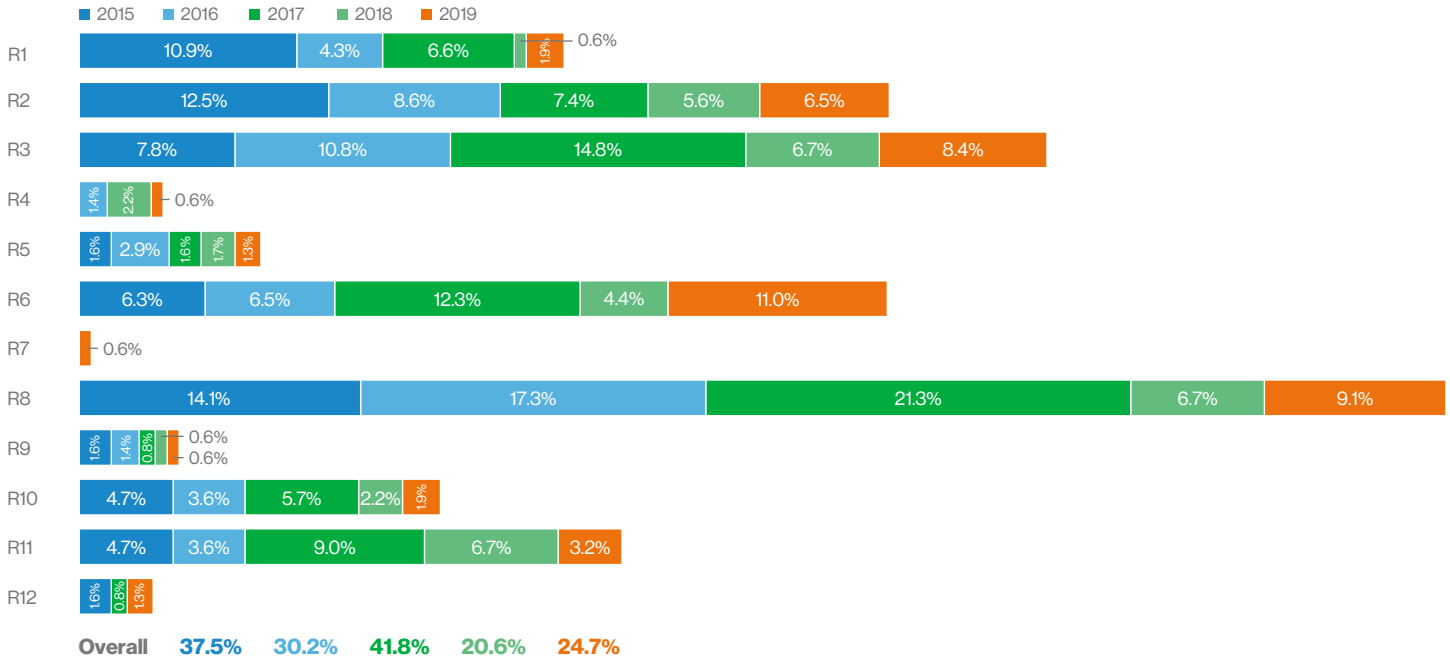


Figure 8. Compensating controls



Compensating controls

Requirement 8 (Authenticate access) is the most compensated key requirement over the five-year period, followed by Requirement 3 (Protect stored cardholder data).

Requirement 6 is the most compensated requirement in 2019.

In 2019, organizations applied compensating controls under Requirement 7 (Restrict access) for the first time.

1: Install and maintain a firewall configuration

This requirement covers the correct use of a firewall to filter traffic as it passes between internal and external networks, as well as traffic to and from sensitive areas within the organization's internal networks.

Full compliance

Continuing the downward trend from the 2019 PSR, the ranking for Requirement 1 dropped from sixth to seventh place. The number of companies demonstrating full compliance was 68.8%, which is a drop of 3.9 pp from the previous year.

There were some shining moments; for example, the hospitality sector outperformed other industries in 2019, with 71.4% of organizations reporting full compliance. This was an improvement of 13.5 pp over 2018. In 2019, we noted that the hospitality sector was struggling. It had the highest control gap of the industries and was the most challenged in maintaining compliance with this requirement.

On the downside, the 2019 PSR noted that finance improved in relation to other organizations. This year, however, the finance sector saw the largest drop in compliance for this requirement to 70.6%, a decrease of 7.5 pp from the prior year.

Regionally, APAC achieved the highest overall compliance of all global regions, at 95.7%. The Americas reported the lowest compliance levels across all regions, at 55.3% (-16.7 pp from 2018).

Control gap

For industries struggling to demonstrate compliance with Requirement 1, the news doesn't improve. The control gap for this requirement increased to 7.5% (3.8 pp) compared to 2018 (5.2%). Gaps increased for all Requirement 1 controls, excluding 1.5, which saw a small drop.

In addition to reporting the greatest reduction in full compliance of all the industry sectors, finance saw the highest increase in control gap, widening 3.5 pp to 8.5%. Service providers lagged behind merchants in 2019, with merchants showing a reduction in control gap from 5.9% in 2018 to 5.4% in 2019. Service providers, by contrast, increased their gap by 3.0 pp to 7.9%.

For regional control gaps, the Americas region saw the largest increase of 7.5 pp, while EMEA and APAC both showed improvement over the prior year.

Compensating controls

The use of compensating controls by organizations saw a 1.4 pp increase in 2019. Given that this followed a significant drop from the year before, the practice still has not improved enough to compensate for the drop of 6.0 pp. The EMEA region reported the highest use of compensating controls for Requirement 1 at 5.4%, while the region reported 0.0% in 2018. In the retail sector, 4.2% reported compensating controls for Requirement 1, followed by finance at 2.4%.

Both EMEA and the Americas implemented compensating controls to meet this requirement; none were reported in APAC.

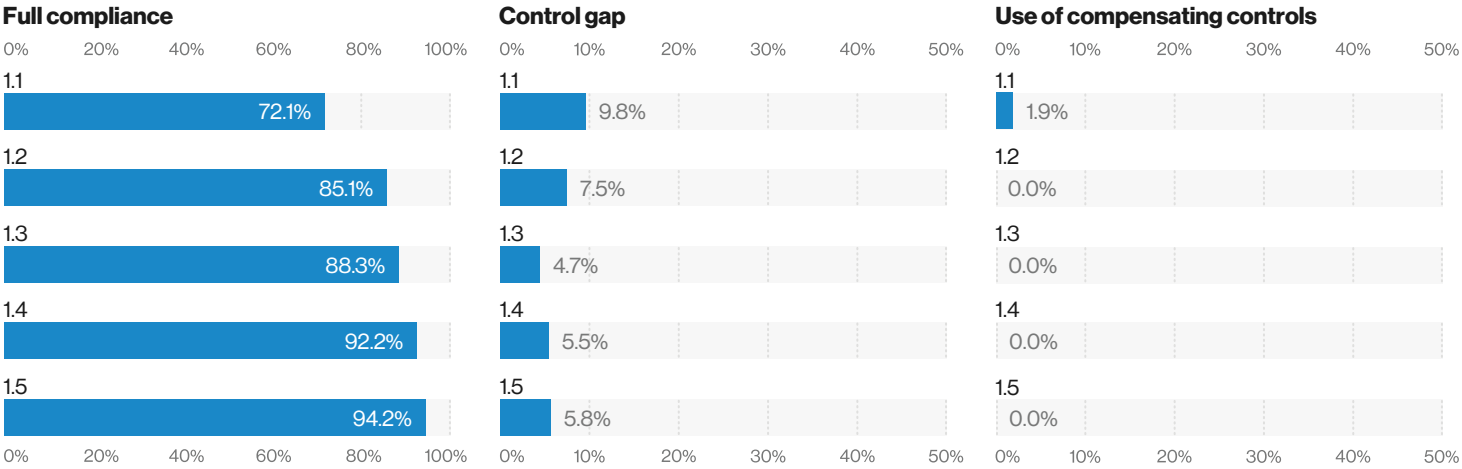
Requirement 1 controls

1.1	Implement firewall and router configurations
1.2	Restrict connections between cardholder data environment (CDE) and untrusted networks
1.3	Prohibit direct public access between internet and CDE
1.4	Install personal firewall software
1.5	Document policies and procedures for managing firewalls

State of control/test procedure

Control 1.5 was the third most-compliant control reported in 2019.

Figure 9. 2019 compliance performance (global averages) of Requirement 1– Install and maintain a firewall configuration.



Industry vertical findings

After struggling for a few years, the hospitality sector saw significant gains in full compliance, reporting a 13.5 pp improvement compared to the previous year for Requirement 1. This was coupled with a slight contraction of control gap, suggesting that overall compliance performance is improving in this sector.

The finance sector, reporting both a reduction in full compliance and a moderate increase in control gap, is not able to claim the same accomplishment.

While service providers outperformed merchants slightly in full compliance at 69.7% vs 67.6%, merchants achieved a significantly lower control gap. For organizations that did not report full compliance at interim assessment, this means that fewer control failures were noted for merchants as compared to service providers.

Payment data breach correlation—Req 1

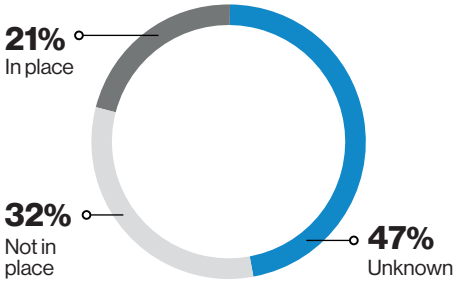


Figure 10. 2014 to 2019 PCI DSS compliance at the time of the breach

Figure 11. Full compliance — Req 1

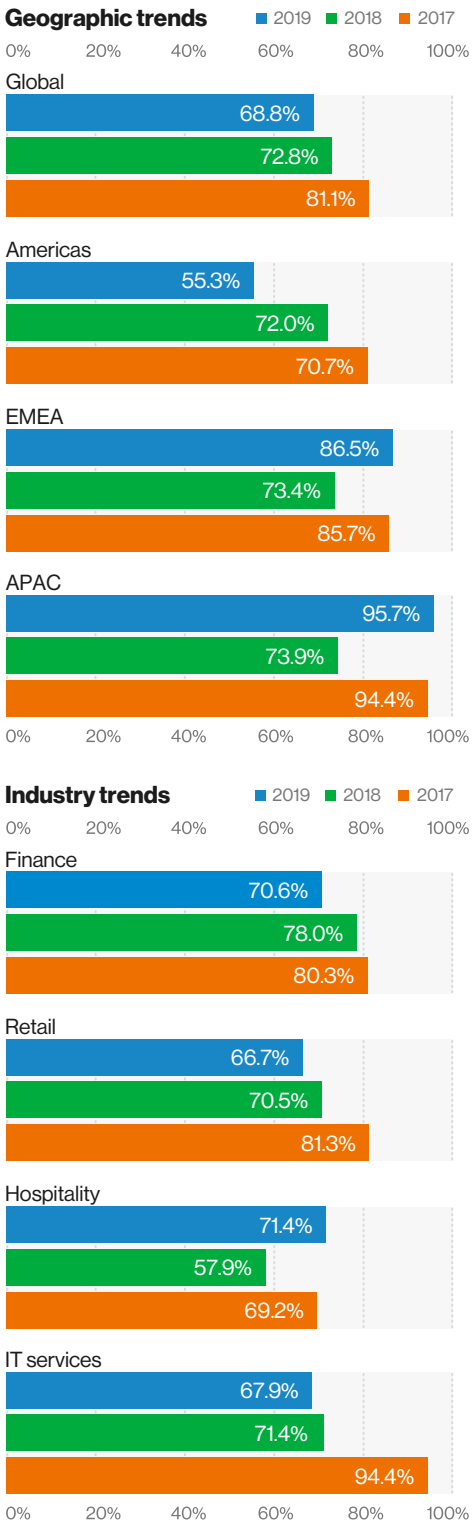


Figure 12. Control gap — Req 1

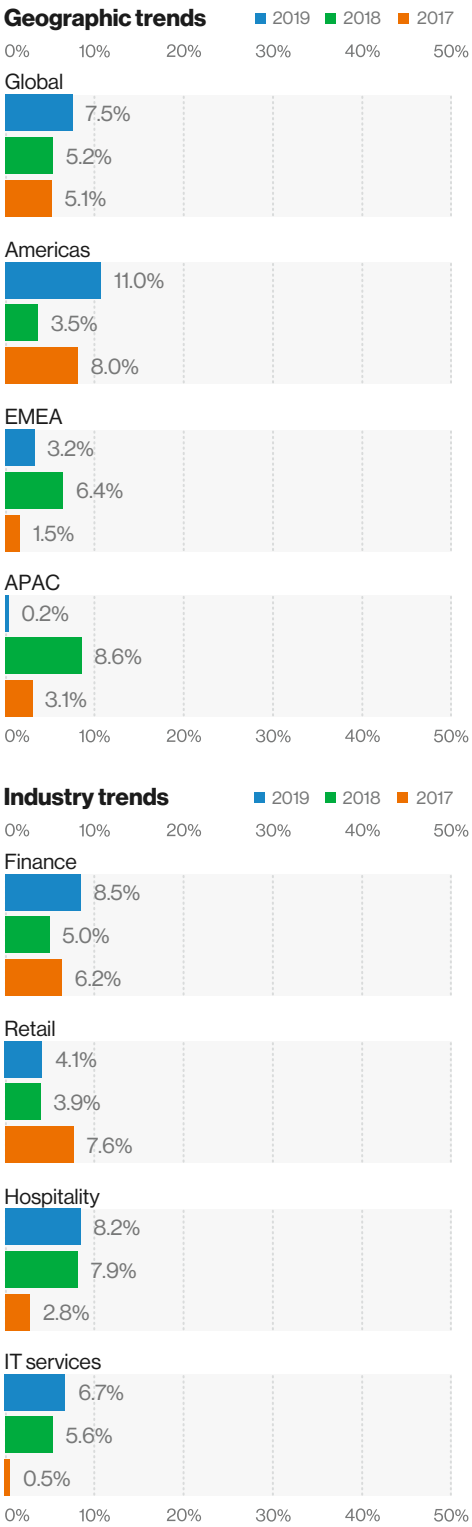
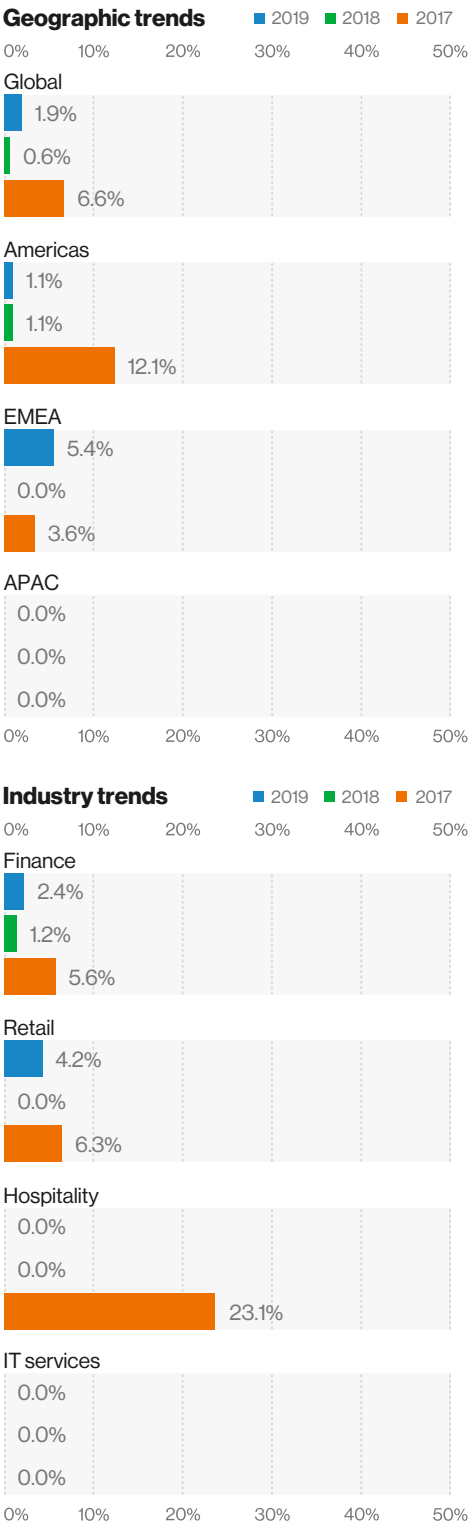


Figure 13. Compensating controls — Req 1



2: Do not use vendor-supplied defaults

This requirement covers the controls that reduce the available attack surface on system components by removing unnecessary services, functionality and user accounts, and by changing insecure vendor default settings.

The full compliance ranking for Requirement 2 went to ninth overall. By contrast, the control gap ranking jumped from 10th in 2018 to fifth in 2019.

Full compliance

Full compliance for this requirement saw a 3.4 pp drop in 2019 compared to the previous year, with 64.9% of organizations achieving compliance at interirm assessment.

In the regional data, the Americas reported full compliance at 47.9%, a 17.7 pp decrease. Compare this to the significant improvements seen in EMEA and APAC at 16.2 pp and 26.1 pp, respectively. APAC achieved 100% full compliance for this requirement.

In the industries data, hospitality reported the lowest levels of full compliance across all industry sectors for this requirement at 42.9%. This was very similar to 2018 figures, with just a 0.8 pp increase for 2019. Retail outperformed other sectors, showing 83.3% full compliance in 2019, a strong improvement (8.3 pp) compared to 2018.

Finally, service providers and merchants were only separated by 2.0 pp, with merchants just slightly ahead at 67.6% full compliance. Merchants achieved an improvement of 2.4 pp over the previous year, but service providers noted a 4.7 pp decrease.

Control gap

While full compliance fell for Requirement 2, the control gap saw a contraction of 1.9 pp at 7.0% in 2019. All subcontrols saw a reduction in control gap, except 2.4, which increased 6.7 pp to 19.2% in 2019.

Surprisingly, merchants saw a significant decrease in the control gap of 9.3 pp (to 3.2%) in 2019. Service providers, by contrast, remained consistent with 2018 figures, noting just a 0.3 pp increase to 8.1% in 2019.

Consistent with the decrease in the Americas' compliance figures, there is a corresponding increase in control gap (3.7 pp). This ran counter to the other global regions, which both reported reductions. APAC noted the most impressive contraction, reducing from 13.0% in 2018 to just 0.2% in 2019.

All industry sectors except finance reported a contracting control gap in 2019. Finance noted only a nominal increase of 0.6 pp over the previous year to 7.9%.

Compensating controls

Maintaining its ranking of fourth compared to the previous year, a minor increase in use of compensating controls was observed in 2019.

EMEA topped the global regions at 18.9%, which was an increase of 11.1 pp on the previous year. APAC reported no compensating controls.

The retail and hospitality sectors noted the greatest use of compensating controls in 2019 across all sectors at 4.2% and 7.1%, respectively. This was a slight increase for retail of 1.9 pp, but represented a reduction of 3.4 pp for hospitality.

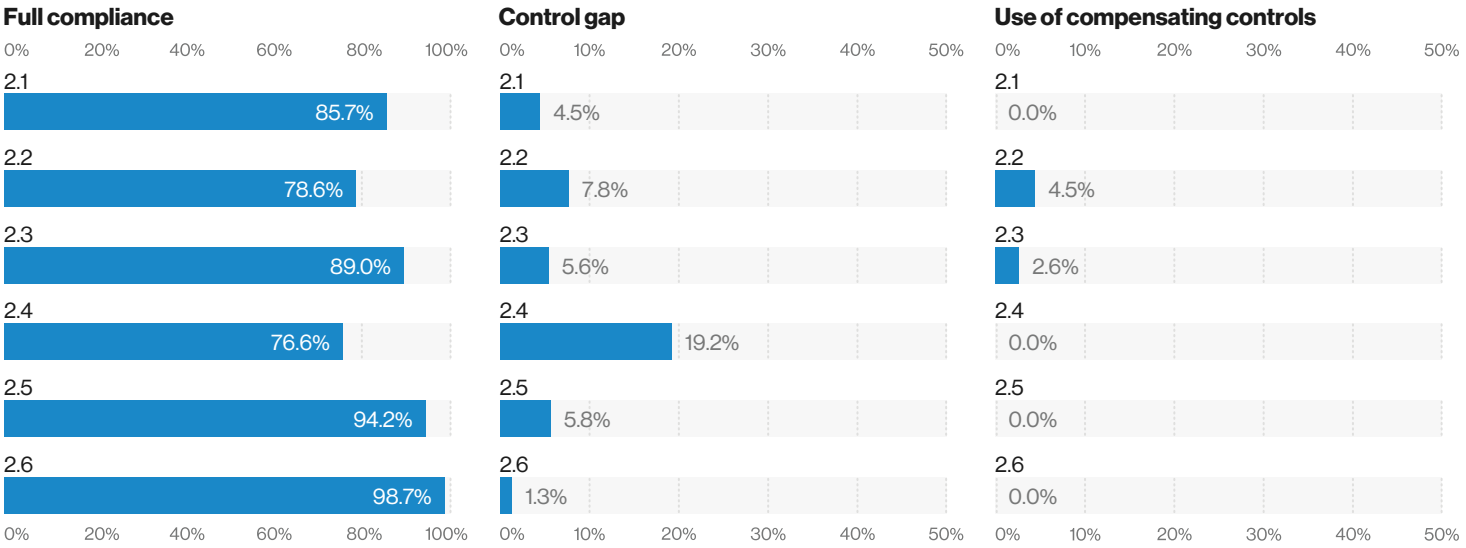
Requirement 2 controls

2.1	Change vendor-supplied defaults, disable unnecessary accounts
2.2	Develop configuration standards
2.3	Encrypt non-console administrative access
2.4	Maintain an inventory of in-scope system components
2.5	Documented policy and procedures for managing vendor defaults
2.6	Shared hosting provider data protection responsibility

State of control/test procedure

Controls 2.2 and 2.4 both reported in the bottom 20 controls for full compliance in 2019, while 2.6 was the most compliant control noted in 2019.

Figure 14. 2019 compliance performance (global averages) of Requirement 2—Do not use vendor-supplied defaults.



Payment data breach correlation—Req 2

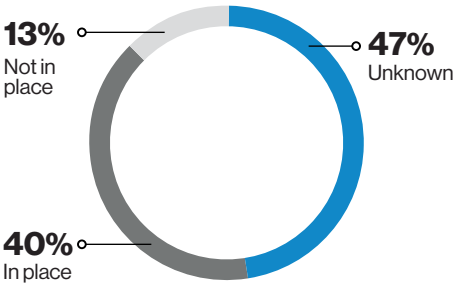


Figure 15. 2014 to 2019 PCI DSS compliance at the time of the breach

Industry vertical findings

Finance reported the largest drop in full compliance in 2019, from 6.1 pp to 65.9%. The sector fell behind, which took over the top spot across industry sectors with 83.3% of organizations achieving full compliance at interim assessment.

All sectors, excluding finance, lowered the control gap, with hospitality and retail noting the largest decreases at 7.3 pp and 6.5 pp, respectively. Merchants overall reduced control gap by 9.3 pp to 3.2% in 2019.

Figure 16. Full compliance—Req 2

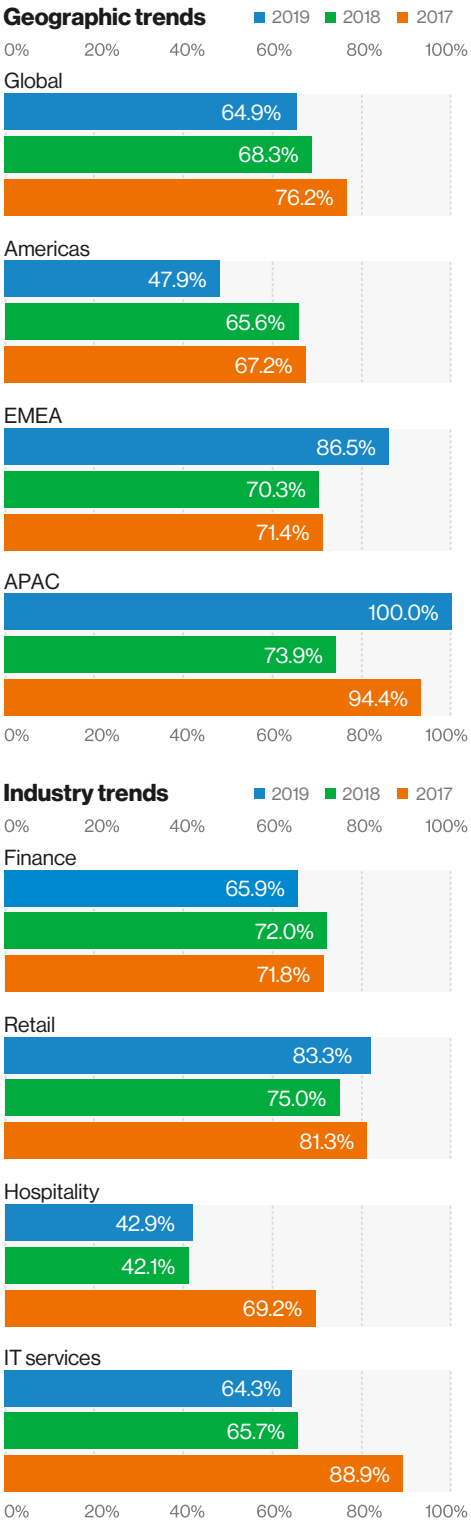


Figure 17. Control gap—Req 2

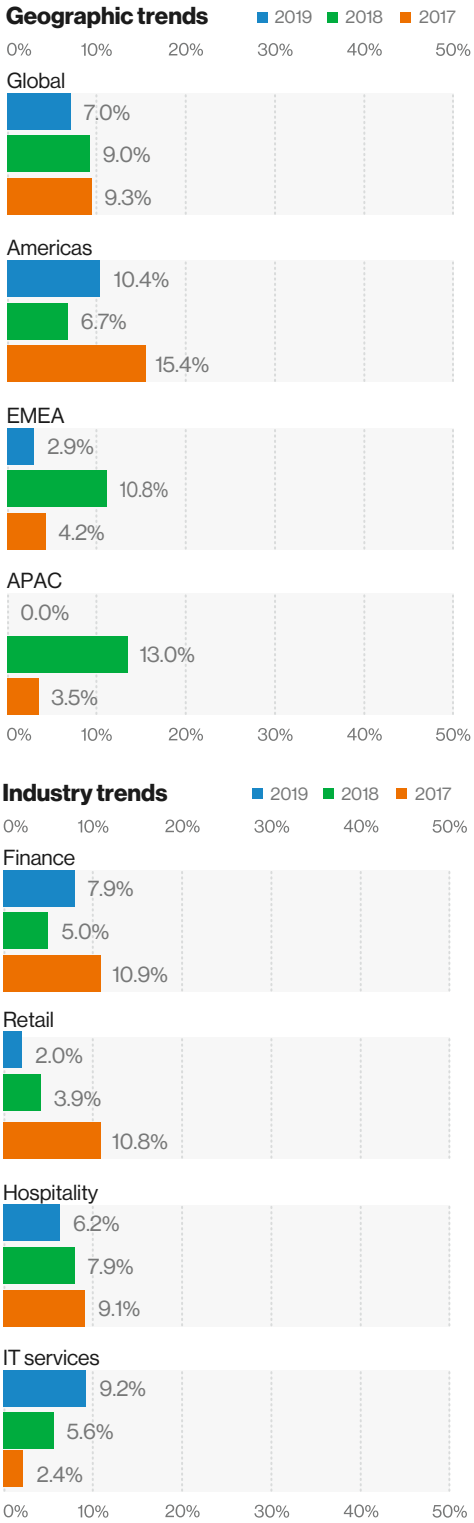
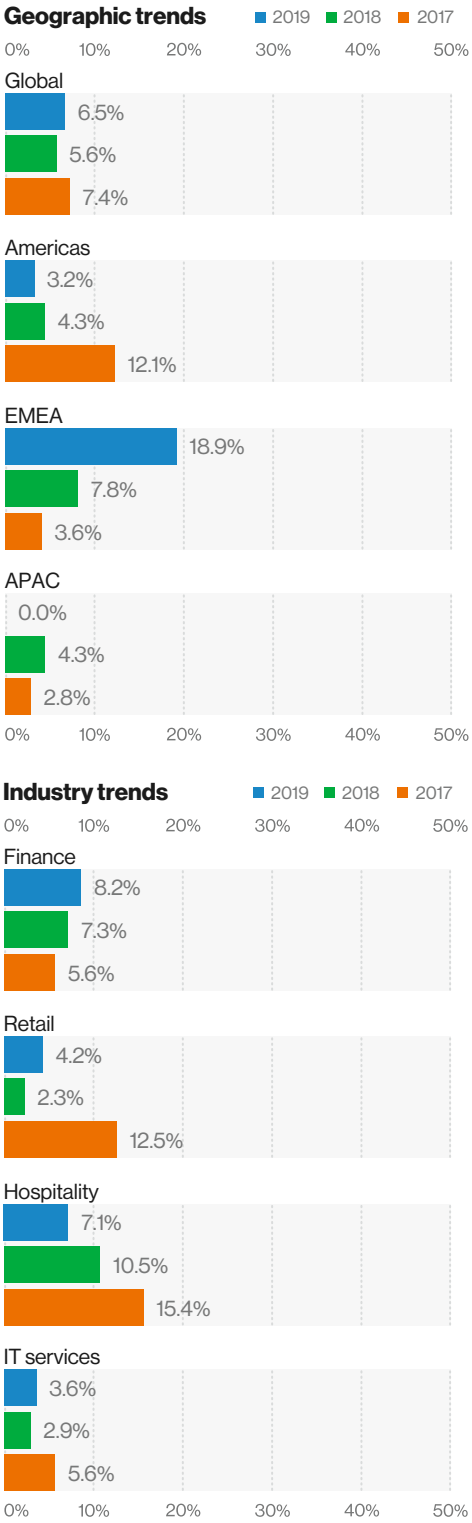


Figure 18. Compensating controls—Req 2



3: Protect stored cardholder data

This requirement covers the protection of stored cardholder data and sensitive authentication data. It states that all stored data must be protected using appropriate methods, and must be securely deleted once it is no longer needed.

Full compliance

The ranking for Requirement 3 improved over the three years leading up to 2018, but it slipped back one place in 2019 to fifth, despite maintaining compliance at 76.6%. Compliance reduced for Controls 3.4, 3.6 and 3.7, where small improvements were reported for the remaining controls.

For the regions, APAC saw the largest improvement of 17.4 pp to 95.7%. EMEA came in second at 83.8%, while the Americas decreased 8.3 pp, falling behind at 69.1% full compliance in 2019.

Merchants achieved full compliance of 79.4%, which is an improvement of 7.7 pp on 2018's figure. Service providers dropped slightly by 2.7 pp to 75.6% in 2019.

For the industry sectors, IT services showed the most significant reduction in overall compliance, dropping 12.1 pp in 2019 to 82.1%. Retail overtook IT to become the top-performing sector for Requirement 3 with 87.5% full compliance, and an 8.0 pp improvement over the previous year.

Control gap

Requirement 3 was ranked second overall for control gap in 2018, but dropped one place in 2019 to third. An increase of 1.9 pp was reported for 2019. Controls 3.1, 3.2 and 3.3 all showed improvement compared to the past year, but the remaining controls noted an increased control gap in 2019.

The Americas region lagged behind EMEA and APAC, reporting a control gap of 8.3%, an increase of 6.0 pp against 2018 figures. Both EMEA and APAC successfully reduced their control gaps to 2.1% and 0.4%, respectively.

The finance and retail industries both noted an increase in control gap of 2.2 pp and 1.3 pp, respectively, compared to the previous year. Hospitality reported the most significant improvement in control gap of 7.2 pp, while IT saw just a 0.1 pp change over the 2018 figures.

Compensating controls

The overall use of compensating controls increased in 2019, up 1.8 pp to 8.4%. Control 3.4 was the most frequently compensated in 2019.

The APAC region saw the largest increase in compensating controls for this requirement, eclipsing the other global regions at 17.4% compared to 7.4% (Americas) and 5.4% (EMEA).

Only the finance and retail sectors reported compensating controls for Requirement 3 – at 12.9% and 8.3%, respectively. Both IT services and hospitality reported compensating controls in previous years, but none are noted in 2019.

The use of compensating controls was relatively evenly split between merchants (5.5%) and service providers (5.7%). This represented a small reduction of 0.3 pp for merchants, but an increase of 1.4 pp for service providers.

Requirement 3 controls

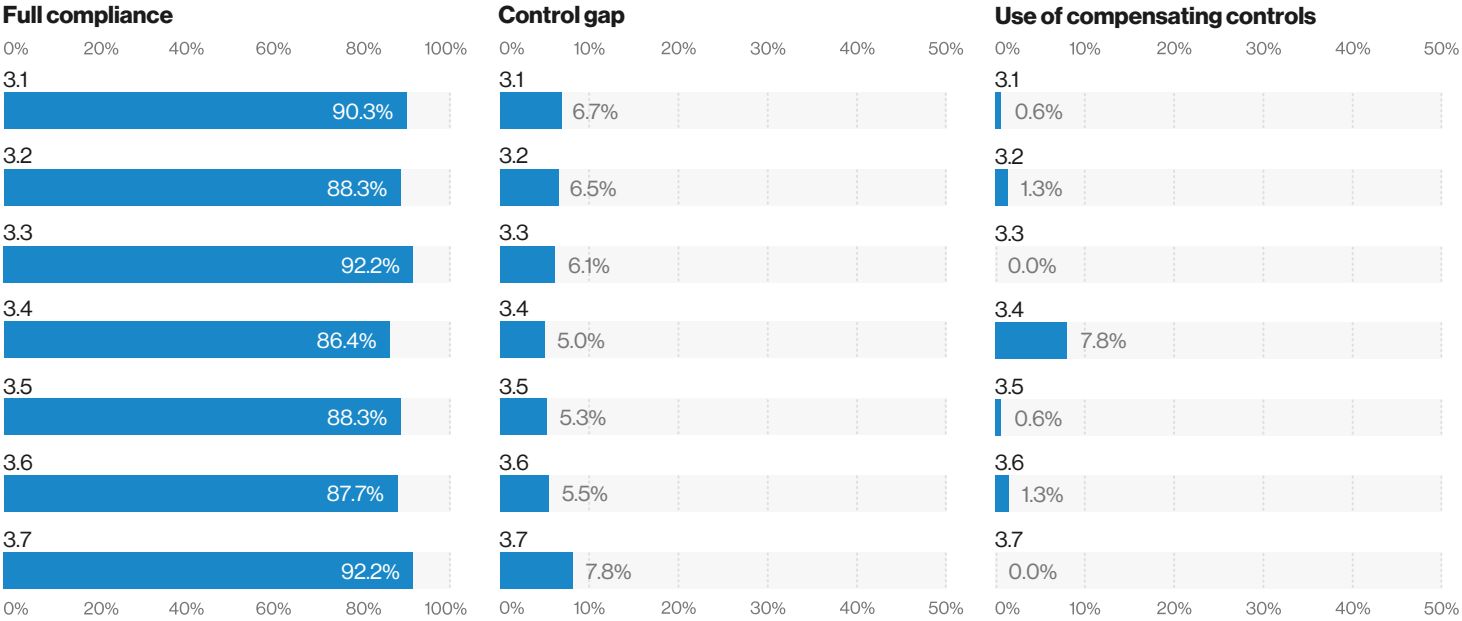
3.1	Keep data storage to a minimum
3.2	Do not store sensitive authentication data after authorization
3.3	Mask primary account numbers (PANs) when displayed
3.4	Render PANs unreadable anywhere they are stored
3.5	Protect keys used to secure stored cardholder data (CHD) against disclosure
3.6	Key-management processes
3.7	Documented policies for protecting stored CHD

State of control/test procedure

No controls from Requirement 3 are reported in the top- or bottom-20 list of the 20 least-compliant controls measured by achievement of full compliance (listed on page 112). However, Control 3.3 and Control 3.7 were equal in 12th position for full compliance. Test procedures 3.5.3, 3.5.3.b and 3.5.3.c are all present in the list of control gaps with the largest increase in gap.

Here are the scores by major controls.

Figure 19. 2019 compliance performance (global averages) of Requirement 3—Protect stored cardholder data.



Industry vertical findings

Retail outperformed other sectors in 2019 at 87.5% full compliance under Requirement 3, also noting an 8.0 pp improvement compared to the previous year. IT services were close behind at 82.1% full compliance, but with a 12.1 pp reduction for the sector compared to 2018 figures.

While lagging behind other sectors in full compliance, the hospitality sector noted a 7.2 pp improvement in control gap, reducing to 3.9% in 2019. Finance reported the largest control gap for this requirement at 8.1%.

Payment data breach correlation—Req 3

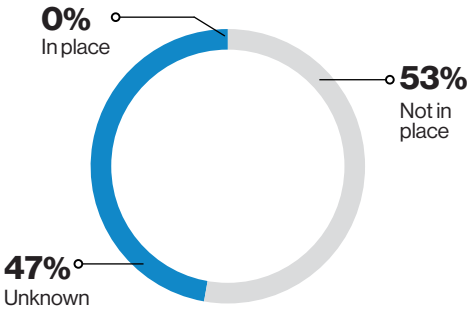


Figure 20. 2014 to 2019 PCI DSS compliance at the time of the breach

Figure 21. Full compliance—Req 3

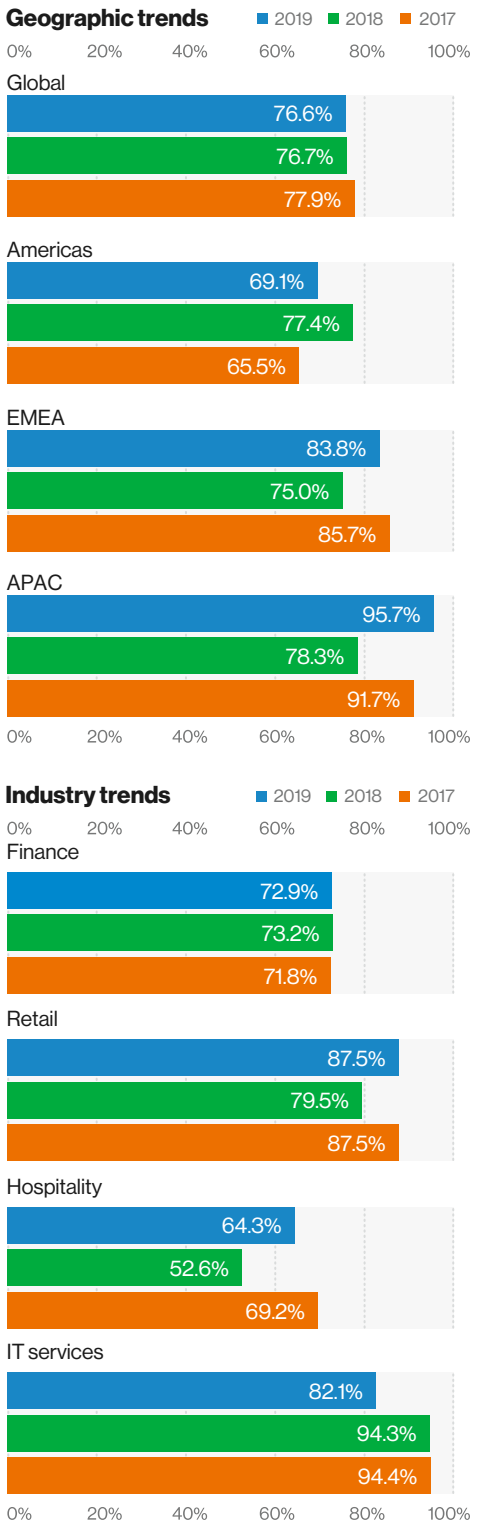


Figure 22. Control gap—Req 3

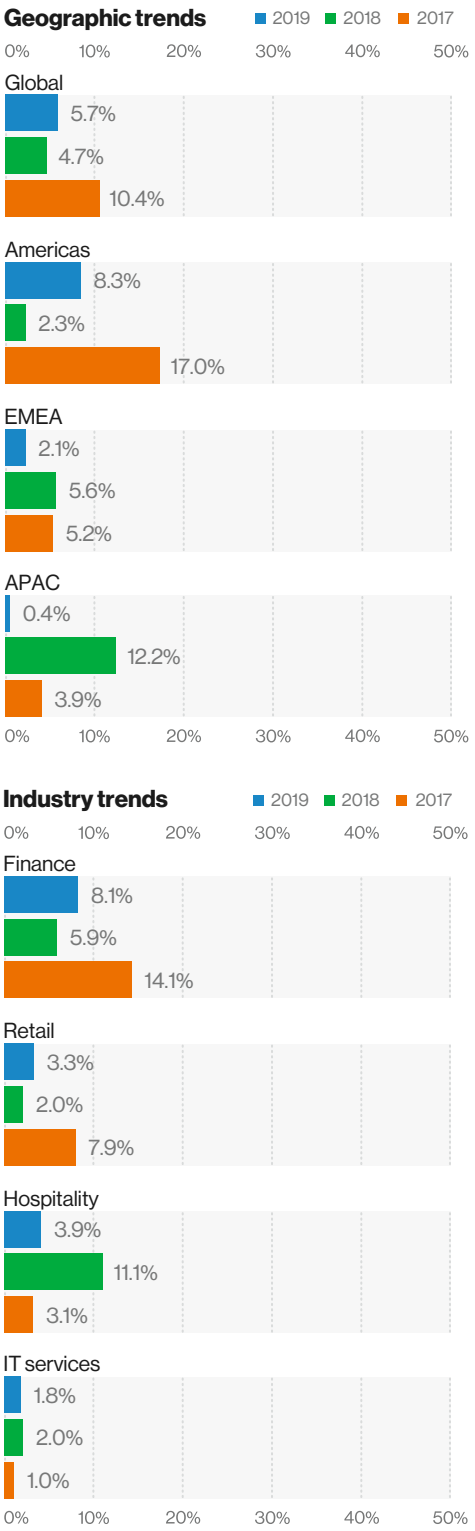
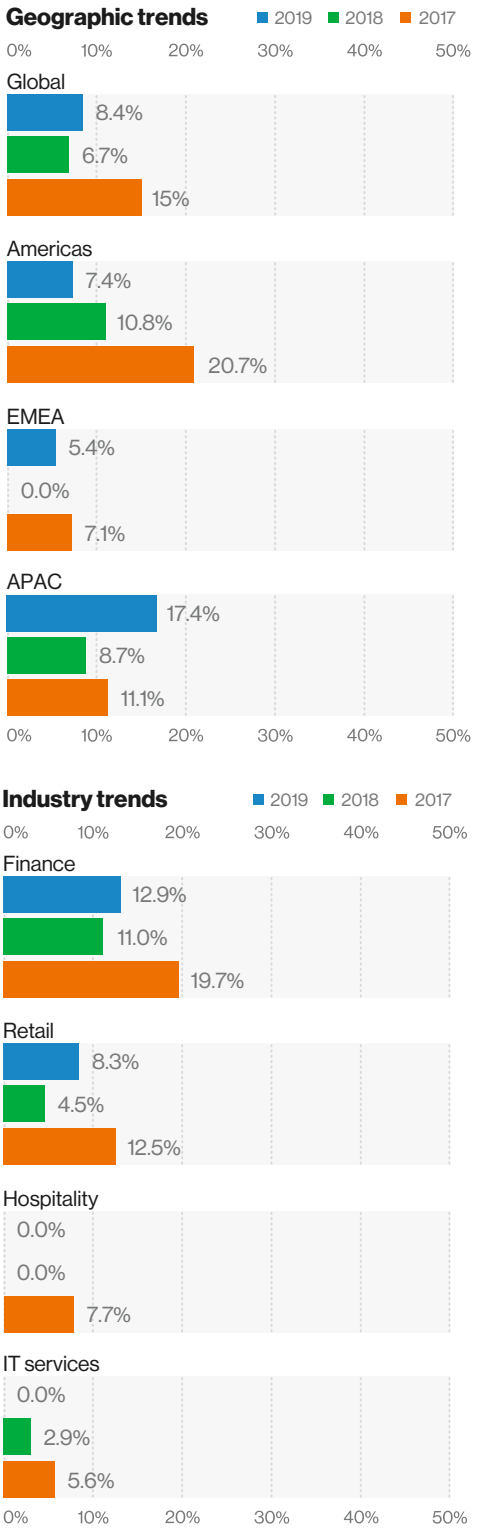


Figure 23. Compensating controls—Req 3



4: Protect data in transit

This requirement is designed to protect cardholder data and sensitive authentication data when transmitted over unprotected networks—such as the internet—where it can be vulnerable to interception.

Full compliance

Requirement 4 was the second most-compliant requirement in the data report this year. Full compliance increased 8.6 pp to 86.4% compared to 2018.

All global regions reported improvements in compliance with this requirement, with APAC reporting 100% compliance.

Turning to the industries, IT services achieved the highest full compliance across all industry sectors at 92.9%. This represented a 10 pp improvement over 2018 figures. However, hospitality reported the greatest improvement with a 22.6 pp increase, achieving 85.7% full compliance within the sector.

Both merchants and service providers noted improvements in full compliance, with increases of 9.2 pp and 8.2 pp, respectively. Service providers marginally outperformed merchants at 86.6% vs 85.3%.

Control gap

Alongside the improvements seen in full compliance, the control gap also reduced in 2019. The 3.6 pp reduction ranks this requirement top for control gap in 2019 at 3.7%. This is a significant promotion from eighth position in 2018.

The APAC and EMEA regions both reported significant contractions in the control gap this year. APAC showed particular improvement, reporting 100% compliance (0.0% gap); an improvement of 12.4 pp on the previous year. A small increase in control gap of 1.5 pp was observed in the Americas, increasing from 4.5% in 2018 to 6.0% in this year's figures.

Both merchants and service providers reduced their control gap in 2019. Service providers reported both a larger reduction and lower gap, outperforming merchants for Requirement 4.

Compensating controls

Compensating control use also fell significantly for Requirement 4, from 2.2% in 2018 to 0.6%. This reduction in compensating controls was observed across all global regions. In fact, no compensating controls were reported in the Americas or APAC for 2019, with reductions of 1.1 pp and 4.3 pp, respectively. The EMEA region also saw a reduction in the use of compensating controls for this requirement, down 0.4 pp to 2.7% in 2019.

The only sector to report compensating controls for Requirement 4 was finance, with a 2.5 pp reduction compared to the previous year.

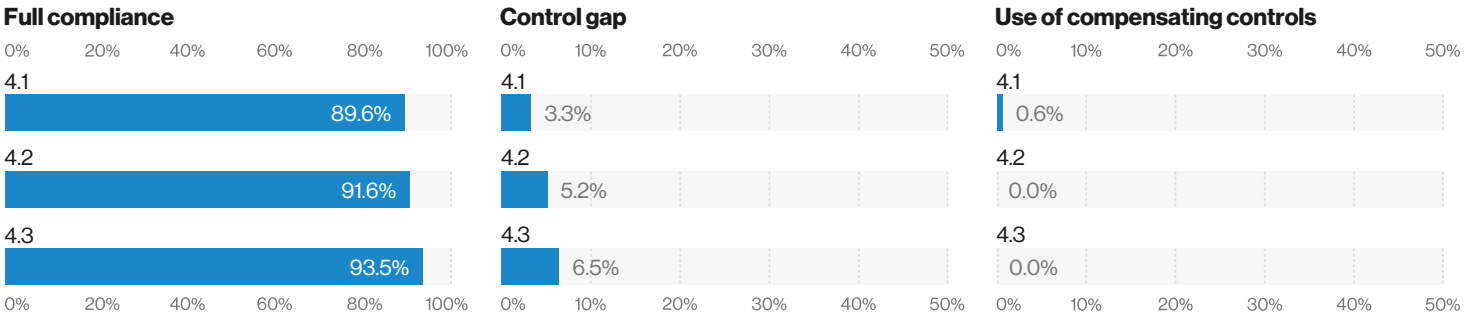
Requirement 4 controls

4.1	Use strong cryptography and protocols
4.2	Never send unprotected PANs by end-user messaging
4.3	Procedures for encrypting transmissions of CDE

State of control/test procedure

Control 4.3 was the sixth most-compliant control reported in 2019. No controls from Requirement 4 featured in the bottom 20. Control 4.1 was the most improved in 2019 for this requirement, reporting an increase of 7.9 pp for full compliance and a reduction in control gap of 4.5 pp, as compared to the previous year.

Figure 24. 2019 compliance performance (global averages) of Requirement 4—Protect data in transit.



Payment data breach correlation—Req 4

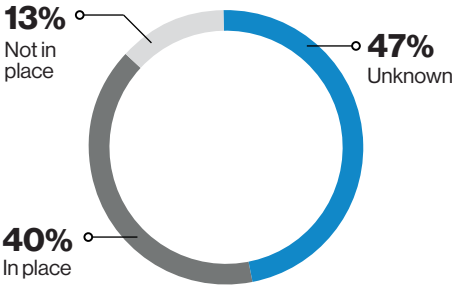


Figure 25. 2014 to 2019 PCI DSS compliance at the time of the breach

Industry vertical findings

- All sectors reported compliance improvements compared to the previous year for Requirement 4
- IT services reported the highest full compliance across industry sectors at 92.9%, with a notable 10.0 pp increase on the previous year
- Hospitality reported the greatest improvement with a 22.6 pp increase, achieving full 85.7% compliance within the sector
- All industry sectors noted contractions in control gap in 2019, with hospitality the most significant at 6.9 pp. Despite a reduction of 4.1 pp, finance reported the largest control gap for this requirement at 5.0%

Figure 26. Full compliance—Req 4

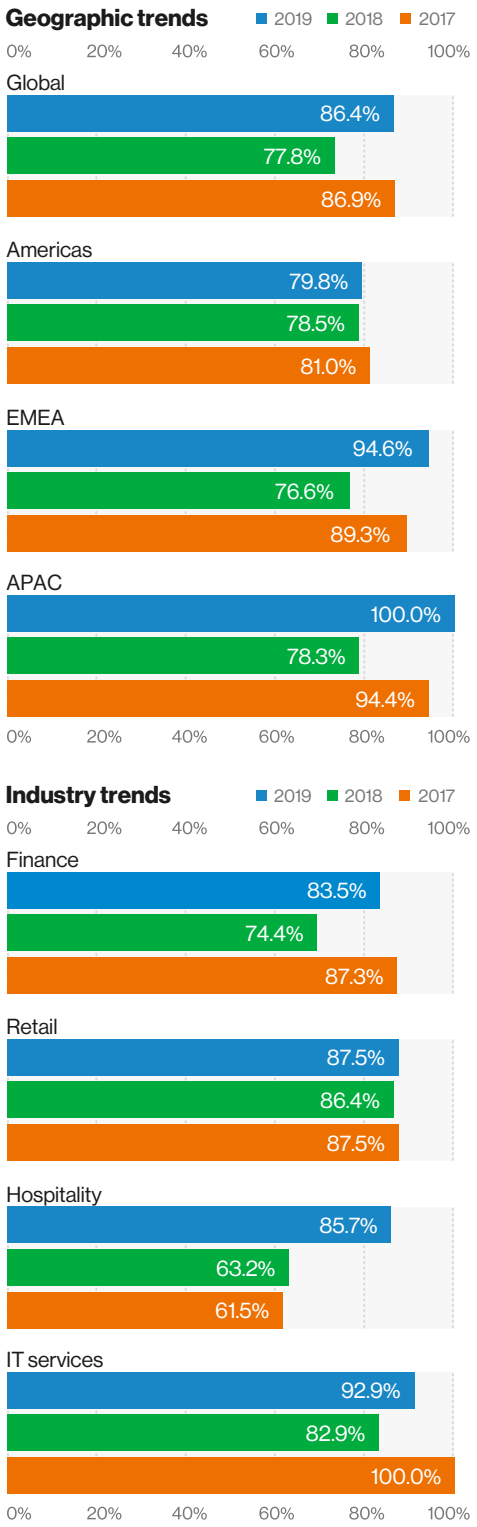


Figure 27. Control gap—Req 4

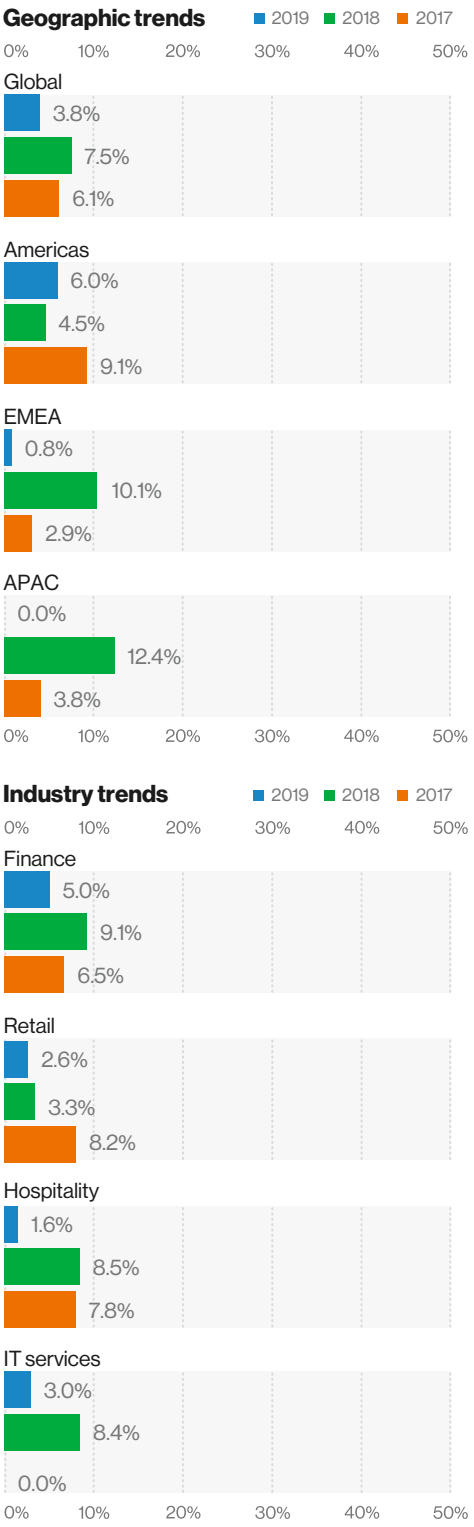
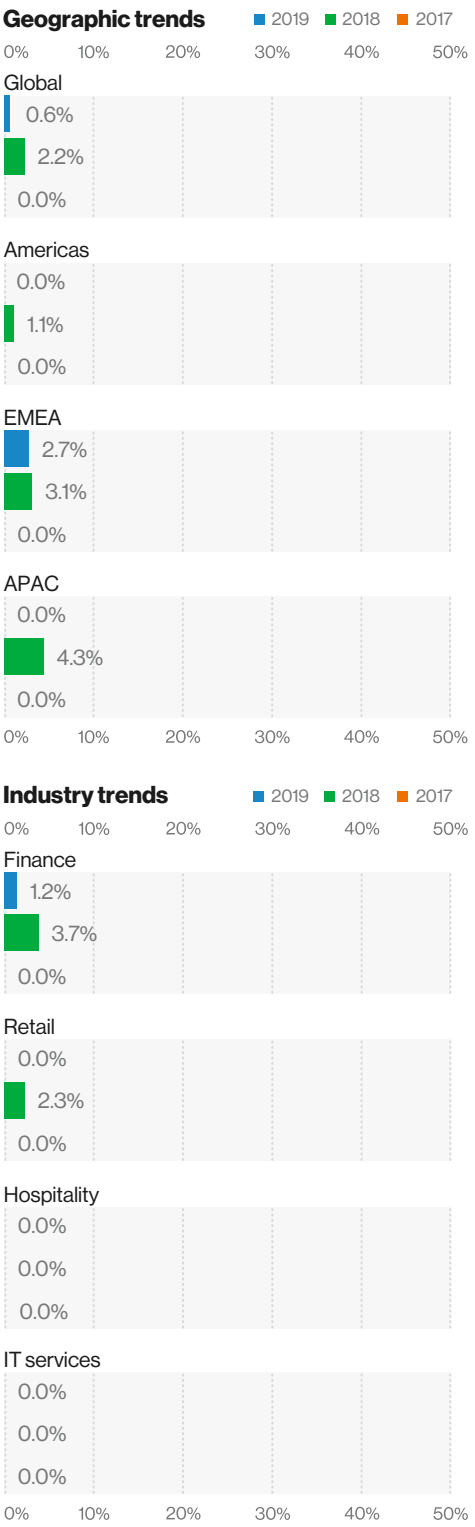


Figure 28. Compensating controls—Req 4



5: Protect against malicious software

This requirement concerns protecting all systems commonly affected by malicious software (malware) against viruses, worms and Trojans.

Full compliance

Requirement 5 dropped from the second-highest full compliance ranking across all industry sectors in 2018 to third place in 2019, with a decline of 3.1 pp. Of the entities reviewed, 82.5% were reported to be fully compliant with the requirement at the time of the interim assessment.

The Americas region showed the largest variance in percentage points among regions from the previous year, declining by 9.4 pp. Both APAC and EMEA reported improvements over 2018 figures, with APAC achieving 100% compliance at interim assessment.

Merchants were found ranked above service providers, reporting 88.2% compliance with a 1.3 pp increase from 2018, whereas service providers were at 81.5% compliance with a decrease of 3.6 pp.

Control gap

The control gap for this requirement deteriorated in 2019. The gap increased by 3.8 pp to 9.6%. This resulted in a six-place drop to 11th overall, the lowest ranking ever for this requirement.

The Americas noted a 7.6 pp increase in control gap as compared to the previous year, to 13.9%. The EMEA region contracted by 1.0 pp to 4.4% in 2019.

All controls reported an expanding control gap, a position reflected across all industry sectors. Both merchants and service providers saw a widening control gap. Service providers reported the larger gap at 9.9%, but merchants saw the most increase compared to the previous year at 5.3 pp, to 8.3%.

Compensating controls

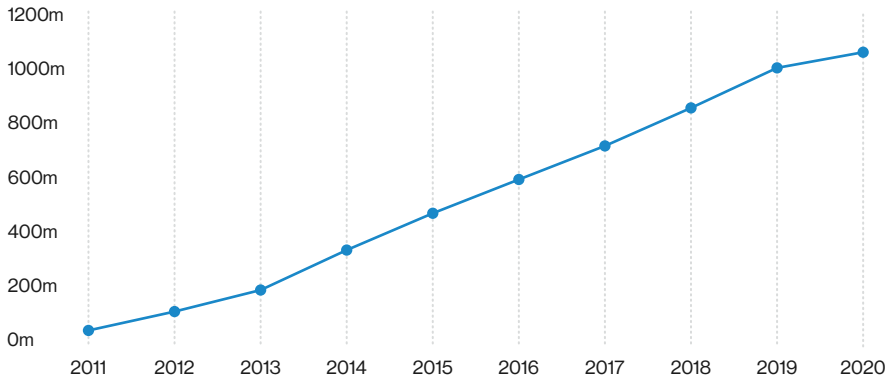
The use of compensating controls fell slightly in 2019, by 0.4 pp to 1.3%. This compares to 1.7% the previous year. Compensating controls were reported against Control 5.1 and Control 5.2 in 2019, but none were recorded for Controls 5.3 or 5.4.

The APAC region reported the most frequent use of compensating controls for this requirement at 4.3%, just ahead of EMEA at 2.7%. The Americas recorded no compensating controls for Requirement 5 in 2019.

Requirement 5 controls

5.1	Deploy antivirus software
5.2	Maintain all antivirus mechanisms
5.3	Antivirus actively running and cannot be disabled
5.4	Document policies for malware protection

Figure 29. Increase in the total number of malware over the past 10 years [101]

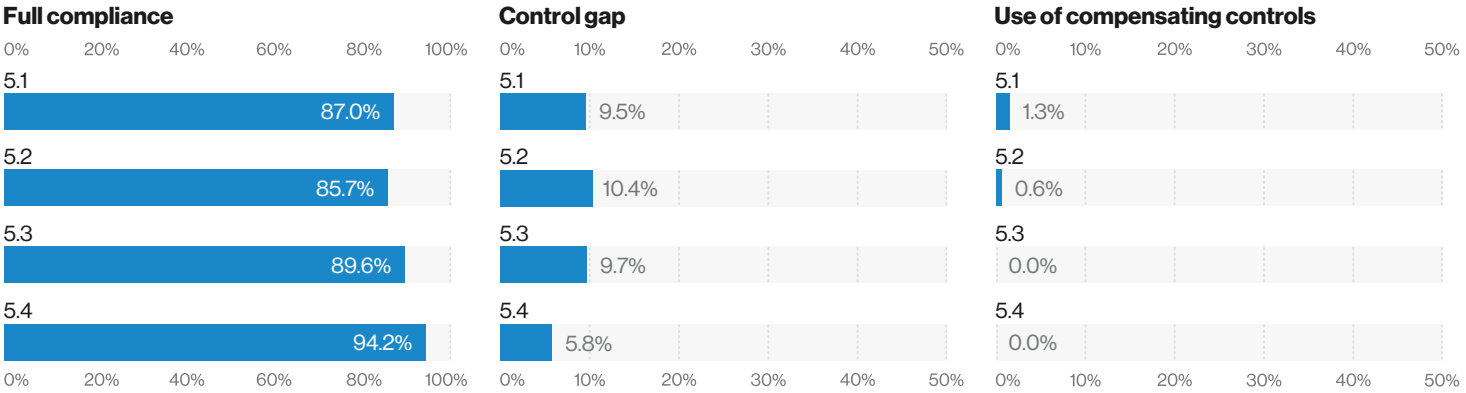


102 AVTest. https://www.av-test.org/en/statistics/malware/

State of control/test procedure

Full compliance reduced in all Requirement 5 controls in 2019, along with increasing control gaps compared to the previous year. Control 5.4, however, achieved a top-five ranking for full compliance, in fourth place. No Requirement 5 controls were reported in the bottom 20 in 2019.

Figure 30. 2019 compliance performance (global averages) of Requirement 5—Protect against malicious software.



Industry vertical findings

The retail sector achieved the highest full compliance across all sectors in 2019 at 87.5%, despite a fall of 3.4 pp compared to the previous year. This drop was only exceeded by IT services, which fell 7.1 pp to 78.6% and was the lowest-performing sector for this requirement in 2019. Hospitality was the only sector to report a slight improvement in full compliance in 2019, of 1.5 pp.

The control gap increased across all sectors compared to 2018's figures. IT services saw the greatest increase of 6.9 pp to 12.3%. Finance reported the smallest change as compared to the previous year at 2.1 pp, but had the next-largest control gap at 10.7%. Retail reported the lowest control gap for Requirement 5 at 4.9%.

Only finance reported compensating controls to satisfy Requirement 5 controls in 2019. Hospitality and IT services both recorded their use the previous year.

Payment data breach correlation —Req 5

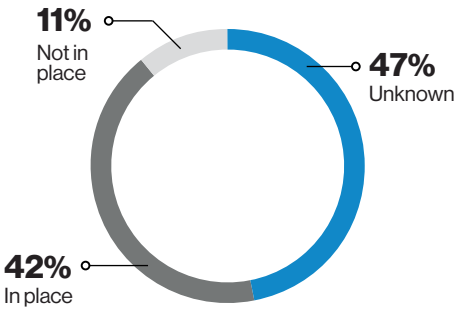


Figure 31. 2014 to 2019 PCI DSS compliance at the time of the breach

Figure 32. Full compliance—Req 5

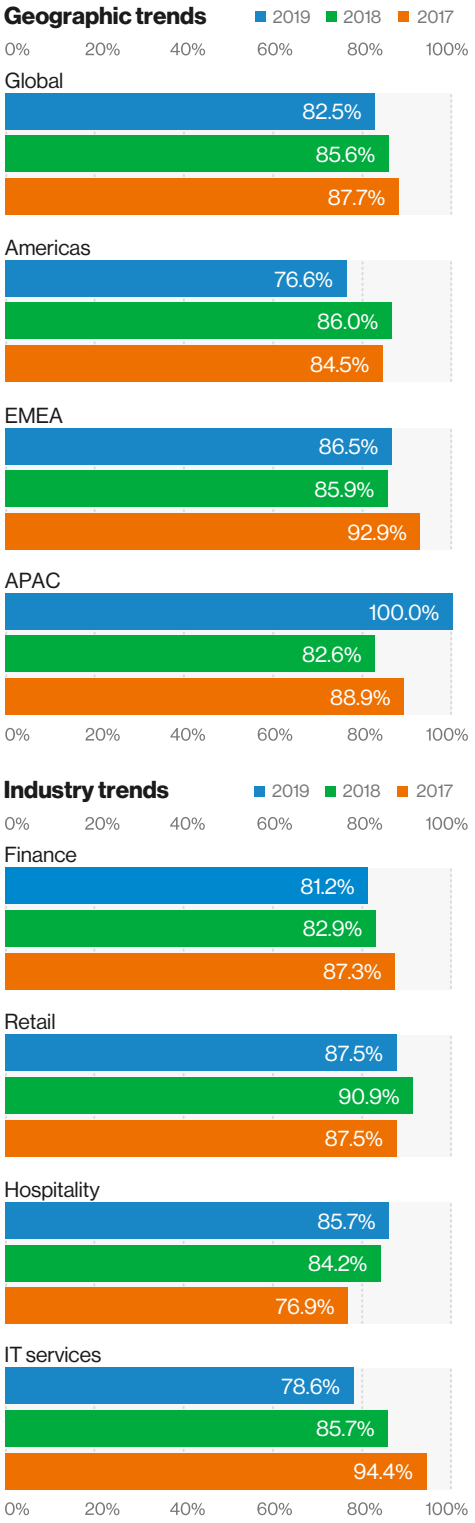


Figure 33. Control gap—Req 5

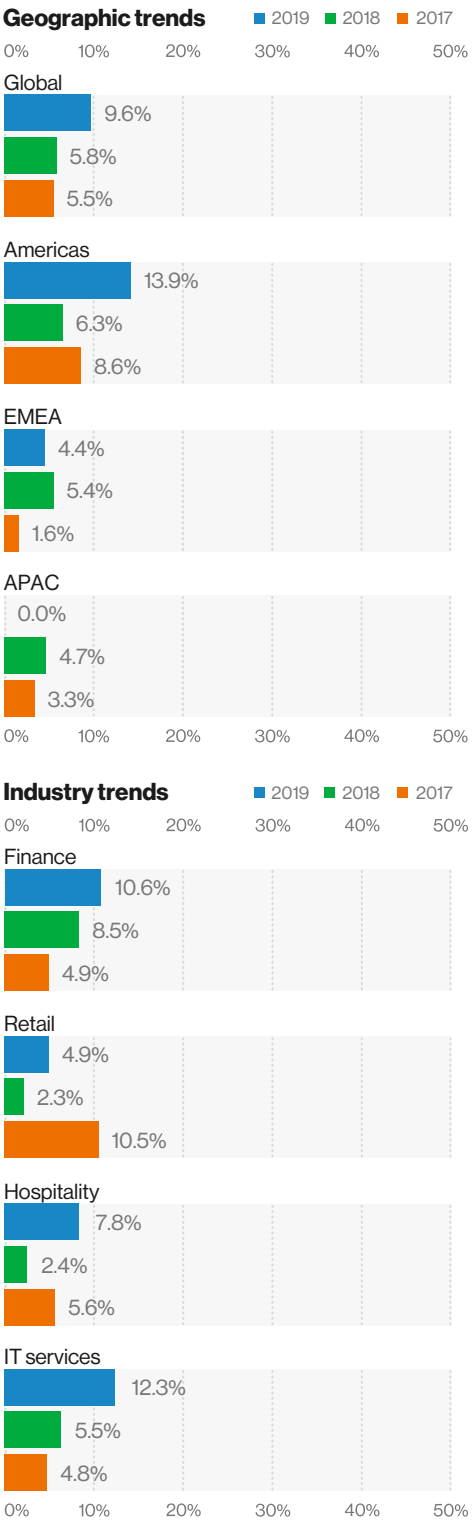
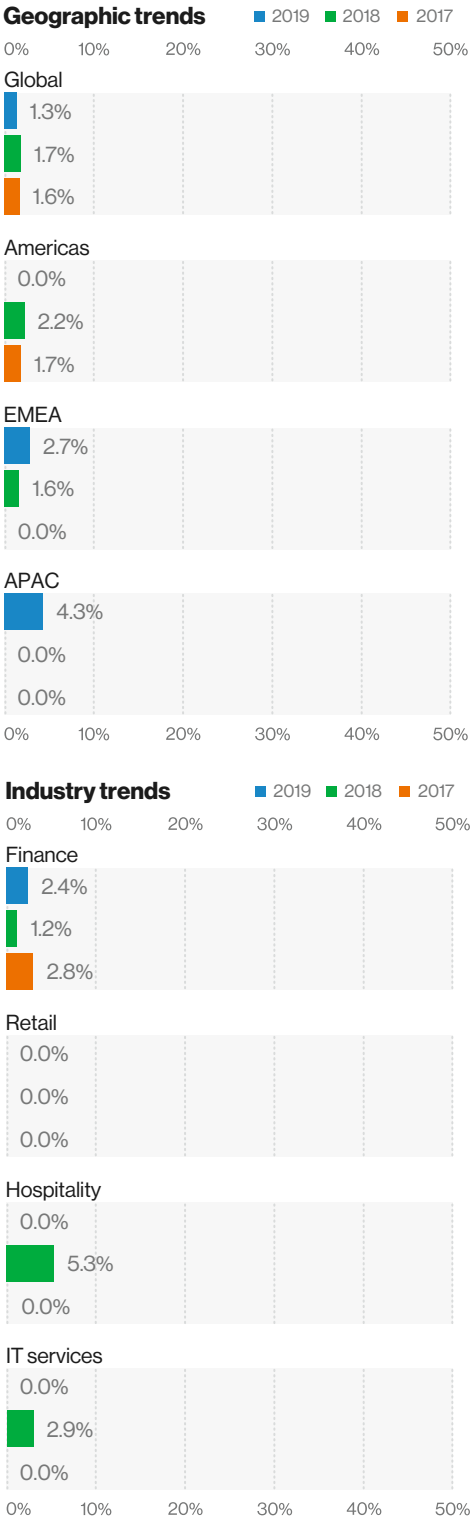


Figure 34. Compensating controls—Req 5



6: Develop and maintain secure systems

This requirement covers the security of applications and change management. It governs how systems and applications are developed and maintained, whether by the organizations or third parties.

Full compliance

Requirement 6 remains one of the poorest-performing requirements, ranking 10th overall for full compliance, despite seeing a 4.3 pp improvement in 2019 to 60.4% full compliance as compared to the previous year. All controls were observed to have achieved only minor improvements in full compliance as compared to the previous year.

APAC significantly outperformed other global regions, achieving 95.7% full compliance at interim assessment, which is more than 30 pp higher than EMEA, the next-best performing region.

Hospitality recorded the highest full compliance across all industry sectors, achieving 64.3% full compliance. Hospitality also saw the largest gains in full compliance, with an increase of 16.9 pp as compared to 2018. Both merchants and service providers noted improvements in full compliance, with increases of 11.8 pp and 1.5 pp, respectively. Merchants reported slightly higher compliance figures at 61.8% vs 59.7%.

Control gap

The control gap remained relatively consistent in 2019, showing just a 0.6 pp increase as compared to the previous year at 6.8%.

APAC and EMEA both noted a reduced control gap in 2019. EMEA saw a 4.8 pp contraction to 2.6%, while APAC lowered their gap from 9.9% in 2018 to just 0.1% in 2019. The Americas reported a 5.5 pp increase in control gap, counter to the other global regions.

The finance sector reported the largest control gap in 2019 at 9.1%, representing a 1.8 pp increase on the previous year. Retail also saw a minor increase of 0.1 pp to 2.4%. Both hospitality and IT services noted contracted control gaps as compared to 2018. Hospitality successfully reduced its control gap by the largest margin by 8.0 pp to 4.7%, which, in addition to the improvements in full compliance, suggests an overall positive trend for compliance.

Compensating controls

Requirement 6 was the most frequently compensated in 2019, at 11%. This was an increase of 6.6 pp as compared to the previous year, with APAC reporting the highest use of compensating controls across all global regions. Control 6.2 was the most-often compensated control at 10.4%; however, this was a reduction of 7.1 pp since 2018.

Looking at APAC reports, 30.4% noted compensating controls for this requirement, followed by EMEA at 10.8% and the Americas at 6.4%. Use of compensating controls increased across all regions in 2019.

By sector, compensating controls were split between finance, retail and IT services, with finance using them most frequently at 14.1%. This was an increase of 6.8 pp as compared to the previous year. Retail reported a 10.2 pp increase, the largest growth across all sectors in 2019, coming in just behind finance at 12.5%. Finance was 14.1%.

Requirement 6 controls

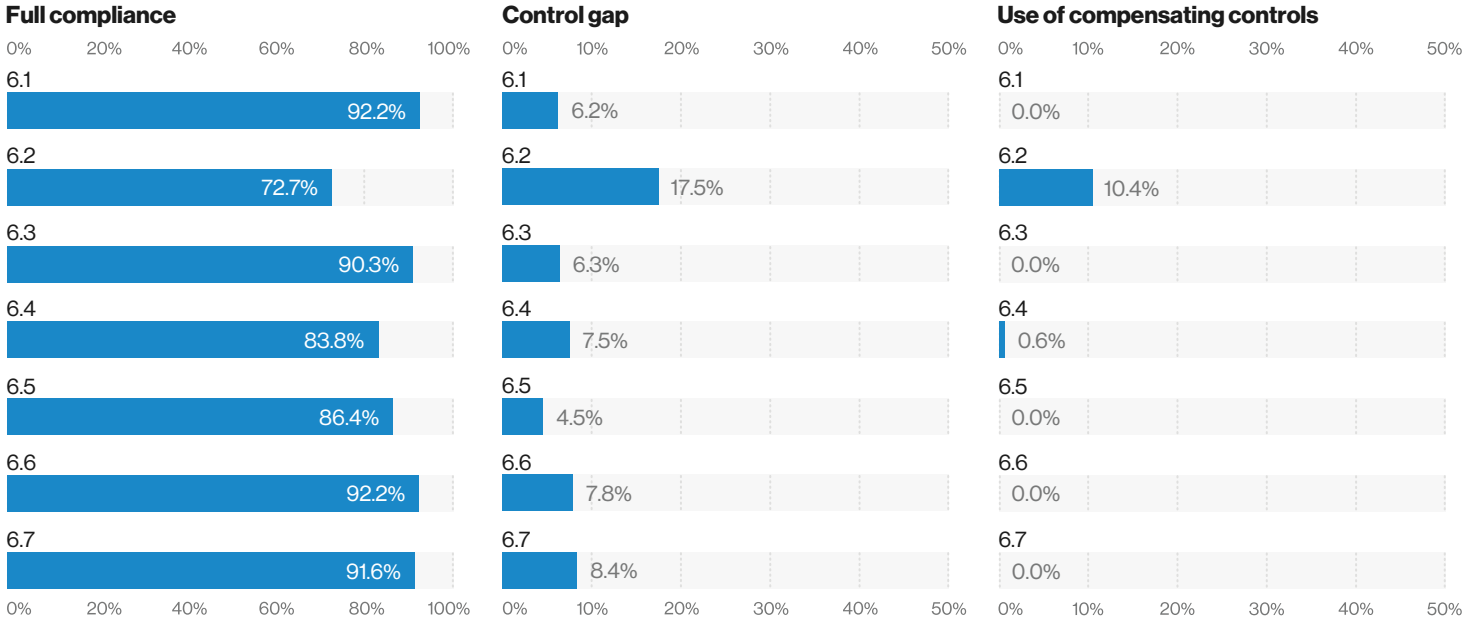
6.1	Use reputable outside sources for vulnerability info
6.2	Protect components and software from known vulnerabilities
6.3	Develop secure software applications
6.4	Follow change control processes
6.5	Address common coding vulnerabilities
6.6	Protect public-facing web applications against known attacks
6.7	Policies and procedures for secure systems and apps

State of control/test procedure

Improvements in full compliance were noted for all Requirement 6 controls in 2019, with Control 6.5 and Control 6.6 reporting the largest increases of 4.1 pp and 4.4 pp, respectively.

Control 6.2 remains one of the least compliant controls in 2019, ranking within the bottom five overall.

Figure 35. 2019 compliance performance (global averages) of Requirement 6—Develop and maintain secure systems.



Payment data breach correlation—Req 6

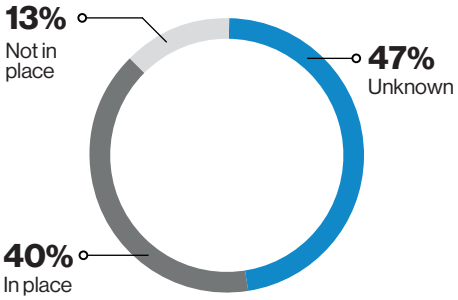


Figure 36. 2014 to 2019 PCI DSS compliance at the time of the breach

Industry vertical findings

- All sectors, other than retail, reported full compliance improvements as compared to the previous year; retail reported just a 0.8 pp drop to 58.3% but was the lowest-performing sector for this requirement in 2019
- Hospitality outperformed other sectors with full compliance at 64.3%, and also saw the largest gains in full compliance of 16.9 pp compared to 2018 figures
- Both finance and IT services achieved notable improvements to decrease their control gap for Requirement 6 controls over the previous year, with finance reporting an increase of 5.1 pp and IT services 3.6 pp
- Hospitality successfully reduced its control gap by the largest margin, by 8.0 pp to 4.7%; in addition to the improvements in full compliance, this suggests an overall positive trend for compliance

Ransomware teams do not just target corporate intellectual property or the personal files on home computers. They can also leverage harvested cardholder data, as demonstrated by the Banco BCR ransomware attack claimed by the Maze threat group in an April 30, 2020. press release. According to the hackers, they infiltrated the Costa Rican bank's infrastructure first in August 2019. After paying the state-owned bank a return visit in February 2020 and seeing that no additional security measures were in place, the Maze group asserted that they exfiltrated 11 million credit card records, 240 of which they initially leaked, in redacted format, online. Rather than encrypting the bank's systems, the group chose to demand a ransom in exchange for the records, but the bank was unresponsive. Thus, on May 21 and May 28, 2020, the Maze group began releasing the cardholder data in a 2 GB weekly feed on the dark web, still in hopes that Banco BCR would pay a ransom demand for the remaining records. Once these first records were released, the ransomware attack became a confirmed data breach, with all attendant legal and regulatory ramifications.[103,104,105,106,107]

Figure 37. Full compliance—Req 6

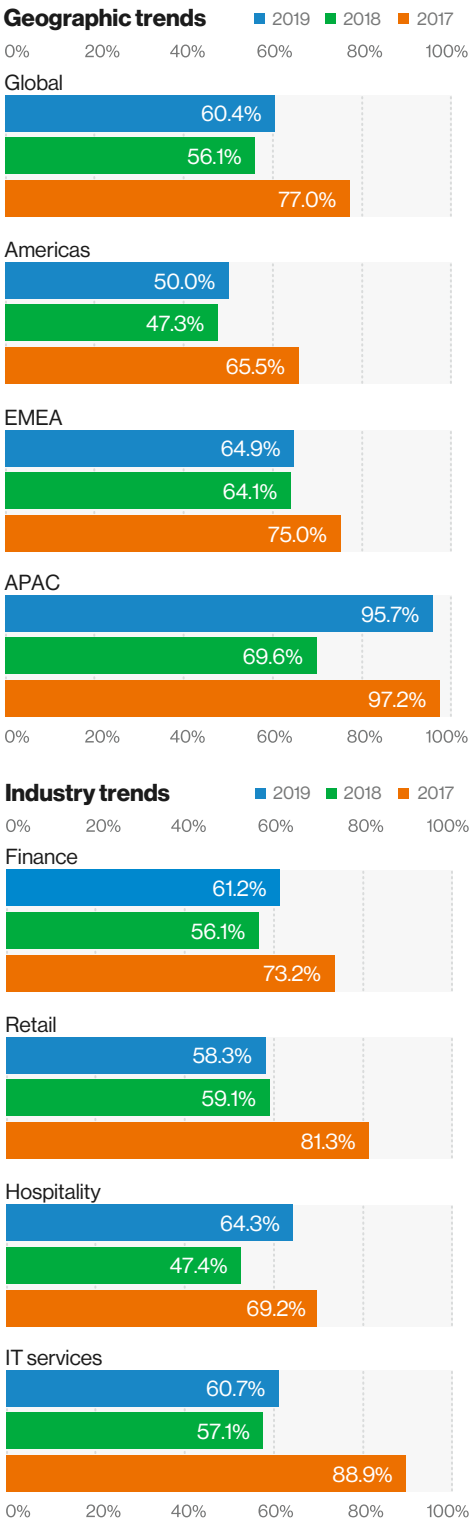


Figure 38. Control gap—Req 6

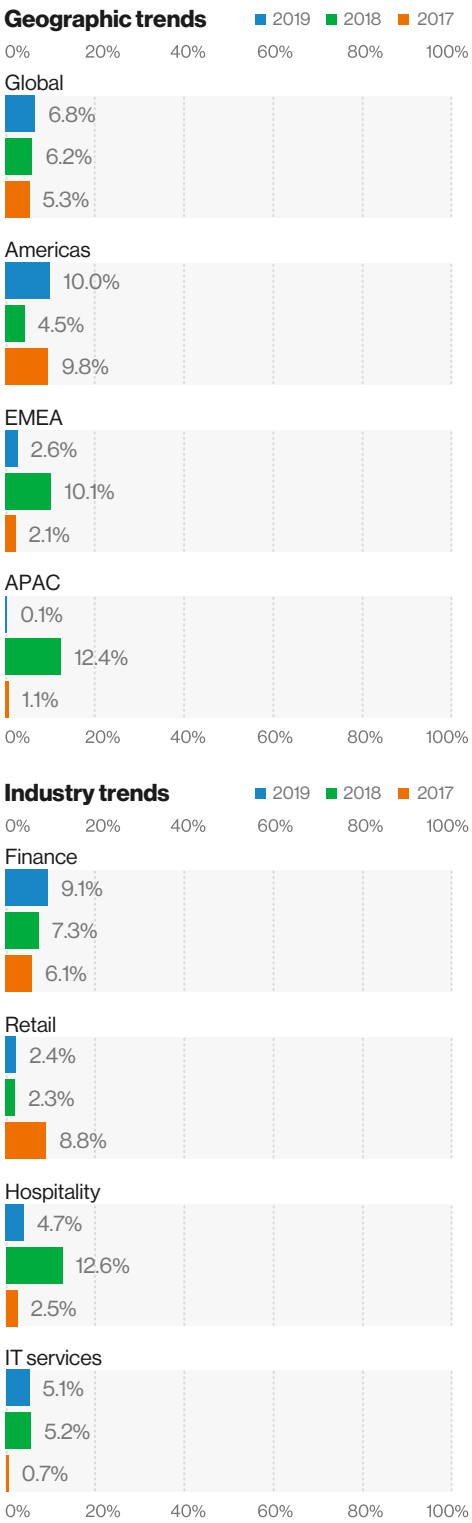
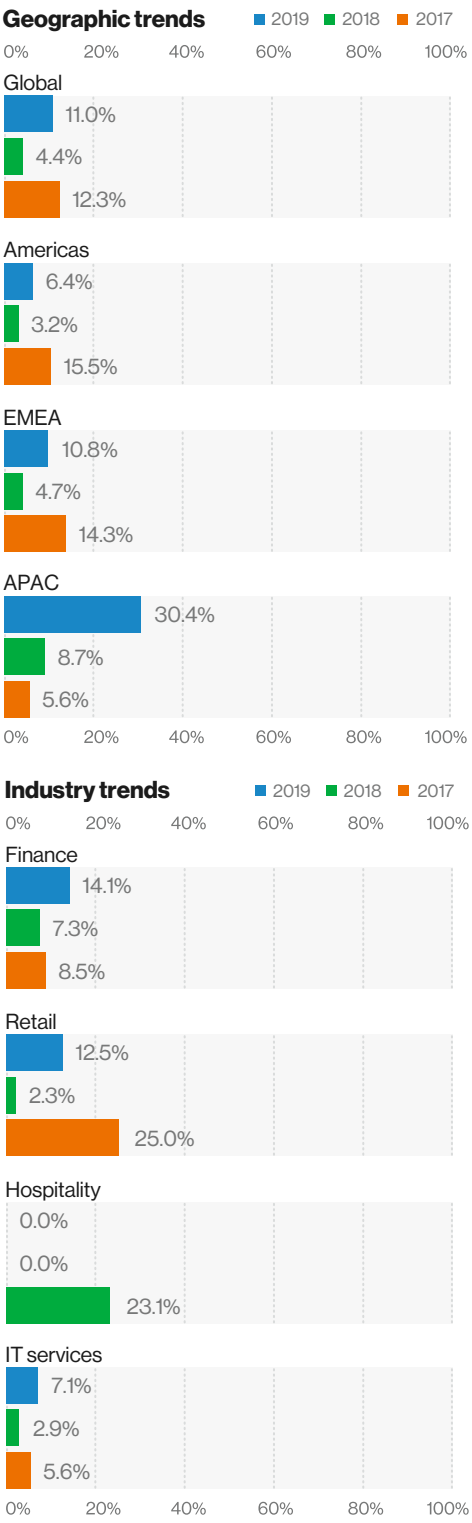


Figure 39. Compensating controls—Req 6



103 https://www.technadu.com/maze-gang-stole-11-million-credit-card-records-banco-bcr/100726/
104 https://www.bleepingcomputer.com/news/security/canadian-insurance-firm-hit-by-maze-ransomware-denies-data-theft/
105 https://www.finextra.com/newsarticle/35891/maze-ransomware-gang-leak-banco-bcr-card-data
106 https://securityaffairs.co/wordpress/103732/cyber-crime/maze-ransomware-bcr-leak.html
107 https://cybleinc.com/2020/05/28/banco-bcr-credit-card-leaks-by-maze-ransomware-operators-part-2/

7: Restrict access

This requirement specifies the processes and controls that should restrict each user's access rights to the minimum they need to perform their duties on a "need to know" basis.

Full compliance

Requirement 7 maintained its first-place ranking for full compliance, as it has done for the last three consecutive years. In 2019, full compliance improved 3.4 pp to 89.0%. Despite full compliance for this requirement improving overall, Control 7.2 and Control 7.3 saw compliance drop slightly.

APAC reported 100% compliance for Requirement 7, with EMEA close behind at 97.3%. The Americas lagged slightly at 83.0%, with a 6.7 pp drop as compared to the previous year.

IT services was the only sector to record a reduction in full compliance, falling 12.1 pp to 82.1%. All other sectors noted improvements, with hospitality the most significant, increasing 22.6 pp to 85.7%. Retail achieved the highest full compliance across all industry sectors at 95.7%, with finance following at 89.4%. Hospitality reported the largest increase in full compliance, improving 22.6 pp to 85.7% in 2019.

Merchants achieved full compliance of 91.2%, an improvement of 12.9 pp on the previous year. Service providers also noted a marginal improvement of 0.2 pp to 88.2%.

Control gap

Requirement 7 fell three places to rank sixth for the control gap in 2019, as overall control gap increased in 2019 by 2.4 pp to 7.4%. All controls noted an increasing gap in 2019, with 7.2 the most significant, reporting a 4.8 pp rise to 8.9%.

APAC reduced its control gap to 0.0%, as all organizations were deemed compliant at interim assessment. The Americas region recorded the largest control gap across global regions for this requirement at 11.8%, which represents a significant increase of 9.1 pp.

The IT services sector reported the greatest control gap across the industries, at 12.7%. This also represents the most significant increase in gap across all sectors, at 9.8 pp, as compared to the previous year. Finance, by contrast, saw a smaller increase of 1.8 pp to 8.3% in 2019.

IT services and finance both noted widening control gaps in 2019, while both retail and hospitality noted contractions. These factors contributed to the increasing control gap noted for service providers of 3.2 pp to 8.2%, as compared to the 5.1% reported for merchants.

Compensating controls

This requirement in 2018 reported no compensating controls, and only a small number were noted in this year's figures, with 0.6% of organizations reporting their use.

Only organizations within the EMEA region used compensating controls for Requirement 7, with the Americas and APAC regions reporting none in 2019.

Only financial services industry organizations reported use of compensating controls for this requirement at 1.2%. Both retail and hospitality had compensating controls in previous years, but none were noted in 2019.

Requirement 7 controls

7.1	Limit access to system components
7.2	Access control system based on need to know, set to deny all
7.3	Policies and procedures for restricting access to CHD

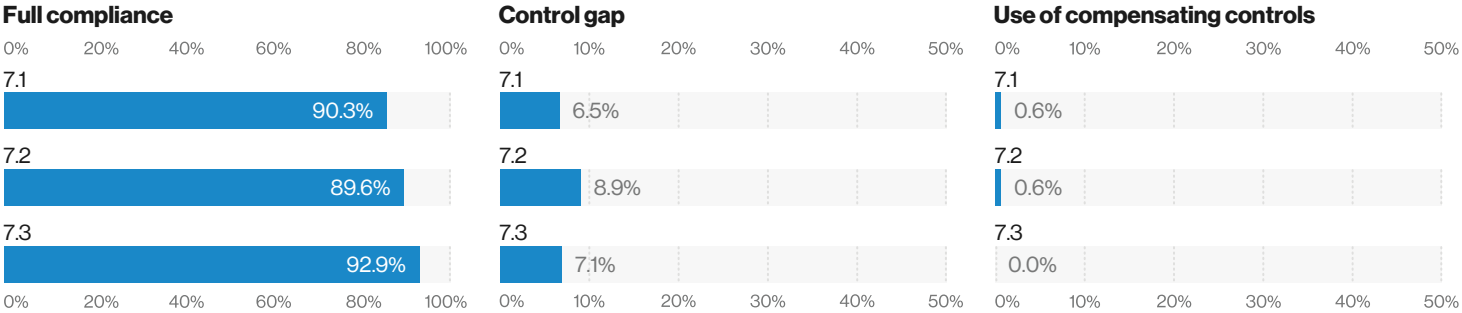
State of control/test procedure

No controls from Requirement 7 are reported in the bottom 10; bottom 20 list of the 20 least compliant controls measured by achievement of full compliance (listed on page 112). However, Control 7.3 ranked in the top 10 most-compliant controls with 9th place.

Test procedures 7.2.1 and 7.2.2 are present in the list of control gaps with the largest increase in gap.

Here are the scores by major base controls.

Figure 40. 2019 compliance performance (global averages) of Requirement 7—Restrict access.



Industry vertical findings

Retail achieved the highest full compliance across all industry sectors at 95.7%, with finance following at 89.4%.

Hospitality reported the largest increase in full compliance, improving 22.6 pp to 85.7% in 2019. IT services was the only sector to see a drop in full compliance in 2019 as compared to the previous year.

IT services and finance both noted widening control gaps in 2019, while both retail and hospitality showed contractions.

Payment data breach correlation—Req 7

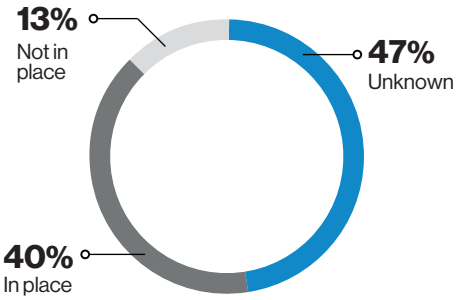


Figure 41. 2014 to 2019 PCI DSS compliance at the time of the breach

Figure 42. Full compliance—Req 7

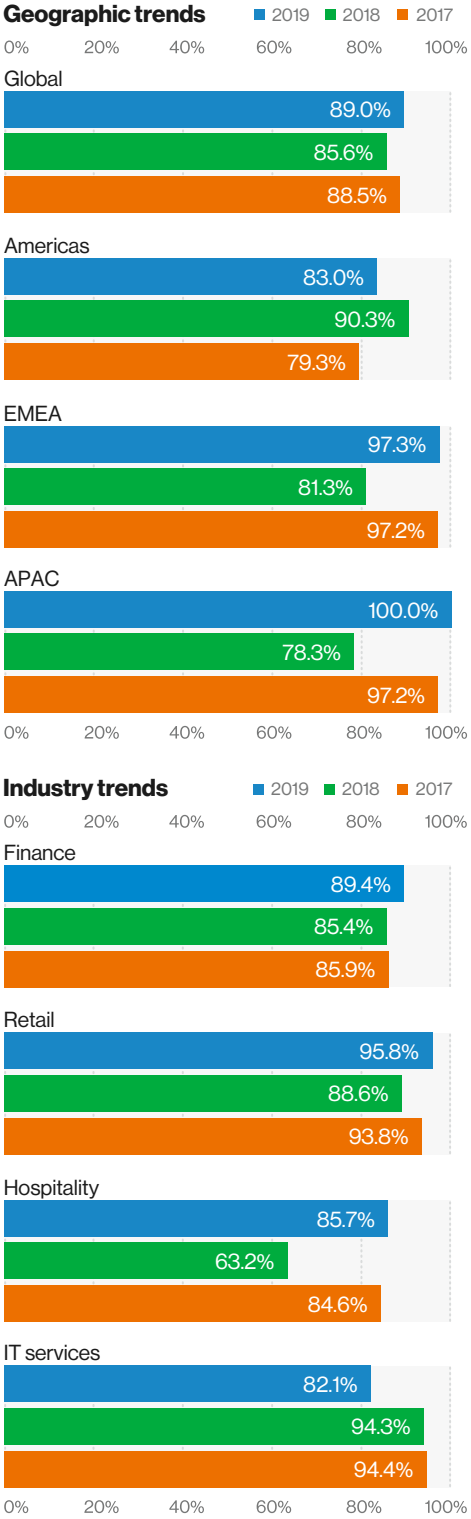


Figure 43. Control gap—Req 7

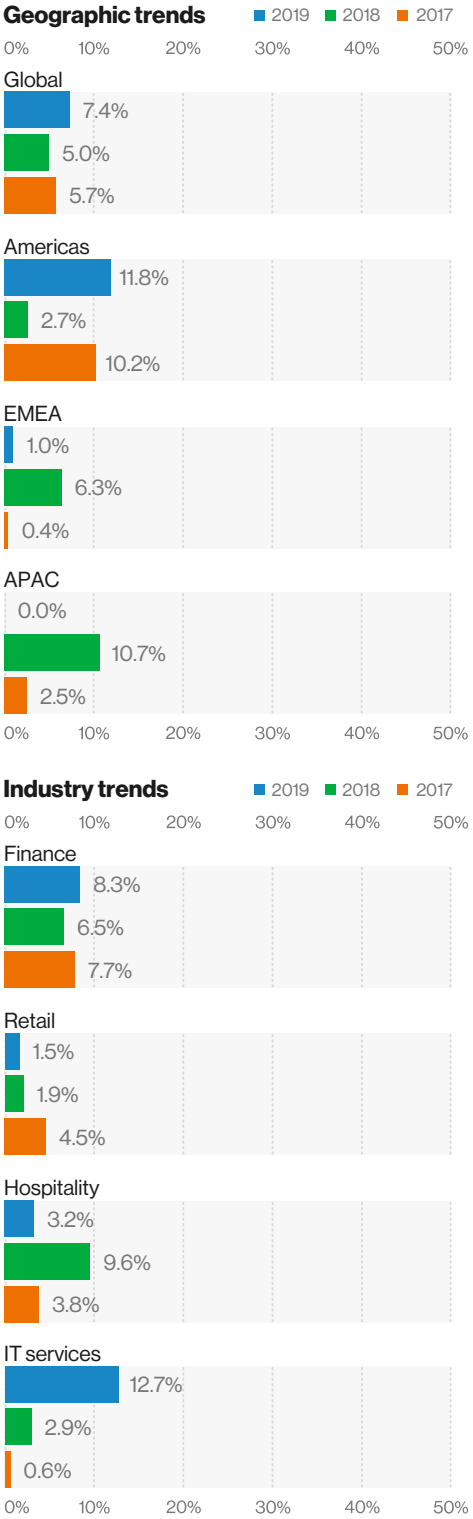
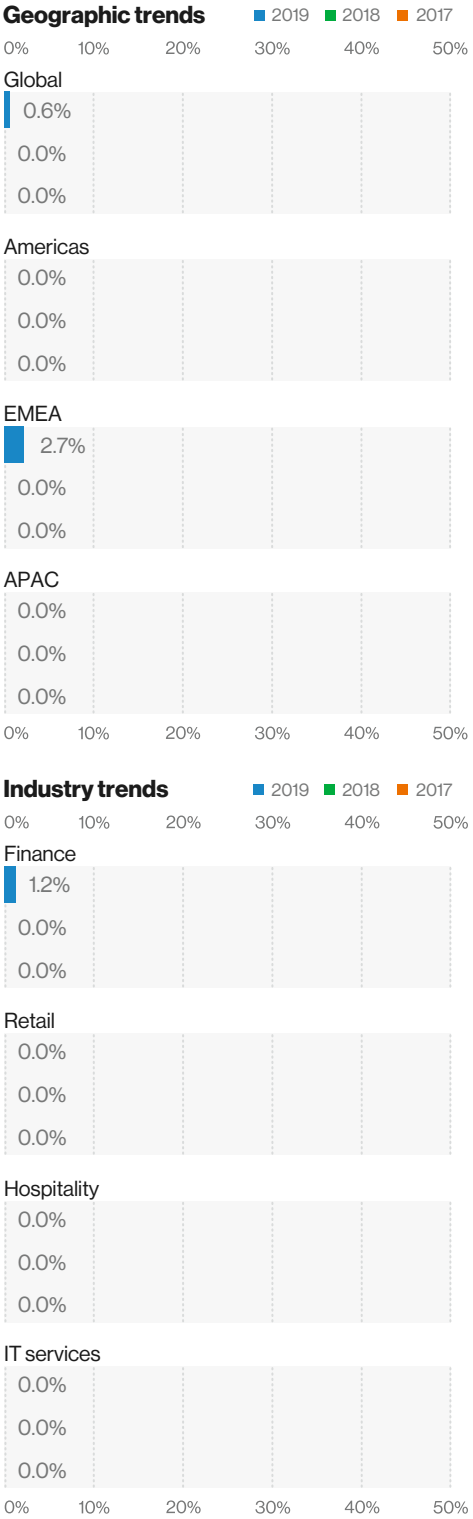


Figure 44. Compensating controls—Req 7



Payment security threats

According to the 2020 Data Breach Investigations Report (DBIR):[108]

- Retail: 99% of incidents are financially motivated, with payment data and personal credentials continuing to be prized. Web applications, rather than point-of-sale (POS) devices, are now the main cause of retail breaches
- Financial and insurance: 30% of breaches are caused by web application attacks, primarily driven by external actors using stolen credentials to get access to sensitive data stored in the cloud. The move to online services is a key factor
- Healthcare: Basic human error accounts for 31% of healthcare breaches, with external breaches at 51% percent (up from 42% in the 2019 DBIR), slightly more common than insiders at 48% (59% last year). This vertical remains the industry with the highest number of internal bad actors, due to misuse of the access granted to allow them to do their jobs
- Credential theft and social attacks, such as phishing and business email compromises, cause the majority of breaches (over 67%), specifically:
  - 37% of credential theft breaches used stolen or weak credentials
  - 25% involved phishing
  - Human error accounted for 22%

108 2020 Verizon Data Breach Investigations Report. https://enterprise.verizon.com/resources/reports/dbir/

8: Authenticate access

This requirement mandates that access to system components is identified and authenticated, requiring that each user be assigned a unique identification.

Full compliance

Requirement 8 moved three places up the rankings of full compliance, rising from ninth in 2018 to sixth in 2019. Seventy-four percent of organizations achieved full compliance at interim assessment for this requirement, representing a 9.6 pp increase compared to the previous year.

All regions reported improvements in full compliance as compared to 2018 figures, with APAC the most significant, increasing 21.8 pp to 95.7%. The EMEA region noted full compliance of 83.8%, with the Americas trailing behind at 64.9%.

Retail topped the industry sectors for compliance at 83.3%, and it reported the most significant improvement of 36.5 pp to 78.6% in 2019. Merchants outperformed service providers, achieving 82.4% full compliance at interim assessment, as compared to 72.3% for service providers. Both merchants and service providers showed increased compliance, as compared to 2018.

Control gap

A small increase in control gap was noted in 2019 of 1.3 pp to 8.2%, with this requirement slipping one place to eighth overall. All controls, with the exception of Control 8.4 and Control 8.8, reported an increasing control gap as compared to the previous year.

Both EMEA and APAC saw a reduction in control gaps in 2019, with APAC reporting just a 0.3% gap. The Americas region saw an expansion of 6.8 pp to 11.3%, the largest across all global regions.

Hospitality and retail both recorded receding control gaps. Retail reported the lowest control gap at 3% across all sectors, but it was hospitality that saw the greatest improvement in gap, lowering it 6.7 pp to 5.8%.

Merchants reduced their control gap overall, by 1.3 pp to 5.8% in 2019, while service providers reported a slight increase of 2.1 pp to 8.9%.

Compensating controls

In 2018, Requirement 8 topped the rankings for compensating controls. This requirement remains one of the most frequently compensated requirements but dropped into second place in 2019, behind Requirement 6. Compensating control use increased for this requirement in 2019, by 2.4 pp to 9.1%.

It was EMEA that most frequently implemented compensating controls for Requirement 8 at 16.2%, with APAC and the Americas reporting at 8.7% and 6.4%, respectively.

The use of compensating controls is seen across most sectors, with retail reporting the most frequent use at 16.7%. This represented a significant increase over the previous year of 14.4 pp.

Requirement 8 controls

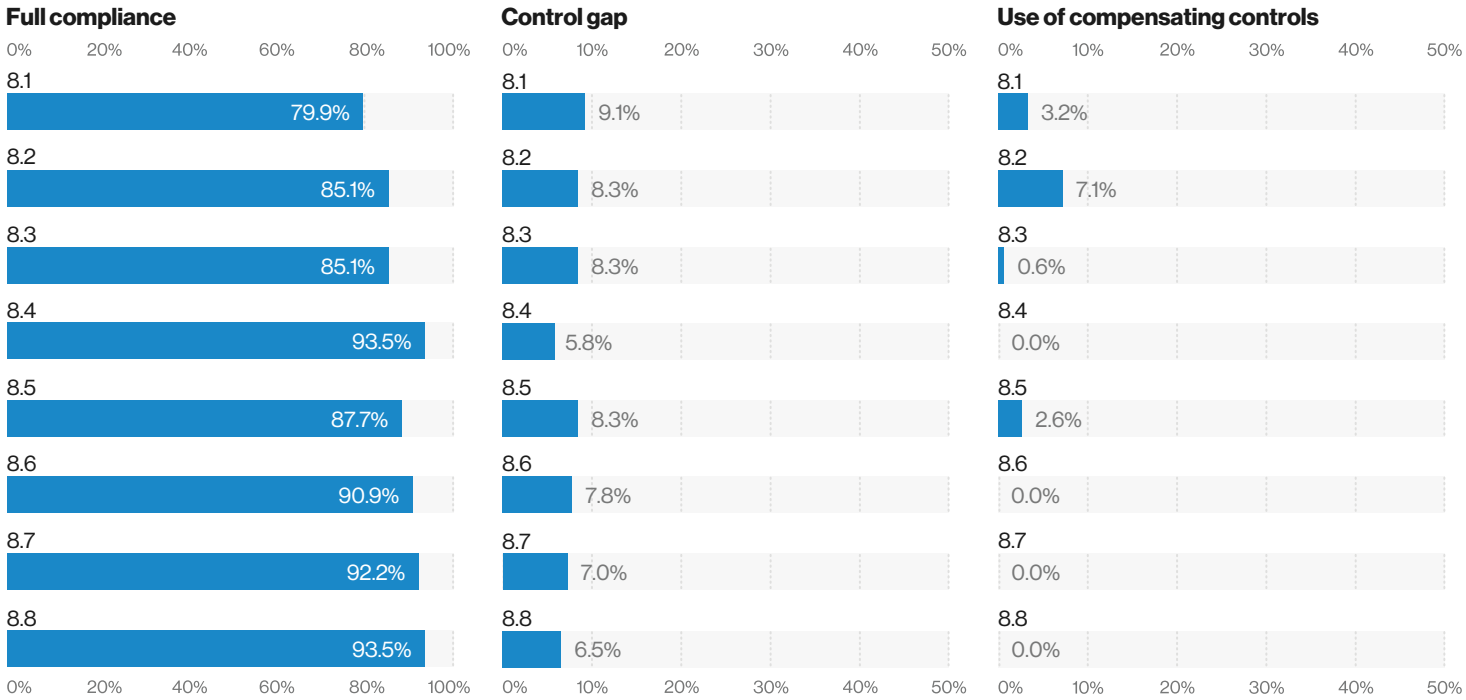
8.1	Policies and procedures for user identification
8.2	Proper user authentication management
8.3	Multifactor authentication for all remote access to CDE
8.4	Communicate authentication policies to all users
8.5	Do not use group, shared IDs
8.6	Authentication mechanisms not shared among multiple accounts
8.7	Restrict all access to any database containing CHD
8.8	Policies and procedures for identification and authentication

State of control/test procedure

Requirement 8 controls feature in both the top and bottom 10 controls in 2019. Control 8.4 and Control 8.8 share sixth position in compliance rankings, with Control 8.1 falling into the 10 worst-performing controls at 71st overall.

Here are the scores by major controls:

Figure 45. 2019 compliance performance (global averages) of Requirement 8—Authenticate access.



Industry vertical findings

All sectors reported improved full compliance figures in 2019, as compared to the previous year. The IT services and finance sectors were outperformed by retail and hospitality in 2019 for full compliance, reflected in the significant growth in compliance reported by merchants of 17.1 pp to 82.4%.

Retail and hospitality sectors both noted a reduced control gap in 2019, reducing 1.2 pp to 3.0% for retail with the small control gap; for hospitality, a 6.7 pp reduction to 5.8%. Both finance and IT services reported increasing control gaps at 2.4 pp to 9.6% and 3.7 pp to 10.0%, respectively.

Hospitality saw no compensating controls for Requirement 8 in 2019. The IT services sector noted a reduction in compensating controls of 5 pp, as compared to the previous year. Both retail and finance reported an increase. Retail reported the highest use at 16.7%, with finance following at 10.6%.

Payment data breach correlation—Req 8

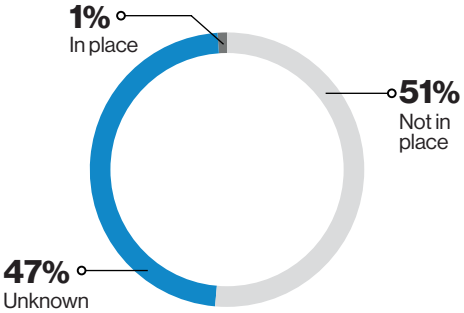


Figure 46. 2014 to 2019 PCI DSS compliance at the time of the breach

Figure 47. Full compliance—Req 8

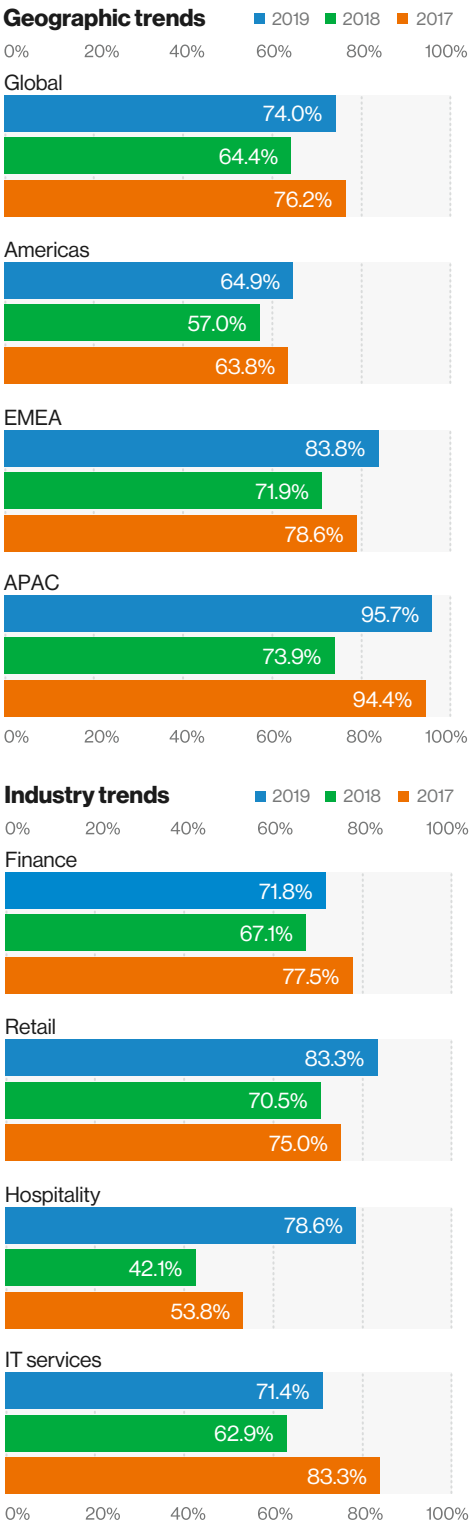


Figure 48. Control gap—Req 8

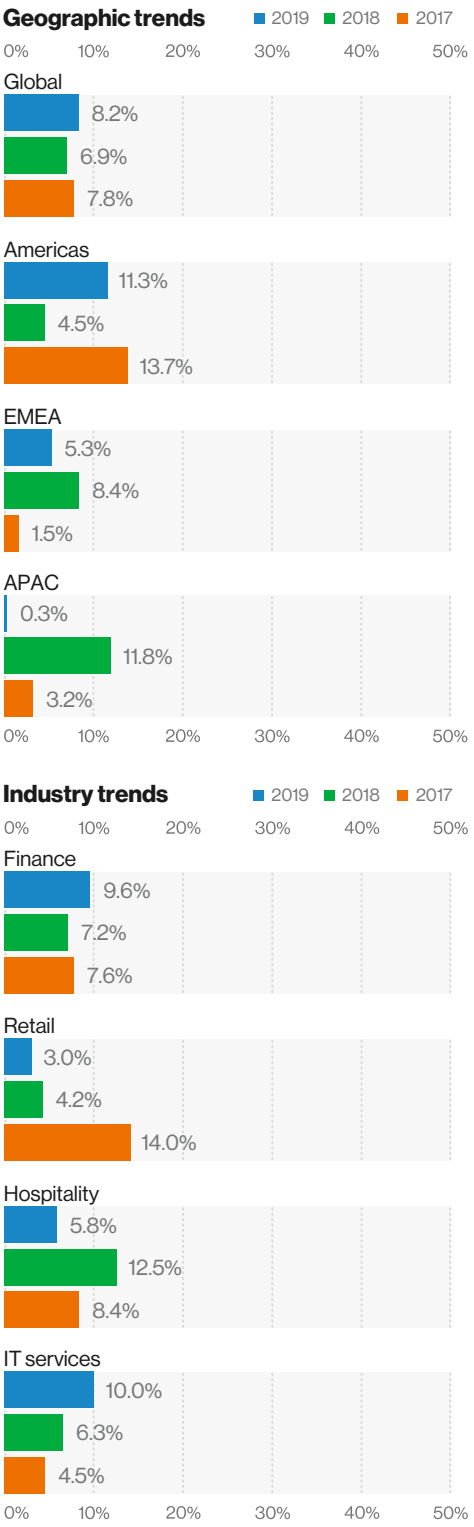
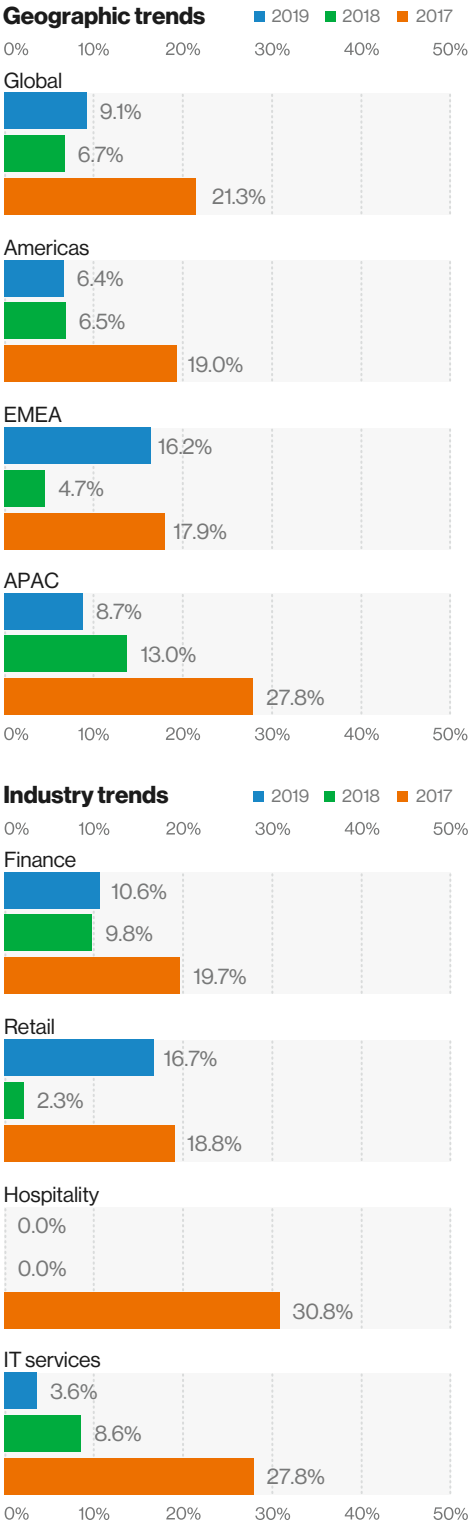


Figure 49. Compensating controls—Req 8



Global highlights

Breaches continue to span the globe, from 15,000 payment cards hacked online in Greece in January 2020 to a suspected state-sanctioned attack that impacted millions of debit cards in Iran in December 2019, to 1.3 million cards with track data (likely skimmed from retailers) in India in October 2019, to 1 million card-present transactions of undetermined origin in South Korea between May and August 2019, to 30 million cards gleaned from malware installed on in-store payment processing systems and fuel dispensers at potentially all Wawa locations in December 2019.[109, 110, 111, 112, 113, 114, 115, 116]

Password protection

Even today, password protection of databases containing payment card transaction details is not a given. In April 2020, an estimated 2.5 million card transaction records were exposed to the internet for three weeks, due to the lack of a password on the database server. Earlier, in January 2020, 6.7 million records dating back to 2013 were left online, also without a password protecting the database. In this instance, truncated and tokenized PAN was included rather than full PAN, but detailed personally identifiable information (PII) was present, sufficient to contact the cardholders and confirm the breach.

109 https://techcrunch.com/2020/04/22/paay-unencrypted-credit-card-data/
110 https://techcrunch.com/2020/01/28/cornerstone-payments-credit-cards/
111 Greece (Jan 2020): https://www.thenationalherald.com/archive_economy/arthro/greek_banks_cancel_15_000_credit_debit_cards_over_tourist_site_hack-35150/
112 Iran (State actor, such as U.S. or Israel, suspected; sophisticated infrastructure attack aligned with protests that burned local bank branches—Dec 2019): https://www.nytimes.com/2019/12/10/world/middleeast/Iran-bank-hacking-protests.html
113 https://www.timesofisrael.com/irans-banks-were-hacked-minister-admits-but-experts-doubt-his-claimed-culprit/
114 India (1.3 M with track data; skimmers suspected; selling for $100/card—Oct 2019): https://www.zdnet.com/article/details-for-1-3-million-indian-payment-cards-put-up-for-sale-on-jokers-stash/
115 South Korea (1 M, infrastructure attack suspected, rather than skimmers—selling for $40/card—Aug 2019) https://www.zdnet.com/article/breach-alert-in-south-korea-after-1m-card-details-were-put-up-for-sale-online/
116 United States (30 M, malware installed on in-store payment processing systems and fuel dispensers at potentially all Wawa locations—Dec 2019) https://krebsonsecurity.com/2020/01/wawa-breach-may-have-compromised-more-than-30-million-payment-cards/

9: Control physical access

This requirement stipulates that organizations must restrict physical access to all systems within the PCI DSS scope and all hard copies of cardholder data.

Full compliance

Full compliance with Requirement 9 increased 4.5 pp from 2018, to 81.2% in 2019, for a fourth overall ranking for the fourth consecutive year. Physical access monitoring Control 9.2 and Control 9.5 had the highest shares (92.9%), while Control 9.1 and Control 9.10 had the lowest (89.0%). Control 9.9 showed significant improvement over 2018's figure of 87.8%, coming in at 92.2% this year.

The APAC region maintained 100% full compliance, a significant improvement over the 73.9% achieved in 2018. EMEA had 83.8%, up from 75.0% in 2018. The Americas region followed with 75.5%, which was down from 2018's figure of 78.5%.

In terms of industries, retail, once again, performed poorly with this control, with just 62.5% achieving full compliance, a 1.1 pp drop since 2018. IT services performed significantly better than retail, at 82.1%, but this was still a decrease of 0.7 pp. Financial services did slightly better, at 84.7%, with an increase of 0.6 pp. Hospitality scored the highest rate of compliance, at 85.7%, a significant 22.6 pp increase over the prior year.

Service providers tended to be more fully compliant with this control (at 84.0%), while 70.6% of merchants achieved full compliance with Requirement 9.

Control gap

In 2018, Requirement 9 had the smallest control gap, at 4.5%. In 2019, that share increased by 1.1 pp, to 5.6%, and dropped the requirement's ranking to second. The control with the greatest increased gap was 9.7, with a gap of 7.5%, an increase of 3.6 pp over 2018. Control 9.5 had the smallest control gap, at 2.9%, although it also increased over the prior year by 1 pp.

The APAC region did not record a control gap for this requirement, a decrease of 8 pp over the prior year. EMEA also demonstrated a decreased control gap of 1.9%, a 3.9 pp change since 2018. Only the Americas showed an increased control gap, by 5.8 pp, of 8.5%.

The control gaps for the hospitality (4.3%) and retail (5.3%) industries were close together, with year-over-year decreases of 4.6 pp for hospitality and 1 pp for retail. The smallest control gap for this requirement was attributed to IT services, at 2.2%, improving by 1.2 pp since 2018. Financial services, unfortunately, trailed the other industries, with a gap of 7.3%, which was an increase of 4.3 pp over the prior year.

Merchants had a higher control gap than service providers for this requirement, at 7.2% vs 5.3%. Merchant performance improved by 1.6 pp over 2018; however, the service provider gaps increased by 2.3 pp, year-over-year.

Compensating controls

For the past three years, the number of companies using compensating controls for Requirement 9 has been relatively flat, oscillating between 0.8% and 0.6%, and returning to 0.8% in 2019.

Neither APAC nor EMEA used compensating controls to meet this requirement. However, in the Americas, 1.1% of companies did use alternative controls, particularly for 9.1 and 9.10 subcontrols.

The IT services, financial and retail industries did not leverage compensating controls for Requirement 9, but 7.1% of hospitality companies did.

In 2019, no service providers relied on compensating controls for this requirement, but 2.9% of merchants used them to meet the requirement.

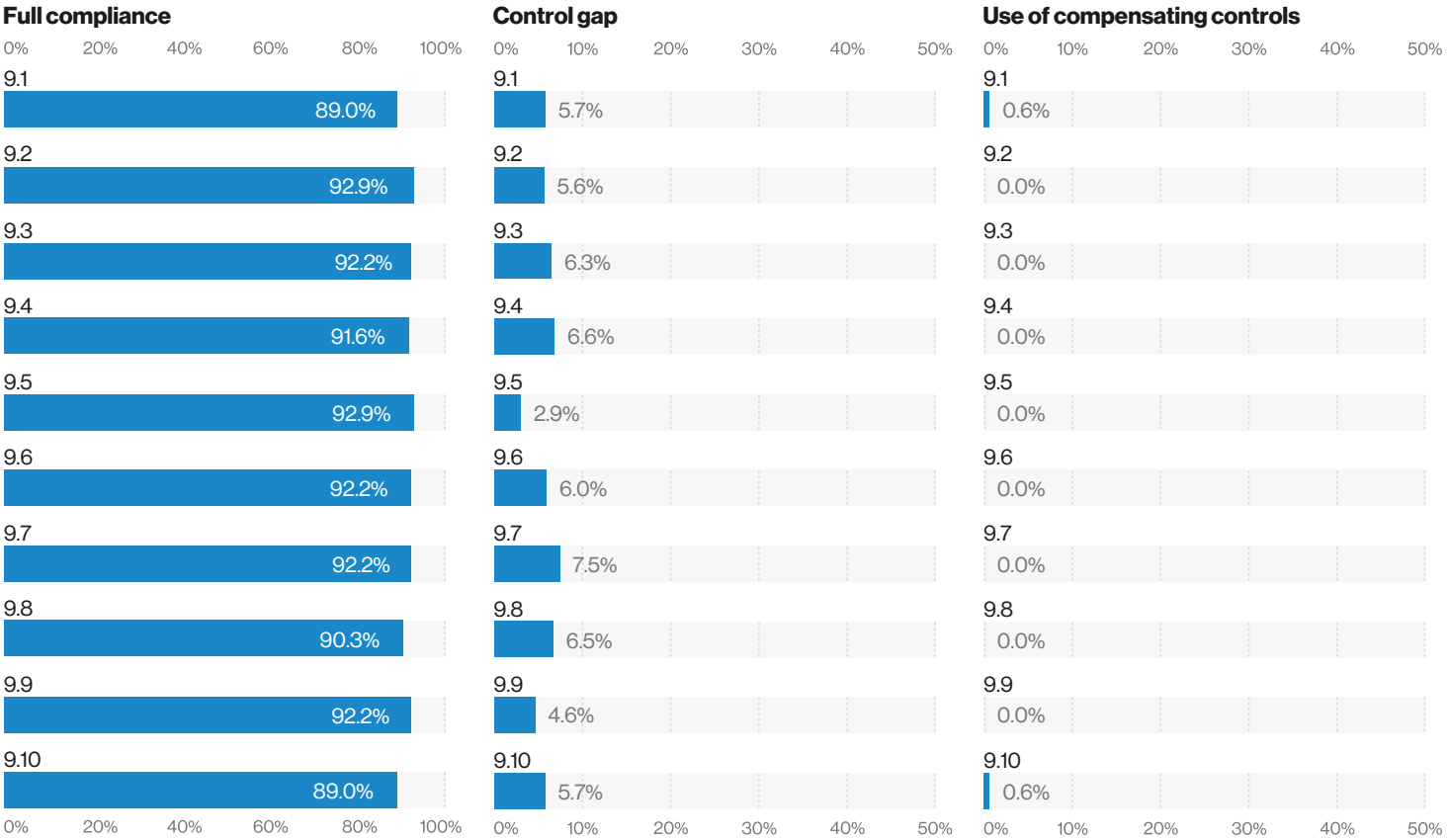
Requirement 9 controls

9.1	Appropriate facility entry controls and monitoring access of CDE
9.2	Distinguish between onsite personnel and visitors
9.3	Control physical access for onsite personnel to sensitive areas
9.4	Procedures to identify and authorize visitors
9.5	Physically secure all media
9.6	Control internal and external distribution of media
9.7	Control storage and accessibility of media
9.8	Destroy media when no longer needed
9.9	Protect data capture devices; tampering/ substitution
9.10	Documented policy restricting physical access to CHD

State of control/test procedure

Six Requirement 9 controls (9.2, 9.3, 9.5, 9.6, 9.7 and 9.8) appear in the top-20 list of most-compliant controls.

Figure 50. 2019 compliance performance (global averages) of Requirement 9—Control physical access.



Industry vertical findings

IT services had the smallest control gap, at 2.2%, and a third-best full compliance showing, at 82.1%, but with a slight performance dip in full compliance and a small improvement in the control gap since 2018.

Financial services had the second-highest full compliance result, with 84.7%, an outcome consistent with 2018 numbers. However, the control gap increased by over 4 pp to 7.3% in 2019.

Hospitality achieved the highest rate of full compliance, with 85.7%, and a significant performance increase of over 22 pp since 2018. Its control gap was also the second lowest, at 4.3%, with a year-over-year decrease of almost 5 pp.

Retail had the lowest rate of full compliance, at 62.5%, and the second-highest control gap, at 5.3%. Year-over-year changes were around 1 pp for each compliance measure.

Service providers outperformed merchants in both full compliance and control gap, by having the higher full compliance ratio (84.0% vs 70.6%) and the smaller control gap (5.3% vs 7.2%).

Payment data breach correlation—Req 9

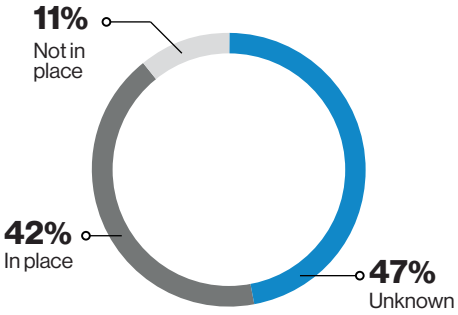


Figure 51. 2014 to 2019 PCI DSS compliance at the time of the breach

Figure 52. Full compliance—Req 9

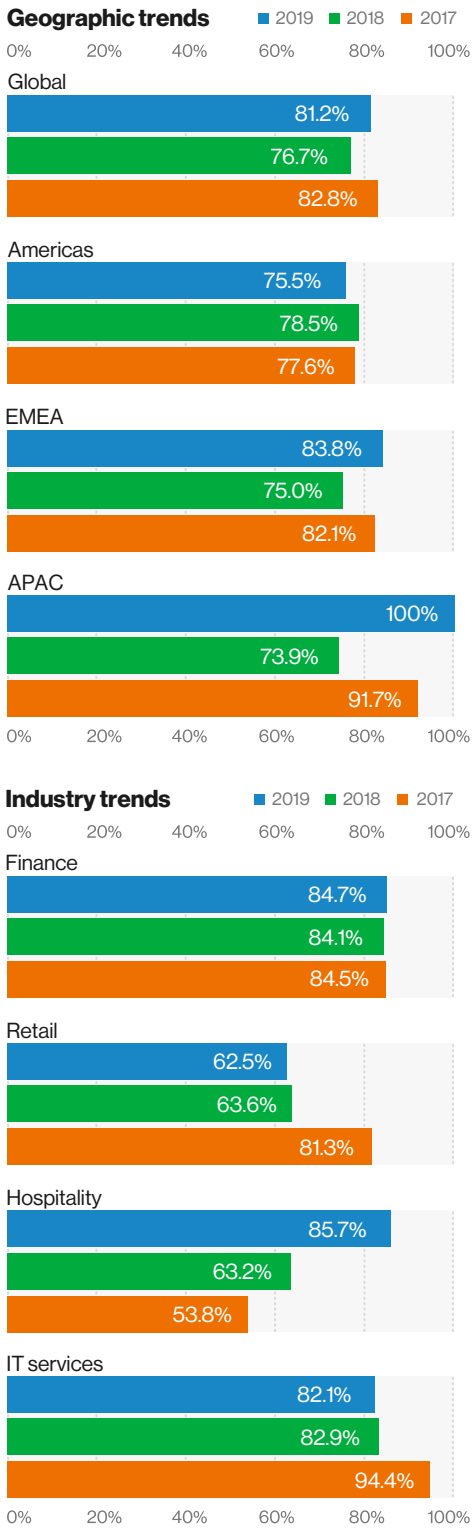


Figure 53. Control gap—Req 9

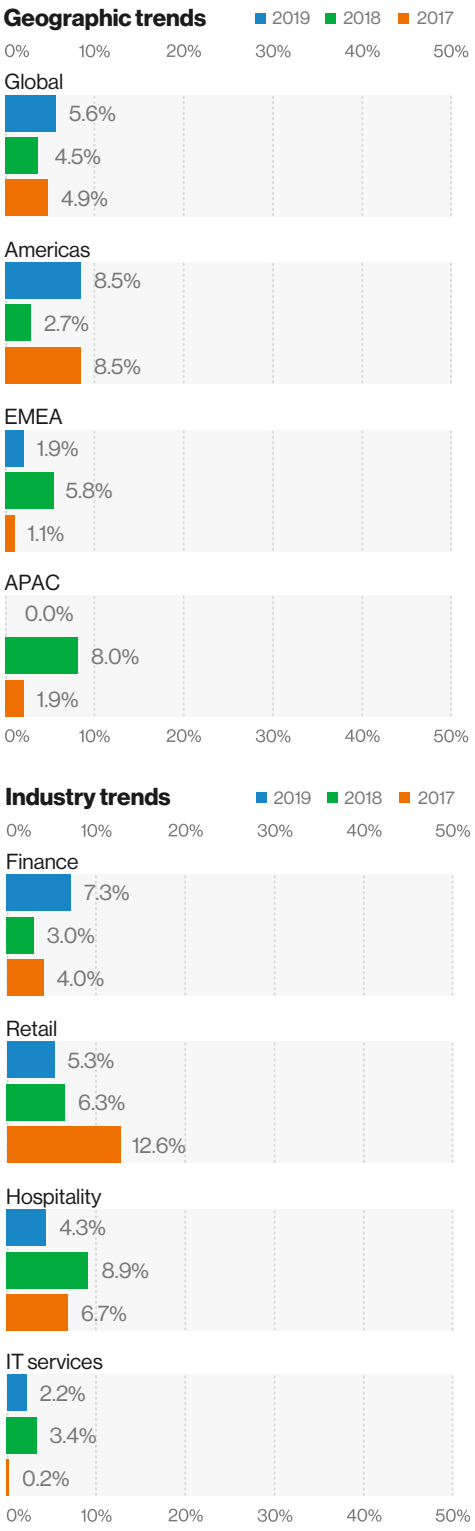
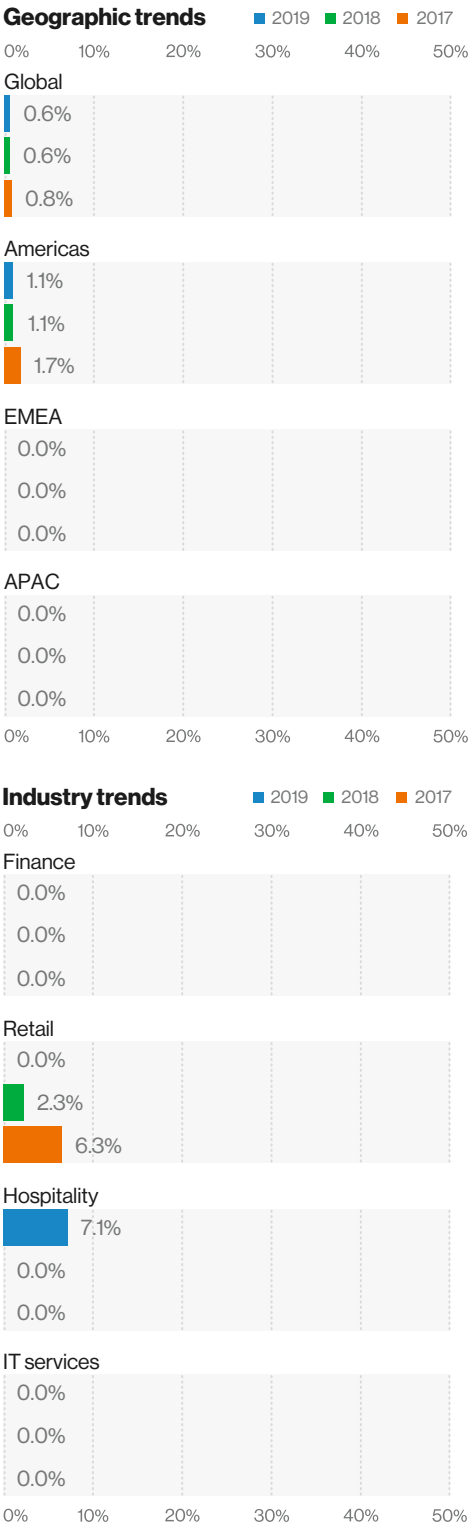


Figure 54. Compensating controls—Req 9



Skimmers are not just found on physical payment terminals. They show up online too, using different attack vectors. Typically, they are grouped under “Magecart malware,” a nod to the first such attacks, which were found on Magento shopping cart platforms. Magecart attacks inject malicious JavaScript code on merchant-managed e-commerce sites and third-party payment pages. They can target the supply chain, as occurred in the Volusion e-commerce platform data breach, or they can appear directly on a merchant’s payment page as injected iFrames, for example. The malicious code can be found in third-party libraries, stenographic images or third-party add-ons. The commonality among the variations is the siphoning of payment card data as online transactions are occurring. With so many possible attack vectors and an increase in the number and creativity of the attacks, what can merchants and service providers do to protect themselves and their customers? Reinforce the basics of patching (Control 6.2), file integrity monitoring (Control 11.5) and logging (Control 10). Bolster detection capabilities by scanning, assessing and testing web applications and critical system components for vulnerabilities (Controls 6.5, 6.6, 11.2, 11.3). Strengthen prevention through applying hardening standards (Control 2.2), anti-malware software (Control 5), identity and access management (Controls 7 and 8), IDS/IPS (Control 11.4), and service provider management (Control 12).[117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133]

117 https://www.fortinet.com/blog/threat-research/payment-card-details-stolen-magecart.html
118 https://www.bleepingcomputer.com/news/security/magecart-attackers-steal-card-info-from-focus-camera-shoppers/
119 https://www.perimeterx.com/resources/blog/2019/latest-magecart-hit-needs-new-approach/
120 Robert Dyas (U.K. retailer; online card skimmer): https://www.theregister.co.uk/2020/04/22/robert_dyas_card_skimmer/
121 PinnacleCart server-side skimmers: https://blog.sucuri.net/2020/04/pinnaclecart-server-side-skimmers-and-backdoors.html
122 Tupperware website: https://www.bleepingcomputer.com/news/security/tupperware-site-hacked-with-fake-form-to-steal-credit-cards/
123 Volusion Magecart attack: https://geminiadvisory.io/breached-volusion-card-data-surfaces-in-dark-web/
124 Cheney Bros. Inc., crafty web skimming domain: https://krebsonsecurity.com/2020/03/crafty-web-skimming-domain-spoofs-https/
125 Fake content delivery network scam: https://blog.malwarebytes.com/threat-analysis/2020/02/fraudsters-cloak-credit-card-skimmer-with-fake-content-delivery-network-ngrok-server/
126 General awareness: https://www.cnbc.com/2020/01/31/fbi-warns-of-new-online-threat-to-personal-credit-card-info.html
127 https://www.cnbc.com/2020/01/31/e-skimming-cyberattack-is-growing-along-with-online-shopping.html
128 https://securityboulevard.com/2020/01/why-iframes-alone-wont-stop-web-skimming-attacks-from-stealing-customer-data/
129 https://www.bankinfosecurity.com/e-commerce-skimming-attacks-evolve-into-iframe-injection-a-12507
130 https://www.pcisecuritystandards.org/pdfs/PCISSC_Magecart_Bulletin_RHISAC_FINAL.pdf
131 https://blog.pcisecuritystandards.org/beware-of-online-skimming-threats-during-the-covid-19-crisis
132 https://www.riskiq.com/what-is-magecart/
133 Zen Cart skimmer: https://blog.sucuri.net/2020/01/zen-cart-paypal-skimmer.html

10: Track and monitor access

This requirement covers the creation and protection of information that can be used for the tracking and monitoring of access to all systems in the PCI DSS scope and synchronization of all system clocks.

Full compliance

Full compliance with Requirement 10 did not shift very much (just a small decrease of 0.4 pp) between 2018 and 2019. And with a share of 66.2% in 2018, it maintained its rank of eighth among the 12 requirements. The control with the lowest adherence was Control 10.5 (log reviews), while Control 10.9 (policies and procedures awareness) had the highest adherence. This is concerning, considering log reviews are a detective control that help significantly with reconstructing (and scoping) a security event.

The APAC region had 91.3% full compliance, while EMEA and the Americas had 78.4% and 55.3%, respectively.

Moving to industries, financial services came in last for this requirement, with just 63.5% of organizations in full compliance. This represents a decrease of 3.5 pp from the prior year. The retail sector had the largest negative variance, with a drop of 15.2 pp from 2018 to 66.7% in 2019. Hospitality had a gain in the opposite direction, with a 13.5 pp increase to 71.4% in 2019. IT services had the best score and improvement, with 75.0% and an increase of 17.9 pp.

Merchants outperformed service providers by just a few percentage points: 70.6% vs 64.7%.

Control gap

The Requirement 10 control gap increased year-over-year by 0.4 pp, to 9.2%, with a rank of 10 out of 12. The greatest gap was attributed to Control 10.1 (12.3%) and the smallest to Control 10.9 (7.8%).

Only 0.3% of companies in the APAC region had a control gap for this requirement. In contrast, the control gap was 6.3% in EMEA and 12.6% in the Americas. APAC demonstrated the greatest improvement, dropping its control gap 18.1 pp from 2018 to nearly 0% in 2019. The Americas region saw a year-over-year uptick in the control gap by 3.9 pp; EMEA remained relatively flat with a 0.8 pp increase.

The retail and IT services industries had the smallest control gaps for this requirement, at 5.3% and 6.8%, respectively. Hospitality and financial services were at the other end of the spectrum, with control gaps of 10.2% and 11.2%.

Merchants and service providers nearly tied in their control gaps, scoring 9.4% and 9.3%. Year-over-year, the merchant percentage increased by 2.3 pp, while the service provider percentage stayed essentially flat (a decrease of just 0.1 pp).

Compensating controls

Between 2018 and 2019, the use of compensating controls to meet this requirement decreased from 2.2% to 1.9%. The ranking remained at sixth for the second year in a row.

The APAC region did not show the use of compensating controls to meet this requirement. In EMEA, 2.7% of companies relied on compensating controls, while American companies did so 2.1% of the time.

In 2019, the IT services, hospitality and retail industries didn't leverage compensating controls for Requirement 10, a shared decrease of 1.9 pp over the prior year. Financial services, however, did see a 2.3 pp increase in the use of compensating controls in 2019, to 3.5% of companies.

No merchants relied on compensating controls for this requirement in the past year, but 2.5% of service providers did use them to meet the requirement.

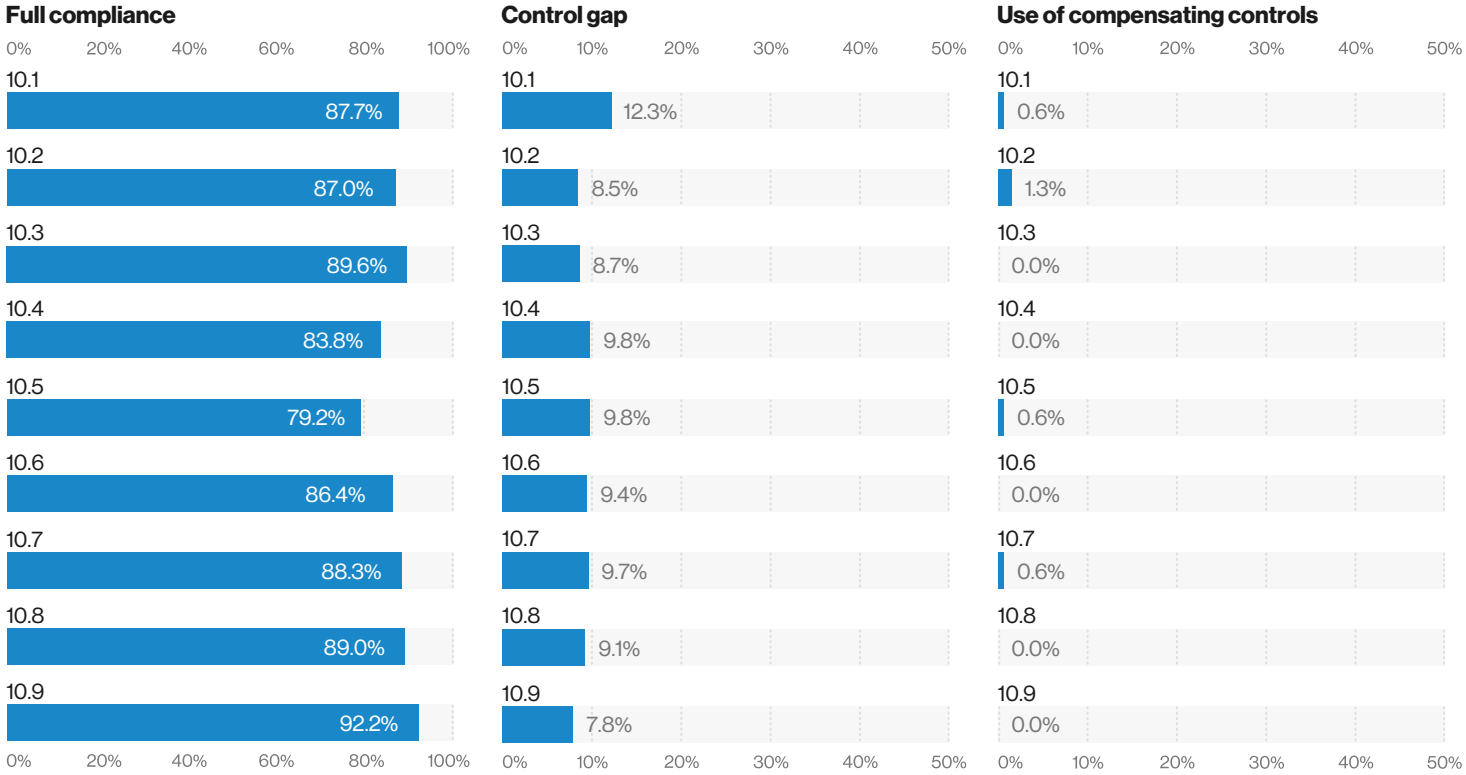
Requirement 10 controls

10.1	Audit trails linking access to individual users
10.2	Automated audit trails to reconstruct events
10.3	Record user ID, date and time events
10.4	Time-synchronization technology
10.5	Secure audit trails so they cannot be altered
10.6	Review logs to identify anomalies or suspicious activity
10.7	Retain audit trail history for at least one year
10.8	Reporting of failures of critical security control systems
10.9	Policies and procedures for monitoring all access

State of control/test procedure

Of all the Requirement 10 base controls, only Control 10.5 appeared in the bottom-20 list of least compliant controls, as the 18th least-compliant base control.

Figure 55. 2019 compliance performance (global averages) of Requirement 10 — Track and monitor access.



Industry vertical findings

IT services was at or near the top of full compliance and control gaps, with a leading 75.0% full compliance rating and a second-best 6.8% control gap.

Financial services ranked last in terms of full compliance with 63.5%, and had the largest control gap with 11.2%.

Like IT services and financial services, retail and hospitality also took separate directions: Retail posted a significant year-over-year drop in full compliance, to 66.7%, while hospitality demonstrated a significant increase in full compliance, to 71.4%. With control gaps, the roles reversed. Retail had the smallest control gap at 5.3%, and hospitality had one of the largest control gaps, at 10.2%.

The net effect of these opposing performances in each of the main merchant industries and each of the main service provider industries was a near-tie in control gap results for merchants and service providers, and a slightly better (by 6%) full compliance showing for merchants over service providers.

Payment data breach correlation — Req 10

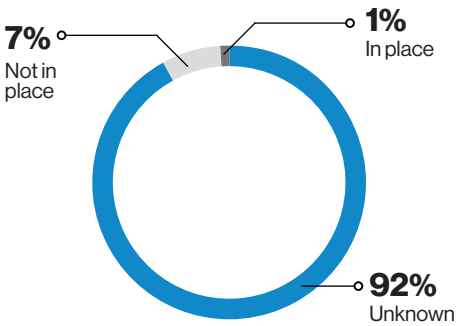


Figure 56. 2014 to 2019 PCI DSS compliance at the time of the breach

Figure 57. Full compliance—Req 10

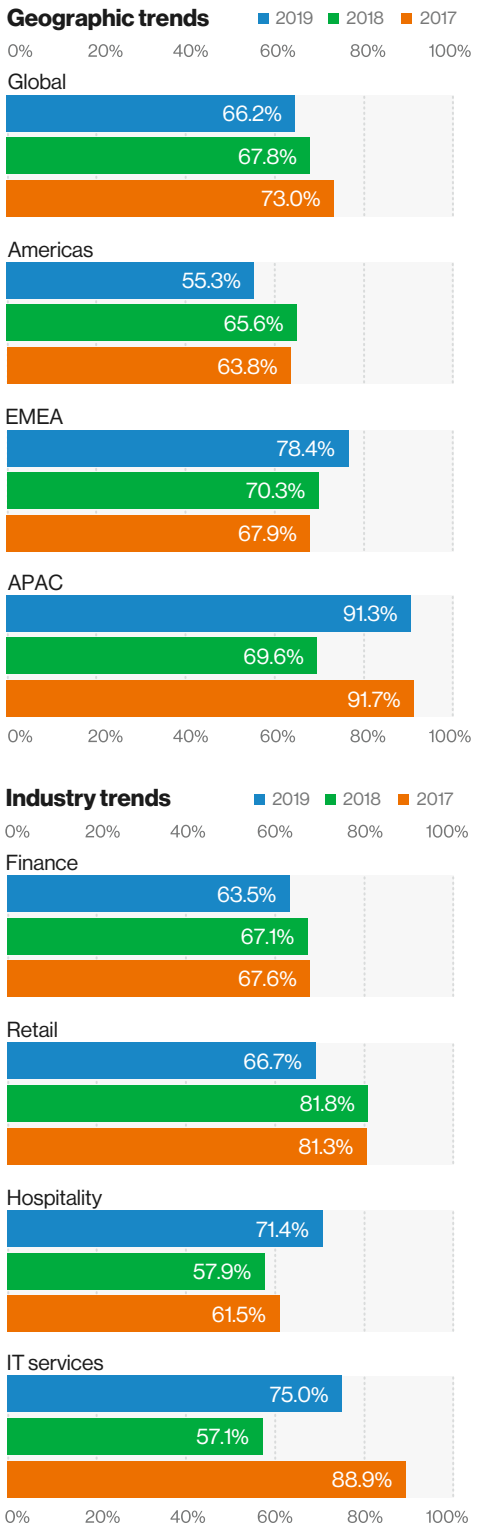


Figure 58. Control gap—Req 10

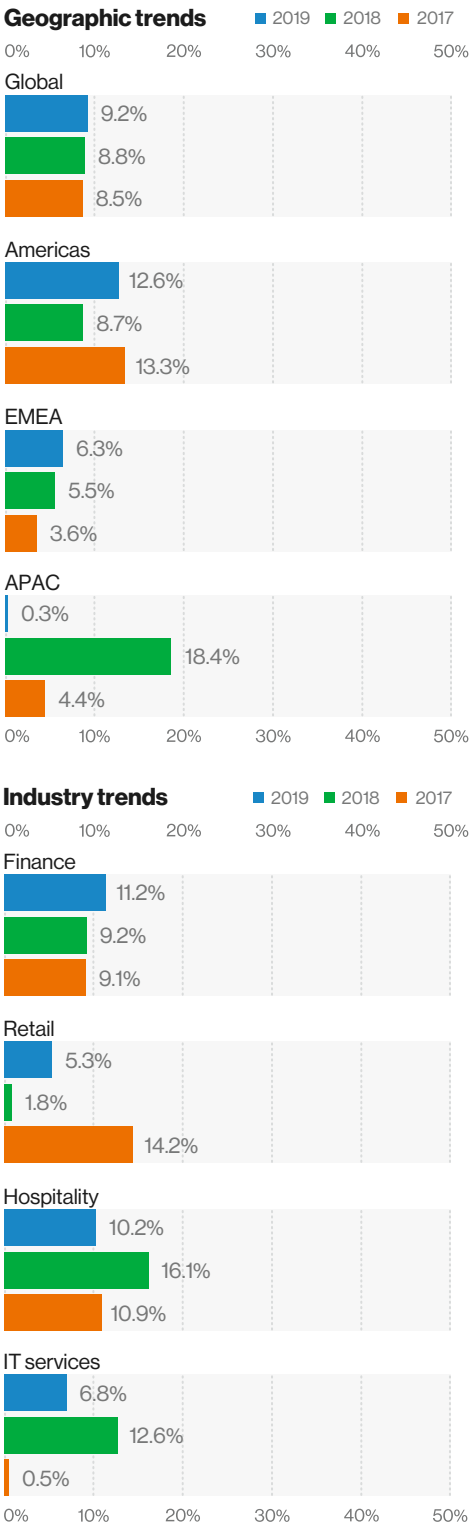
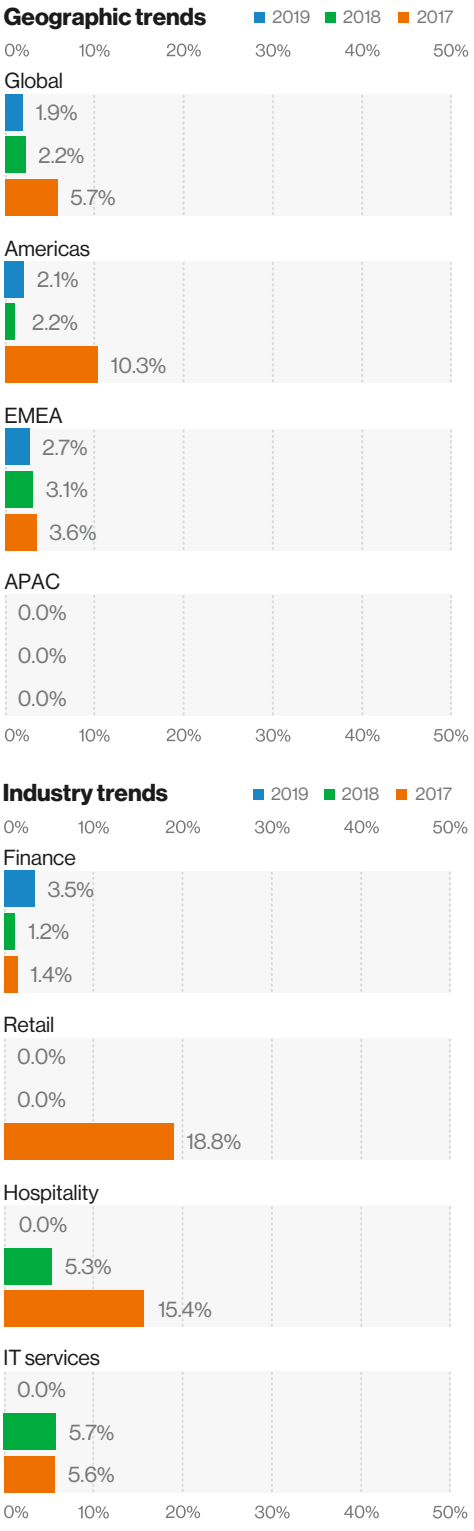


Figure 59. Compensating controls—Req 10



11: Test security systems and processes

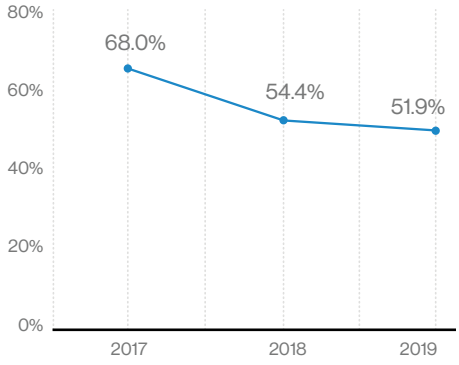
This requirement covers the use of vulnerability scanning, penetration testing, file integrity monitoring and intrusion detection to ensure that weaknesses are identified and addressed.

Full compliance

For the 10th year in a row, Requirement 11 posed the most difficulty for companies trying to achieve full compliance. Those lowest rates of compliance are getting steadily worse, as shown in the graphic below. As in years past, Control 11.2 (scanning) and Control 11.3 (penetration testing) were the lowest-scoring controls. When the data point starts below the 70% mark and continues to decline each year, the trend is approaching very dangerous territory. While these are not easy controls to put in place, they can show value in improving the security posture of the organization, and potentially even staving off a breach if the results are acted on in a timely manner.

Figure 60.

Full compliance over time



For the regional data, APAC led with 95.7% full compliance, a significant improvement over the figure of 69.6% in 2018 (although they still maintained the leader position of the regions for full compliance). EMEA and the Americas followed with 67.6% and 35.1%, respectively.

Looking at the industries, retail struggled the most with this requirement, at 41.7%, with a decrease of 19.7 pp since 2018. Financial services and IT services performed slightly better, at 50.6% and 57.1%, respectively. These two industries stayed relatively constant between 2018 and 2019, with a performance decrease of 1.9 pp for financial services and a performance increase of 2.9 pp for IT services. Hospitality had the largest rate of full compliance, at 78.6%. This share represents an improvement of 31.2 pp over the prior year.

Merchants outperformed service providers by 61.8% to 48.7%, with an improvement of 0.9 pp for merchants and a drop of 3.5 pp for service providers.

Requirement 11 controls

11.1	Test for the presence of wireless access points
11.2	Run network vulnerability scans
11.3	Implement penetration testing
11.4	Use intrusion-detection systems
11.5	Deploy change-detection mechanism
11.6	Documented procedures for monitoring and testing

The trouble with Control 11.2

Too many organizations fail to design, implement and maintain a process that meets the requirements of Control 11.2.

The PCI DSS requires that passing vulnerability scans be obtained on a quarterly basis – internal and external (as applicable). Achieving this result requires that assets in-scope for PCI security are reconciled against an accurate asset inventory (Control 2.4). Next, as new systems are brought online and others decommissioned, scans must be updated to reflect these changes.

Organizations should not, but do, forget that it is required to rescan to verify that the high-risk vulnerabilities (as defined in Control 6.1) have been remediated.

Vulnerability data is typically difficult to consume due to its volume and the need to verify false positives.

Common operational issues associated with Control 11.2 include:

- Delaying until the month before the passing vulnerability scan is due to run the scan, which often leads to the discovery of complex remediation issues that are not possible to resolve within 30 days as required for "Critical" and "High" vulnerabilities
- Changes in staff responsibilities and lack of oversight
- Antiquated and end-of-life (EOL) technologies still present within the assessed environment that have no further support (including "extended" support) availability

Clearly defined documented processes and procedures with assigned roles, responsibilities and accountability need to be in place to effectively manage the battle with the unending appearance of newly released threats.

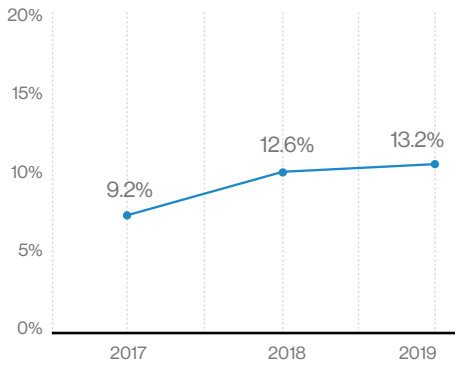
Control gap

In keeping with the trend noted for full compliance, the control gap shares for Requirement 11 have steadily increased over the past three years, as shown in Figure 61 below. The controls with the greatest control gaps are 11.2 – Vulnerability scans (17.1%); 11.3 – Penetration testing (13.7%); and 11.5 – Change-detection mechanism (12.8%).

The APAC region had the lowest control gap, at 0.5%. EMEA and the Americas followed, with 8.1% and 18.4%, respectively.

Figure 61.

Control gap over time



Meanwhile, the retail industry had the smallest control gap for this requirement, at 9.0% with a 2.6 pp increase over 2018. IT services remained relatively constant, with a control gap of 12.8% and an increase of 1.2 pp since 2018. Financial services also stayed somewhat steady, with a control gap of 14.6% and a year-over-year increase of 1 pp. Hospitality was the only industry that improved in performance by shrinking its control gap 10.9 pp, to 13.5%.

Merchants demonstrated a smaller control gap than service providers, at 12.0% and 13.7%, respectively. No significant changes were noted, year-over-year, as the merchant percentage increased by 0.8 pp, and the service provider percentage by 0.7 pp.

Compensating controls

Overall, compensating control usage dropped year-over-year globally by 3.4 pp, to 3.2% of companies. No APAC companies used compensating controls for this requirement, while 10.8% of EMEA companies and 1.1% of American companies used compensating controls. The use of compensating controls increased by 4.6 pp in the EMEA region and decreased by 7.5 pp in the Americas.

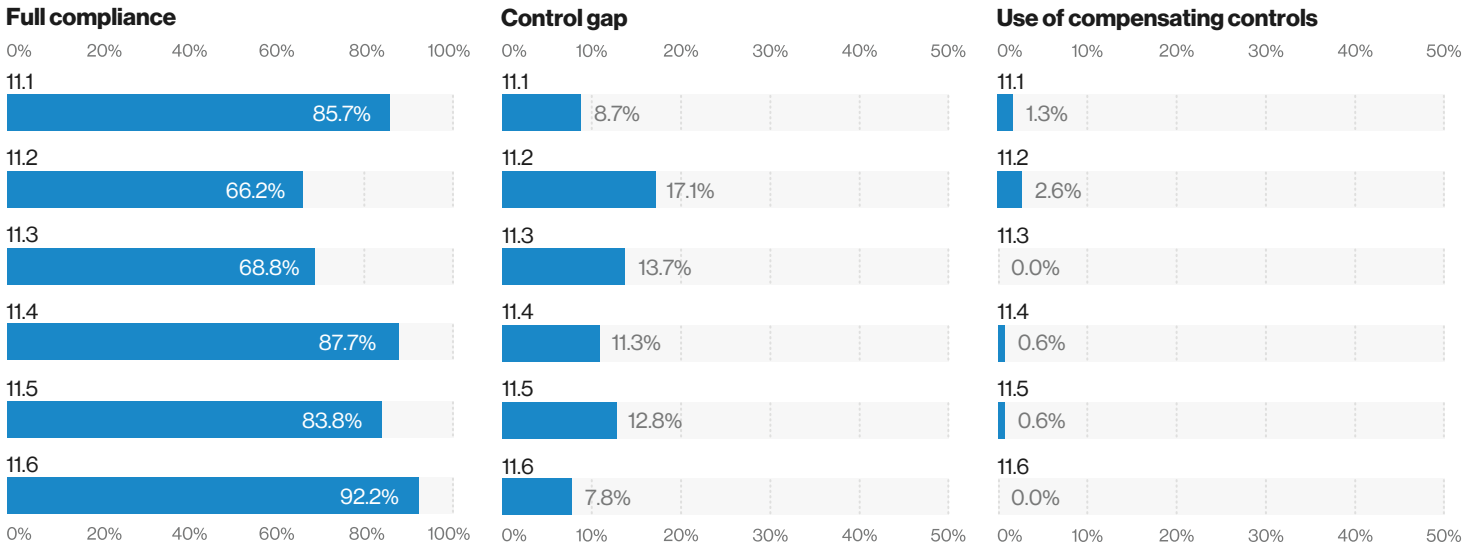
No IT services, hospitality or retail companies used compensating controls to meet Requirement 11 in 2019, with decreases ranging from 4.5 pp to 5.7 pp. Financial services, however, also experienced a 2.7 pp decrease in the use of compensating controls, to just 5.9% of companies.

No merchants relied on compensating controls for this requirement in the past year, but 4.2% of service providers used them to meet Requirement 11, a 3.3 pp decrease over the prior year.

State of control/test procedure

No Requirement 11 base control appears in a top-20 list of compliant controls. But Control 11.2 (scanning) and Control 11.3 (penetration testing) grab bottom-20 honors, with Control 11.2 the least compliant and Control 11.3 the second-least compliant (out of 79 total base controls).

Figure 62. 2019 compliance performance (global averages) of Requirement 11—Test security systems and processes.



Industry vertical findings

In terms of full compliance, while retail had the poorest showing at 41.7%, it also had the smallest control gap. Thus, more retail companies are failing the whole of Requirement 11, but fewer controls are the sources of those failures.

Although hospitality had one of the higher control gaps (at 13.5%), it also showed the most improvement in reducing that control gap by almost 11 pp over the past year. That improvement trend continued with full compliance, where hospitality had the highest adherence rate of 78.6%, with a performance increase of over 31 pp.

Financial services and IT services held fairly steady in both full compliance and control gaps. In full compliance, they were in the 50% to 60% range, with between 2.0 pp and 3.0 pp, year-over-year. Their control gaps increased by about 1 pp, to 14.6% and 12.8%, respectively.

Merchants outperformed service providers in both full compliance and control gap. The full compliance difference was 13.1% in favor of merchants and the control gap was 1.7% smaller for merchants, due to the results from the retail and hospitality sectors.

Payment data breach correlation—Req 11

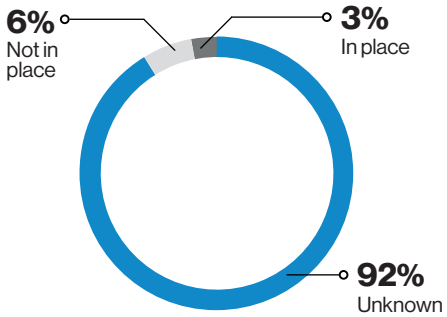


Figure 63. 2014 to 2019 PCI DSS compliance at the time of the breach

Figure 64. Full compliance—Req 11

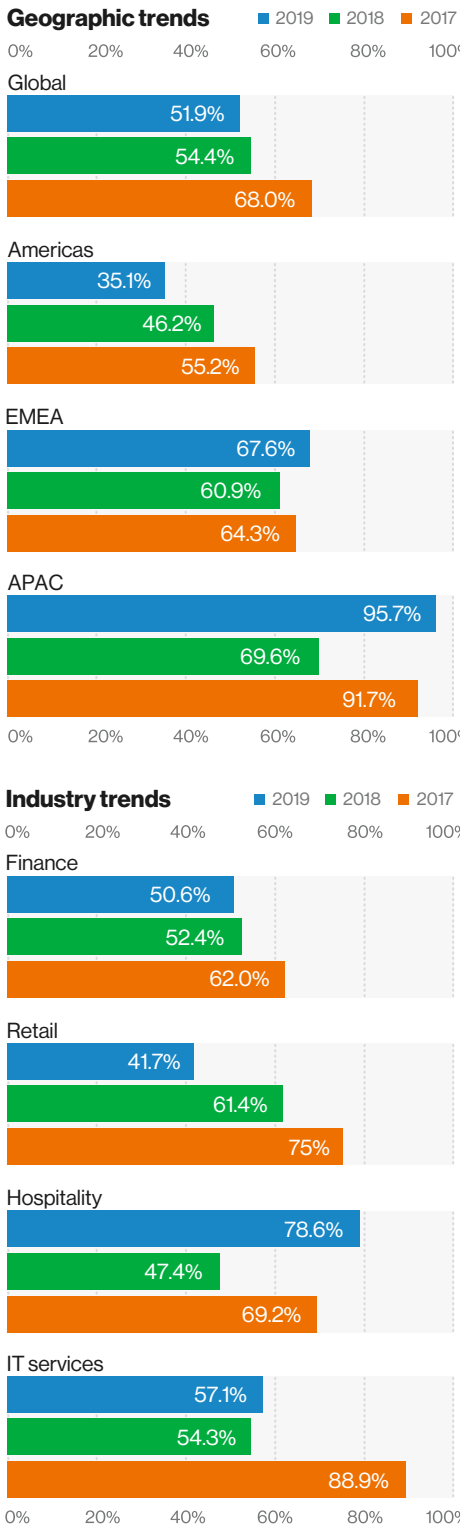


Figure 65. Control gap—Req 11

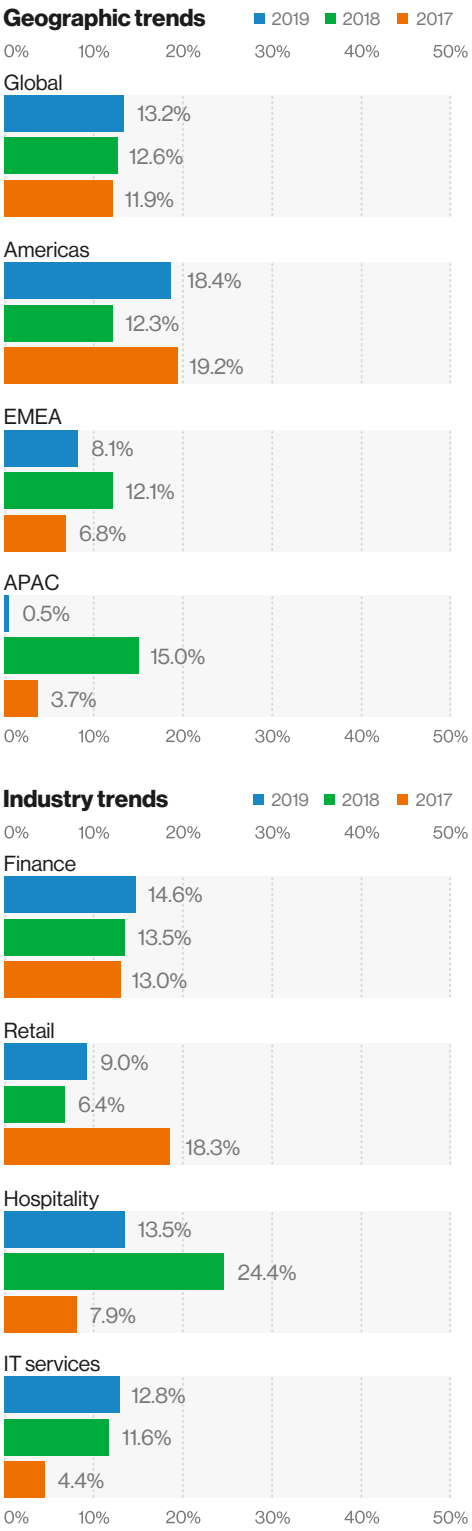
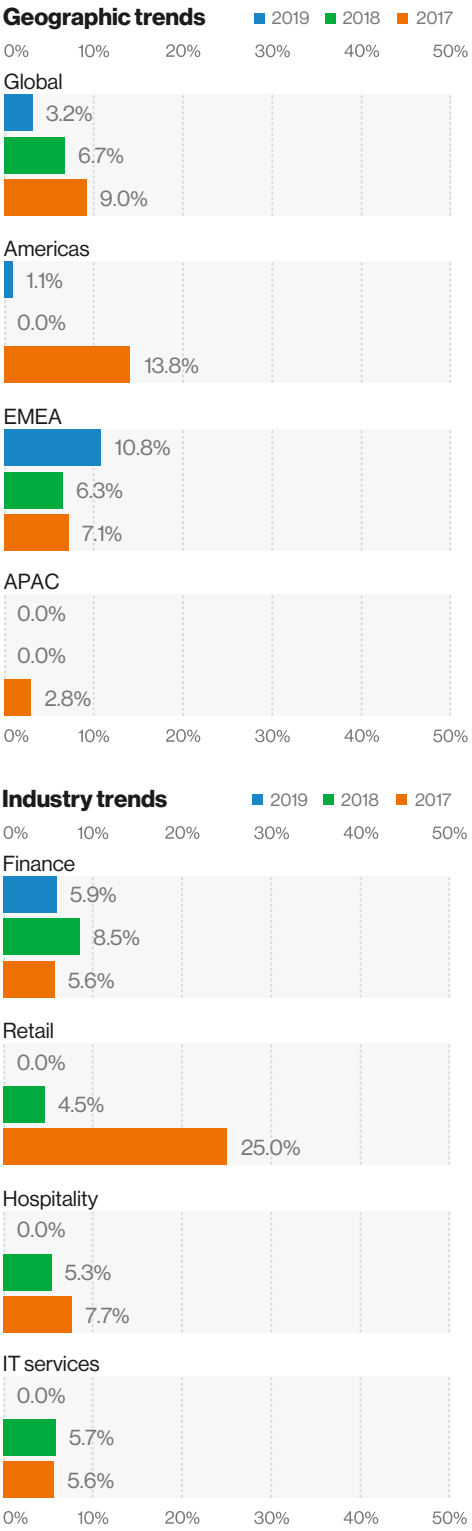


Figure 66. Compensating controls—Req 11



Security testing maturity

The successful design, implementation, monitoring and evaluation (DIME)—followed by improvement—of a security vulnerability management team depends on several organizational processes and capabilities that need to be developed toward higher levels of maturity. A 2019 study on security maturity by Orange Defense (formerly SecureLink) found that, in most organizations, security strategy is absent or lacks maturity. Respondents were asked the following:[134]

Do you have a vulnerability management process?

0.	Absent	51%
1.	Ad hoc	20%
2.	Partial	10%
3.	Documented	3%
4.	Software supported	13%
5.	Regularly reviewed	5%

Is there a penetration testing program in place?

0.	Absent	51%
1.	Ad hoc	21%
2.	Partial	15%
3.	Documented	3%
4.	Software supported	5%
5.	Regularly reviewed	5%

134 Richard Jones, CISO, Orange Cyberdefense 2019 Security Maturity Report, Orange Cyberdefense (formerly SecureLink), 2019. https://orangecyberdefense.com/global/white-papers/2019-security-maturity-report/

12: Security management

This requirement demands that organizations actively manage their data protection responsibilities by establishing, updating and communicating security policies and procedures aligned with the results of regular risk assessments.

Full compliance

Full compliance with Requirement 12 decreased almost 8 pp, from 62.2% in 2018 to 54.5% in 2019. The ranking also decreased from 10th to 11th place.

The APAC region led with 100% compliance, while EMEA attained 59.5% full compliance and the Americas achieved 41.5%. The controls that caused the most difficulty were Control 12.2 (risk assessments), Control 12.6 (security awareness training) and Control 12.8 (service provider management).

Much of the drop in full compliance for Requirement 12 appears to be linked to the financial services and retail sectors. Retail, for instance, had a decrease in performance of 15.2 pp, to 41.7%. Financial services also showed a significant decrease of 11.8 pp to 55.3%, as compared to 2018's report. Hospitality improved its performance by 4.5 pp, for 57.1% full compliance. IT services had the best full compliance rate at 64.3%, showing a 1.4 pp increase.

With most retail organizations driving merchant results and financial services behind service provider numbers, a drop in full compliance for merchants and service providers is to be expected: a 10.9 pp year-over-year decrease to 50% for merchants and a decrease of 7.2 pp to 55.5% for service providers.

Control gap

This year, the control gap decreased by 0.5 pp, to 8.5%. The APAC region had a 0.0% control gap, while EMEA showed a 5.0% gap and the Americas had 11.9%.

In industries, the retail sector had the smallest control gap for this requirement, at 4.6%, with a 2 pp decrease since 2018. IT services also showed improvement, by dropping 1.2 pp to 7.0%.

Not performing as well, financial services increased its control gap slightly, by 0.3 pp to 9.9%. Hospitality improved its performance, with a reduction of 2.8 pp to 10.5%, but still had the largest control gap of the four industries.

Merchants and service providers had very similar control gaps of 8.6% and 8.5%, respectively. Both improved since 2018, with a 1.3 pp drop for merchants and a 0.2 pp decrease for service providers.

Compensating controls

Across all regions, 1.3% of companies used compensating controls, but in reality, this number is derived from EMEA, where 5.4% of companies used compensating controls. Companies in APAC and the Americas didn't use them for this requirement.

No IT services, hospitality or retail companies used compensating controls to meet Requirement 12 in 2019, nor did companies use them in 2018. However, 2.4% of financial services companies did use compensating controls, an increase of 2.4 pp over 2018.

No merchants relied on compensating controls for this requirement in the past year, but 1.7% of service providers used them to meet the requirement, a 1.7 pp increase over the prior year.

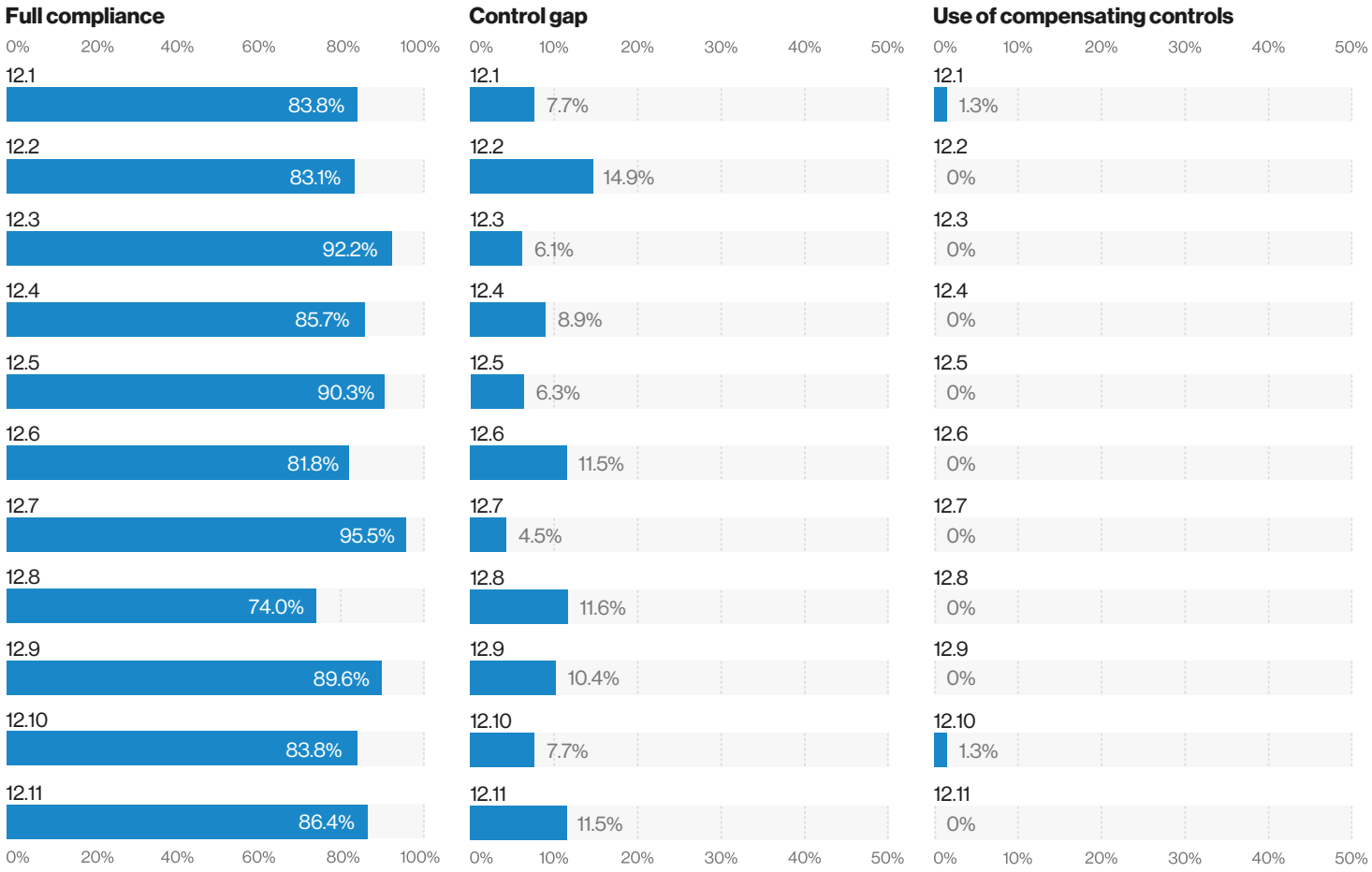
Requirement 12 controls

12.1	Publish, maintain and disseminate security policy
12.2	Implement a risk-assessment process
12.3	Develop usage policies for critical technologies
12.4	Define InfoSec responsibilities for all personnel
12.5	Assign InfoSec management responsibilities
12.6	Implement a formal security awareness program
12.7	Screen potential personnel prior to hire
12.8	Manage service providers with policies and procedures
12.9	Service providers acknowledging responsibility
12.10	Implement an incident response plan
12.11	Additional requirements for service providers

State of control/test procedure

Requirement 12 base controls appear once in the top-20 list of most-compliant controls (Control 12.7—background checks—is fifth). But they appear six times in the bottom-20 list of least-compliant controls: Control 12.10 (incident response) as the fifth least-compliant control, Control 12.1 (information security policy) as the sixth, Control 12.8 (service provider management) as the 11th, Control 12.6 (security awareness) as the 13th, Control 12.4 (information security responsibilities) as the 14th and Control 12.11 (quarterly process reviews for service providers) as the 20th.

Figure 67. 2019 compliance performance (global averages) of Requirement 12—Security management



Industry vertical findings

In terms of full compliance, retail had the poorest showing, at 41.7%, but it also had the smallest control gap. Thus, more retail companies are failing the whole of Requirement 12, but fewer controls are the sources of those failures.

By contrast, financial services had one of the larger control gaps at 9.9%, and one of the lowest full compliance ratings, at 55.3%.

Hospitality had the highest control gap with 10.5%, and the second-best full compliance result, at 57.1%.

IT services had the best full compliance rate at 64.3%, and the second-best control gap, at 7.0%.

In both full compliance and control gaps, merchant and service provider results were very similar: in the 50% range for full compliance and the mid-8% range for control gap. The similar performances of retail companies for merchants, and financial services firms for service providers, drove these comparable outcomes.

Payment data breach correlation—Req 12

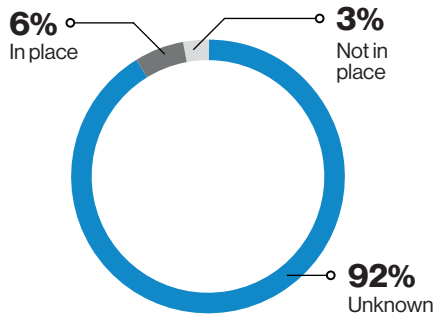


Figure 68. 2014 to 2019 PCI DSS compliance at the time of the breach

Figure 69. Full compliance—Req 12

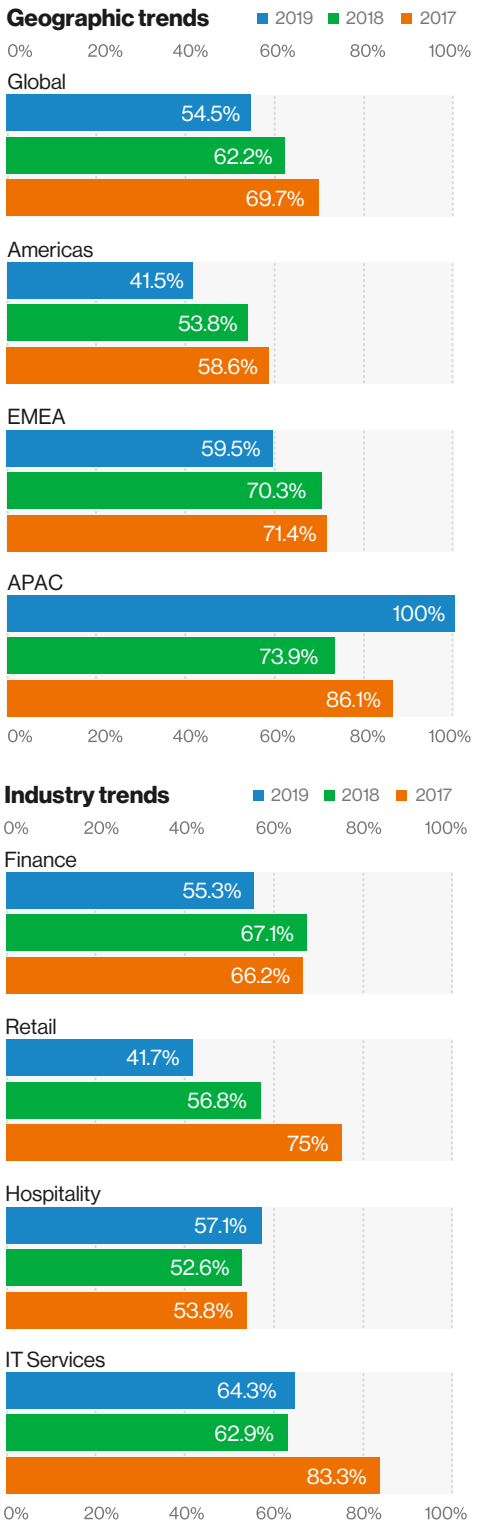


Figure 70. Control gap—Req 12

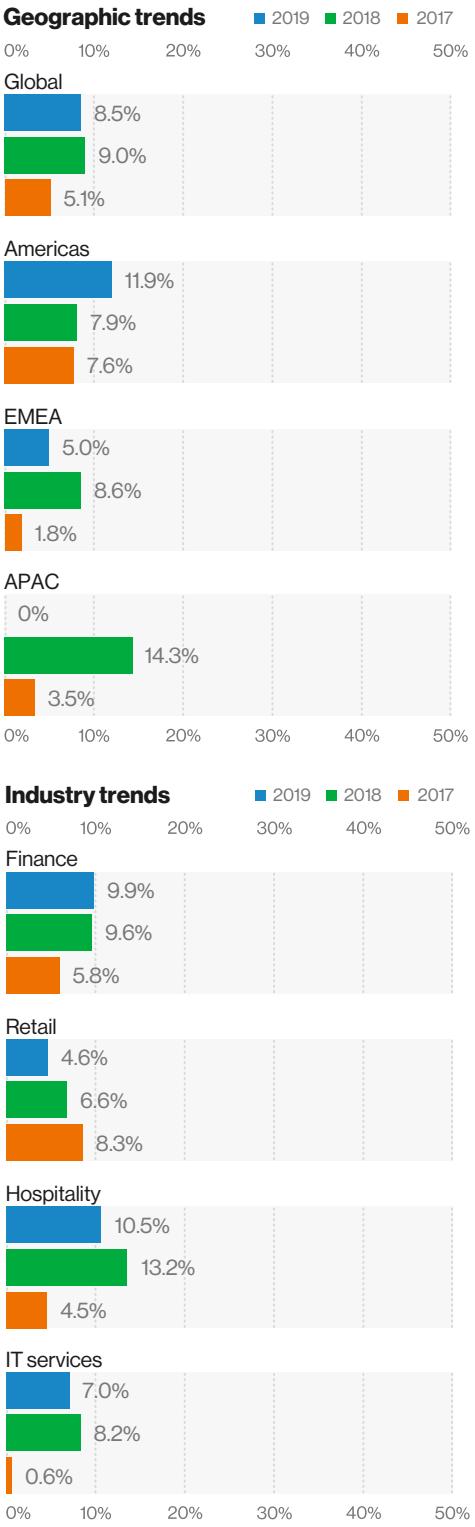
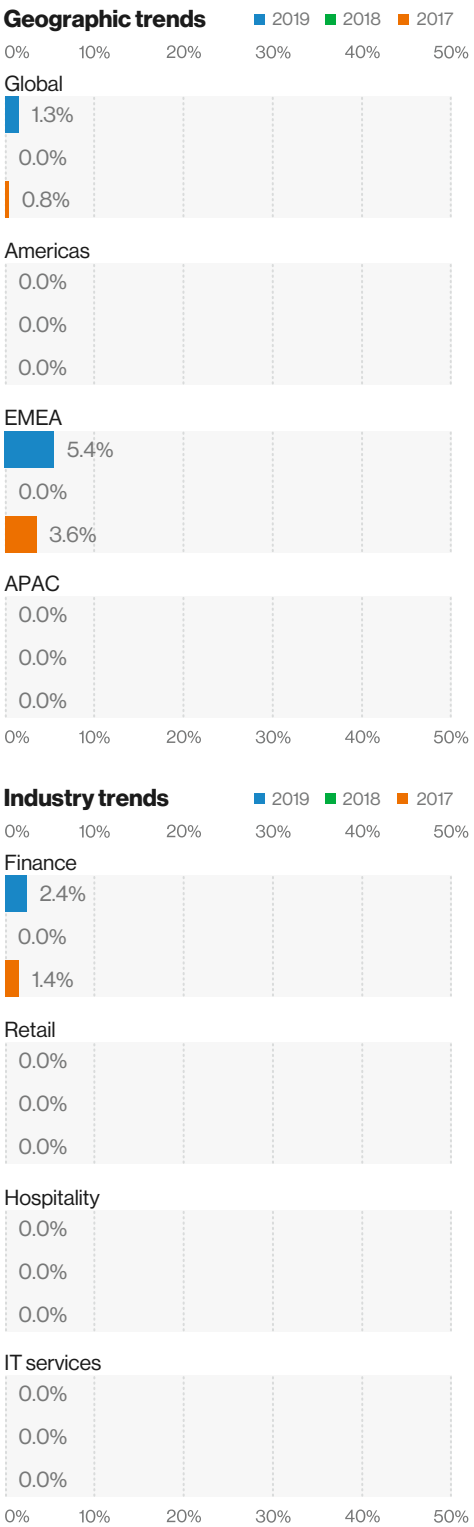


Figure 71. Compensating controls—Req 12



Bottom-20 lists

Requirement 11 continues to present a challenge for organizations to stay on top of obtaining passing quarterly vulnerability internal and external (as applicable) scans. Organizations must ensure that controls are in place such that required scans cannot be missed. Service providers must be extremely alert to this type of monitoring.

While PCI DSS Control 2.4 is not identified in the top five control gaps, it is urgent for organizations to understand the criticality of having a system in place that is properly documented and maintained to reconcile assets that are in scope of PCI DSS along with other business-impacting regulatory requirements.

From all the controls across the DSS, Control 2.4 – Maintain an inventory of system components that are in scope for PCI DSS – experienced the biggest increase in control gap, jumping 18.5 pp from 5.6% in 2018 to 24.0% in 2019.

PCI DSS scope cannot be properly validated with an inaccurate asset inventory.

With Control 1.1 being in second place due to the absence of (or the failure to produce) network device configuration standards, baseline configuration standards are required that are documented and signed off.

The placement of Requirement 6 infractions should not be taken lightly. A breakdown in assessed entities' ability to reconcile installed patches (6.2.b) slopes downward to the fourth-place position of the actual patching occurring in a manner that is compliant with the PCI DSS.

Requirement 8 has shown that issues linger related to the enforcement of the use of unique IDs.

Lastly, Requirement 12 evaluations indicated that organizations have ample room to improve with risk assessment processes and documentation. Maintaining a list of third-party service providers with their compliance statuses was also found too problematic for some entities.

The 20 biggest control gaps

PCI DSS ref	Gap	Description
11.2	33.1%	Run internal and external network vulnerability scans at least quarterly and after any significant change.
1.1	27.9%	Inspect the firewall and router configuration standards and other documentation to verify that standards are complete and implemented.
11.3.3	26.6%	Examine penetration testing results to verify that noted exploitable vulnerabilities were corrected and that repeated testing confirmed remediation.
6.2.b	26.6%	Select a sample of system components and related software, and compare the list of security patches.
6.2	26.0%	Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor patches, and install critical patches within one month.
2.4	24.0%	Maintain an inventory of system components that are in scope for PCI DSS.
11.2.1.b	23.4%	Review internal vulnerability scan reports and verify that all high-risk vulnerabilities are addressed and that the scan process includes rescans to verify remediation.
2.4.a	23.4%	Examine system inventory to verify that a list of hardware and software components is maintained and includes a description of function/use for each.
11.2.1.a	20.8%	Review internal vulnerability scan reports and verify that four passing quarterly scans were obtained in the most recent 12 months.
11.3.2.a	18.8%	Examine the scope of work and results from the most recent internal penetration test to verify that testing is performed: per defined methodology, at least annually, and after significant change.
11.2.2.b	18.2%	Review quarterly ASV scan reports to verify that passing results were obtained.
12.2	16.9%	Implement a risk-assessment process that is performed at least annually and upon significant changes that identifies assets, threats and vulnerabilities and which results in a formal, documented analysis of risk.
11.2.2.a	16.9%	Review output from the four most recent quarters of external vulnerability scans and verify that four occurred in the most recent 12 months.
11.5.a	16.2%	Verify the use of a change-detection mechanism by observing system settings and monitored files, as well as reviewing results from monitoring activities.
1.1.7.b	16.2%	Examine documentation relating to rule set reviews and interview responsible personnel to verify that rule sets are reviewed at least every six months.
11.5	16.2%	Deploy a change-detection mechanism to alert personnel to unauthorized modification of critical files and perform critical file comparisons at least weekly.
12.2.a	15.6%	Verify that an annual risk-assessment process is documented that identifies assets, threats and vulnerabilities and which results in a formal, documented analysis of risk.
8.1	15.6%	Define and implement policies and procedures to ensure proper user identification management for non consumer users and administrators.
8.1.b	15.6%	Verify that procedures are implemented for user identification management.
12.8.1	15.6%	Verify that a list of service providers is maintained and includes a description of the service provided.

Control gap by testing procedure

Biggest increases in gap (2019 vs 2018)

PCI DSS reg	Gap (2019)	Gap (2018)	Description
2.4	24.0%	5.6%	Maintain an inventory of system components that are in scope for the PCI DSS.
2.4.a	23.4%	14.4%	Examine system inventory to verify that a list of hardware and software components is maintained and includes a description of function/use for each.
1.2.1.c	12.3%	5.0%	Examine firewall and router configurations to verify that all other inbound and outbound traffic is specifically denied.
12.2.a	15.6%	8.3&	Verify that an annual risk-assessment process is documented that identifies assets, threats and vulnerabilities and which results in a formal, documented analysis of risk.
3.5.3	6.5%	0.0%	Store secret and private keys used to encrypt and decrypt cardholder data in one or more approved forms at all times.
1.1.7.a	9.7%	3.3%	Verify that firewall and router configuration standards require review of firewall and router rule sets at least every six months.
11.5.a	16.2%	10.0%	Verify the use of a change-detection mechanism by observing system settings and monitored files, as well as reviewing results from monitoring activities.
5.2.d	12.3%	6.1%	Examine antivirus configurations, including the master installation, to verify that log generation is enabled and that logs are retained in accordance with Control 10.7.
7.2.2	8.4%	2.2%	Confirm access control systems are configured to enforce privileges assigned to individuals based on job classification and function.
11.5.b	14.3%	8.3%	Verify the change-detection mechanism is configured to alert personnel upon unauthorized modification of critical files, and to perform critical file comparisons at least weekly.
5.2.b	10.4%	4.4%	Examine antivirus configurations, including the master installation, to verify that antivirus mechanisms perform automatic updates and periodic scans.
8.1.8	13.6%	7.8%	Inspect system configuration settings to verify that system/session idle time-out features have been set to 15 minutes or less.
3.5.3.c	9.1%	3.3%	Examine system configurations and key storage locations to verify that key-encrypting keys are at least as strong as the data-encrypting keys and that they are stored separately.
11.5	16.2%	10.6%	Deploy a change-detection mechanism to alert personnel to unauthorized modification of critical files and perform critical file comparisons at least weekly.
1.1.7.b	16.2%	10.6%	Examine documentation relating to rule set reviews and interview responsible personnel to verify that rule sets are reviewed at least every six months.
3.5.3.b	8.4%	2.8%	Examine system configurations and key storage locations to verify that cryptographic keys are stored in one or more approved forms at all times.
5.1.1	11.0%	5.6%	Review vendor documentation and examine antivirus configurations to verify that antivirus programs detect, remove and protect against all known types of malicious software.
12.2	16.9%	11.7%	Implement a risk-assessment process that is performed at least annually and upon significant changes that identifies assets, threats and vulnerabilities and which results in a formal, documented analysis of risk.
1.1	27.9%	22.8%	Inspect the firewall and router configuration standards and other documentation to verify that standards are complete and implemented.
7.2.1	8.4%	3.3%	Confirm that access control systems are in place on all system components.

Methodology

State of compliance

This research is based on the analysis of quantitative data gathered by QSAs from multiple Qualified Security Assessor Company (QSAC) organizations across the world. The dataset for this 2020 edition is based on information from six sources, with five of them external to Verizon.

These findings are presented globally, with additional comparisons between geographic regions (Americas, EMEA and APAC), between four main industry verticals (financial, retail, hospitality and IT services) and between organization validation type (service providers and merchants).

Dataset

PCI DSS version

All data extracted from PCI DSS compliance assessment reports for statistical analysis carried out for this report were conducted during the year of 2019 and were validated against PCI DSS version 3.2.1. In total, the compliance status of 68,992 PCI DSS controls were assessed in 2019.

Assessments

Producing a PCI DSS assessment report may involve numerous assessments. In several cases, an assessment report is the product of assessments conducted globally or across a specific region. Individual PCI DSS compliance reports consist of between one and in some cases up to 120-plus assessments per report, covering multiple in-scope locations.

Reports

The 2018-2019 comparative analysis is based on an aggregate of 334 PCI DSS compliance validation reports.

- PCI DSS Report on Compliance (2018): 180
- PCI DSS Report on Compliance (2019): 154

For the 2019 assessment year, 43 entities passed their interim compliance validation, demonstrating that they kept all applicable PCI DSS controls in place. Over two-thirds (111) of the entities failed their interim validation assessment due to one or more security controls found to be not in place, with an average control gap of 7.7%.

Trend analysis includes year-over-year comparisons to determine how the state of compliance has evolved over multiple years. These changes in contributors and the potential changes in their areas of focus add a layer of difficulty when identifying trends over time.

The accompanying figures show the breakdown by industry and region from 2019 PCI DSS assessment Interim Report on Compliance (IROC) data gathered from organizations for this report.

Country representation

Primary locations where assessments were conducted (in-scope locations include more than 60 countries):

Americas: Brazil, Canada, Chile, Mexico, United States, Uruguay

APAC: Australia, Hong Kong, India, Malaysia, New Zealand, South Korea, Taiwan, Thailand

EMEA: Denmark, Finland, France, Germany, Ireland, Italy, Kingdom of Bahrain, Netherlands, Norway, South Africa, Switzerland, Ukraine, United Kingdom

The PSR analysis process

Our overall process remains intact and largely unchanged from previous years. All assessment data included in this report was individually reviewed and converted to create a common, anonymous aggregate dataset. The collection method and conversion are the same between contributors. In general, three steps were used to accomplish the dataset:

1. Collection of PCI DSS v3.2.1 IROC assessment reports
2. Conversion of the data into a normalized and anonymized form. All contributors received instruction to omit any information that might identify organizations or individuals involved
3. Submission of the data to the Verizon PSR data science team for aggregated analysis

Data eligibility

For a potential entry to be eligible for the PCI DSS compliance validation corpus, several requirements must be met. The entry must be data from a confirmed PCI DSS validation assessment conducted by a QSA who completed an IROC. In addition to meeting the baseline definition of "Interim Report on Compliance," the entry is assessed for quality. We then create a subset of compliance report data that passes our quality filter.

In addition to having the level of details necessary to pass the quality filter, the assessment reports must be within the time frame of analysis. For the 2019 dataset, this includes PCI DSS assessments conducted between January 1 and December 31, 2019.

What percentage of total PCI DSS compliance validation assessments that are conducted worldwide each year is covered in the survey? We do not know. We only have access to the data for the validation assessments that were conducted by Verizon and contributing QSACs.

Regional representation

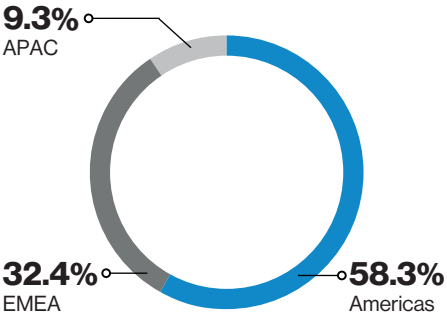


Figure 72. 2018-2019 PCI DSS dataset: by region

Industry representation

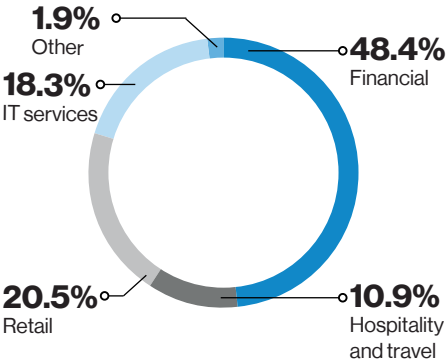


Figure 73. 2018-2019 PCI DSS dataset: by industry

Validation type

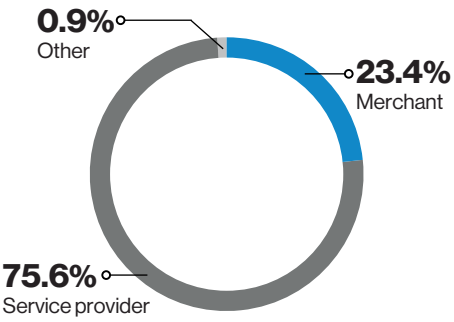


Figure 74. 2018-2019 PCI DSS dataset: validation type

Validation levels

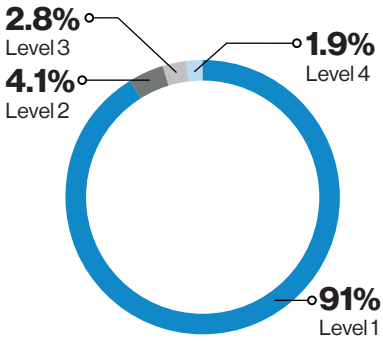


Figure 75. 2018-2019 PCI DSS dataset: validation levels

Sample selection

There are guidelines for the sample size, or percentage of a population, in order to come up with meaningful results. How does our sample size measure up in terms of yielding statistically significant results?

Verizon makes liberal use of confidence intervals to allow us to analyze smaller sample sizes. We adopted a few rules to help minimize bias in reading such data. Here we define "small sample" as fewer than 30. Sample sizes smaller than five are too small to analyze. For small samples, we may determine the value as within some range or values being greater/less than each other.

Noncommittal disclaimer

We would like to reiterate that we make no claim that the findings of this report are representative of all PCI DSS compliance assessments for all organizations at all times. Even though the combined records from all our contributors more closely reflect reality than any of them in isolation, this dataset is still a sample. Although we believe many of the findings presented in this report are appropriate for generalization (and our confidence in this grows as we gather more data and compare it to that of other security organizations), bias undoubtedly exists.

While this dataset may not be flawless, this report provides the most comprehensive version of compliance data Verizon has yet created since we began documenting it in 2010.

The findings are based on aggregated demographic information. While aggregations are made up of individual organizations, individual organizations are not made up of aggregations. It's not a two-way street. There are limitations to the extent these aggregations can be useful in making decisions. Therefore, when reading the findings of this report, you should not make assumptions about their applicability to individual organizations. Some findings and conclusions require additional contexts and data to add more value on the individual level.

"Anything can be measured. If a thing can be observed in any way at all, it lends itself to some type of measurement method. No matter how 'fuzzy' the measurement is, it's still a measurement if it tells you more than you knew before."[135]

—Douglas W. Hubbard

Payment data breach correlation

Six-year data breach correlation trends

The breach correlation data included in each of the 12 Key Requirements sections of this report is separate from our PCI DSS assessment dataset. It comes from forensic investigations into organizations following a breach of payment card data. Verizon has more than a decade's worth of PCI DSS compliance vs breach correlation data, and publishes these findings in each edition of the PSR. Within the PSR dataset, organizations undergoing regular compliance validation do not overlap with those that experienced a breach. From 2010 to this most recent dataset, there is no evidence of any Verizon PCI DSS customers experiencing a data breach.

In this analysis, Verizon considered the aggregate historical analysis of the PCI compliance of organizations that experienced a confirmed PCI data breach for investigations that were carried out by the Verizon Threat Research Advisory Center (VTRAC) team between 2014 and 2019.

State of DSS compliance at the time of a data breach
The breach correlation graphs indicate three metrics for individual requirements along with trend data:

- **In place:** The percentage of cases where a PCI DSS Key Requirement was found to be "in place" at the time of the breach
- **Not in place:** The percentage of cases where a PCI DSS Key Requirement was found to be "not in place" at the time of the breach
- **Unknown:** The percentage of cases where the actual condition of the key requirement at the time of the breach is unable to be determined based on forensic evidence

A PFI investigation is focused on three key missions:

- Determine whether a PCI data breach occurred
- If yes, determine whether there were significant PCI compliance deficiencies
- If yes, determine which deficiencies if any caused or contributed to the breach

The determination of the state of compliance of the breached entity is made during the investigation, to determine what the condition of PCI DSS compliance was at the time of the breach, which may have occurred weeks, months or even years earlier. The PCI Forensic Investigators (PFIs) document all of the specific PCI DSS requirements and subrequirements that were not in place at the time of the breach and thus may have contributed to the data compromise.

"In place" may only be used for fully assessed requirements. "Fully assessed" is an attestation by a QSA that includes a complete and thorough testing of all subrequirements in accordance with completing a Report on Compliance (ROC).

6 years

Dataset time span

2014 to 2019

1 and 1,105

Between 1 and 1,105 locations affected per breach

Trends: PCI DSS compliance status

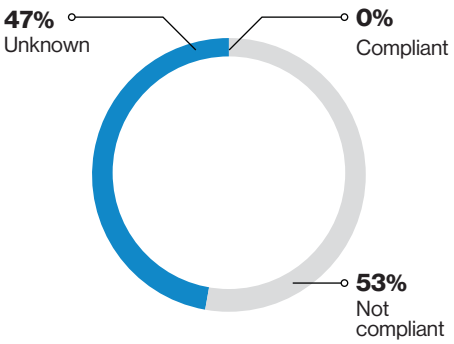


Figure 76. Six-year average. State of compliance at the time of the breach. Unknown indicates lack of evidence of compliance.

Organization size

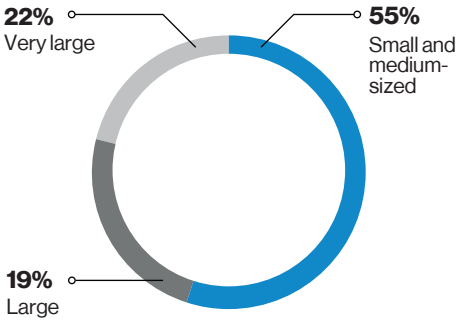


Figure 77. Confirmed payment card data breaches

Very small, small and medium-sized (1 to 10,000), large (10,001 to 50,000), very large (50,001 to over 100,000)

Breached organization size

Very small	1 to 10	**12%**
Small	11 to 100	**7%**
Medium	101 to 1,000	**19%**
	1,001 to 10,000	**17%**
Large	10,001 to 25,000	**2%**
	25,001 to 50,000	**17%**
Very large	50,001 to 100,000	**5%**
	Over 100,000	**17%**

Countries

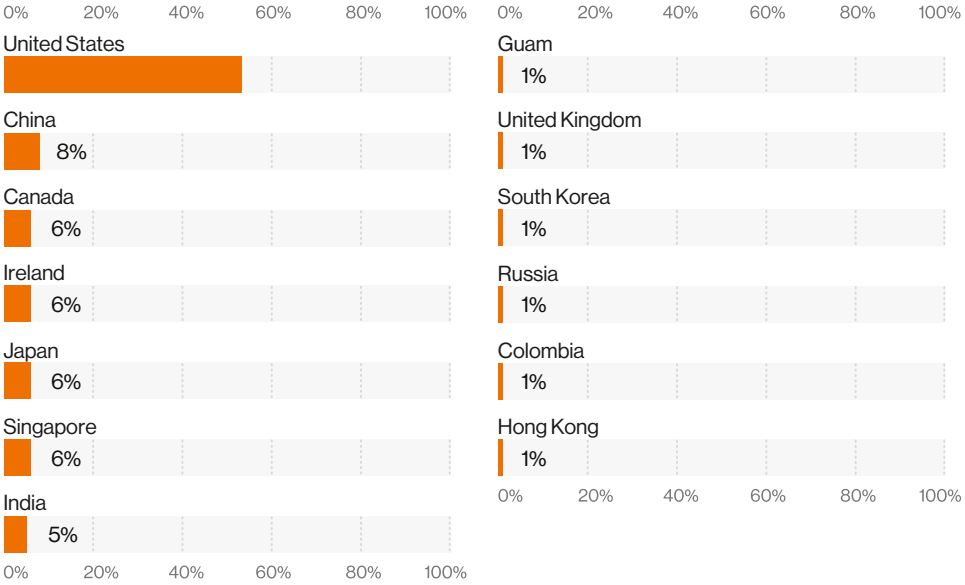


Figure 78. The combined set of confirmed payment card data breaches occurred across 13 countries.

135 Douglas W. Hubbard, How to Measure Anything, Third ed., Wiley, 2014.

04 Appendices

Appendix A: Evolving mobile security

By Dennis Merenguelli, Enterprise Mobile Security Lead, Wireless Business Group

In the past few decades, mobile devices completely transformed the way we live and work. This pervasive adoption of mobile devices provides numerous advantages. In the enterprise space, mobile devices are the primary means of communication between end users and important information resources. Mobile devices also completely changed how consumers access digital content, communicate and purchase goods and services. At the same time, malicious actors leveraged the passive attitude of mobile users to exploit devices and monetize stolen data.

The evolving and broad landscape of mobile devices exposes them to a variety of security threats, and the industry lacks comprehensive protection methods. Additionally, workforce changes, such as those created by the coronavirus pandemic, are exacerbating the problem, as documented in Wandera's recent report "Analysis: Internet traffic related to coronavirus – the good and the bad" (see Figure 79).[136]

Safe vs unsafe connections to COVID-19-related domains

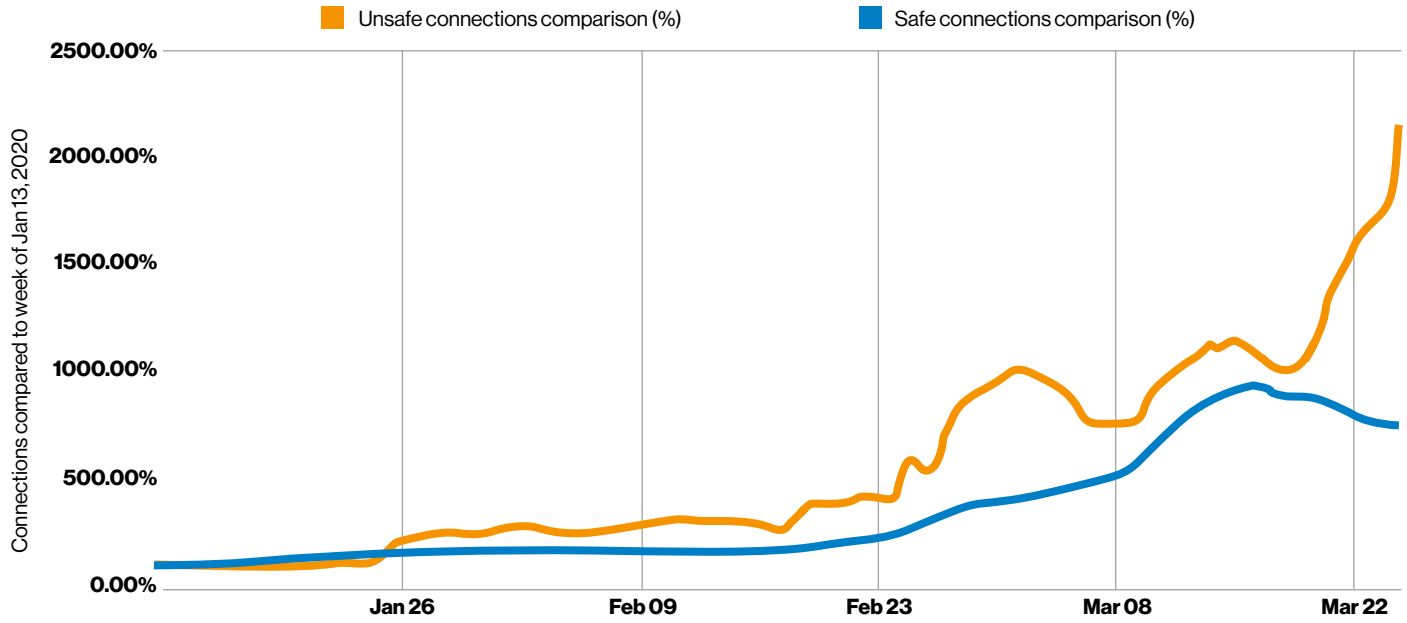


Figure 79. COVID-19-related domains, compared to equivalent connection in the week of Jan 13, 2020. Data provided by Wandera.

136 Liarna LaPorta, "Analysis: Internet traffic related to coronavirus – the good and the bad," Wandera, Apr 10, 2020. https://www.wandera.com/analysis-covid19-internet-traffic/

Every year, the number of companies suffering mobile security compromises has risen and, despite what's at stake, many organizations still sacrifice security to expedite profitability, according to Verizon's Mobile Security Index (MSI) 2020 report.[137] Mobile security has become a critical issue as internet traffic generated by mobile devices surpassed traffic generated from traditional desktop devices.

Attacks on mobile devices are not only increasing in frequency, but are getting more sophisticated, according to the MSI 2020. The report discusses how users, devices, networks and applications are the major threat vectors that malicious actors leverage to compromise mobile devices. These vectors are key when developing applications, such as payment applications, to ensure organizations address all aspects of the threat landscape. (See page 63 of the Verizon 2019 PSR mobile security appendix for additional information on skyrocketing global mobile traffic and applications that can address mobile concerns.)[138]

In early March 2020, the National Institute of Standards and Technology (NIST) published the special publication (SP) 800-124[139] to address the challenges of securing mobile devices and demonstrate management tools that enterprises can use to secure their networks. The models provided by the NIST framework provide organizations with an understanding of what to look for when developing applications that will carry sensitive corporate or personal data.

Consumers that fell for one phishing link often fell for many.

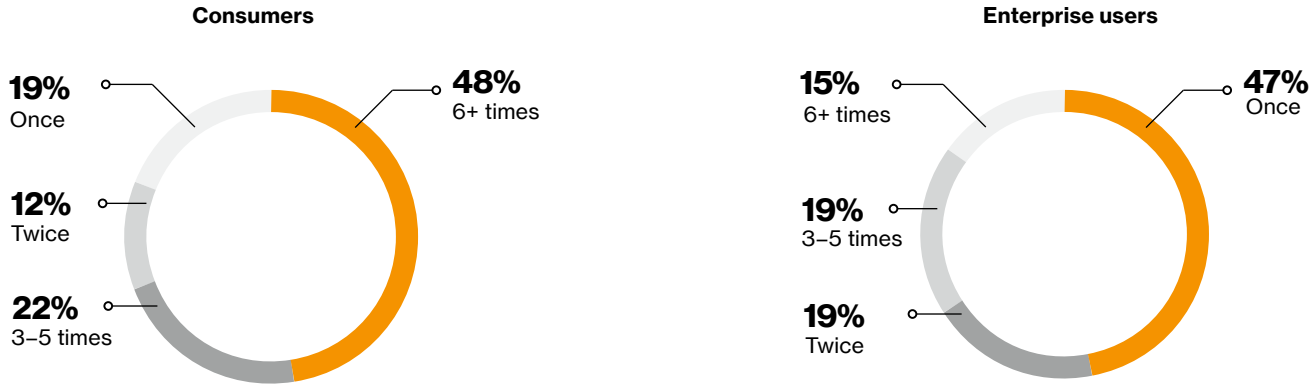


Figure 80. Number of phishing links clicked on by users who clicked at least one link. Data from Verizon Mobile Security Index 2020.

137 Verizon Mobile Security Index 2020. https://https://enterprise.verizon.com/resources/reports/mobile-security-index/

138 Verizon 2019 Payment Security Report, page 63, 2019. https://www.verizon.com/business/resources/reports/payment-security-report/

139 "Mobile Device Security: Cloud and Hybrid Builds," National Institute for Standards and Technology, Feb. 2019. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-4.pdf

Joshua Franklin National Institute of Standards and Technology Information Technology Laboratory: Kevin Bowler, Christopher Brown, Spike E. Dog, Sallie Edwards, Neil McNab, Matthew Steele, The MITRE Corporation, McLean, VA

COVID-19 threats emerge.

Cybercriminals and nation-state hackers are taking advantage of the coronavirus pandemic and turning their attention to mobile devices to spread malware, including spyware and ransomware. Researchers at the security firm Lookout have tracked a malicious Android® application called "corona live® 1.1," which hides surveillance spyware. Initially, the application does not request any special permissions, but subsequently requests access to photos, media and device location. The application also attempts to gain permission to take pictures and record videos.[140]

Opportunistic malicious actors also are finding new ways to harvest credentials by setting up fake COVID-19 sites. These scams vary from phishing attacks that lure users with information about coronavirus cures and charities to mobile apps that collect keystrokes from mobile devices. With many organizations leveraging email, text messages and applications to keep the population informed, these actors are taking advantage of the increased communication to infiltrate victims' devices. Since January 2020, thousands of domains relating to stimulus packages or relief packages found their way onto the internet—hundreds with suspicious domains, dozens deemed malicious. Accessing these sites from the mobile space can be impactful to payment applications as these threats can install keyloggers, such as EventBot, to harvest credentials from users' financial applications (i.e., PayPal Business, Coinbase® and TransferWise®).[141]

Mobile payments increase.

Mobile payments refer to any payment using a mobile device. Adopted rapidly in recent years, they are reshaping the way we purchase goods. Mobile payments have multiple advantages over traditional banking. Customer experience, rewards programs, fast transactions and the mere fact that they reduce the footprint in our wallets are just some advantages of paying with mobile devices. The coronavirus pandemic has impacted consumer behavior as well by driving customers to use contactless methods of payment with mobile devices. Although card-present payments are still #1 in North America, contactless payments are forecasted to increase eightfold between 2020 and 2024.[142]

Mobile payments are evolving rapidly and can take on different forms, such as Near Field Communication (NFC), sound waves-based payments, magnetic transmission, mobile wallets, Quick Response (QR) code payments, internet payment (using a mobile browser), payment link (using a link sent via email or SMS), SMS payments, direct carrier billing, mobile banking and cryptocurrency exchanges. Although all of these are designed to be secure while processing transactions, there is still the chance of compromising the host device and leaking vital information about the account holder, as in the example of the EventBot malware.

Mobile payment providers must continuously analyze their strategy to secure mobile payments to prevent fraud inherent in their method of purchasing goods. According to the RSA Quarterly Fraud Report Q4 2019, 72% of fraud transactions originated in the mobile channel, and specifically, 59% of fraud transactions were attributed to mobile browsers.[143] As we see in Verizon's MSI 2020 report, the number of organizations suffering a compromise involving a mobile device went up to 33% in 2019.

Vulnerabilities on operating systems (OS) and apps allow attackers to infiltrate their exploits to hijack legitimate payment applications and exfiltrate information by tricking users into granting permissions. Mobile Threat Defense (MTD) provider Lookout, in collaboration with Promon, reported an Android exploit called StrandHogg found in the Google Play® store, which leveraged this technique to steal information from the unknowing user.

A mobile-related compromise can lead to downtime, loss of data, compromise of other devices, damage to reputation, regulatory penalties and loss of business. Financial organizations are starting to look at partnering with MTD providers to implement its machine-learning capabilities to detect abnormal behavior on the apps that reside within the mobile device to detect, protect and respond to malware targeting these payment applications.

Fraud attack distribution

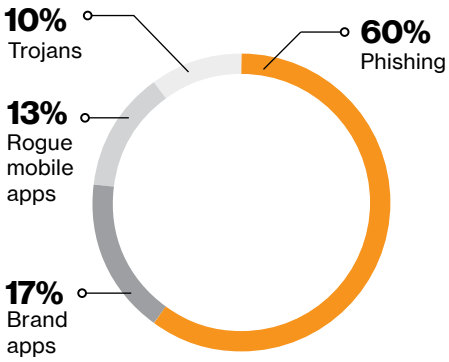


Figure 81. Data from the RSA Quarterly Fraud Report, 4th Quarter.

140 Kristin Del Rosso, "New Threat Discovery Shows Commercial Surveillanceware Operators Latest to Exploit COVID-19," Lookout, Mar 18, 2020. https://blog.lookout.com/commercial-surveillanceware-operators-latest-to-take-advantage-of-covid-19

141 Daniel Frank, Lior Rochberger, Yaron Rimmer and Assaf Dahan, "EventBot: A New Mobile Banking Trojan Is Born," Cyberreason, Apr 30, 2020. https://www.cybereason.com/blog/eventbot-a-new-mobile-banking-trojan-is-born

142 "North America's Online Payment Market 2020 — Pre-Pandemic and Deviated Growth Projections due to COVID-19." GlobeNewswire, May 7, 2020. https://www.globenewswire.com/news-release/2020/05/07/2029577/0/en/North-America-s-Online-Payment-Market-2020-Pre-Pandemic-and-Deviated-Growth-Projections-due-to-COVID-19.html

143 RSA Quarterly Fraud Report, 4th Quarter, RSA, 2020. https://www.rsa.com/en-us/offers/rsa-fraud-report-q4-2019

The zero trust approach

What is zero trust, and why is it imperative to the mobile workforce? Zero trust, by definition, is a set of security measures that organizations should not automatically trust anything inside or outside their defined perimeter. In a zero trust environment, an organization must continuously verify users and devices while providing conditional access on an as-needed basis to digital resources such as email, applications, documents and information.

Creating a zero trust environment around the mobile workforce requires integrating unified endpoint management (UEM), identity access management (IAM) and MTD tools. UEM is a method to secure and control devices from a single console. IAM is a framework of policies and technologies for ensuring that the proper people in an enterprise have appropriate access to technology resources. In general, MTD solutions collect and analyze indicators of compromise to identify anomalous behavior and counter threats. MTD gains threat intelligence from the devices they support and other external sources.[144]

MTD tools leverage AI and machine-learning algorithms to continuously analyze mobile devices and identify patterns of malicious behavior. Having MTD providers that can integrate with existing UEM providers is crucial to develop a strong mobile security posture.

IAM has greatly evolved in the last several years, providing a framework that helps organizations identify and verify the user. Multifactor authentication leverages another medium, such as SMS or email, to verify the user, but cutting-edge providers leverage the techniques to continuously authenticate users. These providers look at attributes, such as behavioral biometric analysis, to detect suspicious keyboard and mouse actions that could indicate an imposter. Contextual authentication analysis is another attribute that analyzes location, time or methods to ensure that login attempts are valid.

In summary, zero trust adoption cannot rely on a single product or service, and there is no industry-standard architecture that defines it. As organizations go through a digital transformation and integrate mobility into it, they must look at solutions that can integrate with one another to protect, detect and respond to mobile or application threats.

Protection of mobile payment applications is becoming more complex as malicious actors find ways to bypass current security measures, such as multifactor authentication. Protecting the applications and user credentials will require the involvement of both the mobile app developers and users to set parameters to ensure all transactions made are legitimate.

Mobile-payment application developers are already looking into integrating MTD mechanisms to ensure devices are not compromised before users enter sensitive information. Developers are also starting to explore continuous authentication tools that go beyond an SMS and/or an email to protect users. These tools are designed to develop a behavioral profile of end users to authenticate them.

New mobile payment applications should be designed with the next generation in mind. Having security controls that can be adjusted to users' needs—such as geofencing, which looks at where transactions are made, or methods to verify transactions that are over a given amount of money—are options that can be integrated into mobile payment apps to elevate security postures.

1. **Involves users, devices, data, applications and transport**
2. **Must integrate multiple solutions**
3. **Must be revised continuously**
4. **Includes a framework to identify, enable, protect, detect and respond**

144 "Reviews for Mobile Threat Defense (MTD) Market," Gartner, 2020. https://www.gartner.com/reviews/market/mobile-threat-defense-solutions

Appendix B: PCI DSS compliance calendar with the 6 Constraints and 9 Factors

By Dyana Pearson, Halli Goodman and Sky Hackett, Senior Consultants, Verizon PCI Security Practice

The primary purpose of the calendar is to provide a visual representation of the tasks and activities that organizations are required to implement and maintain across their PCI DSS compliance environment.

Verizon 2020 PSR compliance calendar

Business as usual (BAU)	Requirements	Tasks
		Scope maintenance: Perform manual and automated searches for PAN and review network device configurations as scope changes. **Compensating control maintenance:** Review and perform functions supporting the continuity of compensating controls, as defined during the annual PCI DSS assessment.
1	1.1.2 1.1.3	Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks. Current diagram that shows all cardholder data flows across systems and networks.
2	2.x 2.4	Maintain updated configuration standards (supported versions of operating systems, devices and applications). Maintain an inventory of system components that are in scope for PCI DSS.
3	3.5.1 3.6	Maintain a documented description of the cryptographic architecture. Retire or replace keys as necessary, in alignment with documented key management procedures.
4	4.x	Monitor transmission encryption protocol configurations and mechanisms.
5	5.1.2	Evaluate evolving malware threats to confirm whether systems considered not commonly affected by malicious software continue to not require antivirus software.
6	6.1 6.2 6.4	Use reputable external security resources to identify new security vulnerabilities and assign a risk rating to newly discovered security vulnerabilities. Ensure that all system components and software are protected from known vulnerabilities by installing vendor-supplied patches. • Install critical security patches within a month of release • All applicable vendor-supplied security patches are installed within an appropriate time frame (for example, within three months) Follow change control processes and procedures for all changes to system components.

PCI DSS compliance requirements. PCI DSS version 3.2.1 contains 252 requirements, 79 base controls and 440 security test procedures.

Key Requirements	Requirements	Test procedures
Requirement 1	22	38
Requirement 2	12	35
Requirement 3	23	52
Requirement 4	4	12
Requirement 5	6	13
Requirement 6	29	46
Requirement 7	10	11
Requirement 8	25	48
Requirement 9	27	45
Requirement 10	35	47
Requirement 11	17	38
Requirement 12	42	55
Total	**252**	**440**

PCI DDS version	1.1	2.0	3.2	3.2.1
Released (year)	2006	2010	2016	2018
Number of pages	50	75	139	139
Control objectives	6	6	6	6
Key requirements	12	12	12	12
Total controls	64	62	79	79
Total requirements	207	211	252	252
Test procedures	—	338	443	440

It is essential to have an effective management system in place to coordinate the implementation and maintenance of all the requirements. We updated the calendar and included the 6-Constraints-and-9-Factors tasks into business-as-usual, daily, weekly, quarterly, biannual, annual and after-significant-changes frequencies. Descriptions have been provided for each task, with additional, select callouts and one comprehensive example (for Control 11.2.1).

6 Constraints and 9 Factors	Examples
Capacity: Evaluate the bandwidth of your team. **Capacity:** Evaluate the technical and soft skills of your team.	
Control life-cycle management: Review and keep track of the age of BAU control systems. How are the controls holding up? Are they still operating efficiently and as intended, or should they be retired and replaced with more efficient or effective controls?	
	For Control 2.4 (maintain an accurate asset inventory), consider the following questions: Does my team have sufficient time to maintain an accurate asset inventory on a BAU basis? What additional resources, tools or processes might be needed to adequately maintain this control? If spreadsheets are used or questionnaires are sent annually to system owners, can the organization transition to a CMDB that would ensure an accurate inventory in real time? What steps might be needed to ensure quality inputs as the environment changes and systems are onboarded or decommissioned? What training might my team and the system owners need to properly identify in-scope assets? If a complex CMDB exists in the environment, are there enough staff resources to manage the system so that integration of disparate system types report properly to the main database?

Business as usual (BAU)	Requirements	Tasks
8	8.1.3	Immediately revoke logical access for any terminated users.
9	9.3	Immediately revoke physical access for terminated personnel.
	9.9.1	Maintain an up-to-date list of devices.
	9.9.2	Periodically inspect device surfaces to detect tampering or substitution.
	9.9.3	Train personnel to be aware of attempted tampering or replacement of devices.
10	10.6.2	Review logs of system components, based on the organization's policies and risk management strategy.
	10.8.x	Service providers only: Detect, respond to and report on failures within critical security control systems.
11	11.1.1	Maintain inventory of authorized wireless access points.
12	12.3.9	Activate remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use.
	12.6.1	Educate personnel upon hire.
	12.7	Screen potential personnel prior to hire to minimize the risk of attacks from internal sources.
	12.10.3	Designate specific personnel to be available on a 24/7 basis to respond to alerts.
	12.10.4	Provide appropriate training to staff with security breach response responsibilities.
Daily		
10	10.6.1	Review logs and security events of all critical system components.
At least weekly		
	11.5	Perform critical file comparisons.
Quarterly		
3	3.1	Ensure that stored CHD does not exceed defined retention policies and validate secure deletion purge processes.
6	6.2	Install all applicable vendor-supplied security patches within an appropriate time frame, for example, within three months.
8	8.1.4	Remove/disable inactive user accounts within 90 days.

6 Constraints and 9 Factors	Examples
Capability: Evaluate the technical and soft skills of your team.	**Capability:** • Does the vulnerability management team have the right tools to perform analysis? • Does the vulnerability management team have relevant knowledge to conduct scans and accurately interpret results? • Does the vulnerability management team receive ongoing training on their job duties and industry developments? • Do team members have the correct knowledge to identify industry-accepted sources and vendor resources for vulnerability identification? • Is the team capable of identifying the correct system owners for actioning of vulnerability data?
Commitment: Confirm the buy-in of all stakeholders to the program.	**Commitment:** • Is overall accountability formally assigned for the vulnerability management program? • Does management understand the importance of vulnerability management? • Do vulnerability management personnel feel supported to execute their job duties?
Communication: Review the accuracy and completeness of the transmission of program details to involved parties.	**Communication:** • Does the vulnerability management team communicate vulnerability information to system owners and other relevant stakeholders? • How does the vulnerability management team follow up and ensure vulnerability data is actioned? • How does the vulnerability management team communicate ongoing status to management?

Quarterly	Requirements	Tasks
	8.2.4	Change user passwords/passphrases at least once every 90 days.
Second quarter		
11	**11.1**	Test for the presence of unauthorized wireless access points on at least a quarterly basis.
	11.2.1	Perform quarterly internal vulnerability scans.
	11.2.2	Perform quarterly external vulnerability scans.
12	**12.11**	Service providers only: Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures.
	12.11.1	Service providers only: Maintain documentation of quarterly review process to include results of the reviews and review and sign off on results by personnel-assigned responsibility for the PCI DSS compliance program.

6 Constraints and 9 Factors	Examples
Control environment: Thoroughly evaluate the business' values, priorities, management style and overall objectives in the first quarter. Monitor the alignment of governance documentation (policies, standards and procedures) and the organizational structure with these objectives in each subsequent quarter.	**Control environment:** • How well is the vulnerability management team following documented standards? • How well is the vulnerability management team aligning risk rankings with industry methodologies or assigned risk rankings (i.e., CVSS base scores)? • How is the team documenting deviations from assigned risk rankings? Are these deviations formally approved?
Control life-cycle management: Formally review and keep track of the age of each critical control system every quarter. How is the control holding up? Is it still operating efficiently and as intended, or should it be retired and replaced with a more efficient or effective control?	**Control life-cycle management:** • How is the vulnerability management tool in use performing? Should it be replaced/retired? • What tool is the team using to track and action identified vulnerabilities? Is it working well? Should it be replaced/retired? • Do the industry and vendor sources used need to be updated/refreshed? • Should scanning frequency be revisited? How well is it working?
Performance management: Determine the metrics that can be used to evaluate whether a given control is achieving its aim. On a quarterly basis, review those numbers and assess whether adjustments to the controls are needed. If this exercise can be done only once per year, then do so in Quarter 3 as part of annual validation preparations.	**Performance management:** • What metrics are being used to measure the success of the program? • Are these metrics effective? Should they be changed? • Are you meeting your SLAs for actioning vulnerabilities, according to documented standards? • How do you ensure you are capturing all assets? • Are scans effective and tailored to the environment (i.e., authenticated scanning, container-based scanning, gold-image scanning, cloud scanning)? • How many rescans are being conducted?
Self-assessment: Create an in-house methodology for testing the sustainability of the compliance program. Obtain, record and report key metrics on all 6 Constraints and all 9 Factors.	**Self-assessment:** Using your organization's risk assessment methodology, design a self-assessment protocol that aligns with business objectives and measures the successes and failures of your compliance program. Among the details to track might be: • How are you performing with your key performance indicators (KPIs) and metrics? • How many vulnerabilities are carrying over from quarter to quarter? • Are rescans being conducted as required?
Control Design: Review the purpose, function, scope, limitations and dependencies of all critical control systems. Allocate task to Quarter 2, as it should be less busy. (Quarter 1 has a number of startup activities. Quarter 4 is focused on annual validation.)	**Control design:** • Is the team scanning all intended systems? • What limitations does the team have that can be alleviated? • Are the scan results being used to inform other controls, such as patching (Control 6.2)? • How often is the vulnerability management policy or procedure updated to reflect new threats or new risks identified within the organization? **Control risk:** • How are identified vulnerabilities incorporated into risk-assessment processes? • How is this risk managed and monitored on an ongoing basis? • Is adequate budget allocated to ensure that scanners are operational and fully supported?

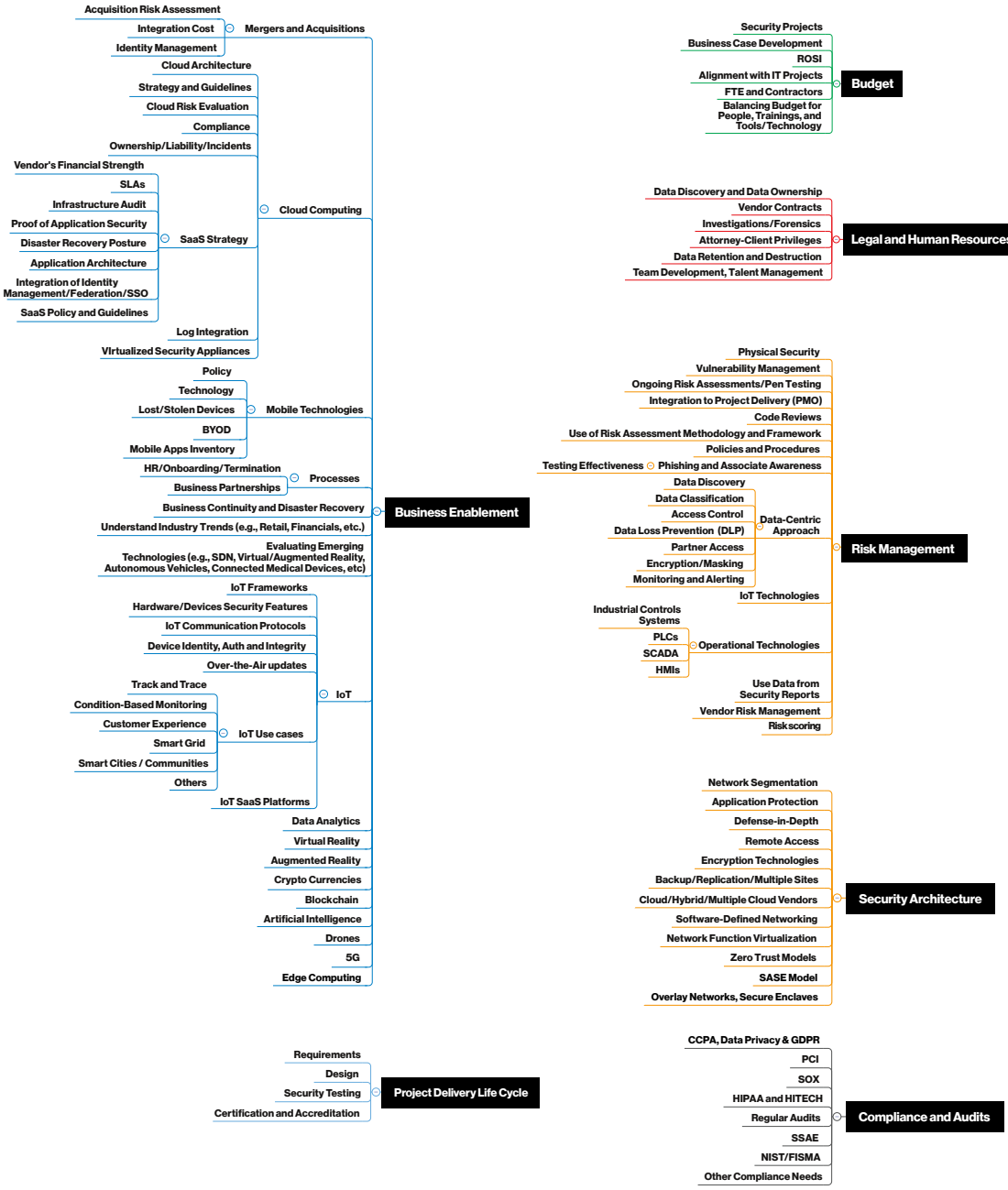
Quarterly	Requirements	Tasks
Third quarter		
Fourth quarter		
Biannual		
1	**1.1.7**	Perform required biannual firewall and router reviews.
11	**11.3.4.1**	Service providers only: If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls.

6 Constraints and 9 Factors	Examples
Control robustness: Review the ability of each critical security control to remain effective in meeting its objective, despite disruption. **Control resilience:** Review the ability of each critical security control to rapidly recover from disruptive events.	**Control robustness:** • Does the vulnerability management tool identify all known vulnerabilities for scanned technologies? • Does the vulnerability management tool provide sufficient reporting capabilities? • Does the vulnerability management tool allow easy addition of new assets to the environment? Or is this process arduous and inefficient? • Do the industry sources used provide enough information? Are there better sources that could provide more comprehensive data? • With an increased scanning load, how do the scanners perform? • Should additional CPUs or storage be allocated to the scanners to ensure their uptime? **Control resilience:** • How often are tool outages experienced? • How fast can the team and the tool respond to a scanning system failure? • How much time do the team and the tool need to have an operational control in place again? • How often does the tool fail to connect to systems being scanned? • How much interference/network disruption is caused by the tools/conducting the scans?
Maturity measurement: Model, with a set of structured levels, the behaviors, practices and processes that can reliably sustain PCI compliance. Evaluate the compliance program against this model for an indicator of progress.	**Maturity measurement:** • What would an ideal internal vulnerability scanning process look like in your organization? How would it function? What would the desired outcomes be? How does your organization measure against those goals today? • How much has the vulnerability management process improved over time? What other areas for improvement could be addressed? • What inefficiencies or redundancies could be eliminated?
Reference the "at least annually" constraints and factors.	**Additionally (not necessarily quarterly constraints or factors):** **Capacity (BAU constraint):** • Does the vulnerability management team have sufficient personnel? • Does the vulnerability management team have sufficient budget for improvement, training and investment in new tooling? **Culture (annual constraint)** • Do systems owners who receive vulnerability information take it seriously? How receptive are they? Do they respond to vulnerability management personnel quickly? Or is actioning put on the “back burner”?
Capacity: Evaluate the bandwidth of your team. **Capability:** Evaluate the technical and soft skills of your team. **Control life-cycle management:** Informally review and keep track of the age of BAU control systems. How are the controls holding up? Are they still operating efficiently and as intended, or should they be retired and replaced with more efficient or effective controls? **Competence:** Evaluate the quality of the work of your team. This task can coincide with performance reviews and should be incorporated into KPIs.	**Capacity:** For Control 1.1.7 (ruleset reviews), consider the following questions: Does my team have enough bandwidth to perform these reviews on a biannual basis? Are they equipped to review all of the in-scope network devices ACLs? What tools are they using to perform these reviews? Are any of these tools failing or in need of replacement? Could the process be automated? Can parts of it be outsourced? What is the final product produced by my team? Can it be improved, and can the results of these reviews be used as inputs in other risk analyses and budget decisions that need to be made?

At least annually	Requirements	Tasks
		Executive summary: PCI DSS assessment scoping confirmation activities.
	6.5	Train developers in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities.
	6.6	Review public-facing web applications manually or via automated mechanisms at least annually.
	9.5.1	Store media backups in a secure location, preferably an offsite facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security.
	9.7.1	Properly maintain inventory logs of all media, and conduct media inventories.
	11.3.1	Perform external penetration testing.
	11.3.2	Perform internal penetration testing.
	11.3.4	If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls.
	12.1.1	Review the security policy and update the policy to reflect changes to business objectives or the risk environment.
	12.2	Perform a formal, documented analysis of risk.
	12.4	Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.
	12.6.1	Educate personnel on security awareness and information security policies.
	12.6.2	Require personnel to acknowledge that they have read and understood the security policy and procedures.
	12.8.4	Maintain a program to monitor service providers' PCI DSS compliance status.
	12.10.2	Review and test the incident response plan.
After changes		
	6.4.6	Implement all relevant PCI DSS requirements on all new or changed systems and networks, and update documentation.
	6.6	Review public-facing web applications manually or via automated mechanisms after any significant change.
	11.2.3	Perform internal and external scans, and rescans as needed.
	11.3.1	Perform external penetration testing.
	11.3.2	Perform internal penetration testing.
	11.3.4.x	If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls.
	12.1.1.x	Update the security policy when the environment changes.

6 Constraints and 9 Factors	Examples
Self-assessment: Conduct an all- or half-day lessons-learned session, to use quarterly metrics and personnel anecdotes to measure performance and progress of the compliance program over prior 12 months. **Culture:** Assess the degree to which critical security controls are embedded in (or institutionalized by) the organization.	
Capacity: Evaluate the bandwidth of your team. **Capability:** Evaluate the technical and soft skills of your team. **Control life-cycle management:** Informally review and keep track of the age of BAU control systems. How are the controls holding up? Are they still operating efficiently and as intended, or should they be retired and replaced with more efficient or effective controls?	

Appendix C: CISO responsibilities



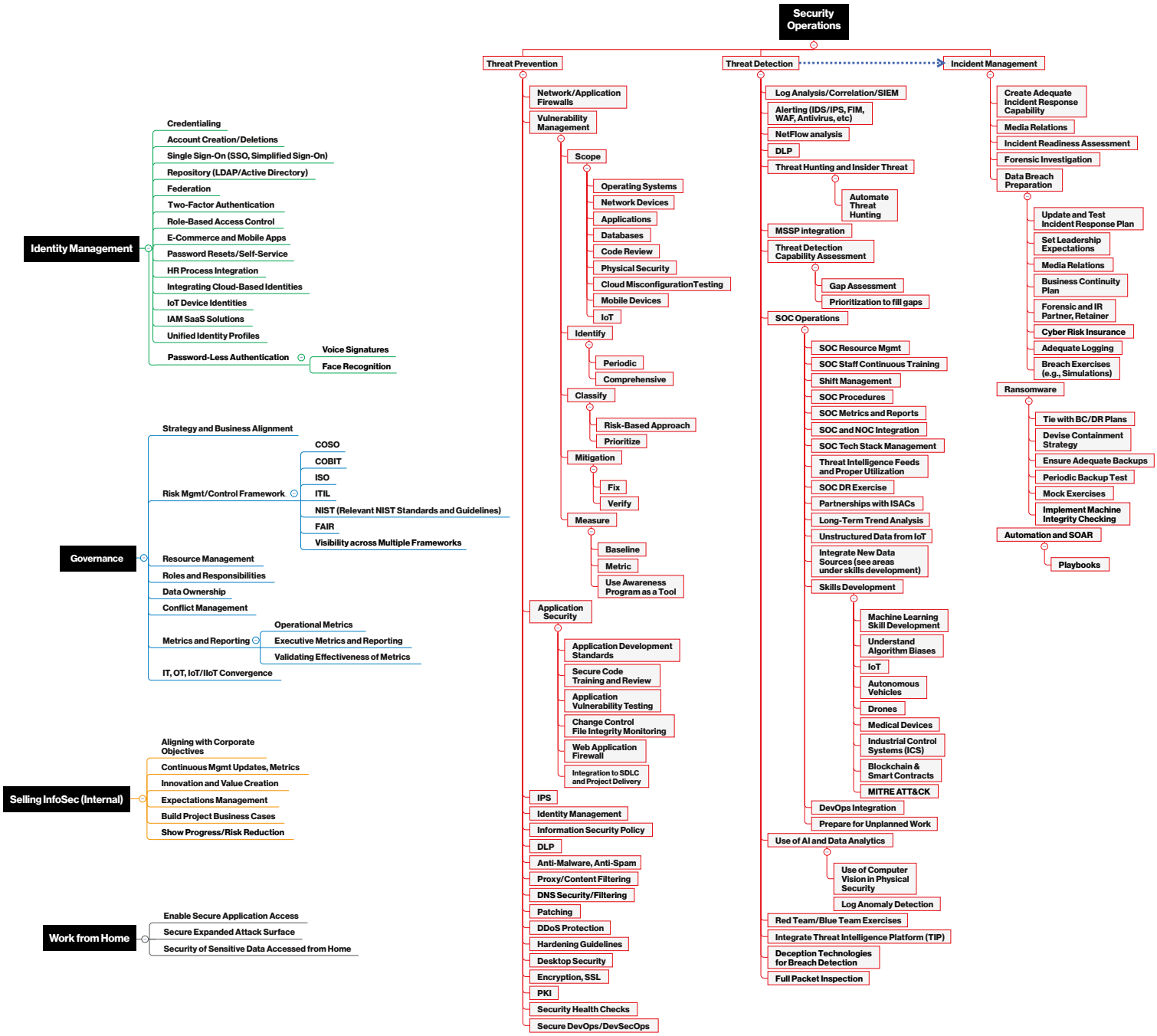
InfoSec professionals responsibilities

Focus Areas for 2020

- Improve SOC analyst productivity with SOAR
- Reduction/consolidation of tools/technologies
- Better protection and monitoring of cloud
- Explore new architecture models like SASE
- Consider zero trust, secure enclaves
- Edge computing security
- Include deception technologies as part of security tools
- COVID-19 and work from home

Rafeeq Rehman
Distinguished Architect, Cybersecurity Verizon

Last Update - June 13, 2020
Twitter@rafeeq_rehman
Version 2020
Downloads
http://rafeeqrehman.com


Identity Management
Credentialing
Account Creation/Deletions
Single Sign-On (SSO, Simplified Sign-On)
Repository (LDAP/Active Directory)
Federation
Two-Factor Authentication
Role-Based Access Control
E-Commerce and Mobile Apps
Password Resets/Self-Service
HR Process Integration
Integrating Cloud-Based Identities
IoT Device Identities
IAM SaaS Solutions
Unified Identity Profiles
Password-Less Authentication
Voice Signatures
Face Recognition
Governance
Strategy and Business Alignment
Risk Mgmt/Control Framework
COSO
COBIT
ISO
ITIL
NIST (Relevant NIST Standards and Guidelines)
FAIR
Visibility across Multiple Frameworks
Resource Management
Roles and Responsibilities
Data Ownership
Conflict Management
Metrics and Reporting
Operational Metrics
Executive Metrics and Reporting
Validating Effectiveness of Metrics
IT, OT, IoT/IIoT Convergence
Selling InfoSec (Internal)
Aligning with Corporate Objectives
Continuous Mgmt Updates, Metrics
Innovation and Value Creation
Expectations Management
Build Project Business Cases
Show Progress/Risk Reduction
Work from Home
Enable Secure Application Access
Secure Expanded Attack Surface
Security of Sensitive Data Accessed from Home
Security Operations
Threat Prevention
Network/Application Firewalls
Vulnerability Management
Scope
Operating Systems
Network Devices
Applications
Databases
Code Review
Physical Security
Cloud MisconfigurationTesting
Mobile Devices
IoT
Identify
Periodic
Comprehensive
Classify
Risk-Based Approach
Prioritize
Mitigation
Fix
Verify
Measure
Baseline
Metric
Use Awareness Program as a Tool
Application Security
Application Development Standards
Secure Code Training and Review
Application Vulnerability Testing
Change Control File Integrity Monitoring
Web Application Firewall
Integration to SDLC and Project Delivery
IPS
Identity Management
Information Security Policy
DLP
Anti-Malware, Anti-Spam
Proxy/Content Filtering
DNS Security/Filtering
Patching
DDoS Protection
Hardening Guidelines
Desktop Security
Encryption, SSL
PKI
Security Health Checks
Secure DevOps/DevSecOps
Threat Detection
Log Analysis/Correlation/SIEM
Alerting (IDS/IPS, FIM, WAF, Antivirus, etc)
NetFlow analysis
DLP
Threat Hunting and Insider Threat
Automate Threat Hunting
MSSP integration
Threat Detection Capability Assessment
Gap Assessment
Prioritization to fill gaps
SOC Operations
SOC Resource Mgmt
SOC Staff Continuous Training
Shift Management
SOC Procedures
SOC Metrics and Reports
SOC and NOC Integration
SOC Tech Stack Management
Threat Intelligence Feeds and Proper Utilization
SOC DR Exercise
Partnerships with ISACs
Long-Term Trend Analysis
Unstructured Data from IoT
Integrate New Data Sources (see areas under skills development)
Skills Development
Machine Learning Skill Development
Understand Algorithm Biases
IoT
Autonomous Vehicles
Drones
Medical Devices
Industrial Control Systems (ICS)
Blockchain & Smart Contracts
MITRE ATT&CK
DevOps Integration
Prepare for Unplanned Work
Use of AI and Data Analytics
Use of Computer Vision in Physical Security
Log Anomaly Detection
Red Team/Blue Team Exercises
Integrate Threat Intelligence Platform (TIP)
Deception Technologies for Breach Detection
Full Packet Inspection
Incident Management
Create Adequate Incident Response Capability
Media Relations
Incident Readiness Assessment
Forensic Investigation
Data Breach Preparation
Update and Test Incident Response Plan
Set Leadership Expectations
Media Relations
Business Continuity Plan
Forensic and IR Partner, Retainer
Cyber Risk Insurance
Adequate Logging
Breach Exercises (e.g., Simulations)
Ransomware
Tie with BC/DR Plans
Devise Containment Strategy
Ensure Adequate Backups
Periodic Backup Test
Mock Exercises
Implement Machine Integrity Checking
Automation and SOAR
Playbooks

Appendix D: Suggested reading

> 1. **Decide, before you start, that you're going to change three things about what you do all day at work. Then, as you're reading, find the three things and do it. The goal of the reading, then, isn't to persuade you to change, it's to help you choose what to change.**
> 2. **If you're going to invest a valuable asset (like time), go ahead and make it productive. Use a Post-it or two, or some index cards or a highlighter. Not to write down stuff so you can forget it later, but to create marching orders. It's simple: If three weeks go by and you haven't taken action on what you've written down, you wasted your time.**
> 3. **It's not about you, it's about the next person. The single best use of a business book is to help someone else. Sharing what you read, handing the book to a person who needs it... pushing those around you to get in sync and to take action—that's the main reason it's a book, not a video or a seminar. A book is a souvenir and a container and a motivator and an easily leveraged tool. Hoarding books makes them worth less, not more.**
>
> **Effective managers hand books to their team. Not so they can be reminded of high school, but so that next week she can say to them, 'are we there yet?'"**
>
> **– Seth Godin, "How to read a business book," Seth's blog, May 21, 2008. https://seths.blog/2008/05/how-to-read-a-b/**

This suggested reading list is a goldmine of information for security professionals tasked with managing security, data protection and compliance programs. One of the best ways to develop proficiency and master data security is to absorb the wealth of information accumulated from experts in the last two decades. CISOs need to brush up regularly on guidance from the best and brightest.

This list includes new additions to the list published in the Verizon 2019 Payment Security Report, page 85.[145] The focus of this list is strategic guidance for CISOs. Without well-educated and inspired management leadership, a compliance program likely will lag or be inadequate.

The list of 12 books is divided into the following categories to help narrow your selection:

1. CISOs and leadership
2. Strategy and security strategy
3. Security culture
4. Risk management and security strategy
5. General security

145 Verizon 2019 Payment Security Report, page 85. https://enterprise.verizon.com/resources/reports/payment-security/

CISOs and leadership						
	Year	**Title**	**Author**	**Publisher**	**Pages**	**ISBN**
1	2012	The Essential Deming: Leadership Principles from the Father of Quality	W. Edwards Deming	McGraw-Hill Education	336	978-0071790222 https://www.amazon.com/dp/0071790225
2	2017	Why CISOs Fail: The Missing Link in Security Management—and How to Fix It	Barak Engel	Auerbach Publications	158	978-1138197893 https://www.amazon.com/dp/1138197890/
3	2019	Cyber Security: The Lost Decade Why large organizations still struggle with decade-old security problems—and how to fix them	JC Gaillard	Blurb	230	9780464376569 https://www.blurb.com/b/9666102-cyber-security-the-lost-decade-2019-edition

Strategy						
1	2010	The Business Model for Information Security	ISACA	ISACA	74	9781604201543
2	2010	Security Strategy	Bill Stackpole, Eric Oksendahl	Routledge	346	978-1439827338 https://www.amazon.com/dp/1439827338/
3	2015	The Strategy Handbook—Part 1: Strategy Generation (A Practical and Refreshing Guide for Making Strategy Work)	Jeroen Kraaijenbrink	Effectual Strategy Press	199	978-9082344301 https://www.amazon.com/dp/9082344300/
4	2017	The Strategy Handbook—Part 2: Strategy Execution	Jeroen Kraaijenbrink	Effectual Strategy Press	197	978-9082344332 https://www.amazon.com/dp/9082344335/

	Year	Title	Author	Publisher	Pages	ISBN
Security culture						
1	2015	People-Centric Security: Transforming Your Enterprise Security Culture	Lance Hayden	McGraw-Hill Education	416	978-0071846776 https://www.amazon.com/dp/0071846778/
Risk management and security strategy						
1	2015	Risk Savvy: How to Make Good Decisions	Gerd Gigerenzer	Penguin Books	336	978-0143127109 https://www.amazon.com/dp/0143127101/
2	2018	Cyber Risk Management: Prioritize Threats, Identify Vulnerabilities and Apply Controls	Christopher J. Hodson	Wiley	224	978-1119429517 https://www.amazon.com/dp/0749484128/
3	2019	Managing Cyber Risk, 1st Edition	Ariel Evans	Routledge	136	978-0367177744 https://www.amazon.com/dp/0367177749/
General security—history and vendors						
1	2020	Security Yearbook 2020: A History and Directory of the IT Security Industry	Richard Stienno	It-Harvest	328	978-1945254048 https://www.amazon.com/dp/1945254041/

Verizon 2020 Payment Security Report

Published October 6, 2020

Editorial team

Lead author

Ciske van Oosten

Co-authors

Anne Turner, Cynthia B. Hanson, Dyana Pearson, Dennis Merenguelli, Sky Hackett

Data analysts

Anne Turner, Dyana Pearson, Ron Tosto, Suzanne Widup, Sky Hackett

Contributors

Emmanuel Baeyens, Franklin Tallah, David Kennedy, Rafeeq Rehman, John Galt, Halli Goodman, Jyri Ryhanen, Loic Breat

Content editor

Cynthia B. Hanson

Co-editors

Anne Turner, Dyana Pearson, Sky Hackett, Rein van Koten, Suzanne Widup

Security assurance practice

PCI and payment security consulting practice

Global lead: Sean Sweeney

PCI security practice managers

APAC region: Sebastien Mazas

Americas region: Franklin Tallah

EMEA region: Gabriel Leperlier

Global intelligence: Ciske van Oosten

Team email

paymentsecurity@verizon.com

PCI DSS data contributors

Third-party contributors

The Advantio Team, Dustin Rich (A-Lign), Héctor Guillermo Martínez, Alberto España, Rogelio Nova, Russell M. Latimer (GMSectec), Anthony Petruso, Michael Vitolo (MegaPlanIT), Jacob Ansari (Schellman)

WP10650920