



State of Cybersecurity Report 2019



Contents



Foreword	II
Editor's note	III
In the spotlight	IV

Executive summary

1

- 02 Changing attacker stratagem
- 04 Changing defender stratagem

Security trends by industry

6

- 07 Energy, Natural Resources & Utilities
- 09 Manufacturing
- 11 Consumer
- 13 Health
- 15 Banking, Financial Services & Insurance
- 17 Communications



State of attacks, breaches and law

19

- 20 Analysis of 2018 data breaches
- 22 Analysis of global threat intelligence insights
- 25 Cyberweapons
- 28 Vulnerabilities in cyber defenders
- 30 Regulations

State of cyber resilience

32

- 35 Security governance
- 41 Security practices



State of collaboration

52

- 53 Multi-stakeholder collaboration in cybersecurity
- 56 Threat intelligence feeds
- 57 Information sharing
- 58 Cyberattack simulations
- 59 Cyber insurance

Future of cybersecurity

60

- 61 Cybersecurity patents
- 64 Seed investment trends in cybersecurity start-ups
- 65 PUF-based authentication for IoT security: An alternative approach
- 68 Security pillars of 5G

Methodology & demographics

71

Contributing partners

74

Credits & key contributors

75

Wipro's Cybersecurity & Risk Services

76

References

77



Raja Ukil

*Senior Vice President, Global Head,
Cybersecurity & Risk Services*

@raja1847

[linkedin.com/in/rajaukil/](https://www.linkedin.com/in/rajaukil/)

Dear Readers,

Wipro is happy to present the third edition of the “State of Cybersecurity Report (SOCR)”. Our journey with this report started with the publication of the first edition in 2017 and since then, the readership has grown to over 1000+ security leaders around the world. Cybersecurity has become a board-level concern today, due to escalating nation-state attacks. In fact, the World Economic Forum’s (WEF) Global Risk Report 2019 has rated cyberattacks amongst the top 4 global risks, only behind climate change, extreme weather events and natural disasters.

Cyberattacks have moved on from traditional techniques and have become more targeted and sector-specific. Attackers are operating in stealth mode making attribution of attacks more difficult.

Digital transformation has taken centre-stage and new technologies like cloud and IoT are increasing the attack surface of an organization’s digital assets. As a consequence, attackers around the world are arming themselves with innovative tool sets. In order to provide resistance to impending attacks, it is crucial for organizations to heighten their level of preparedness and strive to achieve proactive resilience.

Over the years to achieve resilience, organizational structures relating to ownership of cybersecurity and data privacy have evolved. The heightened awareness of cyber risks by the board, has driven the evolution of the role of the CISO. Over 21% of CISOs surveyed are directly reporting to or have operational visibility to the CEO. Security budgets are also on the rise, with almost one-third of organizations surveyed having a security budget which is greater than 8% of their overall IT budget.

The report also captures the changing strategies used by attackers and highlights how organizations today are bolstering their defenses to stay one step ahead. It concludes with a peek into the cybersecurity areas that will be pertinent in the near future.

We hope that you will benefit from the global and industry-specific insights available in this edition of the State of Cybersecurity Report and that together, we will be able to make our enterprises more resilient to withstand and recover from future attacks!



Josey V George

Editor-in-Chief: State of Cybersecurity Report 2019
Practice Head, Cloud & IoT Security @ CRS

@joseyvg

[linkedin.com/in/josey-george](https://www.linkedin.com/in/josey-george)

Dear Readers,

Welcome to yet another edition of Wipro's annual "State of Cybersecurity Report (SOCR)!"

This year, we have a spectrum of research findings that will be presented across 5 sections of the report.

The executive summary is not to be missed as it lays out the cybersecurity paradigm as a battle of stratagems between attackers and defenders. We are hoping that our readers can recognize some of these stratagems from their experiences in protecting digital assets and will explore others that are new.

For those of you who are looking for vertical-specific cybersecurity trends, please do check out the section titled "Security trends by industry." This section in the SOCR holds key insights to benchmark your enterprise against the rest of the industry and this data has come from the 211 organizations that chose to respond to our survey.

What were the most common cyberweapons that enterprises were exposed to? How are countries around the globe tightening breach notification laws? These are the questions that are dealt with in the section titled, "State of attacks, breaches and law."

We are seeing a clear shift in the role of the Chief Information Security Officer (CISO) within organizations. Please read the section titled,

"State of cyber resilience" if you would like to explore how this evolution is happening and how CISO teams are measuring their performance and domain practices.

This year, we have included a contribution from the Data Security Council of India (DSCI)—an industry body for data protection in India set up by NASSCOM®. Thank you Vinayak and DSCI for enriching this year's SOCR with the perspective on "Multi-stakeholder collaboration in cybersecurity." You can jump to the section, "State of collaboration" to find this article and other related research.

I also want to thank Professor Debdeep from the Indian Institute of Technology, Kharagpur, and Professor Ashutosh, Co-Chair of IEEE Future Networks (and staff at Johns Hopkins University) for their insightful contributions on IoT and 5G security respectively in the "Future of cybersecurity" section of SOCR.

I have to also thank our technology partners, Checkpoint, Palo Alto Networks, Intsigths, Denim Group, Device Authority, CyCognito, Rapid7, Tracxn and Fortinet for their support with collaborative research and correlation of the findings.

I hope you will enjoy reading SOCR 2019. If you like our work, please share it with your colleagues in the industry and do continue to write to us with your valuable feedback.



The rise of cryptominers

Around 25% of global organizations were attacked by Coinhive malware last year.

Page 26



Cyber diplomacy

Countries are establishing active cyber diplomacy functions to foster partnerships with each other in the matter of cybersecurity.

Page 53



Vulnerabilities in cyber defenders

Vulnerabilities in security products is an elephant in the room, which often goes unnoticed.

Page 28



Cybersecurity patents

Patents highlight the cybersecurity areas corporations, governments and educational institutions are investing in.

Page 61



Evolving role of the CISO

The CISO role is facing heightened scrutiny from the executive leadership and the board.

Page 35



Security pillars of 5G

A secure 5G ecosystem will help enable vertical use cases that will transform the way humanity lives, works, and engages with its environment.

Page 68





The world as we have created it is a process of our thinking. It cannot be changed without changing our thinking.

Albert Einstein

The third annual edition of the “State of Cybersecurity Report” from Wipro builds on providing a unique perspective of the building blocks that define the global cybersecurity arena. While the report covers a wide spectrum of topics, the long and short of the ensuing cyber spectacle is the real battle that unfolds daily between two broad actors: the attacker and the defender. To understand what played out during the past year and what is possibly in store in the coming

future, one needs to understand their changing stratagems. The strategies that are employed by actors on either side of the cyber divide (attackers and defenders) are constantly evolving but they can be discerned by drawing out recurring patterns that can be observed through the year. The summary below draws insights from different parts of the report to bring together stratagems from either side of the divide.

Changing attacker stratagem

Stratagem 1: Wide diversification is not required, stay focused

Attackers have become more sophisticated, engineering targeted strikes resulting in a higher breach rate (notional records stolen per second), yet cumulative number of significantly recorded breaches has come down by 25%. The health and

financial sectors have been at the receiving end of almost half the cyberattacks perpetuated in 2018. Attackers find it more profitable to steal user data with credentials like passwords, enabling them to launch further strikes and multiply the return.

25%

decrease in number of significant publicly recorded breaches

Exponentially increasing breach rate

232 records/sec
88 records/sec
43 records/sec

48%

of significant publicly recorded data breaches were from the health and financial services sector

38%

of the data records breached/targeted were a combination of Personally Identifiable Information (PII) and security credentials like passwords

Stratagem 2: Don't let go of tried and tested weapons!

The Trojan horse still rules accounting for more than half of the malware attacks—as seen by Wipro's Cyber Defense Center (CDC). The top 10

types of web application vulnerabilities have stayed put during the last few years, making way for attackers to employ repeatable web exploits.

57%

of total malware attacks in 2018 were Trojan attacks (up by 7% from 2017)

25%

of total Trojan attacks were from Heur.AdvML.B & Heur.AdvML.C

22%

of total exploits in 2018 were web exploits (up by 10% from 2017)

15%

of total exploits in 2018 were Remote Code Execution exploits (up by 10% from 2017)

Stratagem 3: Invest in an element of surprise

As technologies advance, so do attacker tactics. As ransomware saw a decline, a surge in cryptominer malware was observed in 2018. Three cryptominer malwares stood out, contributing

to over 80% of cryptominer attacks. As existing vulnerabilities are mitigated, attackers will aggressively migrate to new tactics, keeping the ball rolling.

Mining was on overdrive, ransomware took a backseat

25%
of global organizations were targeted by Coinhive malware in 2018

80%
of cryptomining attacks were from Coinhive, Cryptoloot and JSEcoin

Stratagem 4: Attack the opponent by targeting its generals

Today, organizations expect leaders to have an established social presence. Attackers are leveraging this trend and are creating fake social media profiles and assets to launch whaling attacks. Attackers are targeting companies and

their divisions/products represented in the social space, harming their collective brand reputation. The consumer and retail sectors are targeted more often than others.

26%
of fake social media profiles came from the consumer & retail sector

20%
of fake social media profiles can be traced to LinkedIn

19%
of fake social media profiles can be traced to Facebook

8%
of fake social media profiles can be traced to Twitter

Stratagem 5: Know your opponents DNA

To successfully carry out a sophisticated attack, attackers get intelligence around their targets' assets, suppliers and defenses. Prep work is paramount when partaking in a no-holds-barred

operation. From identifying company and employee assets to analyzing the vulnerabilities in the defense layer, attackers are leaving no stone unturned.

Profiling the company assets, IT staff from public sources

Identifying the type of PII and quantity of data you desire from your target

Firewalls and VPNs have a higher propensity for vulnerabilities with high CVE scores (6.73/10)

Stratagem 1: Crystallizing ownership and accountability in the fleet

With high-profile breaches, security has become a boardroom concern. Organizations are re-establishing governance for security with clearer executive reporting structures. CEOs are feeling the heat, which is evident from the 22% of Chief Information Security Officers

(CISOs) who are reporting straight to the CEO. This number is expected to grow in the coming years. Regulations like GDPR have mandated the position of Data Protection Officer (DPO) in many European organizations, with other countries following suit.

21%

of CISOs report straight to the CEO, while 51% report to the CIO

49%

of organizations have their Line of Business Owner identify critical assets

51%

of European enterprises have a DPO/CPO that is directly accountable for data privacy

44%

of US enterprises have the CISO directly accountable for data privacy

Stratagem 2: Making the case for continuous resilience

Due to digital transformation programs, security budgets as a percentage of IT budgets are on the rise. However, there will be a point where the budgets will plateau. To accommodate this,

organizations are automating processes and building long-term partners to reduce cost without compromising continuous resilience and regulatory compliance.

15%

of organizations have a security budget of more than 10% of the overall IT budget

67%

of organizations are planning for broad business and process automation to lower costs

31%

of organizations will rationalize the portfolio of providers and build long-term partners

65%

of organizations are tracking and reporting regulatory compliance

Stratagem 3: The question is not about IF, but WHEN

The question is not about if but when the unthinkable breach materializes. Organizations are preparing themselves for the inevitable by partaking in cyberattack simulations coordinated by national

CERTs (Computer Emergency Response Teams) and industry regulators. In addition, more and more organizations are choosing to take up dedicated cyber insurance policies.

31%

of organizations participate in cyberattack simulation exercises coordinated by national CERTs

28%

of organizations participate in cyberattack simulation exercises coordinated by industry regulators

39%

of organizations have a dedicated cyber insurance policy—up by 12% from 2017

25%

of organizations are carrying out security assessments in every build cycle—up by 4% from 2017

Stratagem 4: Empower and bring the “common” back in common sense

Humans are the weakest link in security and organizations are only as strong as the weakest link. Employee negligence and lack of awareness continue to cause security

incidents. Enterprises will have to continue to invest in security education through e-Learning and other mediums to strengthen the human dimension of security.

72%

of organizations say employee negligence and lack of awareness is a top cyber risk

64%

of organizations say insider threat is a top risk

81%

of manufacturing organizations say that lack of awareness is a top cyber risk

87%

of organizations use e-Learning or CBTs to educate employees on security practices

Stratagem 5: Change is inevitable; progress is optional

With organizations riding the digital wave, cloud and IoT adoption is on the rise. Security strategies need to be enhanced to address this changing landscape to enable a smooth and safe transition.

This could include leveraging and consuming best-of-breed security anywhere, including security from the cloud.

60%

of organizations surveyed expect to have 10% of their asset base disrupted with IoT devices in 2 years

26%

of organizations perform security assessment of IoT devices

40%

of organizations surveyed are migrating customer Personally Identifiable Information (PII) data to the cloud

27.2%

growth seen in cybersecurity related patent filings globally between 2016 and 2018

Stratagem 6: United we stand, divided we fall

Collective wisdom is better than learning in isolation. Organizations are actively consuming intelligence from national CERTs and regulators on a regular basis. To make the sharing

networks more useful, it is paramount that intelligence-sharing is not a one-way street but a symbiotic relationship, thus enriching the value for all participants.

84%

of organizations rely on their SIEM vendors to provide threat intelligence

56%

of organizations are consuming threat intelligence from national CERTs

67%

of organizations are willing to share indicators of compromise—malicious IPs, URLs, domains

33%

of organizations are willing to share attacker tactics, techniques and procedures



Security trends by industry

Energy, Natural Resources & Utilities

Manufacturing

Consumer

Health

Banking, Financial Services & Insurance

Communications

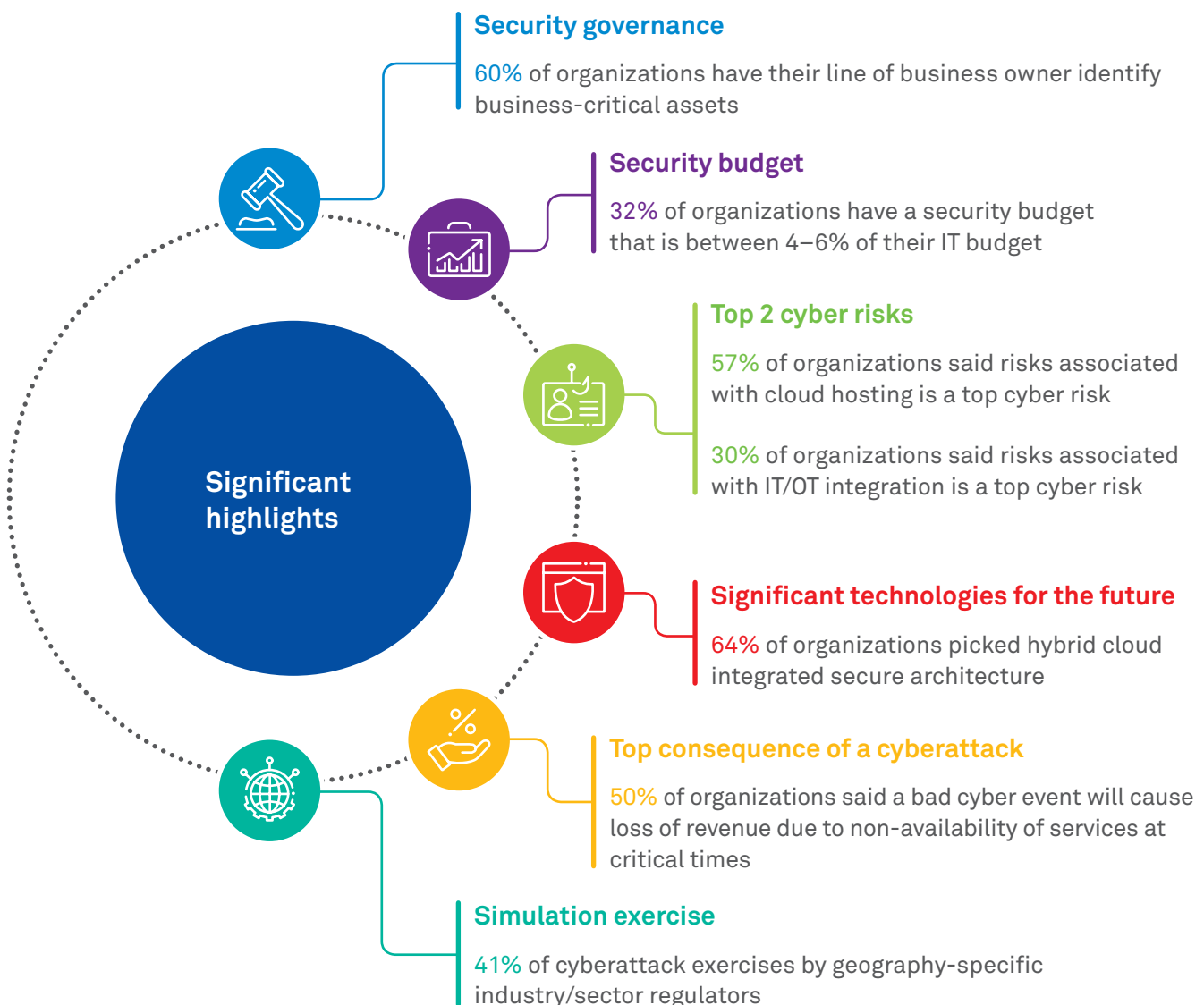
Energy, Natural Resources & Utilities



The energy, natural resources & utilities sector is notable for its dependence on industrial control systems (ICS) and operational technology (OT) and is part of a nation's critical infrastructure. The digital transformation of the sector is being accelerated by technologies such as IoT, making the sector vulnerable to cybersecurity attacks by nation-states, hacktivists, criminals and other adversaries. That situation is compounded by the challenges of the sector's aging infrastructure and changing regulatory and compliance regimes.

The year that was:

Threat actors have targeted government entities in multiple critical infrastructure sectors within the energy, natural resources & utilities space using spear phishing, watering hole and host-based exploits.



Key insights - Energy, Natural Resources & Utilities

• Connected devices and cloud adoption are increasingly exposing cyber-physical systems to the Internet.

• Oil & gas is moving towards industrialized automation, including control and safety systems which can be remotely accessed through a central “hub.”

• The financial loss due to cybersecurity incidents in the energy, natural resources & utilities sector occurs due to production shutdown, critical infrastructure loss, business continuity disruption, financial information theft and intellectual property theft.

• The use of aging infrastructure and of legacy software applications, products and services with known vulnerabilities is a persistent problem.

• Human error factors such as opening an email attachment, inserting a corrupted pen drive, charging IoT devices are common vectors for malware proliferation.

Closing thoughts

The energy, natural resources & utilities sector is increasingly vulnerable to cybersecurity threats and attacks given the pace of digitization, IT/OT convergence, and the potential impact to critical infrastructure, public health and safety, and the environment. Adversaries such as nation-states pose a persistent threat to the sector. Companies are trying to keep up with the sophistication of attackers while reducing the risk to OT infrastructure and protecting confidential information from unauthorized access.

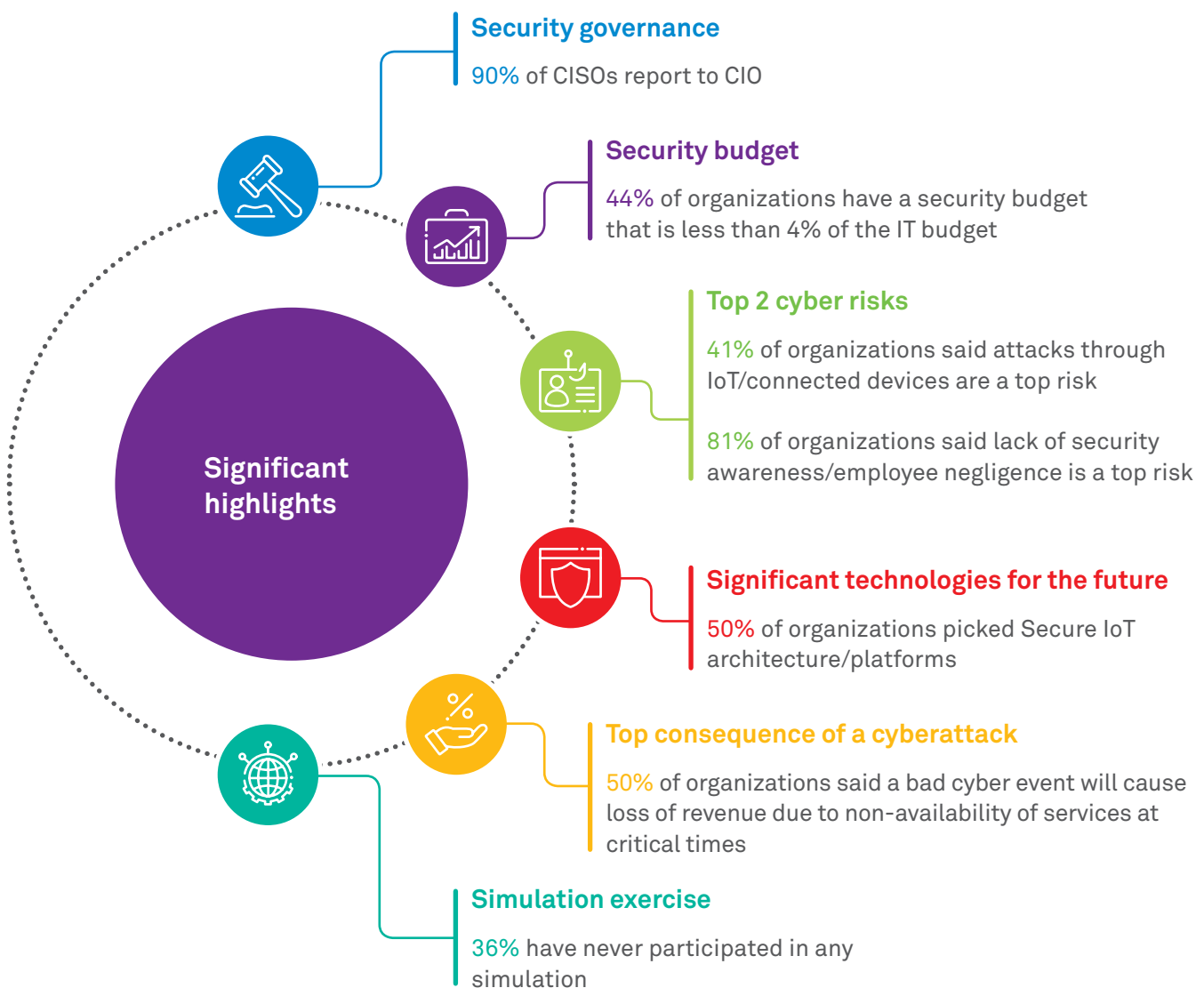
Manufacturing



The global manufacturing industry is being shaken by a revolution in technology. Offensive cyberattacks are actively targeting the sector. However, the maturity of cyber defense responses continues to lag behind other highly targeted sectors like health and banking. The technology revolution driven by Industry 4.0, IIoT and the evident need to address OT security is resulting in significant pressure being placed on CISOs to rapidly assess the risks and put in place strategic programs to defend against ever-increasing threats.

The year that was:

In 2018, there were 52 significant publicly reported breaches in the manufacturing sector, with attackers targeting information pertaining to intellectual property.



Key insights - Manufacturing

Cyberattacks on factories can have a crippling effect on production capacity. Attacks will likely target unprotected legacy OT environments and expose the vulnerabilities of new IoT Smart Factories.

Air gaps are no longer a viable cybersecurity strategy for manufacturing organizations. A new business-focused and converged IT/OT/IoT cyber strategy is required—backed by increased awareness.

Lack of cyber preparedness, with very limited participation in cyberattack simulation exercises are evident across the sector despite the prevalence of high-profile incidents, financial losses and increasing recognition of business risks.

14% of assets offered on the dark web are from this sector; industrial designs, blueprints and manufacturing operating parameters are some of the key sought-after assets.

Closing thoughts

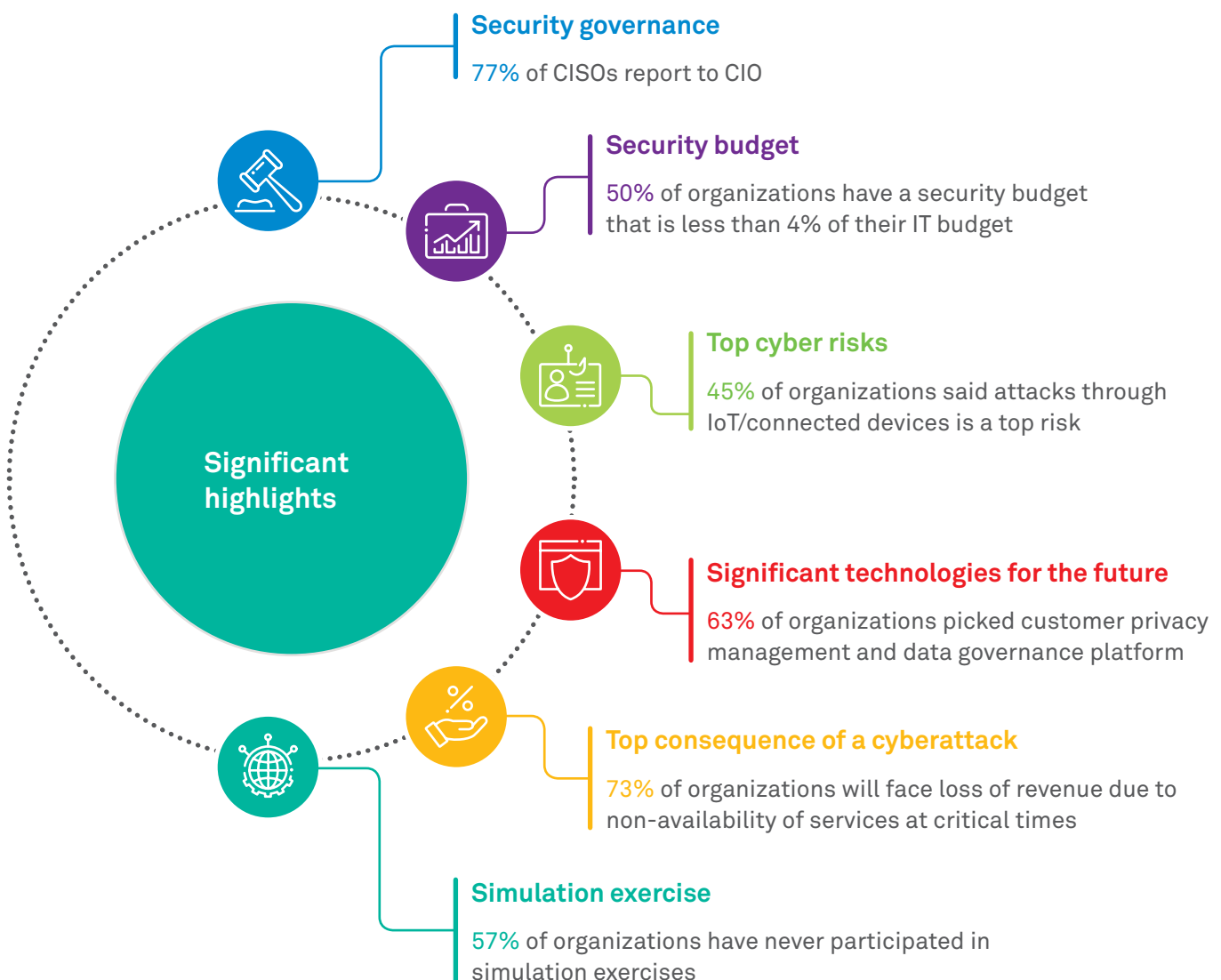
The manufacturing sector is at an inflection point as it responds to the technology revolution impacting its previous modus operandi. Industry 4.0 and Smart Factory production, alongside development of IIoT solutions, will shape the future of the manufacturing sector. The success of these new business operating models is underpinned by effective cybersecurity and data privacy. Establishing an accelerated and sustainable approach to delivering the fundamentals of cyber hygiene is necessary to protect the core business. Failure to address this will have a detrimental impact on consumer and institutional confidence and fundamentally weaken its future trading capability and position in the marketplace. 2019/2020 is likely to see an era of unprecedented cybersecurity investments across the manufacturing sector as organizations play catch-up and seek to rapidly address previous shortcomings and modern risks.



The consumer industry encompasses a vast variety of markets and company profiles, ranging from retail, media, food, consumer products, travel and hospitality, and more. Despite many dissimilarities, most companies in this sector share a few common characteristics and trends when it comes to cybersecurity. Overall, digital transformation is expedited through the adoption of connected technologies across the sector. CISO budgets as a percentage of IT budgets are still low compared to other industries. This will see a change as regulatory pressures increase. The likely key cybersecurity challenge of the consumer industry is to promote data protection at the core of the business culture.

The year that was:

The consumer industry faced 198 significant publicly reported breaches in 2018, with customer card and PII data being the top data sought.



Key insights - Consumer

- Brand security is a legitimate concern as 25% of fake social media profiles/whaling attacks are from this sector.

- Consumer organizations fall prey to phishing attacks with 25% of attacks using registered suspicious domains coming from this sector.

- Erosion of customer trust due to a breach can jeopardize growth in a highly competitive environment.

- Rapid growth of connected devices and IoT in the retail space in applications like smart shelves, automated check-out systems and beacons have expanded their attack surface.

- The changing regulatory landscape with GDPR, PCI, etc., especially on consumer information and privacy, has organizations scrambling to lower cost of regulatory compliance while avoiding dreaded fines.

Closing thoughts

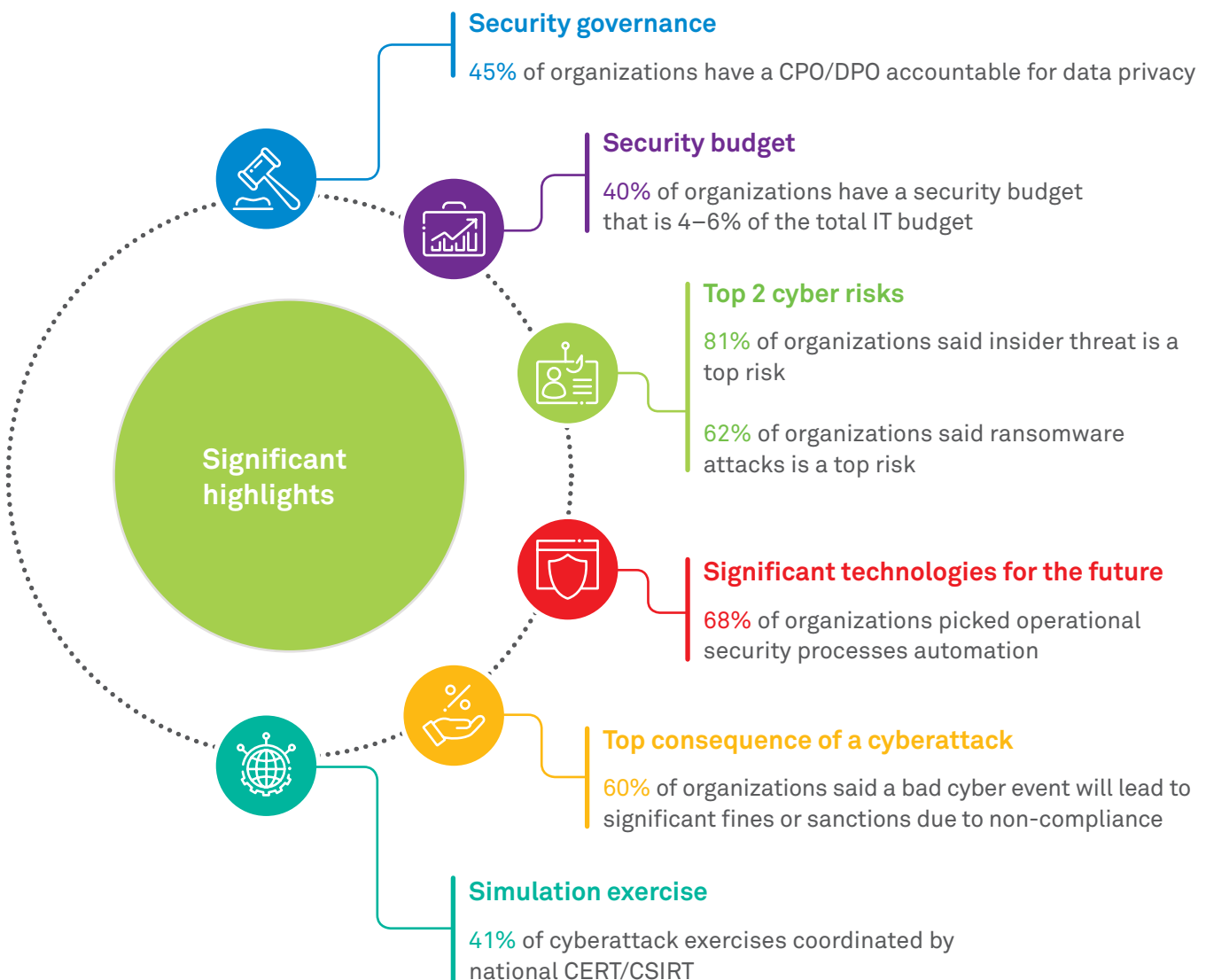
Consumer organizations riding the digital wave have the added pressure of protecting customer data. CISOs are playing catch-up with their security strategy and have a huge opportunity to adopt mature security practices and paradigms to ensure digital resilience.



The health industry has consistently been the most targeted sector in terms of the number of significant cyberattacks over the last few years. Many organizations, especially in the provider space, are known to operate on legacy IT infrastructure, weak from a security perspective and this problem has been compounded with the arrival of the connected Internet of Medical Things (IoMT) that are difficult to secure. Cybersecurity risks are no longer confined to IT assets and data breaches; they are now directly impacting patient safety.

The year that was:

2018 saw 485 significant publicly reported breaches in the health sector. Attackers were after PII and medical records, along with valuable pharmaceutical intellectual property.



Key insights - Health

- As healthcare organizations continue to move Electronic Health Records (EHR) and PII data to the cloud, security and compliance considerations need to be incorporated from the early stages.

- New-age devices for IoMT come with network connectivity that poses serious cybersecurity risks, allowing hackers the opportunity to take remote control of these devices.

- Wearable and implantable healthcare devices, from insulin pumps to monitors and pacemakers, can be vulnerable to attack.

- Ransomware will continue to be a major information security threat to healthcare providers in 2019 and will accelerate the upgrade of legacy systems and associated security controls to mitigate these threats.

- 13% of assets offered on the dark web are from health institutions.

Closing thoughts

The health industry is witnessing a transformation in cybersecurity strategy from a narrow compliance and Health Insurance Portability and Accountability Act (HIPAA)-focused approach to a more comprehensive and security-centric approach. As regulations around the world start to address the safety and security of IoMT devices, healthcare providers will have to step up the game on cyber resilience.

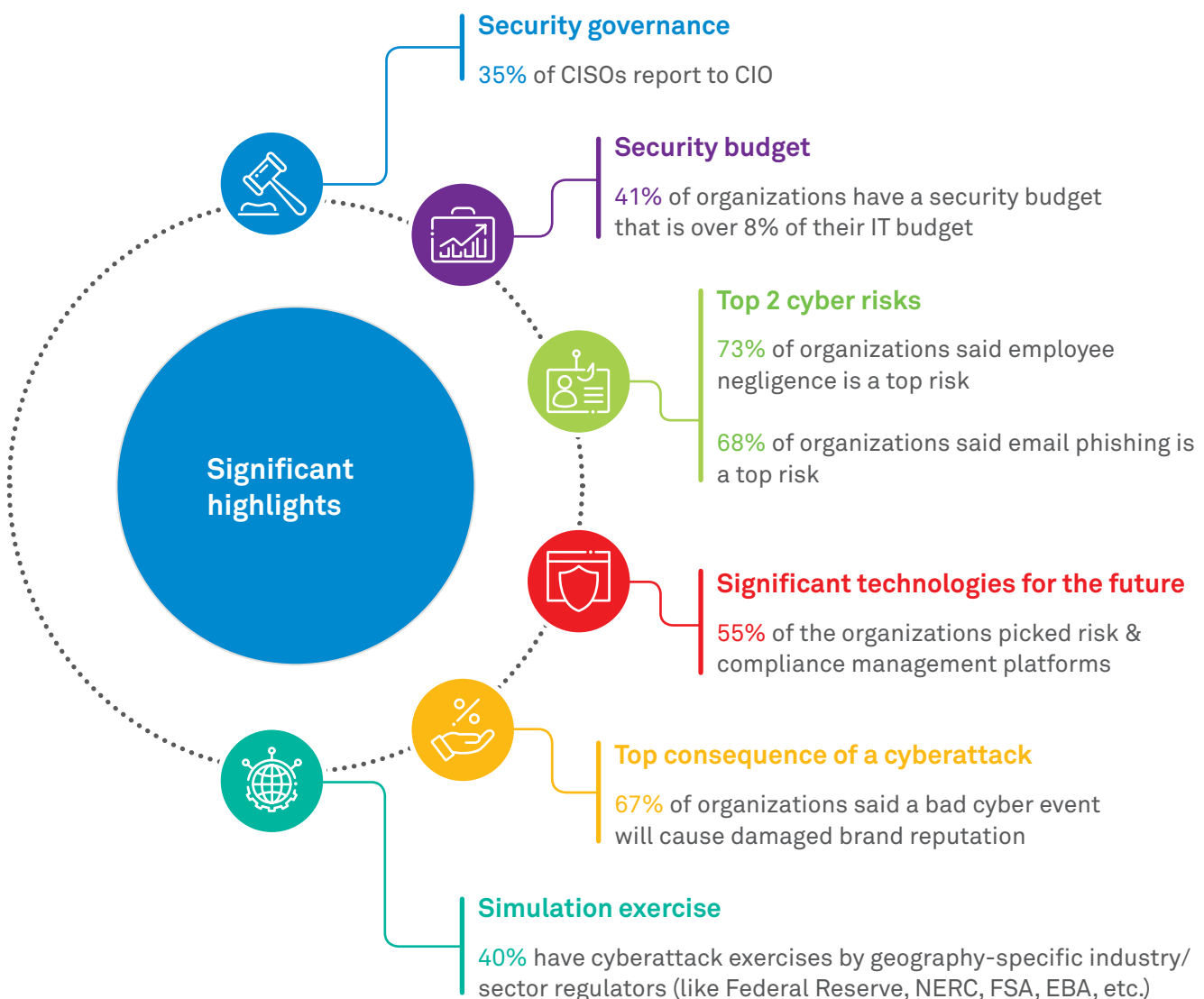
Banking, Financial Services & Insurance



The Banking, Financial Services & Insurance (BFSI) sector is consistently one of the most targeted sectors. Due to the nature of the data it holds, it is also one of the most regulated and mature industries when it comes to cybersecurity. Digitalization has transformed multiple channels and enhanced user experience.

The year that was:

The BFSI industry faced 348 significant publicly reported breaches in 2018, with PII and financial record data being the most sought after.



Key insights - BFSI

36% of suspicious applications are targeted at BFSI organizations with attackers using phishing to get access to user credentials.

European banks will continue to face increasing regulatory pressure, with new regulations like GDPR and Revised Payment Services Directive (PSD2) coming into force.

Banking organizations are now required to enable customers to share their data, in a secure manner, with third parties using APIs. Consumers will then have greater freedom and control in how they interact with their financial service providers. These API interfaces will have to be designed for high security.

24% of assets offered on the dark web are from BFSI organizations. This is not surprising as financial records/ card details are very lucrative.

Since blockchain is getting evaluated as a technology for trade processing, settlement and cross border payments, security practices will play a prominent role in keeping the blockchain safe.

Closing thoughts

Financial institutions have been early adopters of emerging cyber technologies or controls to counter new threats. They need to consciously review their cyber resiliency practices to protect themselves against the onslaught of attacks headed their way.

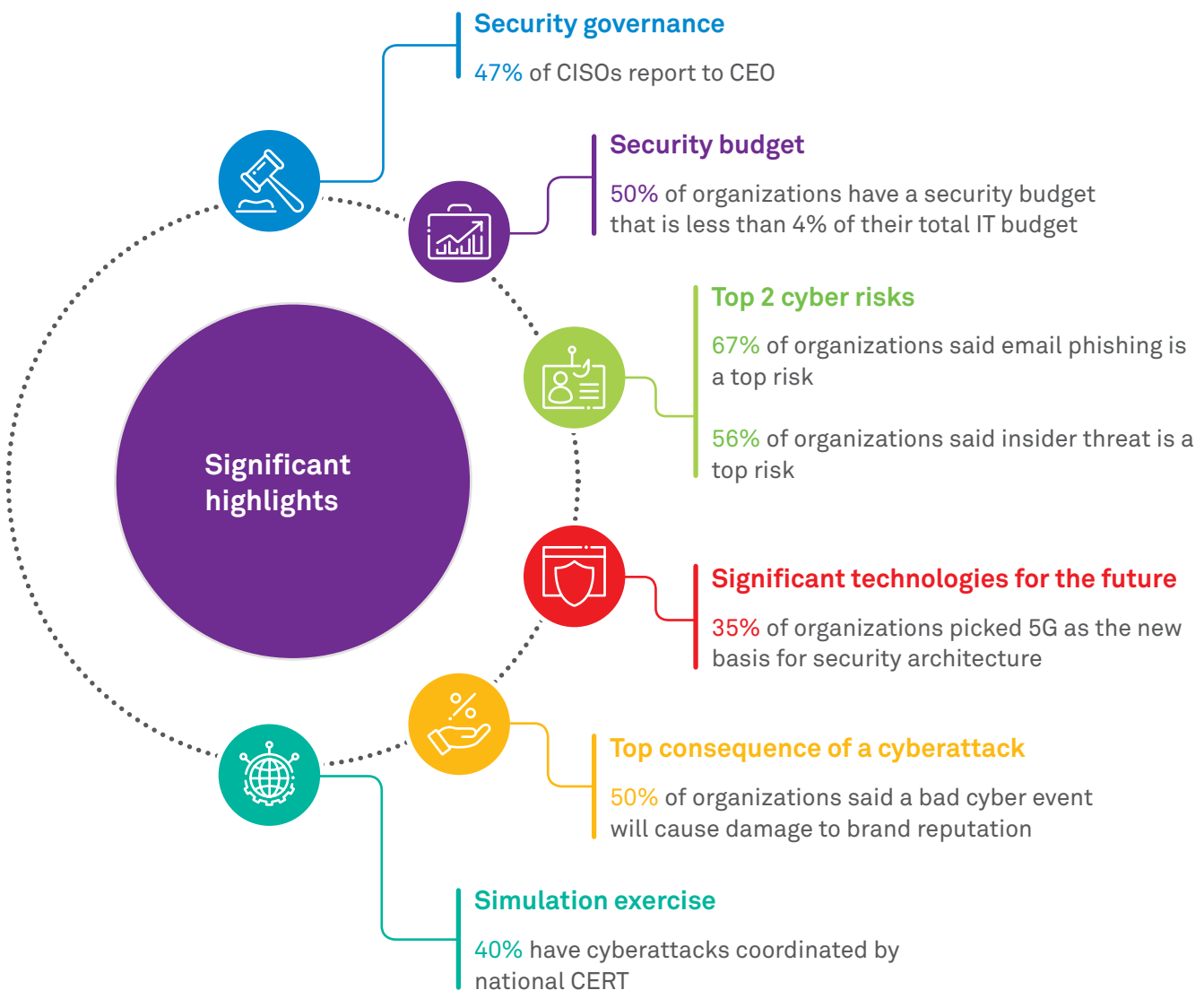
Communications



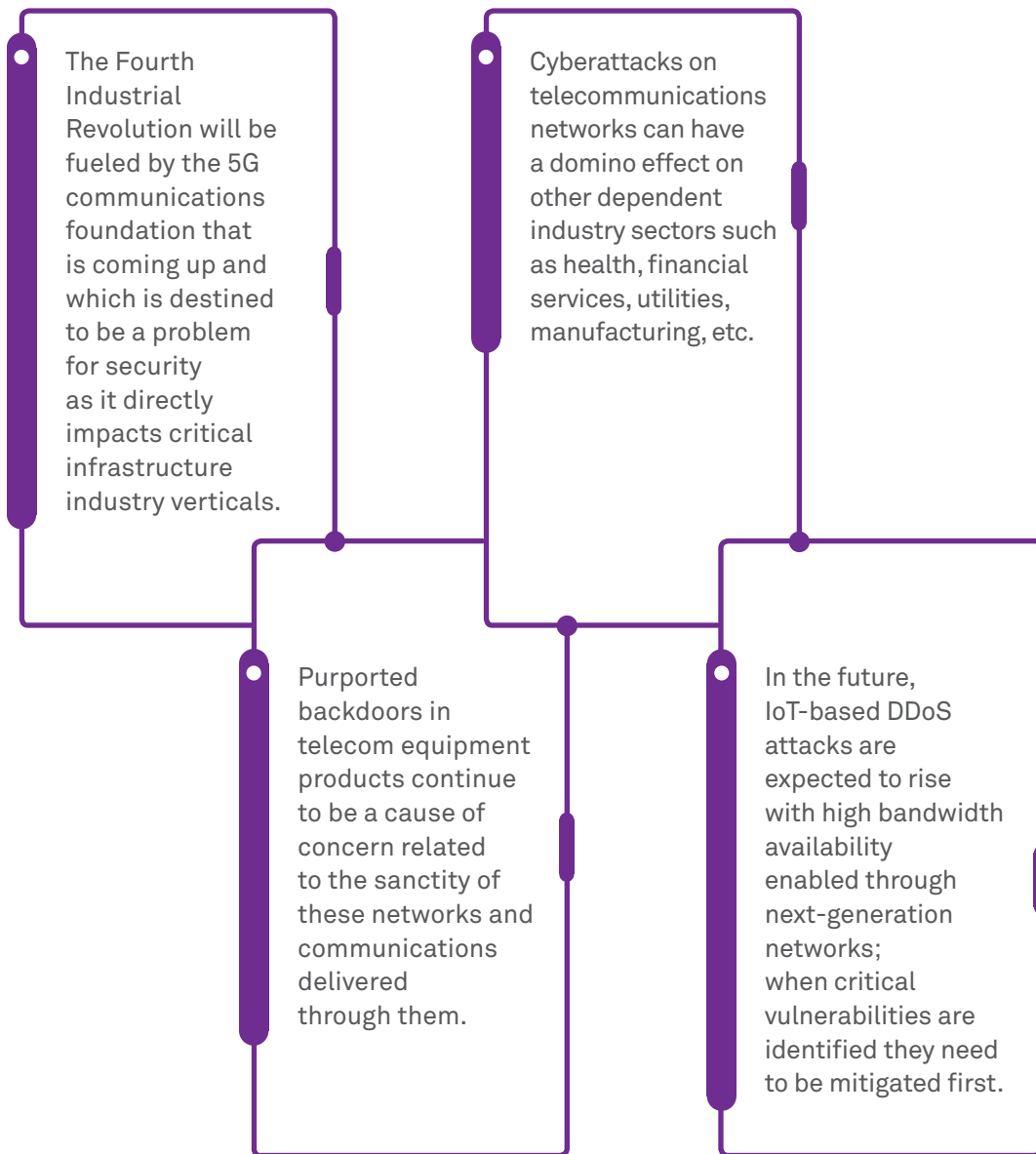
Communications carriers are in the middle of a continuing technological evolution with the emergence of 5G networks. Software Defined Networks (SDN) are transforming network management and cloud computing is helping telcos scale for growth. But with these opportunities, are the risks being ignored? Mobile network security issues have become quintessential with the advent of 5G networks; the progress transforms the communications network into a crucial fuel for the Fourth Industrial Revolution with remote monitoring of industrial systems, utility networks, medical devices and self-driving vehicles.

The year that was:

2018 saw a data breach that exposed millions of customer PII and billing data from a leading European telecommunications company.



Key insights - Communications



Closing thoughts

Adopting a cyber resilience framework that can propel the maturity of security processes and technology in the new-age communications enterprise will help mitigate new emerging risks. User security awareness, consumer identity management, third-party risk management, and good patch management is expected to aid in reducing cybersecurity risks across both the carrier network and organizations attached to it.



State of attacks, breaches & law

Analysis of 2018 data breaches

Analysis of global threat intelligence insights

Cyberweapons

Vulnerabilities in cyber defenders

Regulations



Know your enemy and know yourself and you can fight a hundred battles without disaster.

Sun Tzu

The “State of attacks, breaches and law” section lays out the macro view that defined cybersecurity around the globe in the year that went by. It peeks into the data breaches that shook the world and the weapons of cyber destruction that made it happen. Trends such as the rise of cryptominers and the fall of ransomware indicate the changing attacker stratagems. Further, the section weaves its way into the troublesome territory of analyzing security weaknesses in commercial security

products and what that future holds out for CISOs and their teams as they leverage these products to fortify their defenses. This section concludes with the evolution of breach notification and privacy laws in 23 countries. It calls out countries that have stringent norms to protect consumer data and limit the cross-border flow of information. Overall, this section brings to the forefront the changing strategies employed by attackers.

Analysis of 2018 data breaches

The year 2018 has seen a massive increase in the absolute volume of records that were breached (across publicly reported breaches worldwide). Over 1,700 publicly reported data breaches were analyzed as part of the research. The number of records compromised by these breaches over the past one year has increased by 164% when compared to the previous year. The average number of records lost per second (reported as Breach Rate)

notionally was 232/sec. Based on our 2018 report, health and the BFSI industries continue to be the most targeted by hacking groups across regions.

One very interesting trend that the research points to is that while the volume of records breached has cumulatively gone up, the cumulative number of publicly reported breaches has reduced by over 25% as compared to last year.

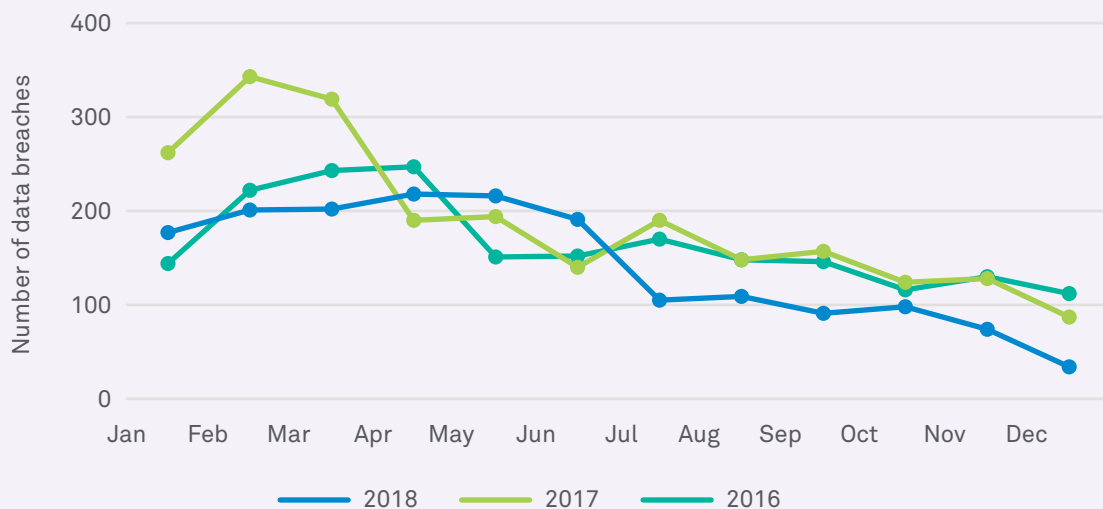


Figure 1: Number of data breaches per month

Data breach analysis across verticals

Large organizations have suffered huge data breaches over the last few years, impacting their brand reputation and leading to an overall loss in revenue.



Global insight

The number of publicly reported breaches has reduced by 25% in one year but the cumulative number of records exposed has increased by 164% to 232 records exposed/second.

Figure 2 shows the split of data breaches across various verticals in 2018. Health and BFSI saw the greatest number of breaches this year.

Vertical insight

The health industry contributed 28% (highest across all verticals) of the total data breaches in 2018.

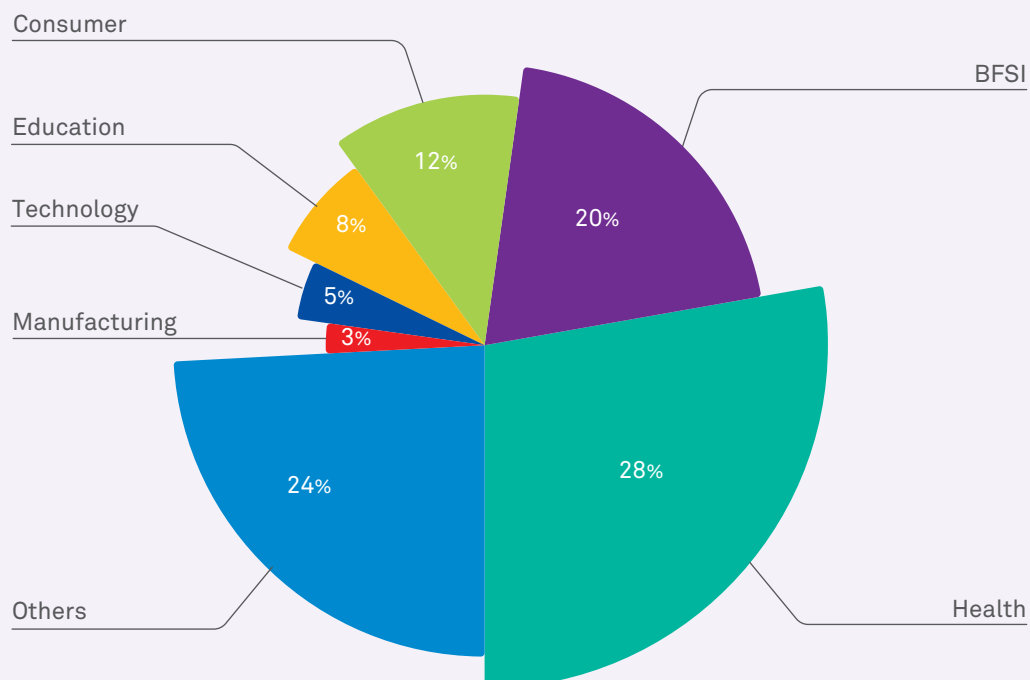


Figure 2: Data breaches spread across industry verticals

What data were the attackers after?

The data breach analysis research also explored the type of data that attackers were after by studying the patterns across the top 40 breaches of 2018. The types of breached data sets encountered were generalized into 10 categories as shown in Figure 3. The findings from this analysis highlight the following trends:

- Basic PII data as a leaked data set category has dropped significantly from 22% reported last year to 5%
- PII + user credentials has increased from 29% last year to 38%
- PII + financial records has increased from 12% last year to 26%

Global insight

Percentage of just basic information loss dropped from 22% to 5%, while PII + user credentials loss rose from 29% to 38% since last year. Many users use the same password credentials across multiple websites, making their passwords attractive.



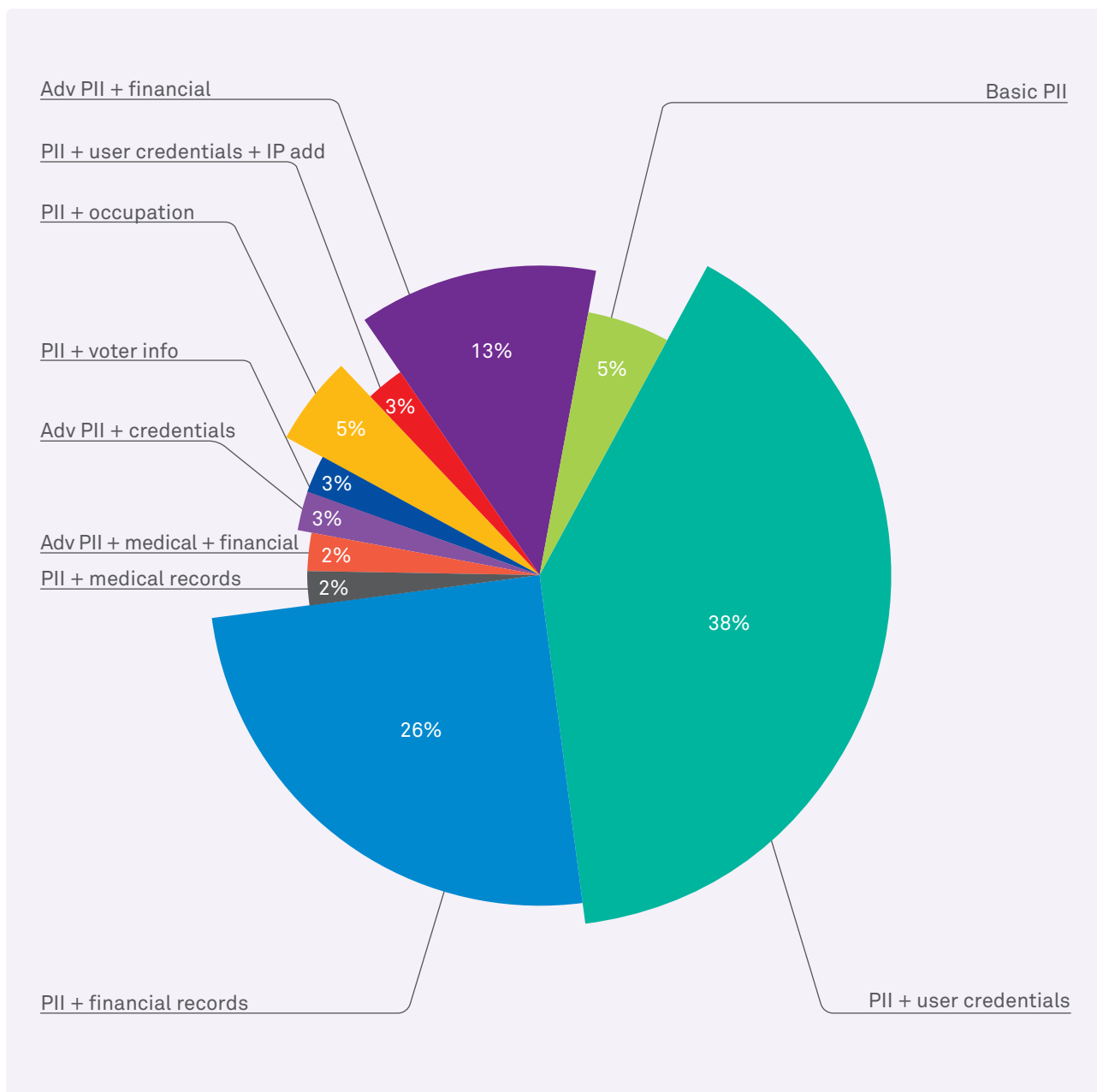


Figure 3: PII analysis of the data compromised

Attackers are more focused and are targeting more specific information in breaches that they perceive have higher monetary value. The trends

also seem to indicate that attackers are gaining more intelligence on the type and location of data that organizations possess.

Analysis of global threat intelligence insights

The following section looks at the different types of attacks targeted at industries. Wipro's venture partner, IntSights—a leading cyber intelligence organization—has contributed this section of the report. Using their external threat protection platform, IntSights threat researchers analyzed over 900,000+ alerts to arrive at their conclusions. The team dived deeper into the area of suspicious social media profiles.

Figure 4 shows the distribution of cyber intelligence alerts accumulated across various industries, spanning areas like phishing attacks on suspicious applications, suspicious social media profiles and various attack indicators like assets offered on the black market and telegram chatter.

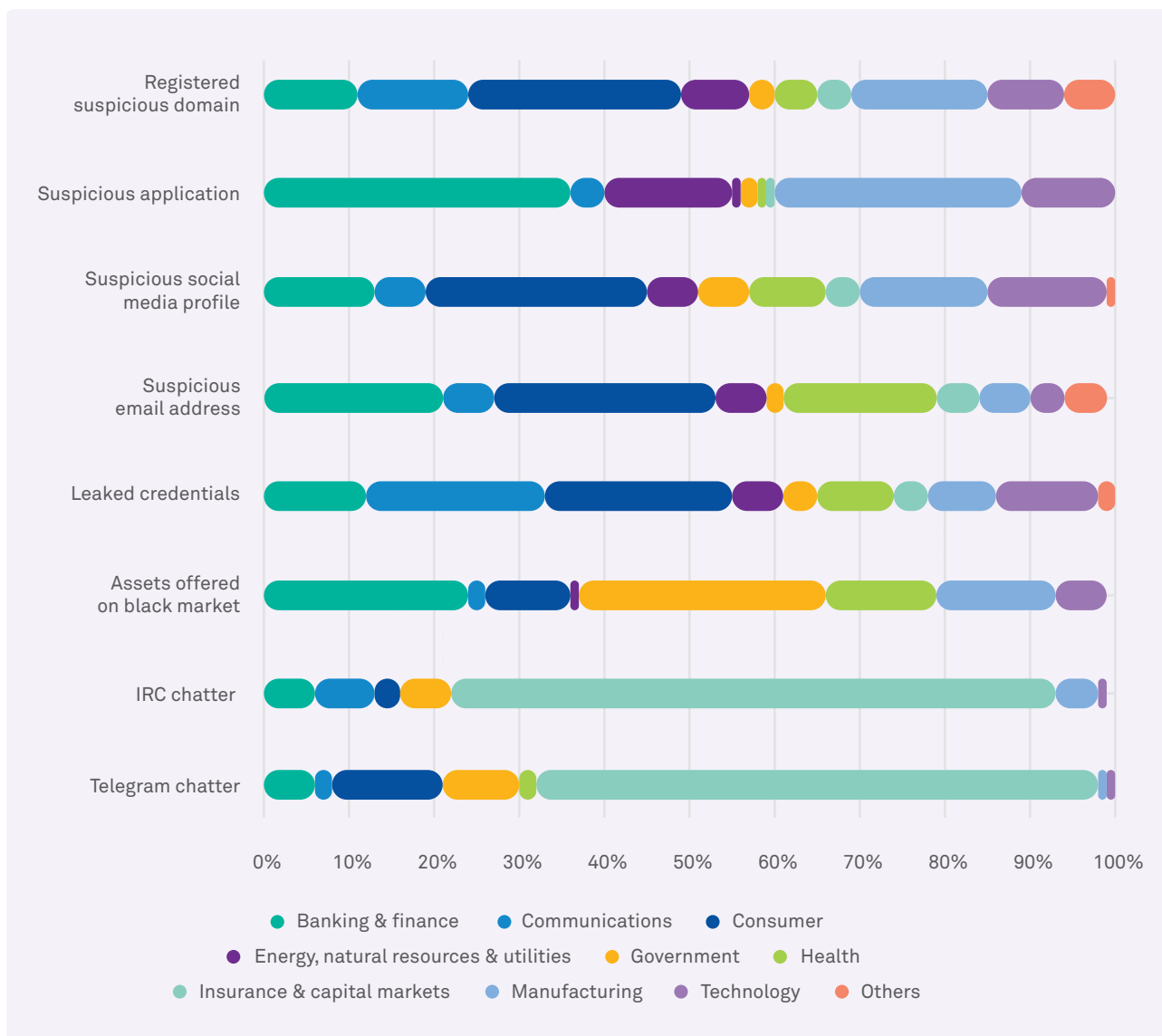


Figure 4: Distribution of threat intelligence alert types by industry

Suspicious social media profiles in 2018

Organizations today hold multiple social media handles to communicate with their customers. Malicious social media handles can put a company's reputation and brand at stake. Brand security is an important part of the defense perimeter of any enterprise. Not only does it mitigate possible image and reputation damages, but it also stops potential social engineering and spear-phishing attacks. For example, impersonating a VIP entity might provide hackers with an easy way to steal privileged credentials or propagate their malicious campaigns. Attackers are leveraging this opportunity and creating fake profiles across all channels of social media.

Are your social media assets at risk?

Hackers deploy fake social media profiles for a variety of reasons. They use it as grounds for phishing and social engineering attacks. Hacktivists and some state-sponsored Advanced Persistent Threats (APTs) deliberately misinform the general public and influence political views through fake profiles.

Criminal actors phish for credentials and confidential proprietary information by executing social engineering attacks disguised as employees of their target. Receiving an email from a familiar person or contact drastically increases the chance of credential theft or malicious infection.

Figure 5 shows how fake profiles are split across source sites. LinkedIn dominates, contributing to 20% of the fake profiles across various source sites.

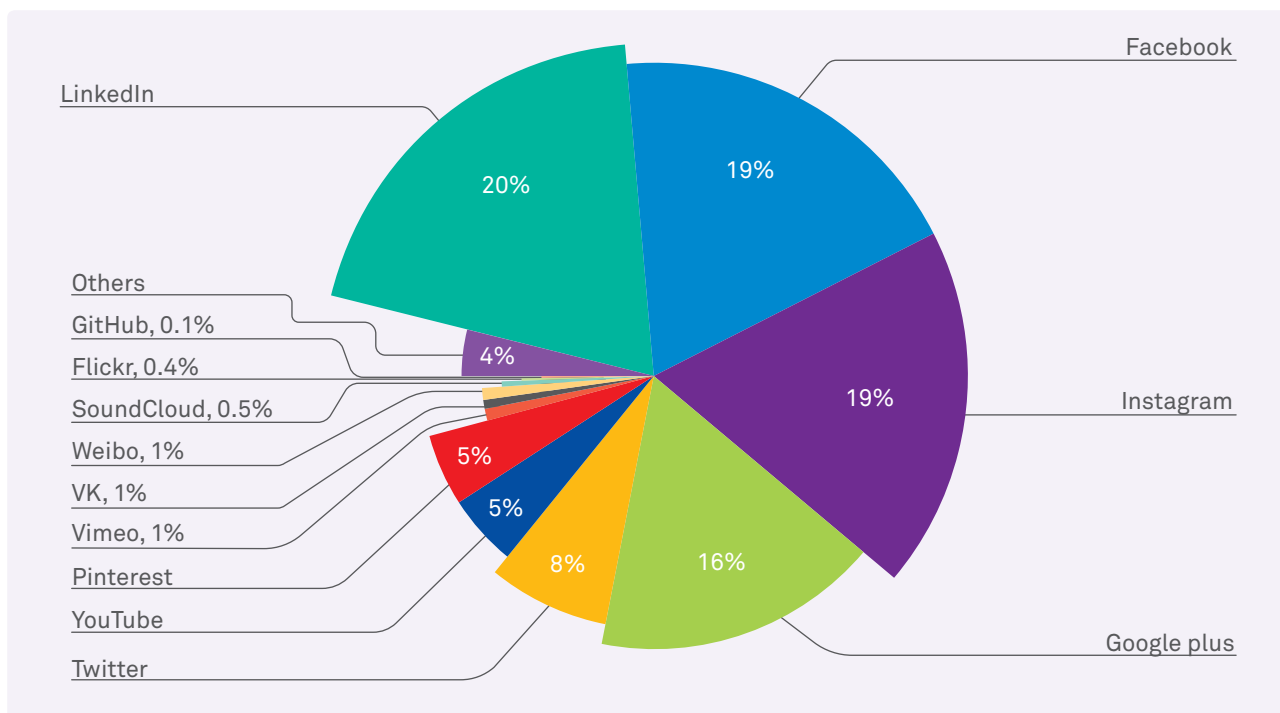


Figure 5: Fake social media profiles by source sites

How targeted is your sector?

Some sectors are more targeted than others. The IntSights alerts data for 2018 highlights that retail (10%), automotive (8%) and financial services (8%) were among the most targeted sectors.

Retail brands are often used for scams and selling fake or stolen merchandise. The retail sector has seen the biggest spike as many criminals go to social media to distribute stolen goods and they do so under the brand of the targeted company.

The assets of the automotive sector are not under direct attack like retail and finance, but its brand sensitivity is still very high. Car companies and auto manufacturers rely heavily on their brand image and recognition. Any damage inflicted to their brand through malicious activity can result in heavy losses to the company. A hacker that spreads a rumor about a car malfunction or safety problem can have a serious impact on the company's reputation and sales, especially if he has an army of fake profiles to back him up.

Financial services are known targets of phishing attacks with elements of social engineering. The use of fake profiles to phish bank clients' credentials and data is a well-known practice of hackers and scammers. In addition, whaling attacks that target CEOs and other C-level executives within the corporate hierarchy were prominent in 2018.

Social media manipulation may be perceived as a lower level threat compared to a direct malware attack, but it is also one of the trickiest ones to detect as it happens far from the eyes of the company and could happen on any social media platform. The extent of the damage of these attacks is often identified when it's too late, so keeping track of social media outlets and making sure your customers engage your official communication channels can go a long way in protecting your brand. As people get more and more connected in cyberspace, we expect these types of attacks to keep rising.



Attacker strategem

Social media is no longer a millennial tool; senior leaders and organizations are on board too. Attackers are aptly using this to go after or impersonate the big fish in the business.

This section was contributed by Wipro's Partner, IntSights (www.intsights.com)

Cyberweapons

In 2018, threat actors became more sophisticated and developed new methods to exploit vulnerabilities in current and emerging technologies. This section of the report analyzes malware attacks detected and thwarted by Wipro's CDC in 2018. 5,250+ incidents from multi-geographic environments were sampled and analyzed. The attack types were identified and the malware threat type, relative distribution

of incidents across four quarters and high incidents of malware families were inferred. Cryptominers have shown a significant growth in the last year and their rise has been highlighted as a critical finding. Overall, attackers are sticking to their tried and tested techniques, like trojans, but at the same time leveraging the bitcoin revolution by introducing various variants of cryptominers.

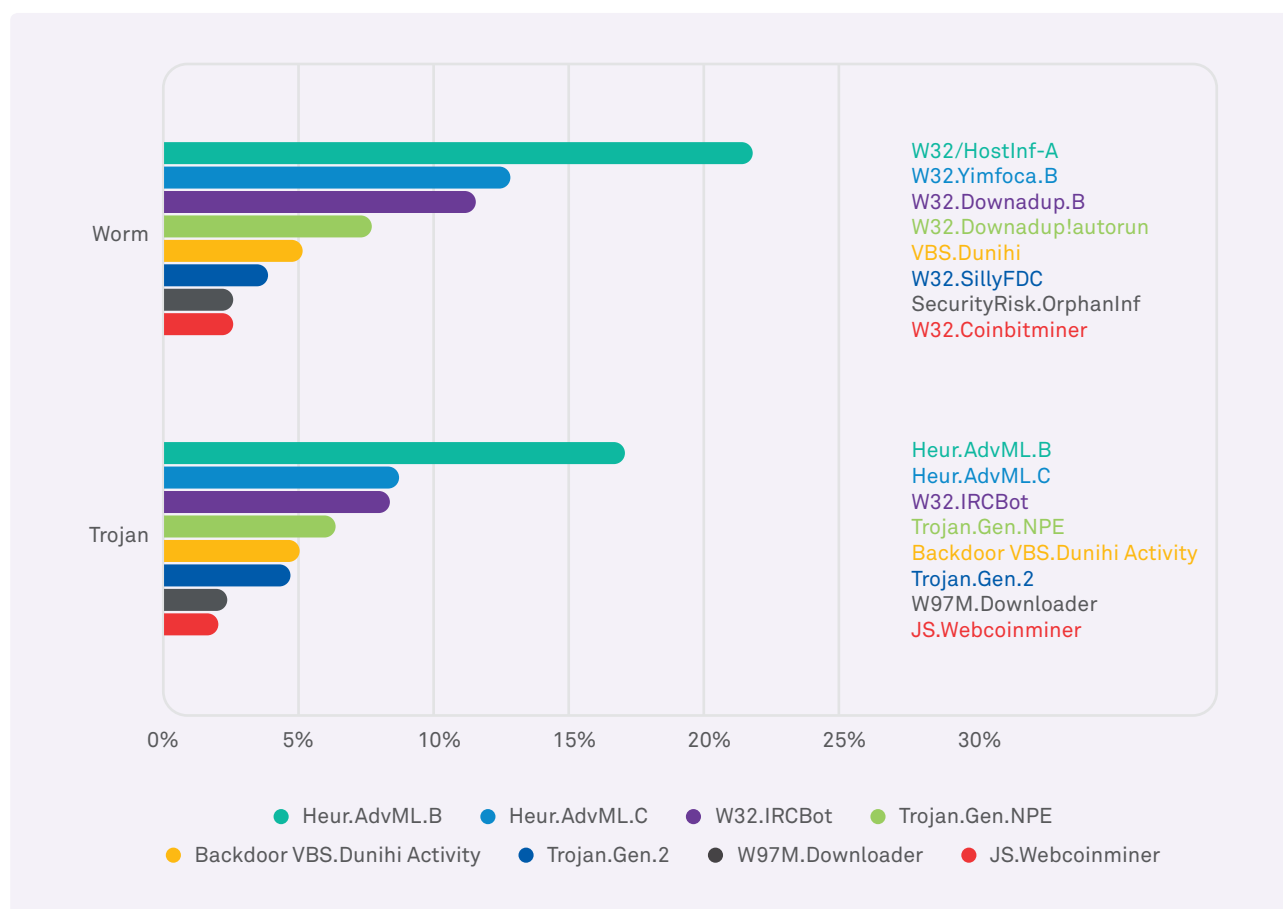


Figure 6: High incidence threats across trojans and worms

Figure 6 shows the high-incidence threats across trojans and worms. Heur.AdvML.B, Heur.AdvML.C, W32.IRCBot, Trojan.Gen.NPE, Backdoor VBS. Dunihi Activity, Trojan.Gen.2, W97M.Downloader and JS.Webcoinminer were found to be amongst the top eight families in the trojan category covering 55% of total incidents.

Global insight

26% of trojan attacks were from the Trojan Heur.AdvML.B and Heur.AdvML.C.



Attacker stratagem

Attackers haven't given up on their established techniques to score the next big payday.

Exploits distribution

Wipro's CDC data revealed that 22% of exploits in 2018 were web exploits, up from 12% in 2017. Remote Code Execution exploits jumped to 15% in 2018, up from 5% in 2017.



Global insight

22% of exploits in 2018 were web exploits.

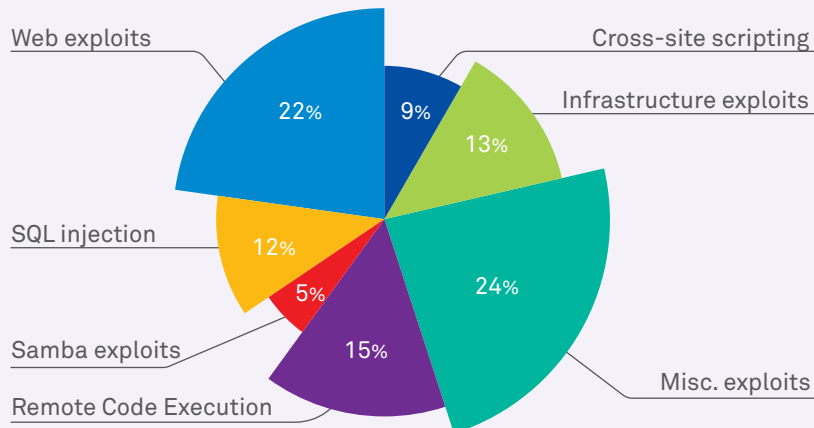


Figure 7: Distribution of exploits

The rise of cryptominers in 2018

This section of the report focuses on cryptominer attacks which have grown significantly in the last one year. The top three cryptominer malwares—Coinhive, Cryptoloot and JSEcoin have contributed to 80% of all cryptomining attacks. These malwares were dominant last year as well.

These web-based cryptominers are seamlessly incorporated into websites and then mobilize web servers for cryptomining. Apart from the three main cryptominers, Rubyminer has shown considerable growth in the first two quarters of 2018. Taking an alternative approach, Rubyminers have exploited vulnerable web servers for cryptomining by simply injecting the code onto unpatched Linux and Windows servers.

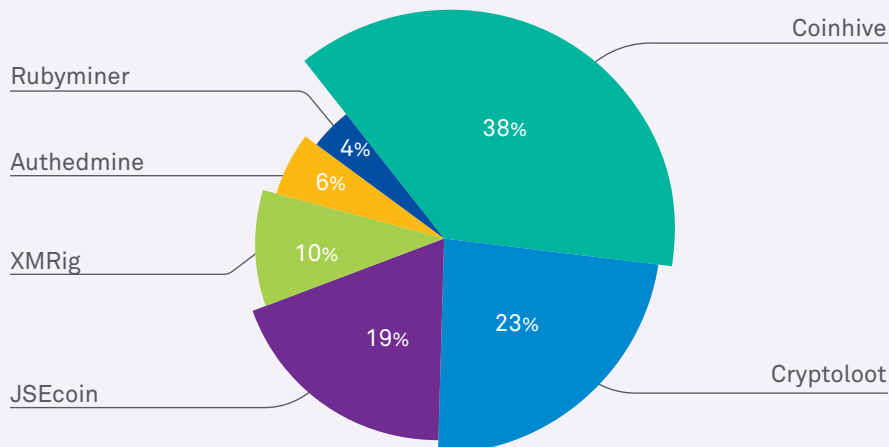


Figure 8: Top cryptominers malwares of 2018



Attacker stratagem

Attackers are developing custom kits and exploits for targeted attacks, bringing in the element of surprise.

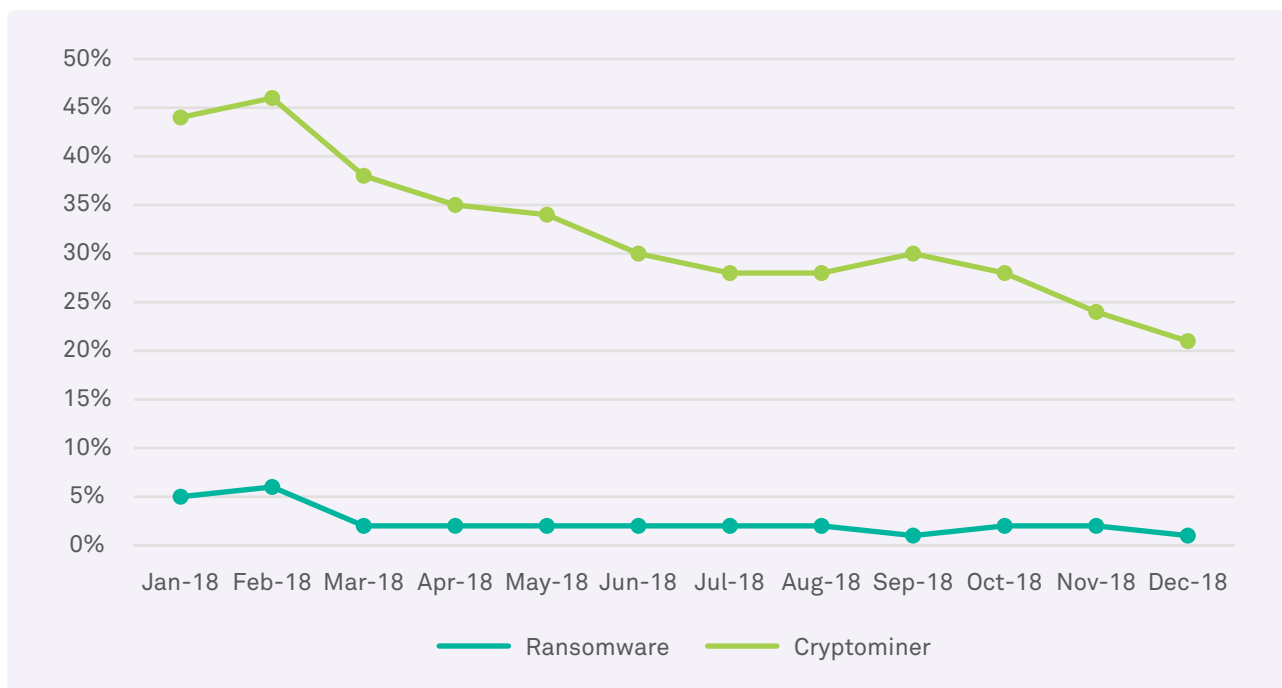


Figure 9: Top cryptominers and ransomware monthly trend, 2018

Figure 9 shows the month-wise trend of cryptominers and ransomware attacks in 2018. Both cryptominers and ransomware have risen in the first quarter of the year and they have subsequently declined in the latter half of the year. Interestingly, Wipro's CDC data also shows a similar trend for ransomware, with attacks decreasing in the latter half of the year.

Global insight

The decreasing trend of specific malware attack types over the year can possibly be attributed to the cumulative learning of the security industry and the update of systems to move from detection to prevention.

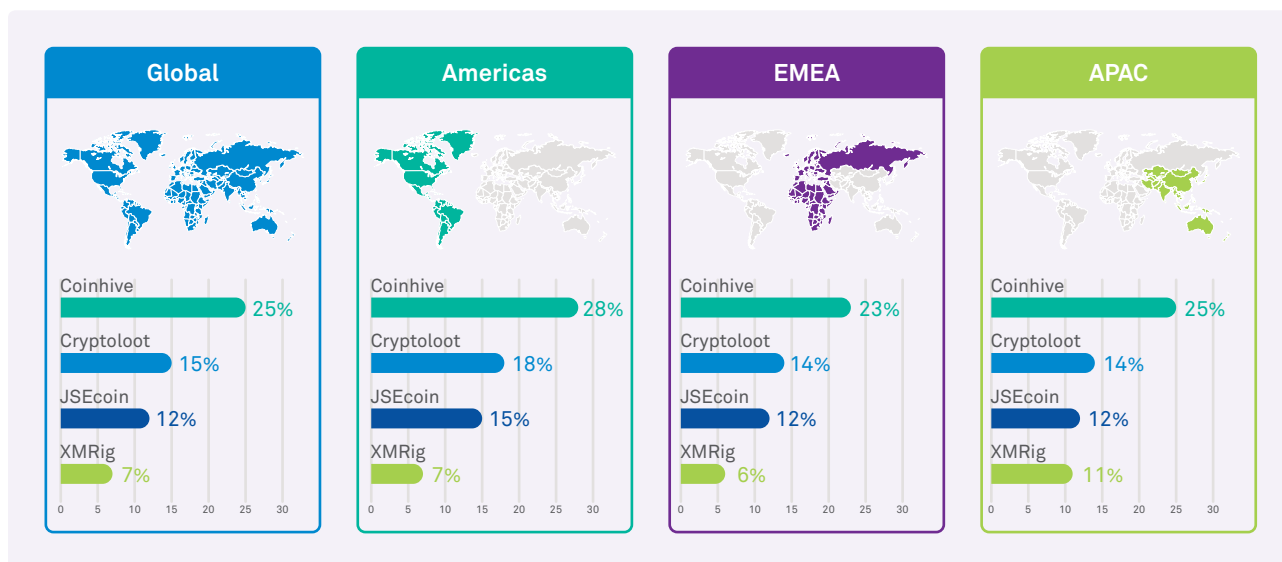


Figure 10: Impact of cryptomining malwares, 2018

Figure 10 shows a global—as well as a regional—view of all the cryptomining attacks in 2018. Around 25% of global organizations were attacked by Coinhive malware which became the most prominent malware of 2018. In all three regions—Americas, EMEA and APAC—it was the

top-most malware used by cryptominers. This can be attributed to the fact that it can be distributed easily through social media advertisements and can spread without the knowledge of end-users. Cryptoloot, JSEcoin and XMRig were the other top malwares used by attackers.



Global insight

Around 25% of global organizations were attacked by Coinhive malware, which became the most prominent malware of 2018.



Global insight

The top three cryptominer malwares—Coinhive, Cryptoloot and JSEcoin—have contributed to 80% of cryptomining attacks.

Partner content credits: “The rise of cryptominers in 2018” was contributed by Wipro’s partner, Checkpoint (www.checkpoint.com)

Vulnerabilities in cyber defenders

Traditional vulnerability management programs in large enterprises are focused on identifying, tracking and mitigating weaknesses in IT operating systems and applications. Vulnerabilities identified in such systems generally age—sometimes into a few months—escalating risks that security governance teams need to track. However, our research over the last three years has shed light on an elephant in the room which is completely overlooked—vulnerabilities in security products! Could this be a golden opportunity for attackers?

Vulnerability trend analysis

The research is based on vulnerability trends derived from yearly vulnerability scores published on the Common Vulnerabilities and Exposures (CVE®) website (https://cve.mitre.org/). CVE is a list of IDs for publicly reported vulnerabilities. The research on security product vulnerabilities looked at multiple product domains such as

antivirus, data loss prevention, Identity & Access Management (IAM), security intelligence & analytics, firewall, VPN, SAST/DAST and others.

The following vulnerability categories were used:

- DoS
 - Code execution
 - Overflow
 - Memory corruption
 - SQL injection
 - XSS
 - Directory traversal
- HTTP response splitting
 - Bypass something
 - Gain information
 - Gain privileges
 - CSRF
 - File inclusion

The 3-year trends for the 13 vulnerability categories have been showcased in Figure 11. The most frequent categories are: DoS, code execution, XSS, gain information and gain privileges. Gain privilege vulnerability category has seen a 129% rise in vulnerabilities.

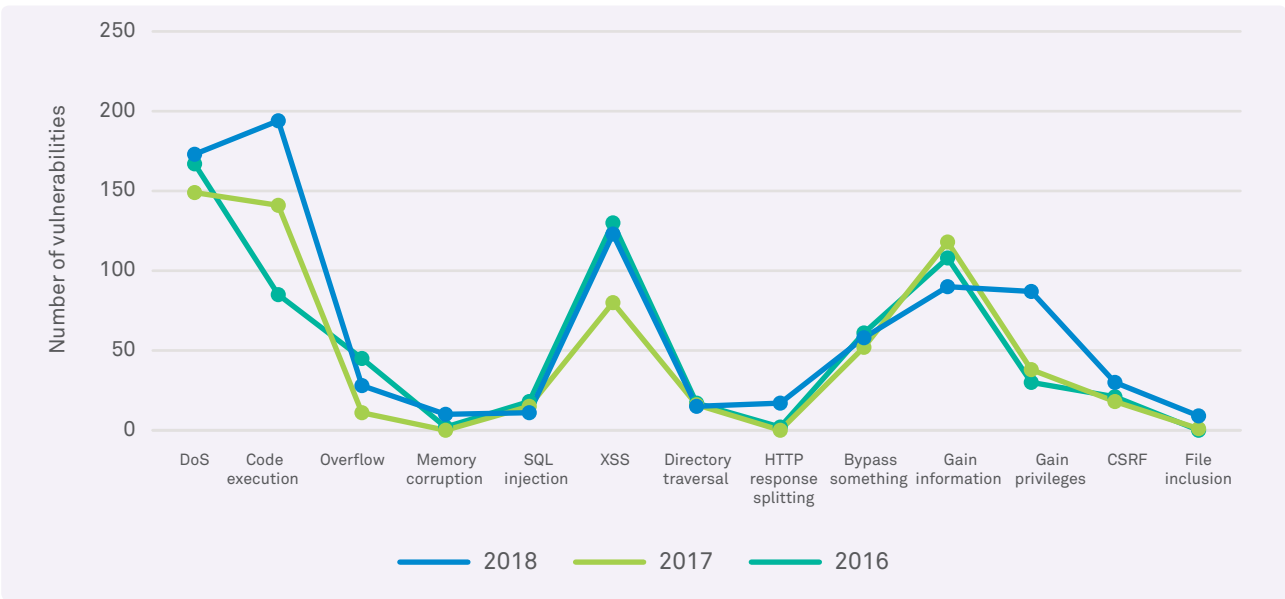


Figure 11: Trend of vulnerability categories in security products

Gain privileges as a vulnerability category saw a significant rise in 2018. Privilege escalation attacks due to the expanded access to systems and data have increased the risk for organizations in the context of data breaches.

Vulnerabilities in security products

In the previous section we looked at the common vulnerability categories across security products. Taking this a step further the research highlights which security product types are more vulnerable to attacks.

A weighted average score of vulnerabilities was arrived upon for each product, the scores of similar products were then aggregated using a weighted average method to arrive at the final product category scores. Look out for the products with high scores as the high scores indicate a higher propensity for vulnerabilities.

Firewall and VPN products topped the table with a score of 6.73, indicating a higher propensity for vulnerabilities. The admin interfaces of these products need to be periodically tested for vulnerabilities and appropriate patches or compensating controls need to be put in place where applicable. Webservices gateway, PKI and IAM product security domains gave the lowest average scores—indicating a propensity for vulnerabilities with lower CVE scores.

Global insight



Firewalls and VPN product domains topped the table—indicating a higher propensity for vulnerabilities while webservices gateways, PKI & IAM products demonstrate a lower propensity for vulnerabilities.

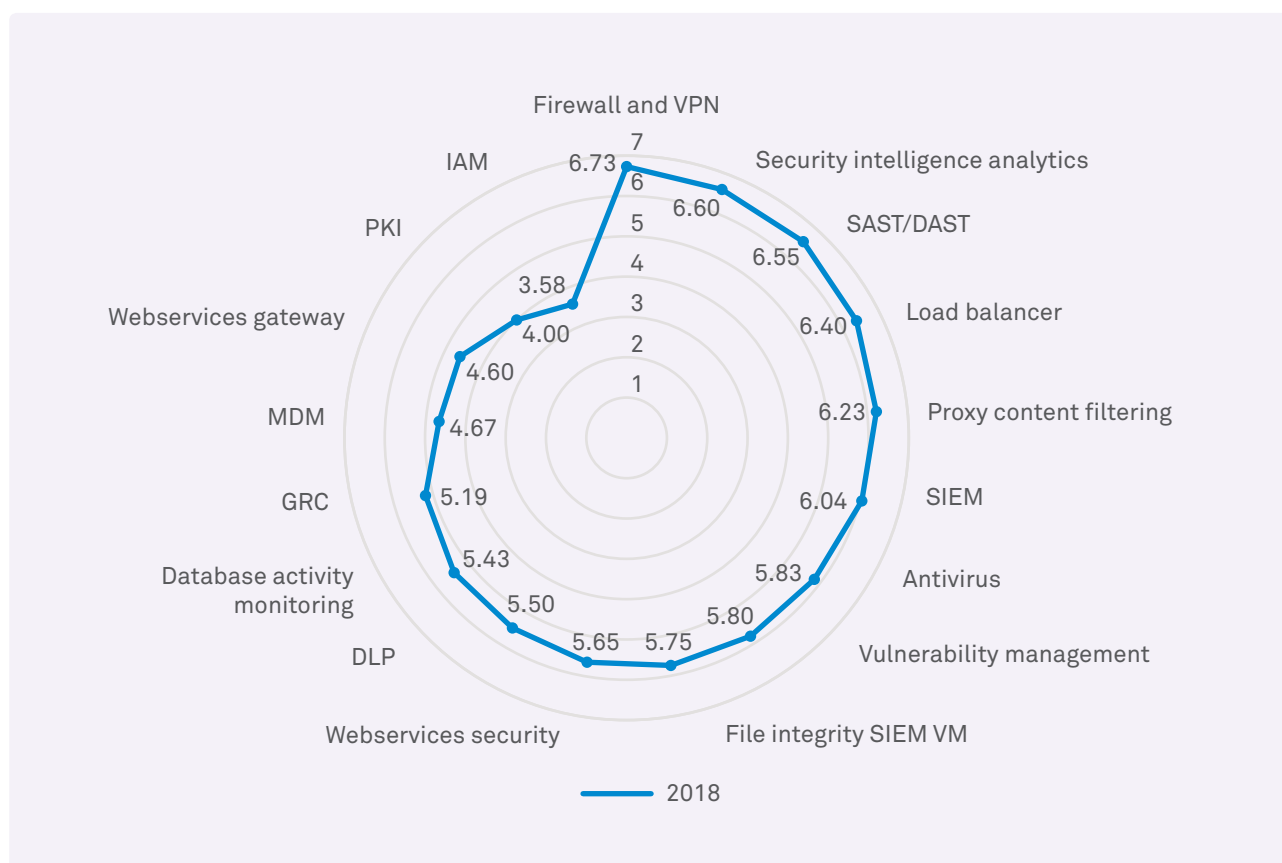


Figure 12: Security domain-wise vulnerability score, 2018

Global insight



A key observation from the vulnerability analysis is that in general, the severity score of vulnerabilities has gone down in 2018—although the cumulative counts of vulnerabilities have gone up.

Regulations

So far, the report has covered information on data breaches, cyberweapons and vulnerabilities in cyber defenders. This section delves into the legal aspect of cybersecurity, with regard to the data privacy regulation landscape across the globe. Defenders need to be wary of the implication of a breach, from a regulations point of view. Wipro's cybersecurity CoE carried out detailed

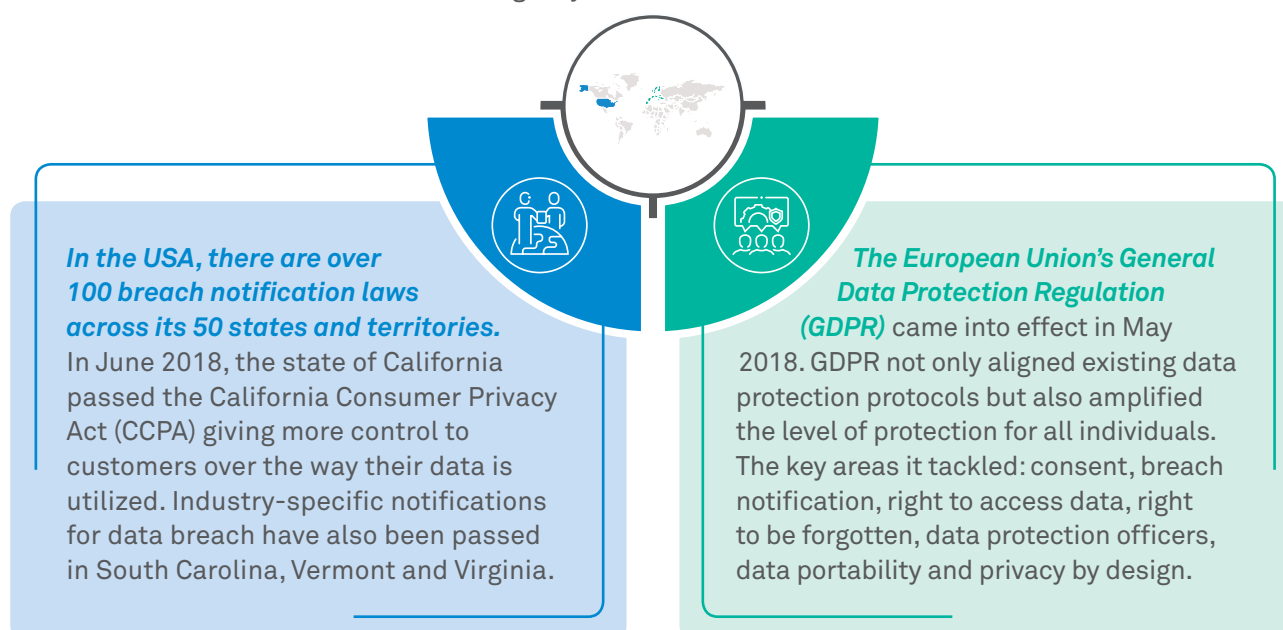
analysis of breach notifications and cross-border data transfer laws across 23 countries. The 23 countries covered are Australia, Brazil, Canada, China, Dubai¹, France, Finland, Germany, India, Italy, Ireland, Japan, Mexico, Norway, Poland, Russia, Spain, Singapore, South Africa, Sweden, Switzerland, UK and USA. The key parameters used to evaluate the data are shown in Table 1.

Focus areas of analyses	Parameters
Data breach notification requirements	<ul style="list-style-type: none"> • Mandatory notification of authority • Breach categorization • Mandatory notification of data subjects • Penalty for lack of disclosure
Restriction on overseas transfer	<ul style="list-style-type: none"> • Consent of data subjects • Outside jurisdiction provides adequate protection • Binding Corporate Rules (BCRs) • Standard Contractual Clauses (SCCs) • Permission of data protection authority

Table 1: Analyzed parameters for different focus areas

For each of the 23 countries chosen, the parameters were analyzed using a weighted average method. Each country was given a total score on a linear scale based on the stringency of

regulations. The scores were used to plot Figures 13 and 14. The higher the country score the more stringent the laws are towards breach notification or overseas transfer.



1. Restricted only to a city based on the available data

Heat map of breach notification laws

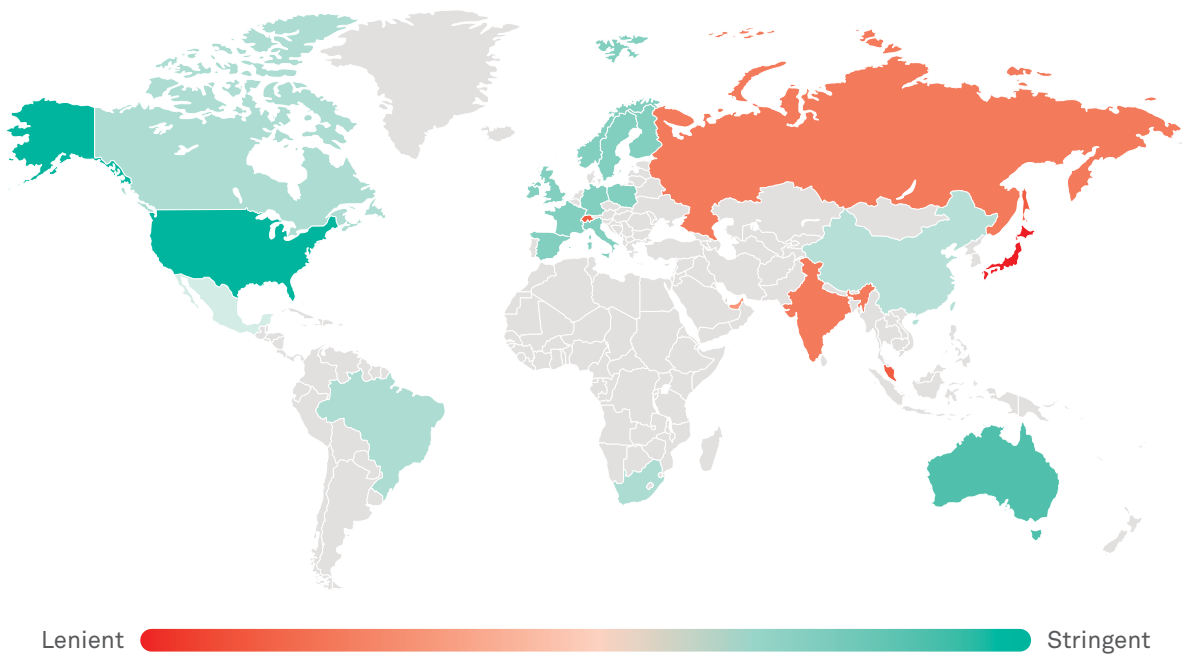


Figure 13: Heat map of country-specific regulations relating to breach notification, 2018

Global insight

The US has strict breach notification laws, while its cross-border data transfer laws are less stringent than GDPR.

Heat map of cross-border data transfer laws

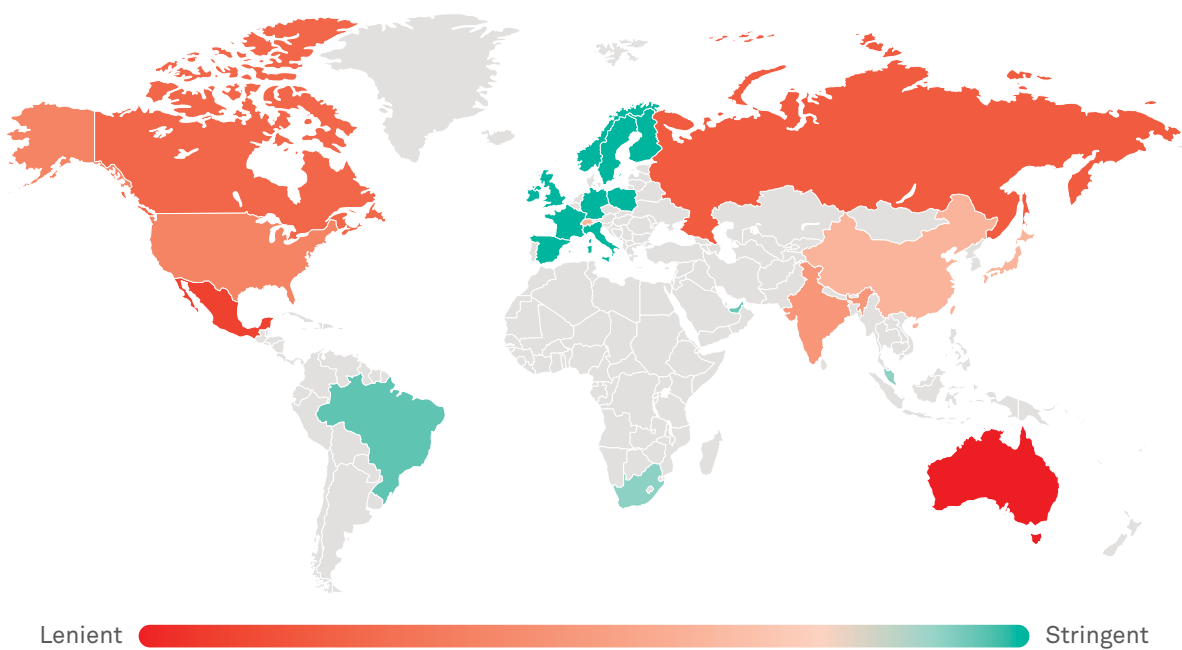


Figure 14: Heat map of country-specific regulations relating to overseas data transfer, 2018



State of cyber resilience

Security governance

- The evolving role of the CISO
- Ownership of data privacy
- Security budget
- Security metrics

Security practices

- Data security
- Application security
- API security
- Network DDoS protection
- Endpoint security
- Security monitoring & analytics
- Cloud security
- IoT security
- Human dimension



If it be now, 'tis not to come. If it be not to come, it will be now. If it be not now, yet it will come—the readiness is all.

William Shakespeare

Cyber resilience has become an existential imperative for the digital enterprise of today. Cyber risks can not only affect the top line by impacting revenue but also impact the bottom line by adding IT, legal and compliance costs before and after the manifestation of a risk. Addressing cybersecurity risks continues to be subservient to an organization's overall risk management efforts. This section presents findings from the primary research carried out with CISO teams across the globe, covering areas such as security governance, security budget, metrics and domain-wise practices. This represents the micro view of the cybersecurity from the organizational standpoint. It takes a peek into the defenders strategies to see how organizations are safeguarding themselves from attackers.

The need for a cyber resilience framework

Cyber resilience needs to be a continuous process to identify opportunities to strengthen cybersecurity posture, while aligning with industry practices. The process of cyber resilience needs to be underpinned by an appropriate framework. Multiple cybersecurity frameworks exist today across industries and geographies. While frameworks may not be “one size fits all,” they do have their advantages of leveraging best practices that are common to most enterprises. The framework also provides a mechanism to communicate the roles and responsibilities, feedback mechanisms and communication imperatives up and down the corporate hierarchy. Figure 15 provides a glimpse of a typical charter of expectations for establishing a feedback-based framework of continuous cyber resilience. But a cyber resilience-centered approach should aim to start with identifying the risks.

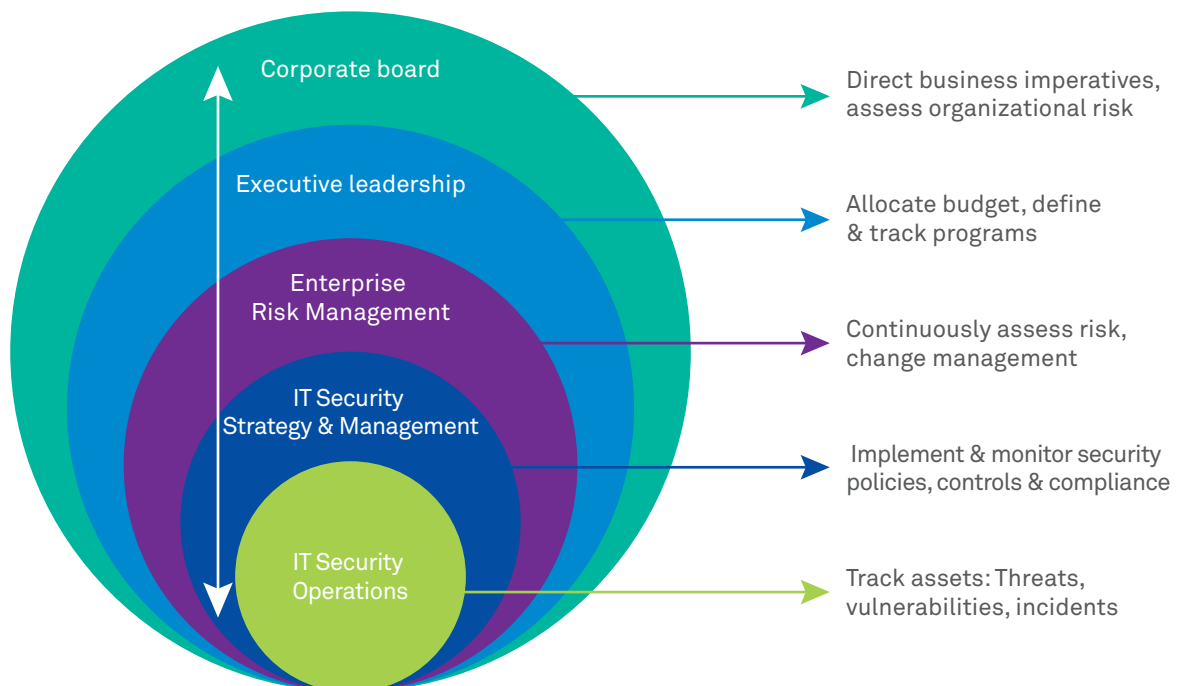


Figure 15: Continuous cyber resilience framework

What are the top cyber risks that organizations face?

The primary research findings of the survey on cyber risks point to the human dimension of risk management. This is often neglected as a control domain, because energies are focused on getting the technology layer to cover for human errors.

The top two findings selected by our respondents were email phishing and employee negligence (see Figure 16 for other risks), both of which can be addressed through a resilient cyberculture within the organization.

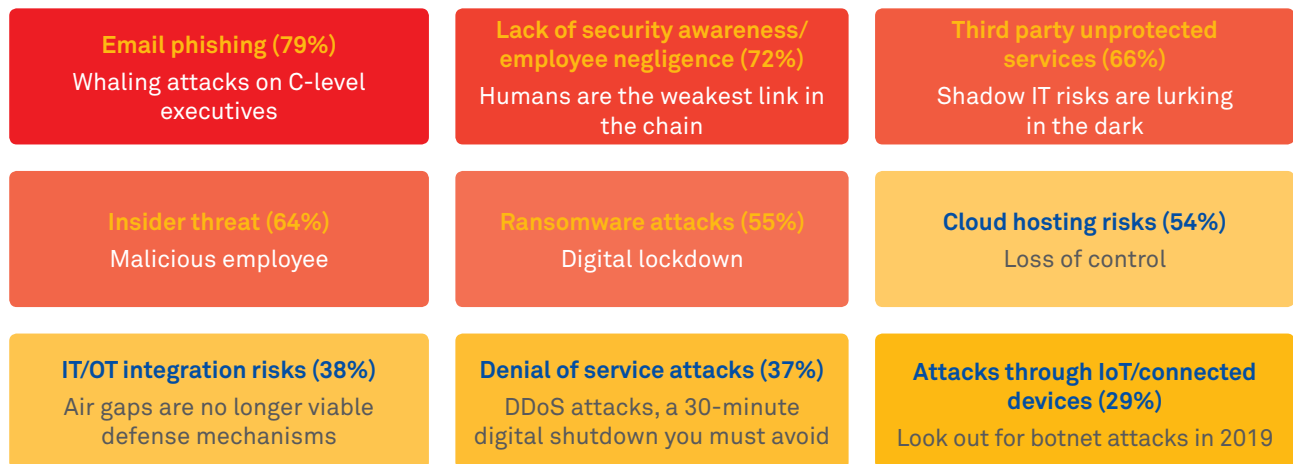


Figure 16: Top cyber risks that organizations face

How will a cyber incident impact your organization?

In our primary research, we asked customers how a serious cyber incident could impact them. The results showed that an impact is industry-agnostic. The top two outcomes were damaged brand reputation and loss of revenue due



to non-availability of services at critical times, both of which tie back into organizational risks.

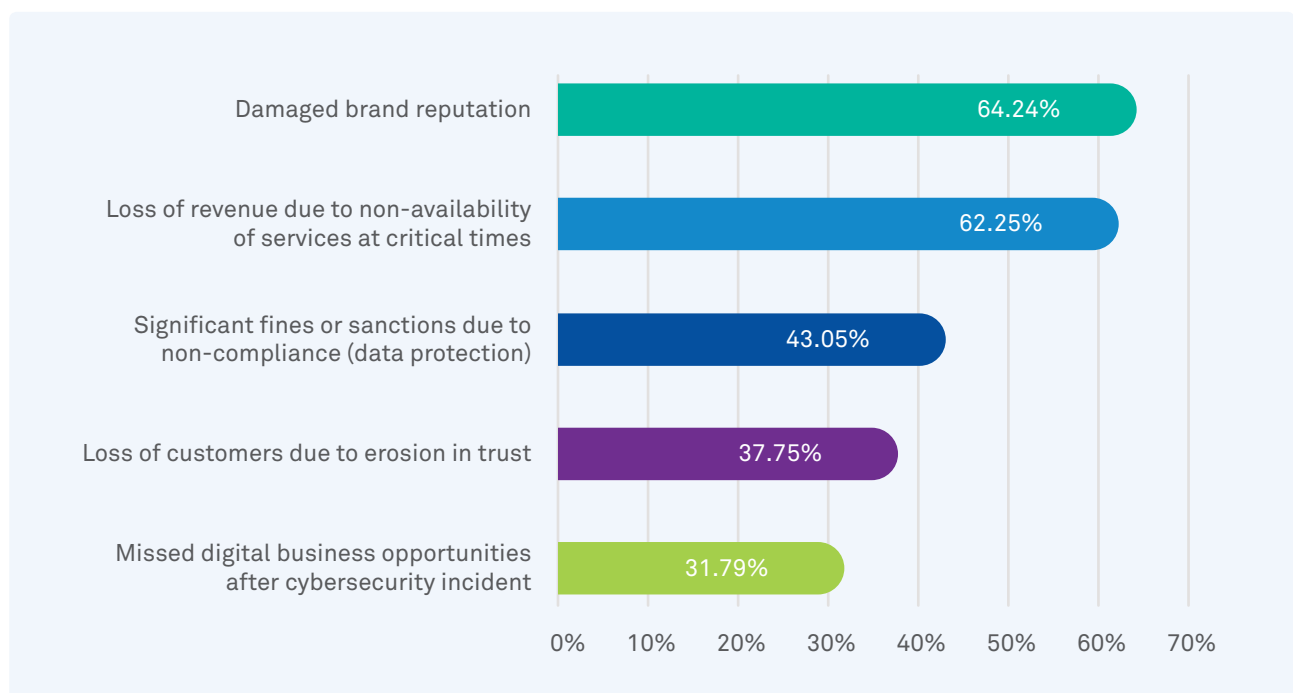


Figure 17: Impact of a cyber incident on an organization

The evolving role of the CISO

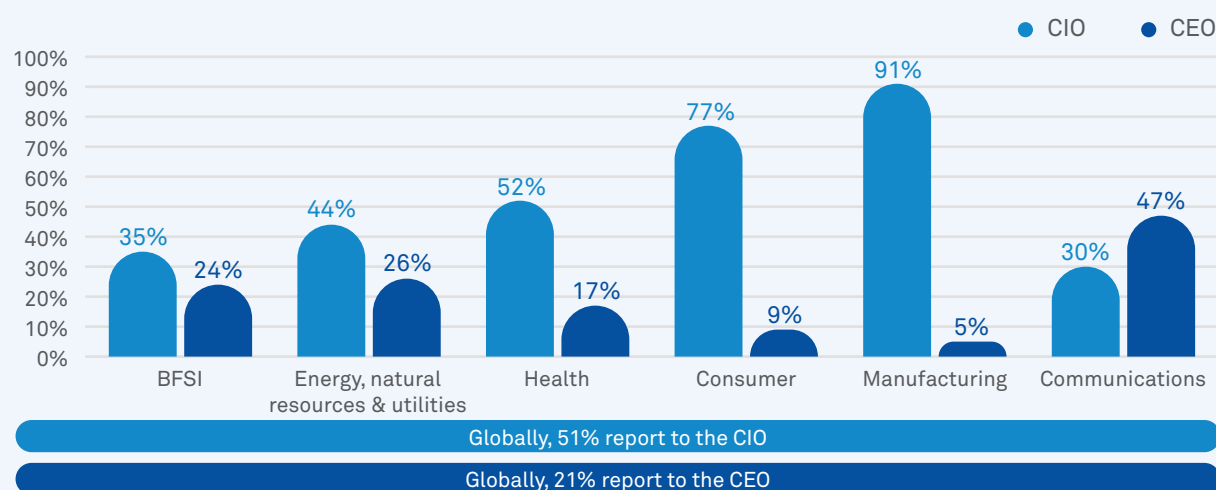
In today's rapidly changing security landscape, a cyberattack—be it large or small—will be detrimental for an organization. Organizations need to equip themselves to prepare for these threats and mitigate the risks. Identifying who will govern information security is the first step. Business leaders are acutely aware of the reality

of an imminent cyberattack as high-profile CEOs are feeling the heat due to data breaches. This has led to the evolution of the CISO's role, which now includes more governance responsibilities along with a heightened scrutiny from the board. Over 21% of CISOs surveyed also indicated that they are now reporting directly to the CEO.

Who does the CISO report to?

The research highlights that the majority of CISOs (51%) today roll up to the CIO. However, a considerable number globally (21%) report directly to the CEO of their organizations.

% of CISOs reporting to the CIO and CEO by vertical



Scope of the CISO's role

More and more CISOs are playing the 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%).

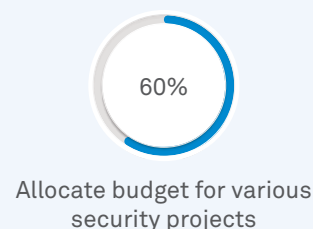
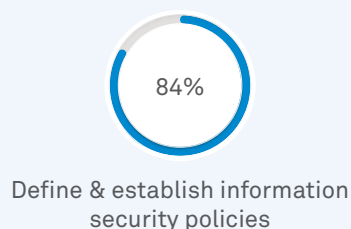
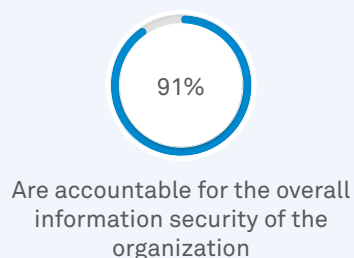


Figure 18: Evolving role of the CISO

The traditional CISO–CIO reporting model has proven to be very effective for better alignment with broader IT teams under the CIO. However, this model could present challenges in the

future, where conflicts of interest might arise due to market pressure to deliver content and functionality with limited resources to address inherent security risks.

Ownership of data privacy

In 2018, the roll out of GDPR by the European Union coupled with high profile breaches brought the importance of data protection into the spotlight. Consumers are now putting pressure on governments and organizations to put checks in place for safeguarding their data.

Rise of the role of CPO/DPO in Europe

So, who bears the onus of data privacy in an organization? Figures 19 and 20 show the ownership

of governance for data privacy in an organization in Europe and the US respectively. In European organizations, there was a notable increase in the number of CPO/DPO roles in 2018. This can be attributed to the GDPR mandate requiring organizations handling personal data on a large scale to have a DPO. The story is different in the US where 44% of the organizations have said that data privacy is the charter of the CISO.

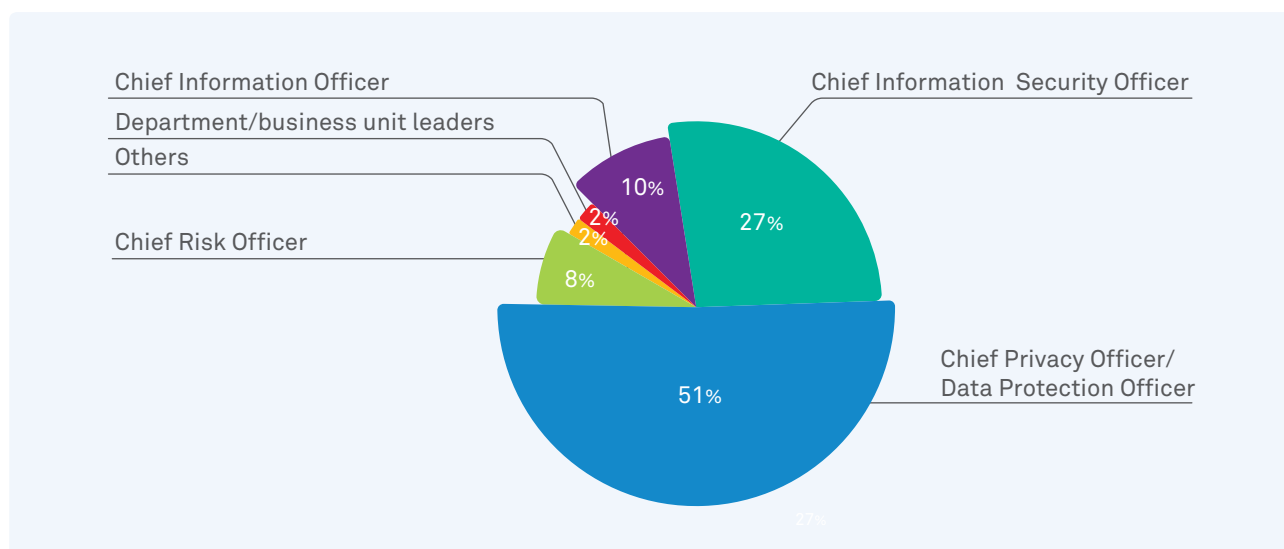


Figure 19: Organizational responsibility for governance of data privacy in Europe

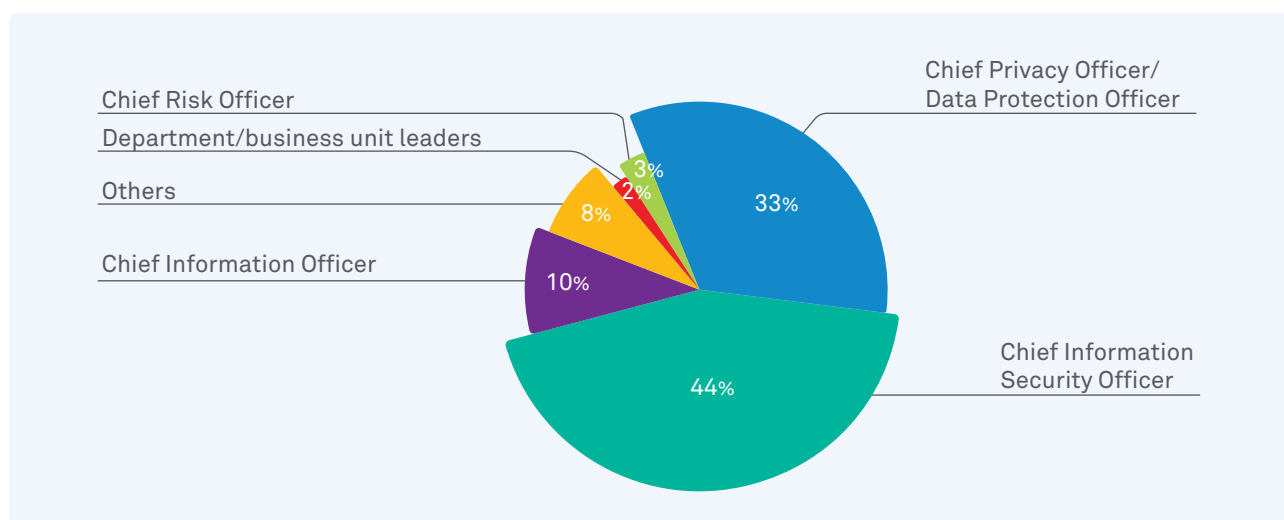


Figure 20: Organizational responsibility for governance of data privacy in the US

Global insight

Worldwide, 72% of respondents said that either a CISO or DPO/CPO is accountable for data privacy in their enterprise.

Defender strategem

Organizations are crystallizing ownership and accountability in their fleets!

Security budget

As cybersecurity is gaining visibility, organizations are stocking up on security skills, processes and technologies to defend themselves against the multitude of threat actors. This protection does not come free or cheap. Thus, security budgets have

increased over the past few years. Figure 21 looks at the percentage of IT budget allocated for security by organizations. 15% of organizations have a security budget that is over 10% of their IT budget. This figure is bound to increase in the coming years.

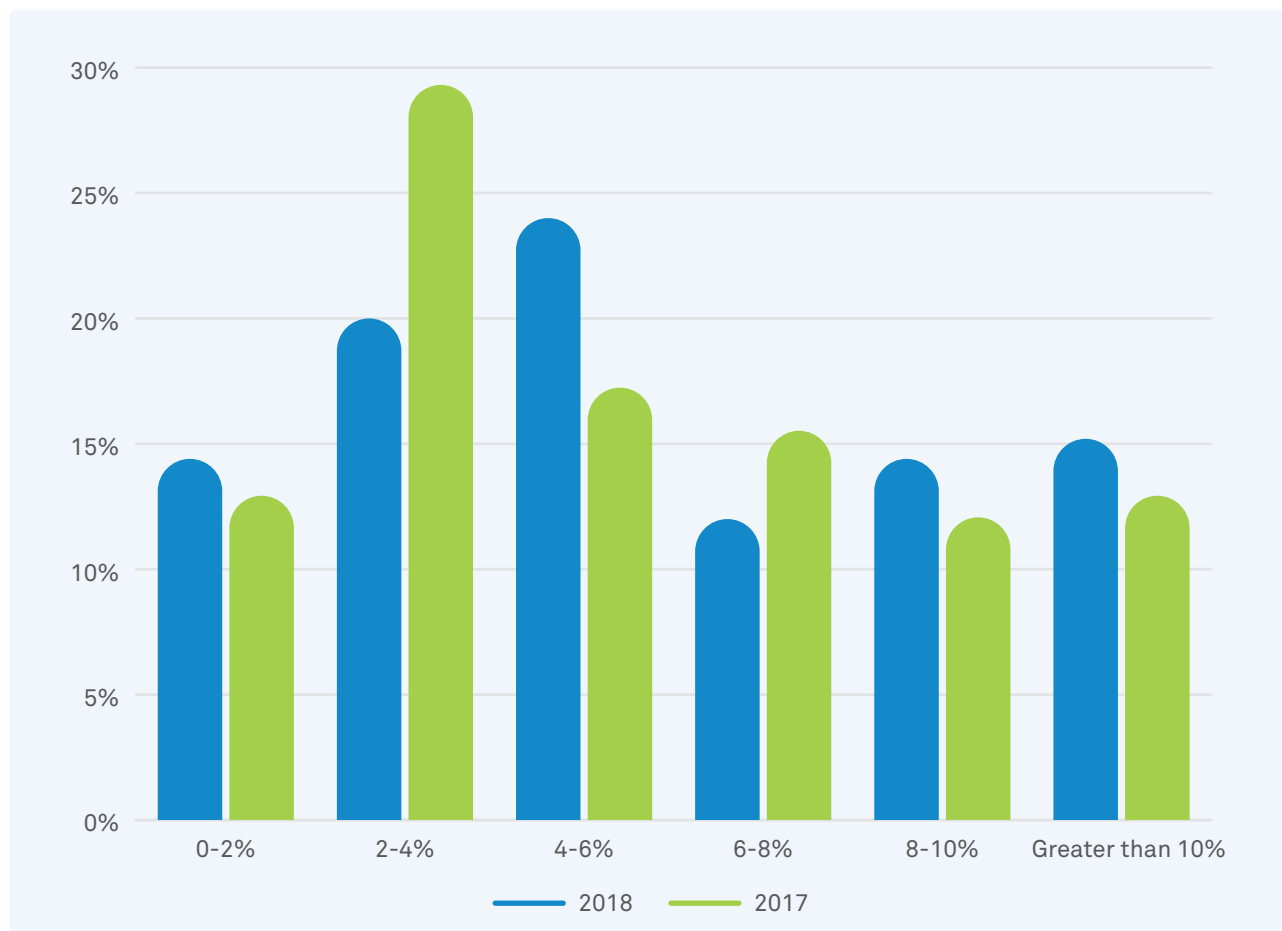


Figure 21: Range of percentage of IT budget allocated for security

The survey asked respondents to identify the revenue band of their organization. This data was correlated with the percentage of IT budget allocated to security, but no correlation was found.

Security budgets will plateau

While security budgets are on the rise, there will be a point where it'll plateau. At that point, how will organizations prepare for the evolving threat landscape? Figure 22 delves into steps organizations will take when the security budget will likely get capped. 67% of

organizations are planning for broad business and process automation to lower costs and release the budget. This, coupled with digital transformation and increase in C-level visibility, should equip organizations to keep their budgets in control.

Vertical insight

23% of BFSI organizations have a security budget greater than 10% of their IT budget.



Vertical insight

71% of health organizations will plan for broad business and process automation to lower costs and release budgets.



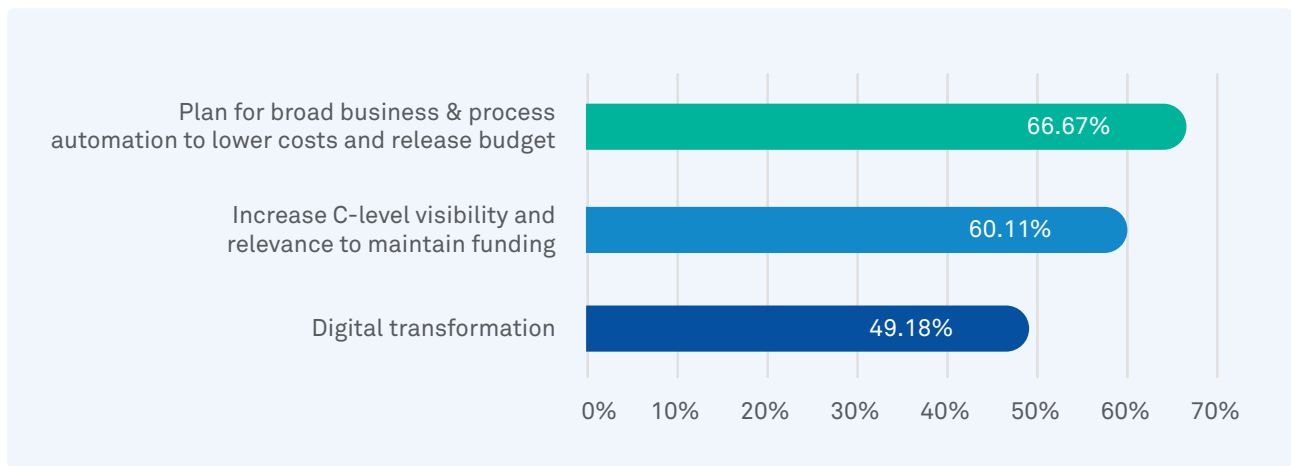


Figure 22: Top three steps organizations are likely to take when the security budget is capped

Security metrics

For organizations that have their security governance in place, security budgets fixed and allocated, security products and services on the go, the next step is measurement. How do you track your efforts/investments? What are the numbers that need to be reported to the management that will indicate the effectiveness and efficiency of the various security investments?

What gets measured, gets done

Research was conducted across three categories of metrics: management, operational and technical. CISO teams chose the metrics tracked by their organization. The data was analyzed from a sector point-of-view to draw insights into how industries are measuring their security practices. Tables 2,3 & 4 show the results and reveal industry trends.

Management metrics

Metrics	BFSI	Energy, natural resources & utilities	Health	Consumer	Manufacturing	Communications	Global average
Time-to-detect and remediate incidents	71%	67%	71%	40%	71%	67%	65%
Cost of detection	31%	19%	24%	13%	21%	7%	19%
Cost of downtime	55%	38%	47%	40%	36%	13%	38%
Cost of incidents	45%	33%	41%	27%	14%	40%	33%
Regulatory compliance	65%	52%	71%	87%	57%	60%	65%
Security spending as % of IT budget	40%	43%	41%	33%	64%	27%	41%

Table 2 highlights the adoption of management metrics across industries

Operational metrics

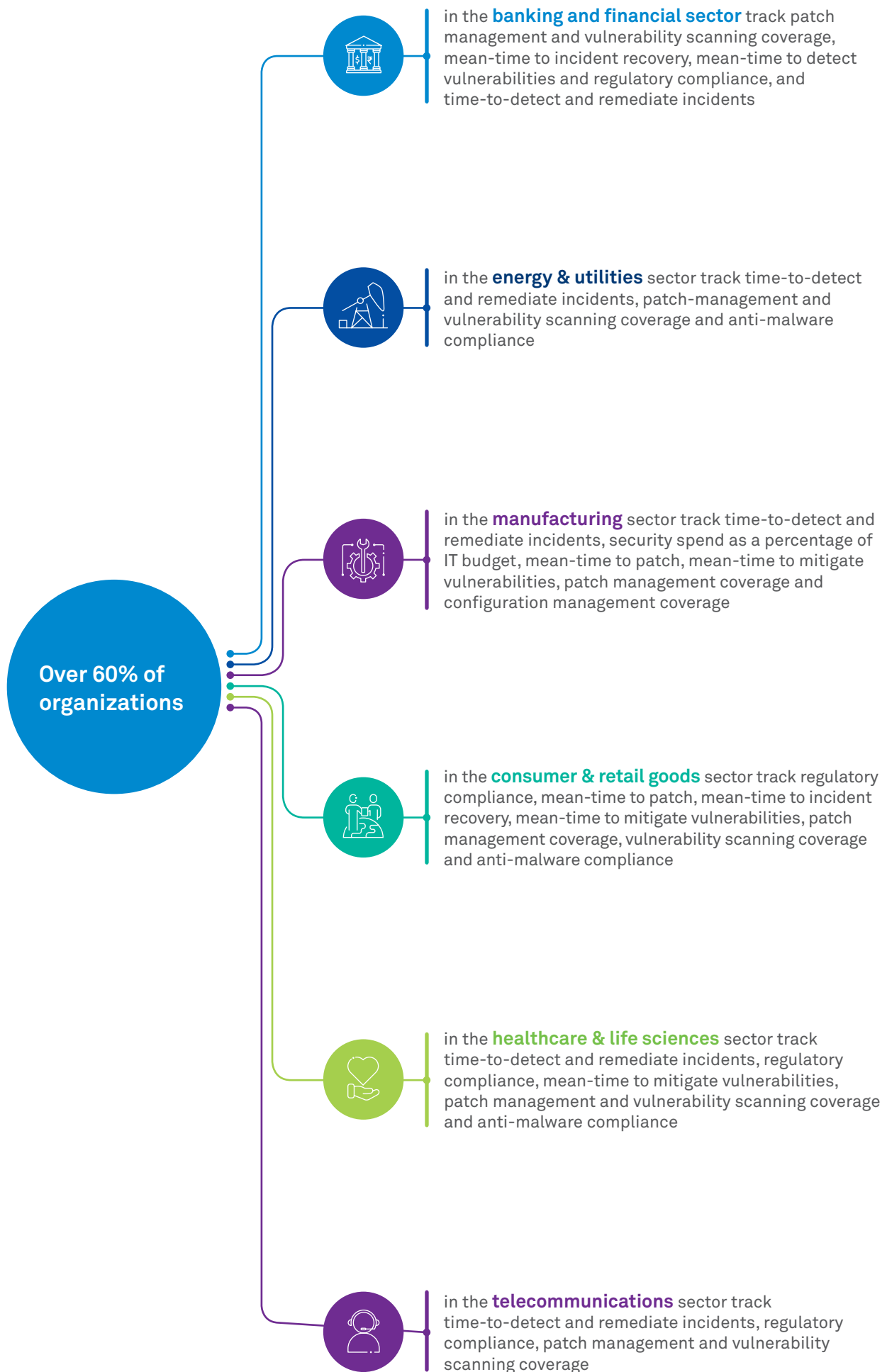
Metrics	BFSI	Energy, natural resources & utilities	Health	Consumer	Manufacturing	Communications	Global average
Mean-time to patch	55%	48%	38%	73%	69%	31%	52%
Mean-time to incident discovery	43%	33%	38%	40%	54%	54%	44%
Mean-time to incident recovery	64%	52%	50%	60%	38%	54%	53%
Mean-time to mitigate vulnerabilities	60%	48%	75%	67%	69%	54%	62%
% of changes with security exceptions	30%	19%	44%	20%	23%	46%	30%

Table 3 highlights the adoption of operation metrics across industries

Technical metrics

Metrics	BFSI	Energy, natural resources & utilities	Health	Consumer	Manufacturing	Communications	Global average
Patch management coverage	76%	86%	63%	75%	60%	60%	70%
Vulnerability scanning coverage	80%	67%	69%	88%	47%	73%	71%
Anti-malware compliance	64%	62%	69%	69%	33%	47%	57%
Configuration management coverage	42%	29%	31%	50%	60%	33%	41%
% of systems with known vulnerabilities	58%	43%	50%	56%	20%	47%	46%

Table 4 highlights the adoption of technical metrics across industries



Security practices

This section has been built up by analyzing the survey responses from CISO teams of over 200 organizations globally about the evolution of their security practices. The findings highlight the changing security landscape in various practices over the past 3 calendar years. The chosen practice areas include: data security, application security, API security, network security, endpoint security, security monitoring & analytics, cloud & IoT security.

Data security

Corporate data has continued to leave the four walls of the data center and diffuse into cloud service provider environments, SaaS applications and mobile devices. Also, digital transformation

initiatives brought digital data assets into the spectrum and regulations like GDPR came into play to ensure that companies set up adequate data security measures.

Have you locked the keys to your kingdom?

With the global focus on data security, this section provides a glimpse into the top security controls used by organizations. The survey respondents ranked data security controls in order of importance. Figure 23 highlights the interesting results obtained. 35% of organizations believe that Privileged Access Management (PAM) is the most effective data security control (a rise from 28% in 2017). This can be attributed to the value privilege accounts have and the damage that would be inflicted if these accounts were compromised. From an industry point of view, 40% of health and manufacturing industries have picked Data Leak Prevention as their top data security control. The “data” they hold—pharmaceutical IPs, patient records, industrial IPs—forms their core and compromising the data can result in severe business impact.

Global insight



35% of respondents felt that Privileged Access Management (PAM) was the most effective data security control.

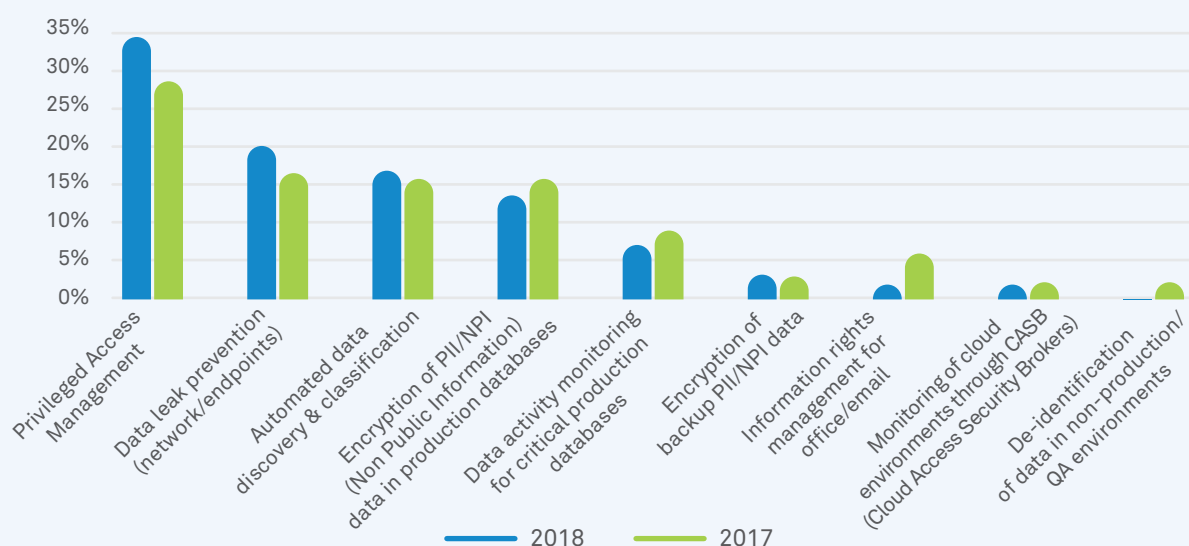


Figure 23: Data security control trend

Vertical insight

40% of health and manufacturing industries have chosen Data Leak Prevention as the most effective control. However, 35% of organizations globally have chosen PAM as the most effective control.



Application security

Application security assessment is an integral part of the software development process. But often organizations mistakenly consider this as an after-release activity. DevOps is making security testing more efficient by integrating automated security assessments during the application development phase.

Security assessments during the development life cycle help organizations identify and minimize security weaknesses in products, before their launch into the market.

How often are applications assessed for security issues?

In the research, respondents were asked about the frequency with which their organizations carry out security assessments for business-critical

applications. 25% of respondents said that they are carrying out the security assessments in every build cycle. This is an encouraging trend considering the fact that only 21% of respondents selected this choice in 2017 and only 20% of respondents selected this choice in 2016 (see Figure 24).

24% of respondents said that they are doing assessments on a yearly basis, which is 2.5% higher than last year. Organizations should preferably carry out security assessments on every build cycle to mitigate risks associated with the applications. Digital transformation is using DevOps to reduce the cycle time and increase the velocity of builds. Therefore, organizations need to adapt their security practices with the ongoing digitization drive.

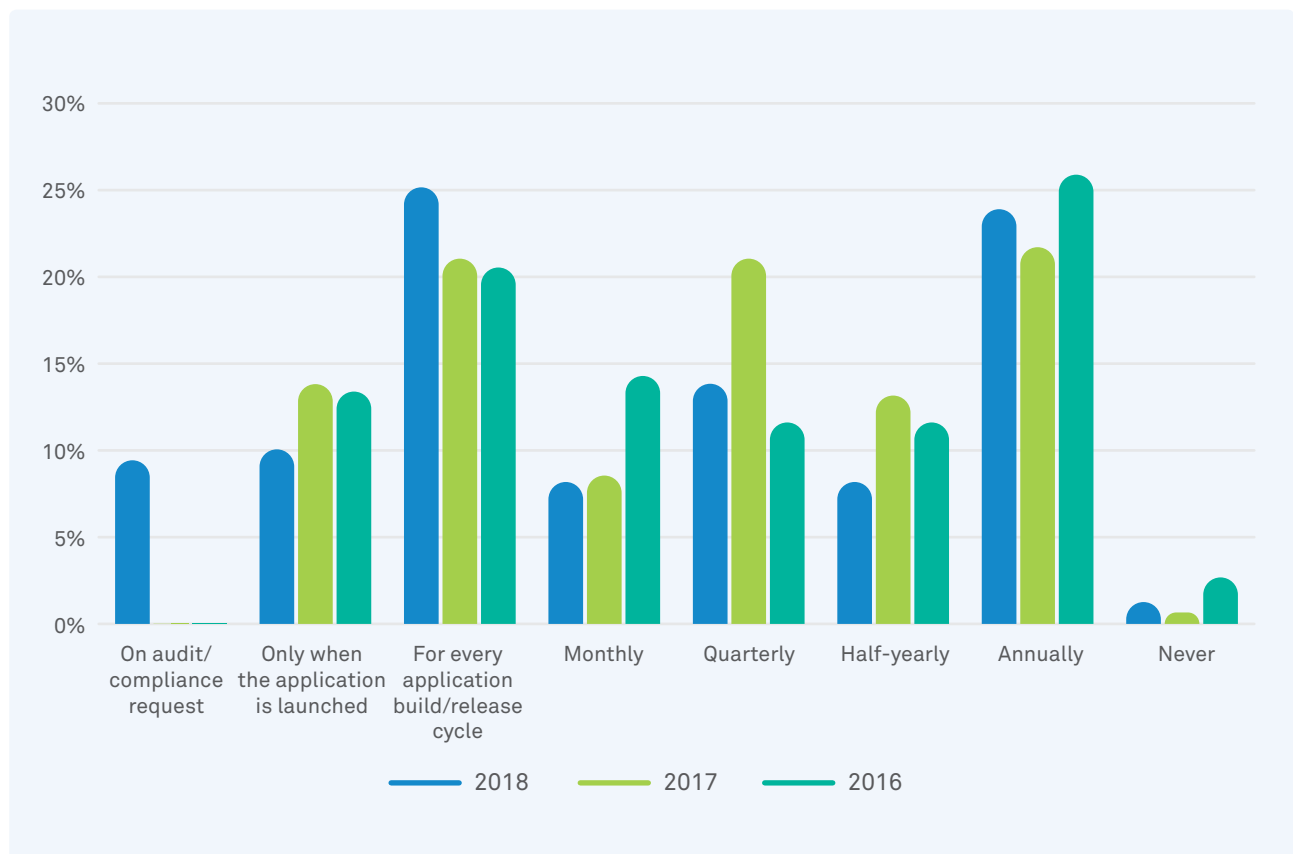


Figure 24: Frequency of security assessment of business-critical applications, 2018 vs. 2017 vs. 2016

Global insight

25% of respondents said that they are carrying out security assessments in every build cycle.

Vertical insight

Security assessments for every application in build/release cycle took the top spot for BFSI, communications and health verticals.

API security

Application Programming Interface (API) is code that is integral to applications and provides users a programmable gateway to access data and functionality—with clearly defined rules. While API security may not be in the limelight, it cannot be ignored as a practice area, as it can increase the attack surface of applications.

Why is API security on the radar now?

- With the rise of mobile applications and connected devices, Representational State Transfer (REST) APIs have grown exponentially over the past few years
- Mobile applications are now used by organizations in all sectors, exposing sensitive data that can be accessed through APIs
- Digital footprint of individuals is growing exponentially; organizations now have an immense amount of big data to store, process and analyze. This data in the wrong hands could be unimaginably disastrous
- Most APIs are accessed over the Internet, which makes them a target for potential sniffing, spoofing and man-in-the-middle attacks

Security considerations



Global insight



By not securing the APIs, enterprises may inadvertently open a window to all their data. Hence, organizations need to invest time and money to implement API security.

Non-technical challenges in implementing security in APIs

Security considerations take a back seat, since rapid software development models, tight timelines and increased delivery pressure place the developer's focus on building API functionality to deliver performant applications

Developers lack training, skills, knowledge and understanding of the security aspects required to secure APIs

Lack of security testing and governance processes in organizations

Cost and complexity of implementing the security features in matured APIs is very high and sometimes requires a huge change in design and architecture

Steps to overcome challenges

From a technical design and architecture standpoint, securing APIs is not necessarily complicated. The key, however, is to make sure that security considerations are implemented. The following steps can help the implementation process:



Continuous training and upskilling of development teams on security considerations of APIs, including secure coding as a competency for development teams



It is crucial that organizations educate teams on the importance and need of adding security in APIs



Implementing the security considerations early in the development life cycle



Carving out a phase for security testing in the development process and on-boarding skilled security personnel to carry out and manage security testing



Set up a governance process and gating criteria for production deployment and ensure its enforcement without any exception

Network DDoS protection

DDoS attacks are on the rise and last year was no different. The year that went by witnessed the biggest DDoS attacks of all time with peak traffic reaching 1.3 terabytes per second. The attack was on a “code-hosting site,” where attackers leveraged the misconfigured memcached systems. Unlike a conventional DDoS attack, there were no botnets involved in the memcached DDoS.

Memcached is a database caching system that is used to clear the memory and speed up web applications. It communicates through the User Datagram Protocol (UDP) which doesn’t need any authentication. In a memcached DDoS attack, the attacker targets the vulnerable memcached server and floods it with spoofed requests. Leveraging the amplification capacity of memcached servers, attackers intensify the effect

up to 50,000X and saturate the target server causing an outage.

Are DDoS defenses getting better?

DDoS mitigation is extremely important to reduce the intensity of an attack. If appropriate anti-DDoS tools are in place, then the organization can curb the intensity of an attack. With attackers adopting new and advanced attacking methods, organizations also need to equip themselves with better defenses.

In the research, we asked respondents about the peak duration of DDoS attacks. Interestingly, there is a significant decrease in the attack duration. In 2018, 13% of attacks lasted less than 30 minutes; in 2017 it was 24%. (see Figure 25).

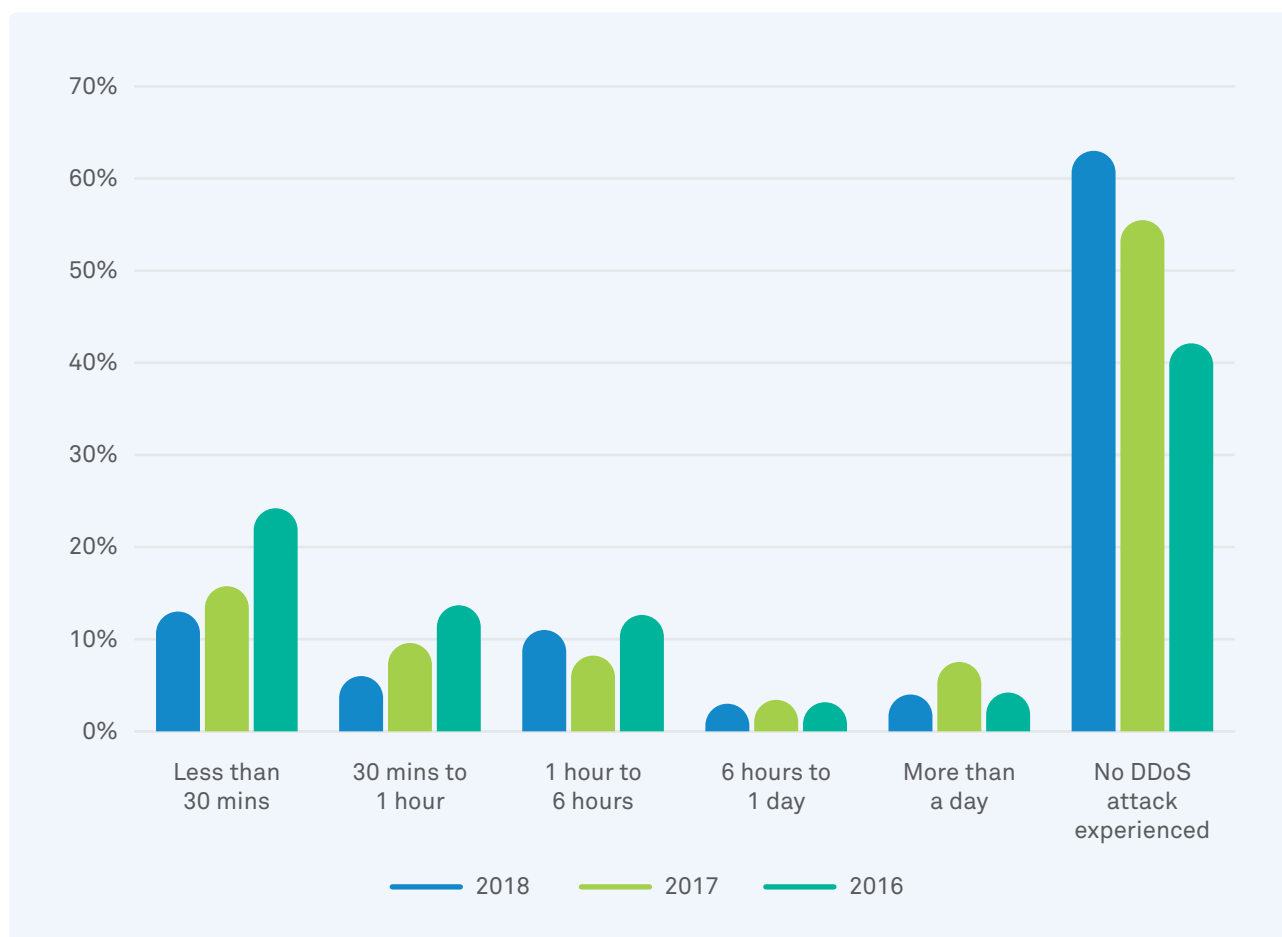


Figure 25: Peak DDoS attack duration, 2018 vs. 2017 vs. 2016



Global insight

In 2018, 13% of attacks lasted less than 30 minutes; in 2017 it was 24%.

Vertical insight

92% of manufacturing organizations have not experienced any DDoS attack in 2018.



Endpoint security

Nowadays, cyberattackers have advanced tools and tactics to launch attacks. Endpoints provide a direct entry for attackers, as they are operated by the weakest link—humans. Stronger security management and patch management techniques are needed to address endpoint vulnerabilities.

The siege of endpoints

In the survey, respondents were asked about the vectors that led to compromise of endpoints. 61% ranked phishing attacks as the most important

vector while 31% of respondents ranked malware hidden in websites as the second most important vector. Compromises via USBs are also among the top vectors that affect endpoint security.

The top vectors that compromise endpoints have been consistent over the past few years. Findings from 2018 and 2017 show phishing emails as the top-most vector that compromised endpoints, followed by malware hidden in websites.

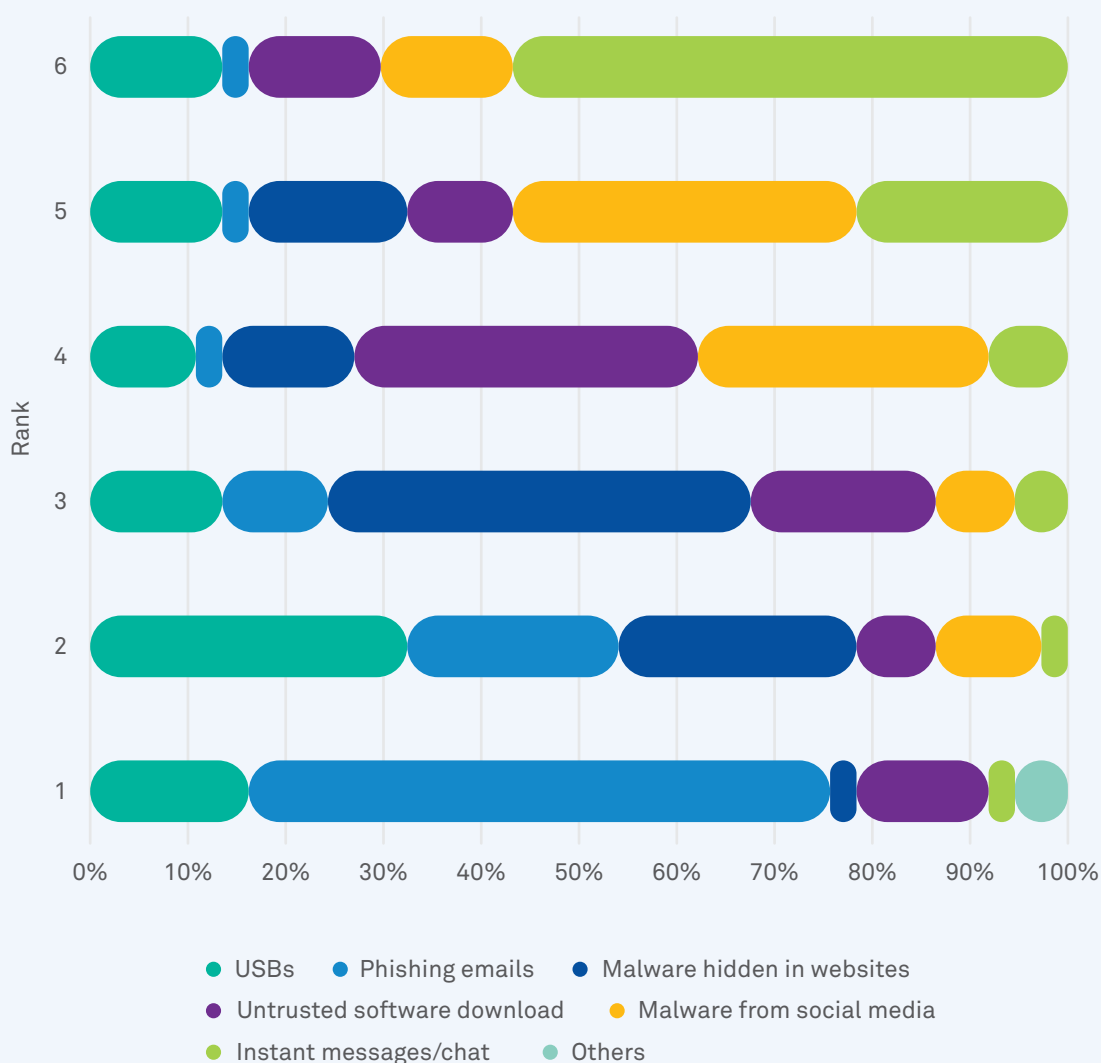


Figure 26: Endpoint attack vectors ranked by frequency, 2018

Global insight



61% of respondents ranked phishing email attacks as the top-most vector for compromise of endpoints.

Security monitoring and analytics

The modern threat landscape is evolving at an alarming rate. The section on “State of attacks, breaches and law” highlighted that cyberweapons were becoming more sophisticated to bypass layers of defenses. Organizations need to continue to strengthen their detective controls in addition to their investments in traditional preventive controls.

ROI-driven management is seeking faster detection and resolution. 65% of survey respondents chose “time-to-detect and remediate incidents” as a key security metric tracked. Figure 27 shows opportunities enterprises want to leverage to improve threat detection.

SOAR is soaring higher

78% of respondents believe Security Orchestration, Automation and Response (SOAR) tools are key to improving the efficiency of threat remediation. This will reduce the dependency on the limited Security Operations Center (SOC) staff and help them tackle relevant alerts.

Threat intelligence and AI/ML-based detection are also notable opportunities to leverage for better threat detection. There is a need to analyze the full spectrum of data available (internal as well as adversary trends and strategies) to provide a unified view and stay ahead of the attackers.

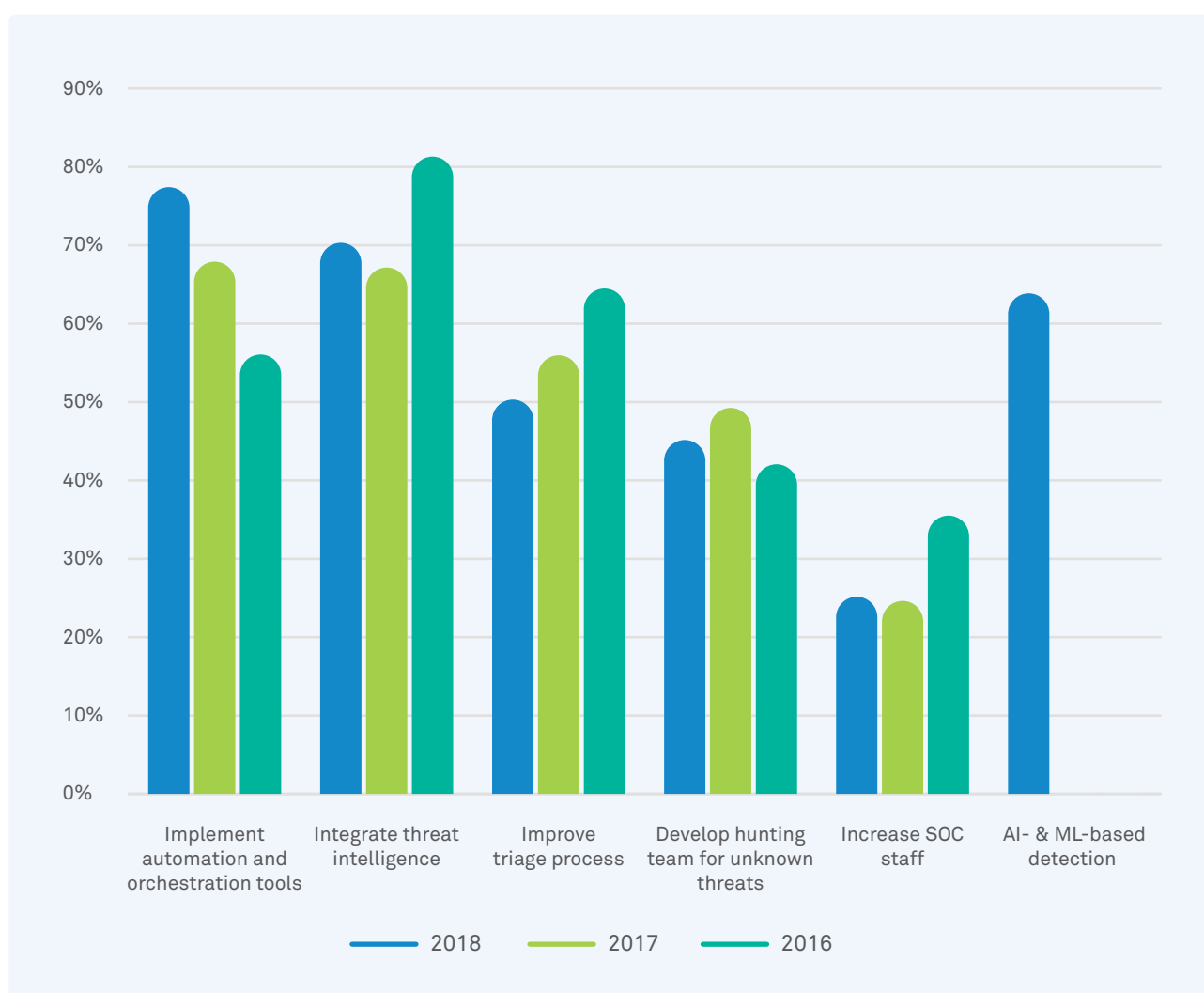


Figure 27: Opportunities to improve threat intelligence capabilities, 2018 vs. 2017 vs. 2016

Global insight

78% of organizations see SOAR tools as an opportunity to improve threat detection.

Vertical insight

71% of banking, health and manufacturing industries track “time-to-detect and remediate incidents.”

Cloud security

As enterprises re-engineer their business processes and systems to address the needs of a digital era, their IT organizations are faced with the 5R dilemma to Refactor, Replace, Re-Platform, Retain or Retire their applications. The approach to the 5Rs has taken a turn from a cloud-averse approach a few years ago to a cloud-first approach today. The “cloud-first” strategy that many trendsetting organizations are following today is underpinned by a well laid-out sub-strategy over two dimensions:

- Poly-cloud approach to avoid lockdown with a CSP
- Hybrid cloud enablement for business continuity and seamless transformation

The poly-cloud approach entails defining and implementing a uniform security strategy with a set of native security controls across multiple CSP platforms. Due to differing maturity levels of security services offered by leading CSP players, enterprises grapple with implementing a uniform security policy across the different cloud environments. However, gone are the days when cloud migration was considered a risk. In fact, when we asked the organizations on the type of data that they are migrating to cloud, 69% called out Employee Information, 45% mentioned Intellectual Property, 41% said Business Finance Records and 40% mentioned customer PII. 70% of US firms have indicated that Secure Hybrid Cloud Architecture are the way to go for the future. The cloud is here to stay and hence security teams have to find the best way to protect it.

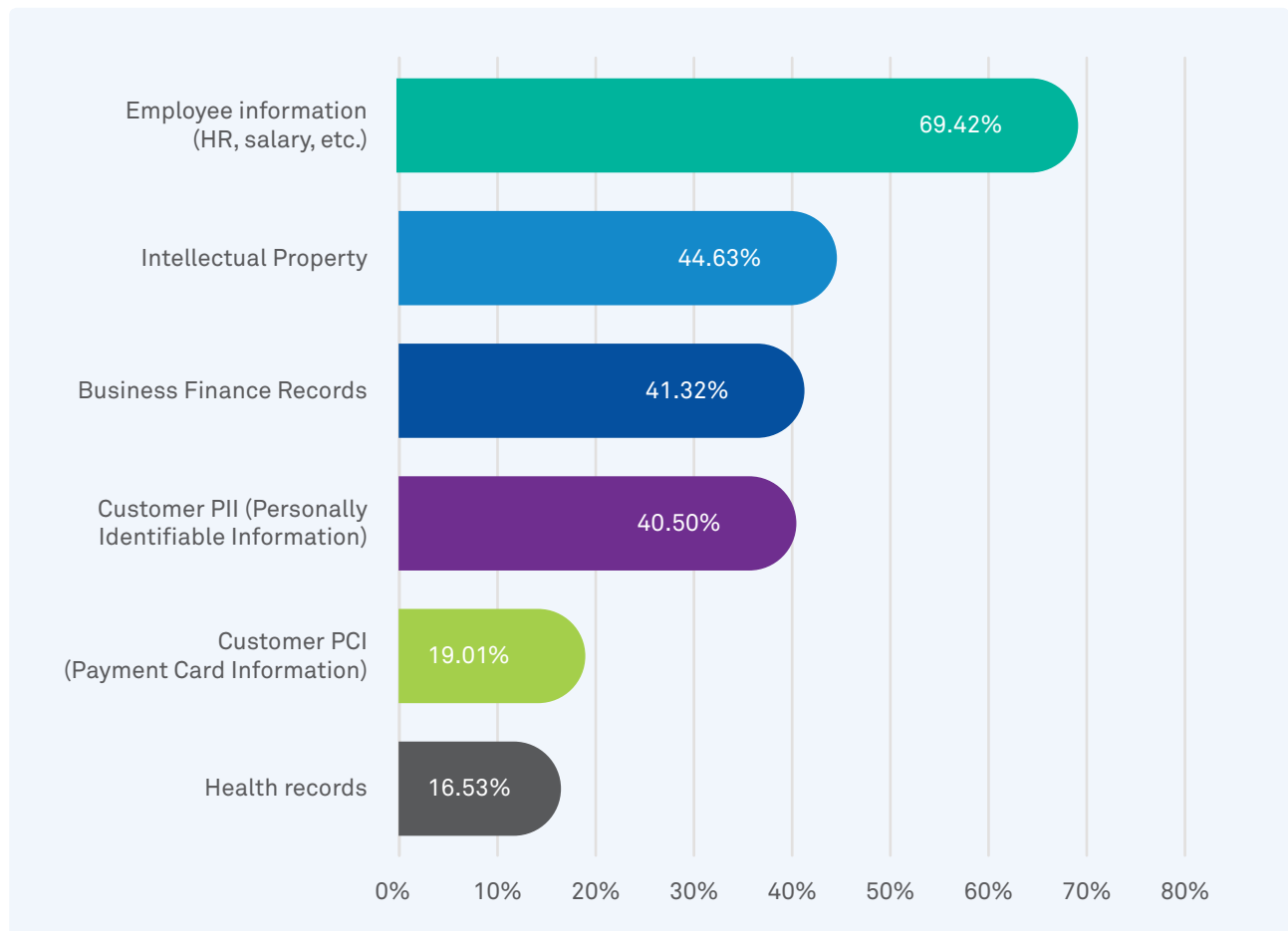


Figure 28: The data organizations are migrating to cloud

Defender stratagem

Change is inevitable, progress is optional. Organizations need to continuously build up their defenses against threats targeted towards emerging technologies.

What are the security risks on the cloud?

The survey respondents rated the following: Open Web Application Security Project (OWASP) Top 10

weaknesses in cloud apps at 31% followed by cloud account hijacking/privilege escalation at 28%.

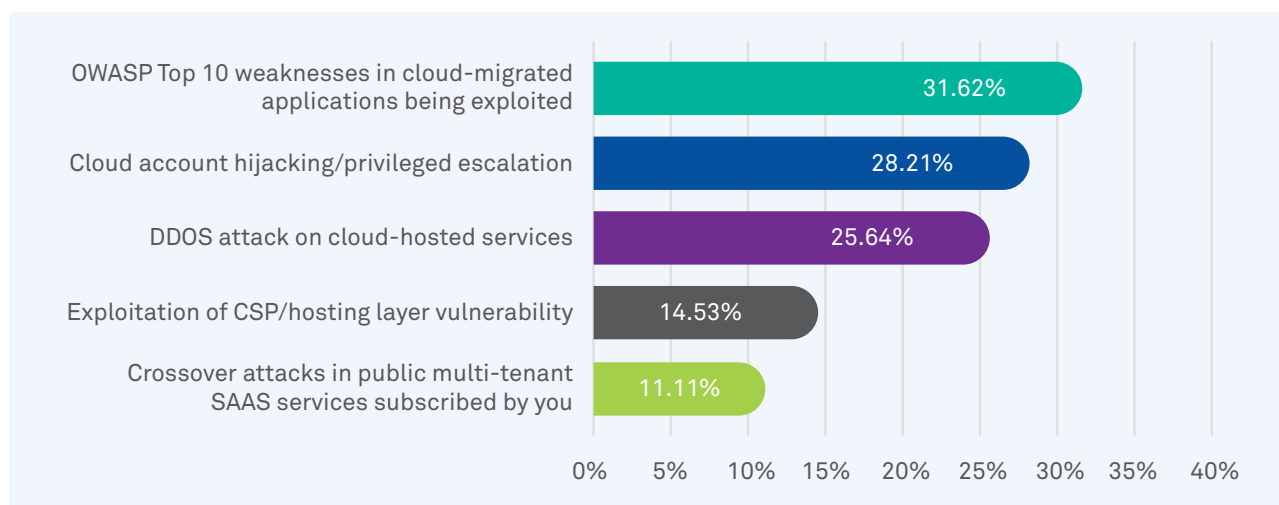


Figure 29: Top technical security risks on the cloud

OWASP Top 10 vulnerabilities in custom web applications have been a recurring challenge for most organizations. As seen from the graph above, cloud account hijacking has emerged as a threat across customer CSP environments and the same poses serious risks to customers actively engaged in a cloud-first strategy. Research by our partner Palo Alto Networks reinforces these findings and the following section dives more deeply into modes of account hijacking and best practices that can be applied by customers to minimize the risk.

Cloud root account compromise: An increasing challenge

The advent of infrastructure as code in cloud environments propelled the fast migration and deployment of workloads into the cloud. This resulted in a steep increase in risky configurations being multiplied across cloud environments. Cloud security teams were thus rightly focused on detecting risky configurations and minimizing their threats. However, today the focus of external threat actors has shifted to the compromise of enterprise root accounts associated with Google, AWS or Azure. A research report by the Palo Alto Networks global threat intelligence team on 5 key cloud security trends indicates that 29% of organizations have detected potential account compromises. The same research also showed that 27% of organizations allow administrative activities using root accounts. Such attacks could be limited if organizations were

to minimize the use of root accounts, and enable their use via multi-factor authentication only.

Related to the account compromise use case is another trend where hackers are creating unauthorized API access keys on compromised cloud accounts. These API keys can then be utilized to remotely administer the environment, perform reconnaissance and ultimately siphon off personally identifiable information or sensitive data. The same research by Palo Alto Networks indicates that 41% of access keys in enterprise cloud environments have not been changed for more than 90 days. Another example of a backdoor access to administrative root access was a compromise that happened using a Google Kubernetes® server that was not password-protected. The compromise indirectly enabled access to many API access keys with admin privileges.

The key recommendations for securing public cloud environments can be summarized as follows:

- Prevent use of root accounts for general administrative activities
- Enable MFA for all privileged public cloud accounts
- Policy-based forced rotation of API access keys
- Monitor Privileged User Behavior using AI-based profiling
- Enforce network security policies for their container services

Partner Content Credits: The above piece was contributed by Wipro's partner Palo Alto Networks (<https://www.paloaltonetworks.com/>)

IoT security

The advent of Industry 4.0 and the Industrial Internet of Things (IIoT) revolution are causing a quantum shift in organizational attitudes to cybersecurity across all sectors. An exponential increase in the number of connected devices within organizations is being anticipated across all sectors. Currently, over 70% of survey respondents identified an asset base of less than 5% connected IoT devices, yet the same respondent population expects that this will rise to 10% in around 60% of organizations within two years.

Significant concerns remain as to who is responsible for IoT security, with device manufacturers often neglecting to ensure security by design and leaving the onus of cyber defense to the consuming organization.

Blended controls approach for IoT

Our research shows that all sectors are cognizant of the increasing prevalence of

connected IoT devices and the security risks they pose. However, a worrying trend is evident in the singular control approach to IoT security whereas a blended controls approach covering the development life cycle through to deployment and end-of-life management is necessary. Given the current absence of IoT device manufacturers accepting liability for security, organizations need to consider an overall strategy to address IoT security risks around infrastructure (networks), applications (access control), authentication (device and data) and physical threats.

Many organizations are struggling to adapt their enterprise IT cyber defenses to address IoT security requirements. The inability to do this is compounded by a skills gap that cannot be easily resolved without a change in strategic approach.

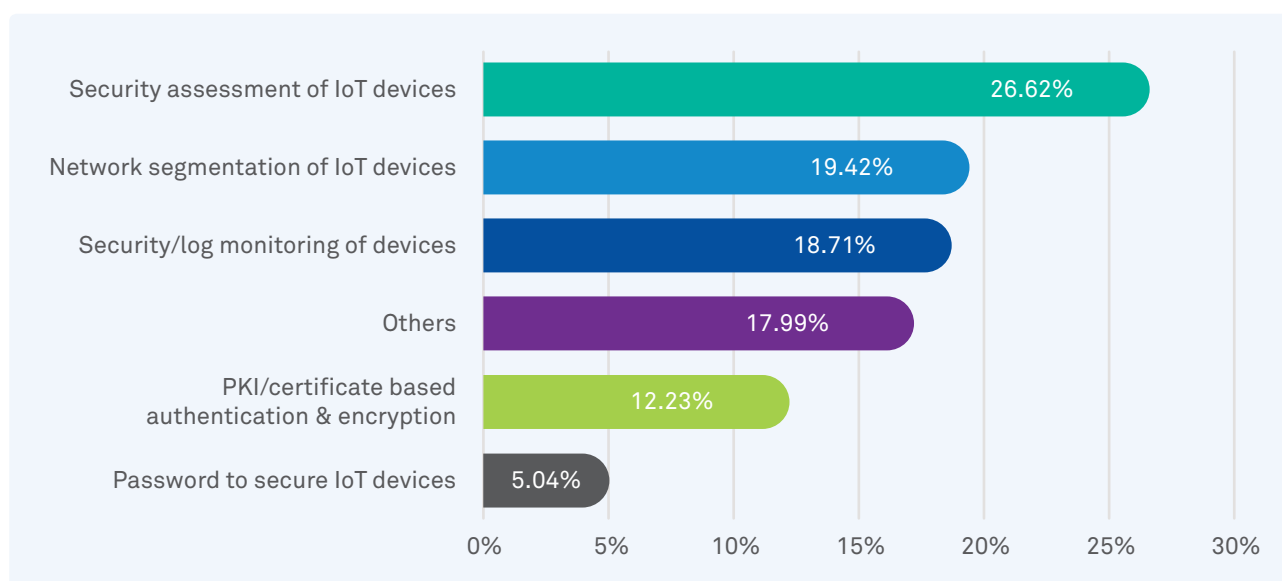


Figure 30: Controls planned to mitigate IoT risks

What is to come in 2019

Organizations impacted by IoT security weaknesses are likely to experience significant financial losses, brand reputation impact and long periods of operational disruption. Therefore, as organizations increase the asset base of connected IoT devices, they are likely to consider significant investments in a new overall approach to cybersecurity that blends traditional enterprise IT with the convergent needs of IoT. 27% of the organizations plan to carry out security assessment of IoT devices, 19% will be

segmenting IoT devices in their networks and 19% will be implementing monitoring controls for their IoT environment.

One of the key enablers of the blended controls approach for IoT is the challenge of authentication. In the last section of this report on the future of cybersecurity, a point-of-view on the use of Physically Unclonable Functions (PUF)-based authentication for IoT security has been presented.

Human dimension

The security practices that have been covered in the previous sections need to come together to build up the technical defenses of an organization. However, these defenses can come crashing down like a pack of cards if the human element is ignored.

For a business to be cyber resilient, cybersecurity needs to be incorporated within the culture of the organization. Employees need to be empowered with knowledge in order to prevent unintentional insider threats and avoid negligence. 72% of organizations surveyed feel employee negligence/lack of awareness is a top cyber risk the organization faces.

How are you addressing the weakest link?

Recognizing the lack of awareness, many organizations are now making sizeable

investments to train their end-users. Figure 31 shows the steps taken by organizations to educate end-users. 87% of respondents have said e-Learning or computer-based training is their approach of choice to educate employees (in 2017, 78% of respondents felt the same). More organizations are partaking in controlled/targeted phishing attack simulation exercises this year (67%) compared to last year (53%).

The data collected revealed that banking and financial organizations follow a trend that is different from other industries. The most significant step followed by 80% of organizations in this industry is to have security policies and formal disciplinary processes in place. This is no surprise, since this is one of the most heavily regulated industries and a breach could involve a direct financial consequence.

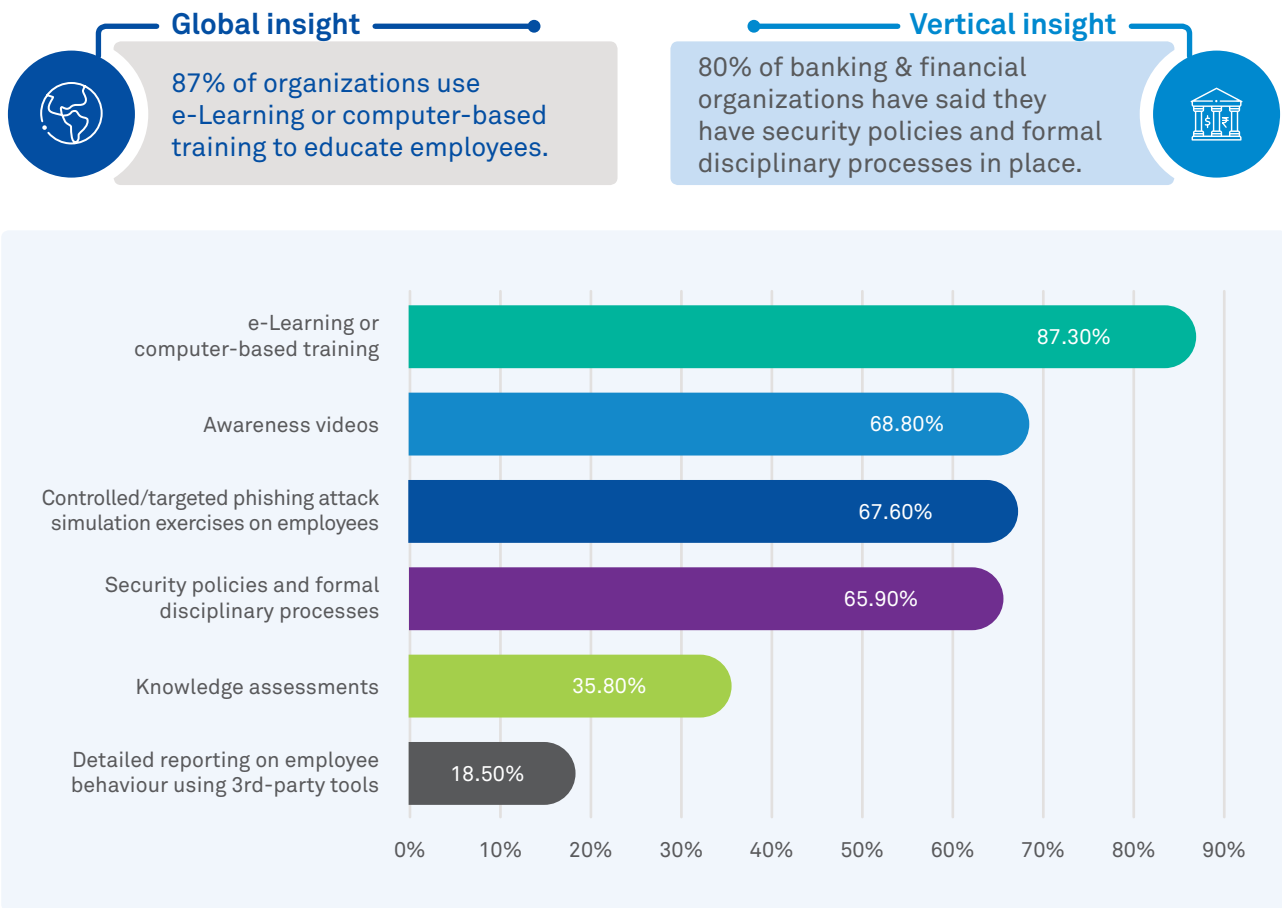


Figure 31: Approaches used to educate users against risky security behavior

Defender stratagem

It's time to empower and bring the "common" back in common sense: The human dimension can no longer be ignored.



State of collaboration

Multi-stakeholder collaboration in cybersecurity

Threat intelligence feeds

Information sharing

Cyberattack simulations

Cyber insurance



If everyone is moving forward together, then success takes care of itself.

Henry Ford

While firms in the same industry compete fiercely in the market, timely collaboration and sharing of cyber intelligence can help them better respond to upcoming cyber threats collectively. This section showcases the meso view which outlines how organizations gather and review threat intelligence as

well as collaborate with regulators/CERTs to partake of cyber exercises. It delves into cyber insurance, an increasingly popular method of risk transfer, and examines its effectiveness and level of adoption. Overall, the positive change in defenders' strategies towards symbiotic collaboration is brought out.

Multi-stakeholder collaboration in cybersecurity

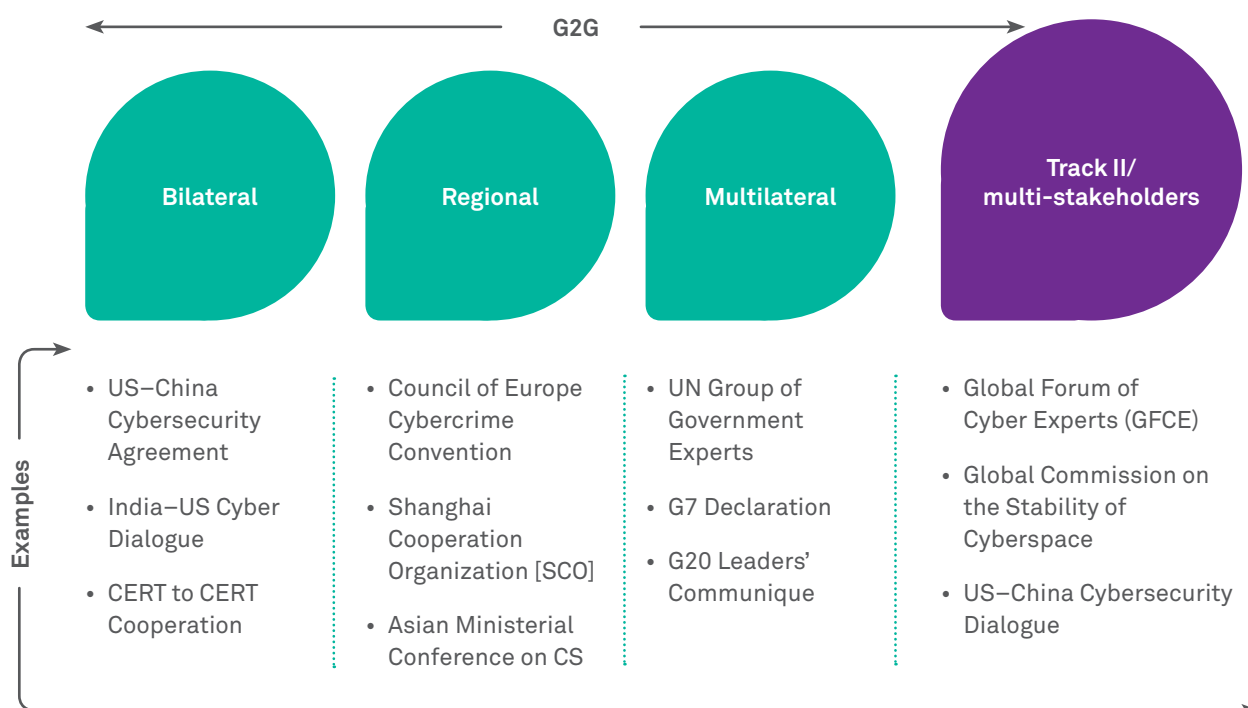
A cybersecurity strategy would be incomplete without laying down a strong foundation for external collaboration. Collaboration furthers the shared goal of moving towards cyber resiliency and ensuring continuity of businesses. This section takes a peek into five examples of collaboration at a government and non-profit organization level. It then delves into an initiative undertaken by the Indian government.

levels. Countries are establishing active cyber diplomacy functions to foster partnerships with each other in the domain of cybersecurity. Governments are elevating cyber diplomacy to the centre stage, with specific efforts, resources and budgets. Governments are encouraging Track II diplomatic efforts to pave the way for an informal mechanism to engage stakeholders, like industry bodies and civil societies. Overall, countries are tackling cybersecurity systematically and enacting special legislations for enablement of external engagements and collaborations.

Avenues of collaboration

1. Cyber diplomacy

Government-to-Government collaboration happens at bilateral, regional and multilateral



2. Coordinated response for incidents and cybercrime

For coordinated, concerted and speedier response to cyberattacks and incidents, that are often transnational in nature, Computer Emergency Response Teams (CERTs) are set up. CERTs are largely set up by respective governments. In some cases, they enjoy legal powers to manage incidents. For example:

- **FIRST** is a premier global body, set up to enable incident response teams by providing access to best practices, tools, and trusted communication. Membership is comprised of CERTs and corporations.

3. Non-profit organizations are doing their bit | ISAC

Information Sharing & Analysis Centre (ISAC) is a non-profit organization wherein peers from an industry join forces to gather threat-related information, distil it and perform analysis to arrive at actionable and shareable intelligence. It is one of the most successful collaboration models. For example, FS-ISAC (Financial Services Information Sharing and Analysis Center) provides financial institutions around the globe with threat

intelligence against cyber threats that could impact the sector.

4. Security of Supply Chain of ICT products

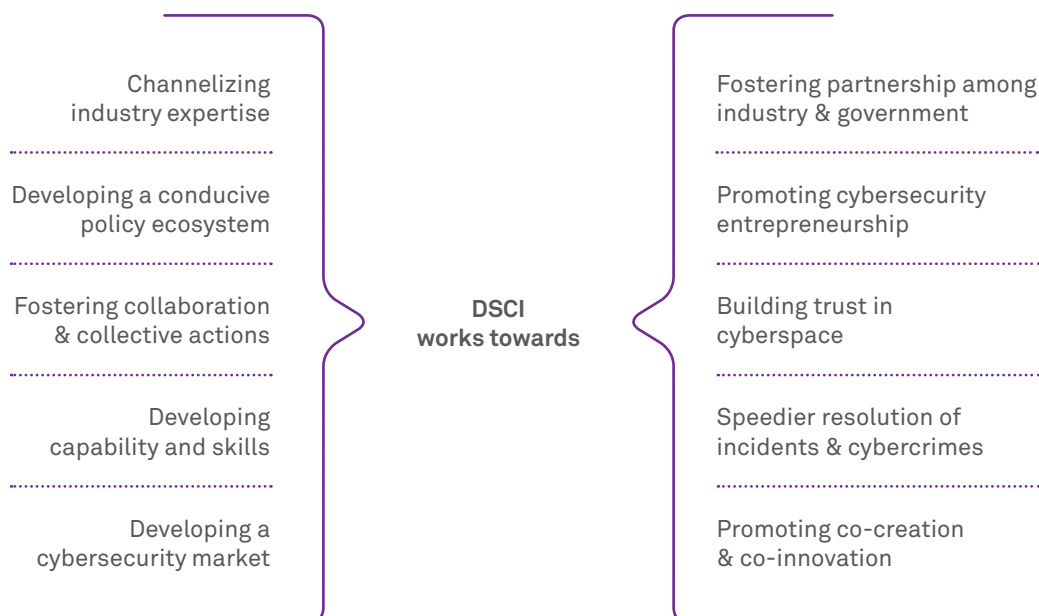
The Common Criteria (CC) Certificate was devised to solve reliability and trust issues associated with IT products. Common Criteria is a means to evaluate IT products and certify them to establish reliability and trust across the boundaries, thereby ensuring ICT supply chain security.

5. World Economic Forum | Centre for Cybersecurity

A global threat should warrant a global response, one that will help shape the future discourse around cybersecurity. With this intent, World Economic Forum has evangelized the idea of a global Centre for Cybersecurity. This envisaged centre, established in 2018, leverages its global network of partners from industries, governments, academia, civil society and international organizations to enhance international security. The goal is to reduce cyberattacks at a global level, anticipate future risks and build an information sharing model between the public and private sector.

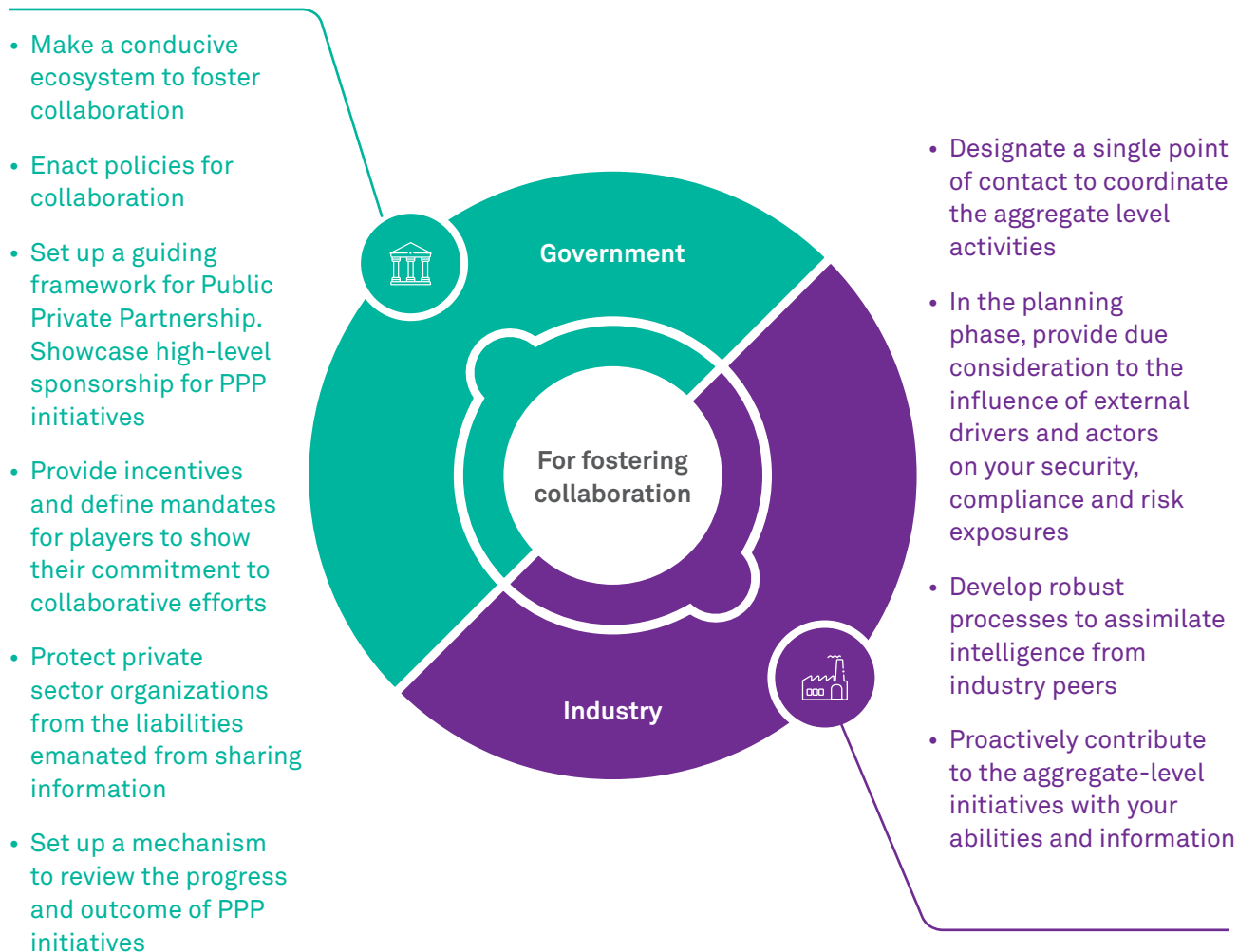
Example of an industry: Government collaboration

Public Private Partnerships (PPP) are vital for enabling collaboration in the realm of cybersecurity and privacy. Institutional mechanisms working at an aggregate level, act as an interface between the government and industry. In India, the IT-BPM industry through its body, the National Association of Software and Services Companies (NASSCOM), set up the Data Security Council of India (DSCI) to foster collaboration in the area of cybersecurity and privacy.



Best practices for government & industry collaboration

Key best practices are highlighted below.



*Partner Contribution: This article was contributed by **Vinayak Godse**, Vice President, Data Security Council of India, , an industry body for data protection in India, set up by NASSCOM®.*

Threat intelligence feeds

Threat intelligence feeds provide daily nourishment to enterprise security teams and automated systems with timely information on tactics, techniques and procedures adopted by prevalent and active threat actors. Security defense solutions are increasingly being equipped with Artificial Intelligence to make cognitive inferences on data as events unfold and determine corrective action leveraging control systems like firewalls, proxies, gateways, etc., that work as rules-based systems. Timely and accurate intelligence feeds on evolving and expanding threats can help organizations tune up the rules in their systems to increase preparedness towards immediate attacks.

Threat intelligence sourcing trends

In the research, we asked organizations about their sources of threat intelligence feeds (Figure 32). Interestingly, organizations are decreasing their reliance on third-party threat intelligence suppliers and in 2018, only 51% of organizations were using third-party threat intelligence suppliers in comparison to 59% in 2017 and 68% in 2016. Instead, they are increasingly relying on their SIEM vendors to provide complementary threat intelligence services.

National CERTs offer intelligence feeds to enterprises and when asked, 56% of respondents confirmed that they are consuming threat intelligence from national CERTs or similar organizations.



Figure 32: Sources for threat intelligence for organizations

Global insight

SIEM is used by 84% of organizations to monitor real-time traffic.

Global insight

74% of respondents use a security analytics team to carry out manual reviews.

Information sharing

Organizations need real-time, internal and external threat intelligence to anticipate and thwart new attacks. Governments and organizations are entering into symbiotic alliances to help one another against intelligent threat actors. Figure 33 highlights the type of information organizations are willing to share

with their industry peers. 67% of organizations are willing to share only the indicators of compromise—malicious IPs, URLs and domains—while 33% of organizations are willing to go one level further and share attacker tactics, techniques and procedures.

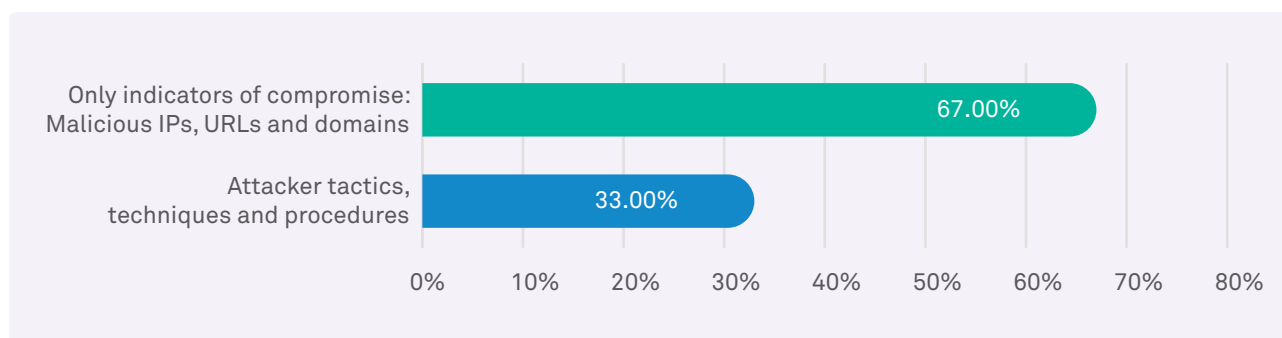


Figure 33: Type of information organizations are willing to share

Barriers to sharing

It is clear from the above figure that not all organizations are willing to pass on information about their attacks. Why does this resistance exist? Figure 34 highlights the reasons for organizations being reluctant to share threat/

attack information with their peer groups. 67% of organizations feel that sharing information can have a negative impact on their reputation while 43% of respondents feel that legally they cannot disclose such critical information to outsiders.

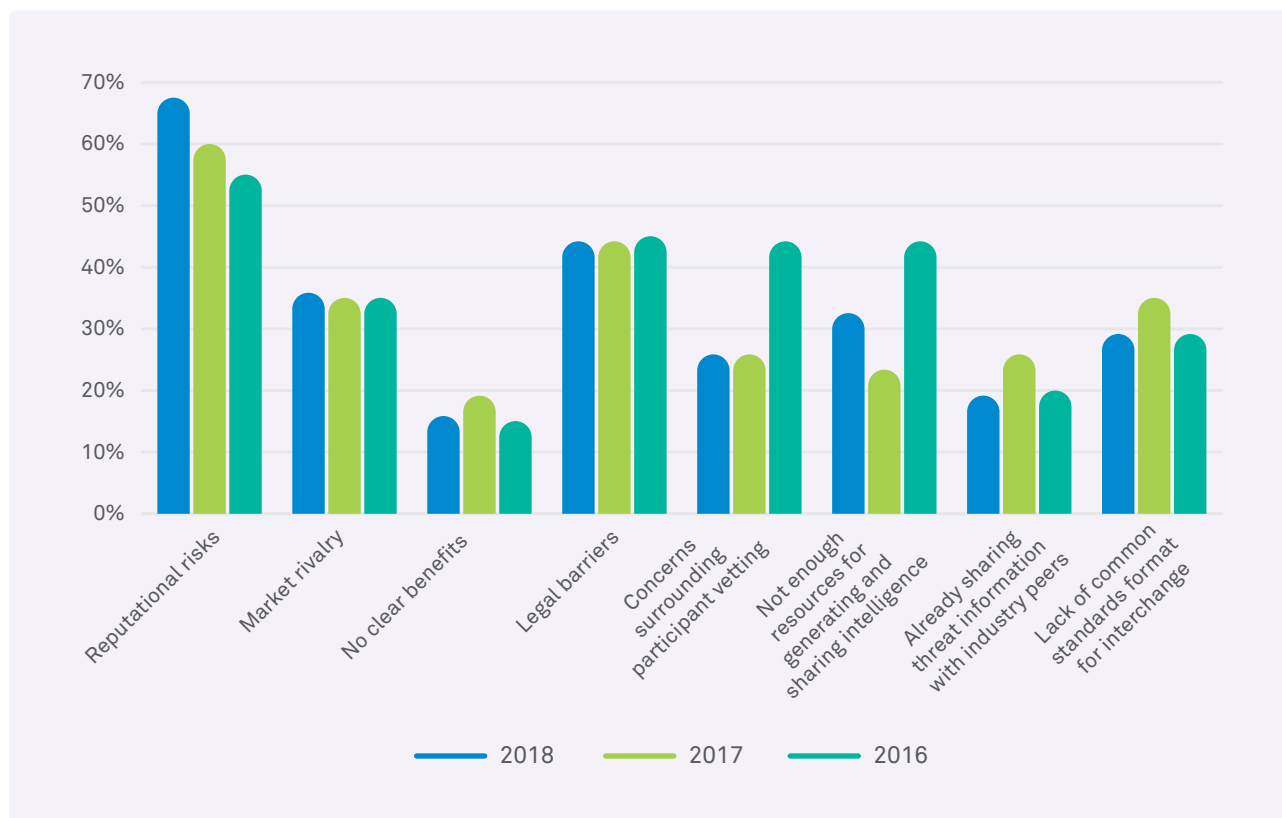


Figure 34: Challenges related to sharing threat information in peer networks

Cyberattack simulations

Cyberattack simulation exercises for a sector will help organizations and regulators practise coordination in the event of a systemic cyberattack. Simulation exercises are like a fire drill, where organizations can invoke and test their incident response protocols.

Industry simulation exercises on the rise

The research found that 31% of organizations participate in cyberattack exercises coordinated

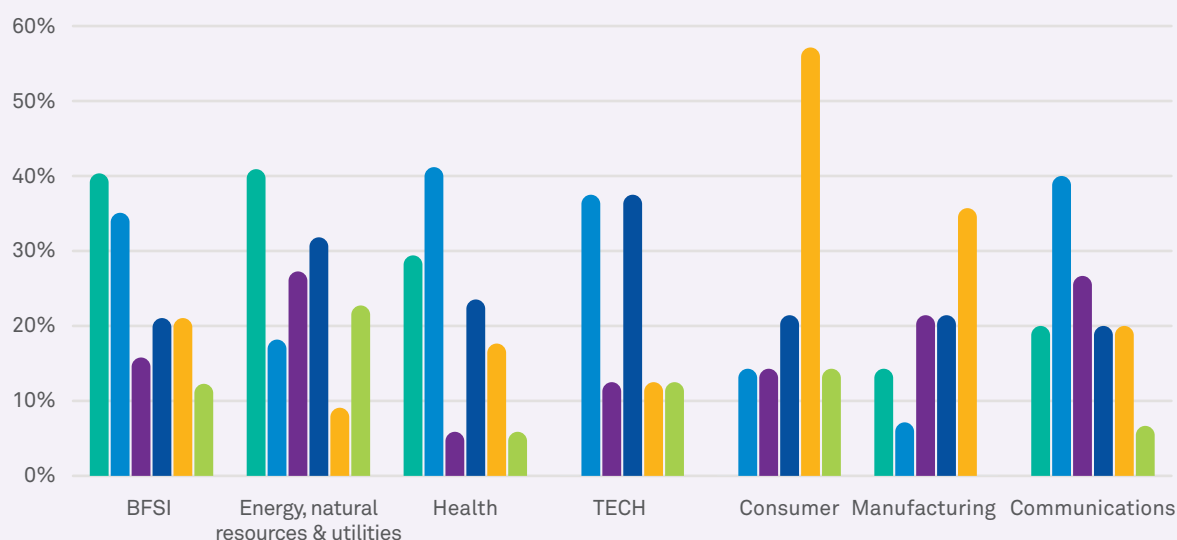
by national CERT/CSIRT. Also, 28% of organizations participate in an attack simulation exercise organized by industry regulators. 40% of the BFSI sector and 41% of health organizations participate in an attack simulation exercise organized by their respective industry regulators. 41% of energy & utilities organizations participate in cyberattack exercises coordinated by national CERT/CSIRT. Research showed that 26% of organizations never participate in any attack simulation exercise.

Global insight

31% of organizations participate in cyberattack exercises coordinated by national CERT/CSIRT.

Vertical insight

57% of surveyed consumer organizations have never participated in any cyberattack simulation exercises.



- Cyberattack exercises by geography-specific industry/sector regulators (like SEC, Federal Reserve, NERC, FSA, EBA, etc.)
- Cyberattack exercises coordinated by National CERT/CSIRT
- Cyberattack exercises coordinated by any governmental/defense agencies
- Cyberattack exercises coordinated by an MSSP
- Never participated in any simulation
- Others

Figure 35: Organizational participation in cyberattack simulation exercises by industry verticals

Defender stratagem

The question is not about IF, but WHEN. Organizations have only one shot to respond to a breach. Practice is pertinent.

Cyber insurance

Enterprises are embracing cyber insurance, complementing their risk mitigation strategy. While security policies and controls need to be the core part of any cyber risk mitigation approach, insurance can help cover monetary expenses that are incurred as a consequence of a breach. Cyber insurance coverage varies across insurers and typically includes the following expenses with their sub-limits: forensic investigations, legal expenses, fines, settlements, identity and credit monitoring, PR costs and IT recovery costs.

The research findings have shown a clear trend in the last three years—65% of organizations have some cyber insurance policy in place showing a relative rise from 55% last year. Around 39% of organizations have a dedicated cyber insurance policy in 2018. This is a significant rise considering only 27% and 26% of organizations had a dedicated cyber insurance policy in 2017 and 2016 respectively.

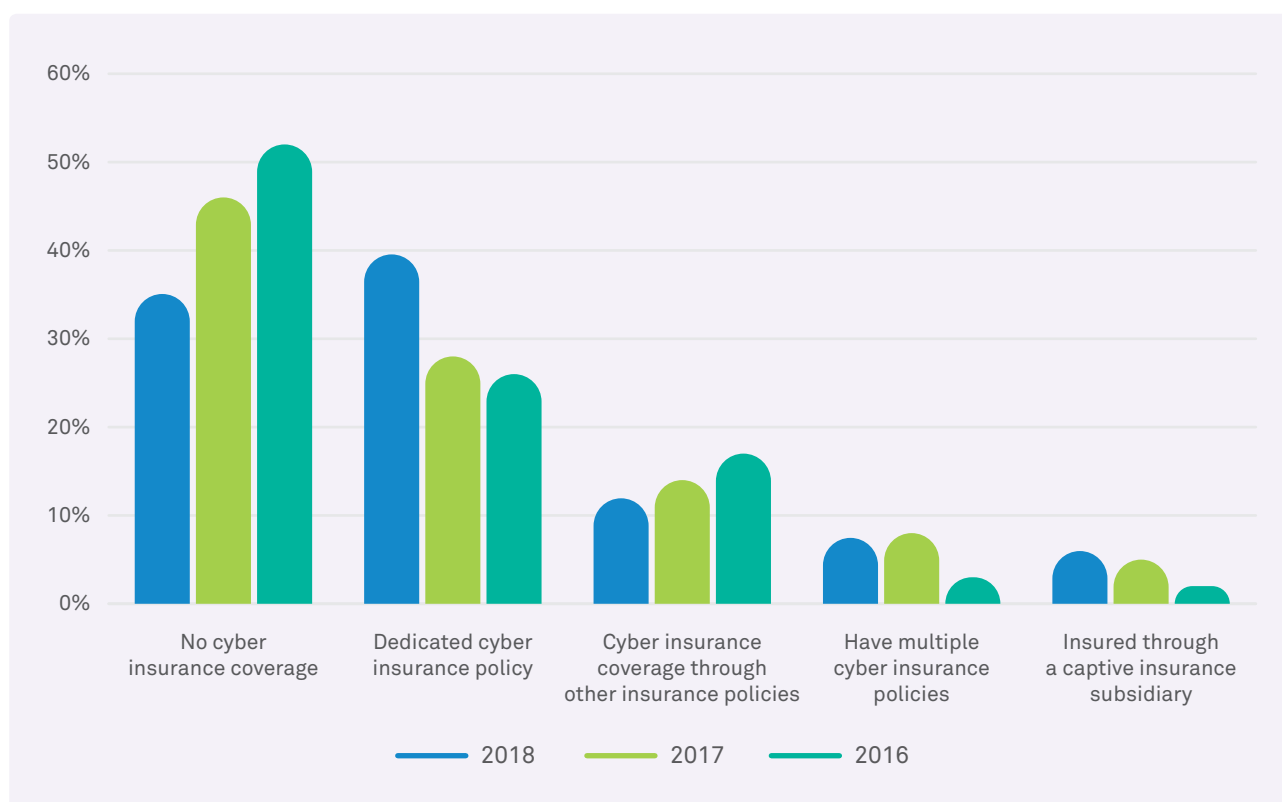


Figure 36: Cyber insurance policy adoption, 2016–2018

Words of caution

Firstly, cyber insurance is a hedging tool that organizations can adopt to minimize the monetary expenses in the event of a breach. But it should not be considered a replacement for a cyber protection program.

Secondly, organizations should read the fine print in insurance policies as they include various restrictions on areas of coverage, jurisdiction, third-party vendors, etc.

Global insight

65% of organizations have some cyber insurance policy in place.

Vertical insight

76% of surveyed health organizations have dedicated cyber insurance policies.



Future of cybersecurity

Cybersecurity patents

Seed investment trends in cybersecurity start-ups

PUF-based authentication for IoT security: An alternative approach

Security pillars of 5G



The future depends on what you do today.

Mahatma Gandhi

This section examines a few select emerging trends that will shape the field of cybersecurity in the coming years. It looks at the in-depth analysis of patents filed in the security space around the globe. This is followed by the research contributed by Indian Institute of Technology, Kharagpur, which provides an insight into

Physically Unclonable Functions (PUF)-based authentication for IoT security. As the number of connected devices increase exponentially, IoT security will play a crucial role not only in the present but also in the future. In closing, this section also highlights the key security challenges and opportunities in 5G networks.

Cybersecurity patents

One way to assess where technology is heading in the cybersecurity space is to look at global trends around patent filings. Patents highlight the areas corporations, governments and educational institutions are exploring through research. It gives a good indication of the technologies that will dominate the cybersecurity space in the coming future.

Scope of research

Research was conducted for three of the top emerging technologies: Research was conducted at the intersection of security practice areas such as data and content security, cloud security, endpoint security etc. with emerging technologies like cognitive computing,

blockchain and IoT. The analysis was done on patents filed from 2016 till the end of 2018 from 17 countries—Australia, Brazil, Canada, China, France, Germany, India, Japan, Mexico, Norway, Russia, Singapore, South Africa, Sweden, Switzerland, UK and USA.

Security patents on the rise

Since 2016, 2,300+ patent families (inventions) have been filed. Remarkably, there has been a 27.2% growth in the number of patents filed since 2016. It is worth noting that the data for 2018 is incomplete due to procedural delays at patent offices across the world in publishing patent-filing data. Figure 37 brings out the yearly rising trend in security patent filings.

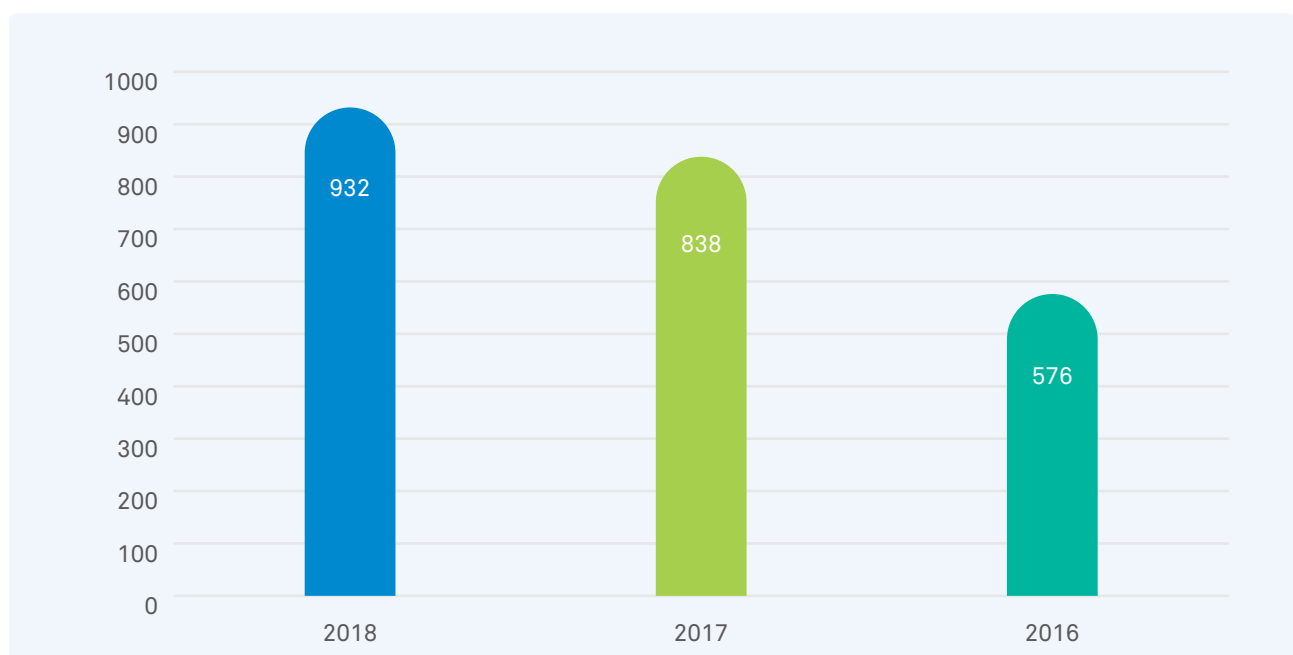


Figure 37: Number of security patents filed globally (2016–2018)

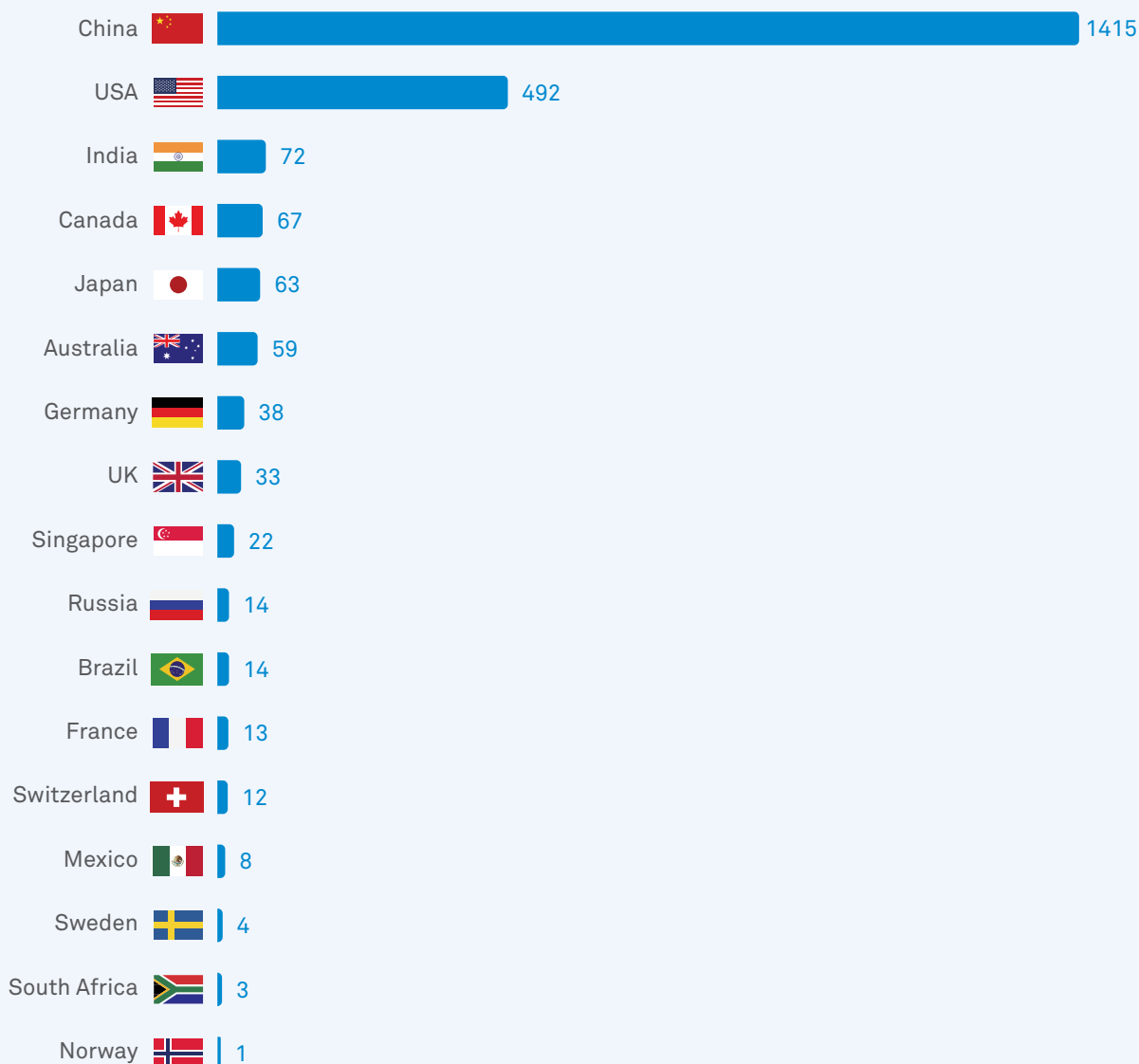


Figure 38: Patents filed by geography (2016 onwards)

Figure 38 presents the cumulative number of cybersecurity related patents filed over 3 years across 17 countries.

Race for patents

It is clear that China has by far surpassed all other countries. The 1,415 patents filed from China were predominantly from eight major corporations and five universities. This healthy split between corporations and universities indicates that academia is actively investing in the development of unique solutions to address the increasing focus on security. Out of the patents filed, only 5% of Chinese patents were filed in US and other jurisdictions. This indicates that Chinese patents are largely indigenous and there is low validity of protection of these patents outside of Chinese jurisdiction (the low percentage may

Global insight

In terms of cumulative patent filings over the period of 2016–18, China (~1,415 patents) and USA (~492 patents) figure on top, followed by India (~72 patents) and Canada (~67 patents).



also be attributable partly to procedural delays in publishing patent data by patent offices, as mentioned earlier). The trend in the number of patents filed shows the growing importance of cyber research, although we cannot verify the quality of these patents.

The US comes second with 492 patents filed over the past few years. Most of the patents were related to user authentication, anomaly detection using machine learning and behavioral analytics.

Cross-section of practice areas in cybersecurity and key technology implementations

For the study, we analyzed the patents across two dimensions—practice area and emerging technologies—and the research brought out some interesting results. Figure 39 shows the number of patents filed by technology and practice area. Data & content security and cloud security are leading with a higher number of patent filings followed by endpoint security. Innovations in data and content security are largely enabled by cognitive computing/AI-related technologies (728 patents), followed by blockchain (686 patents) and analytics (194 patents). Data security includes

protection of data from unauthorized access and includes data encryption, tokenization, and key management practices that protect data across all applications and platforms.

From a technology implementation point of view, cognitive computing/AI has emerged as the top-researched area followed by blockchain and analytics.

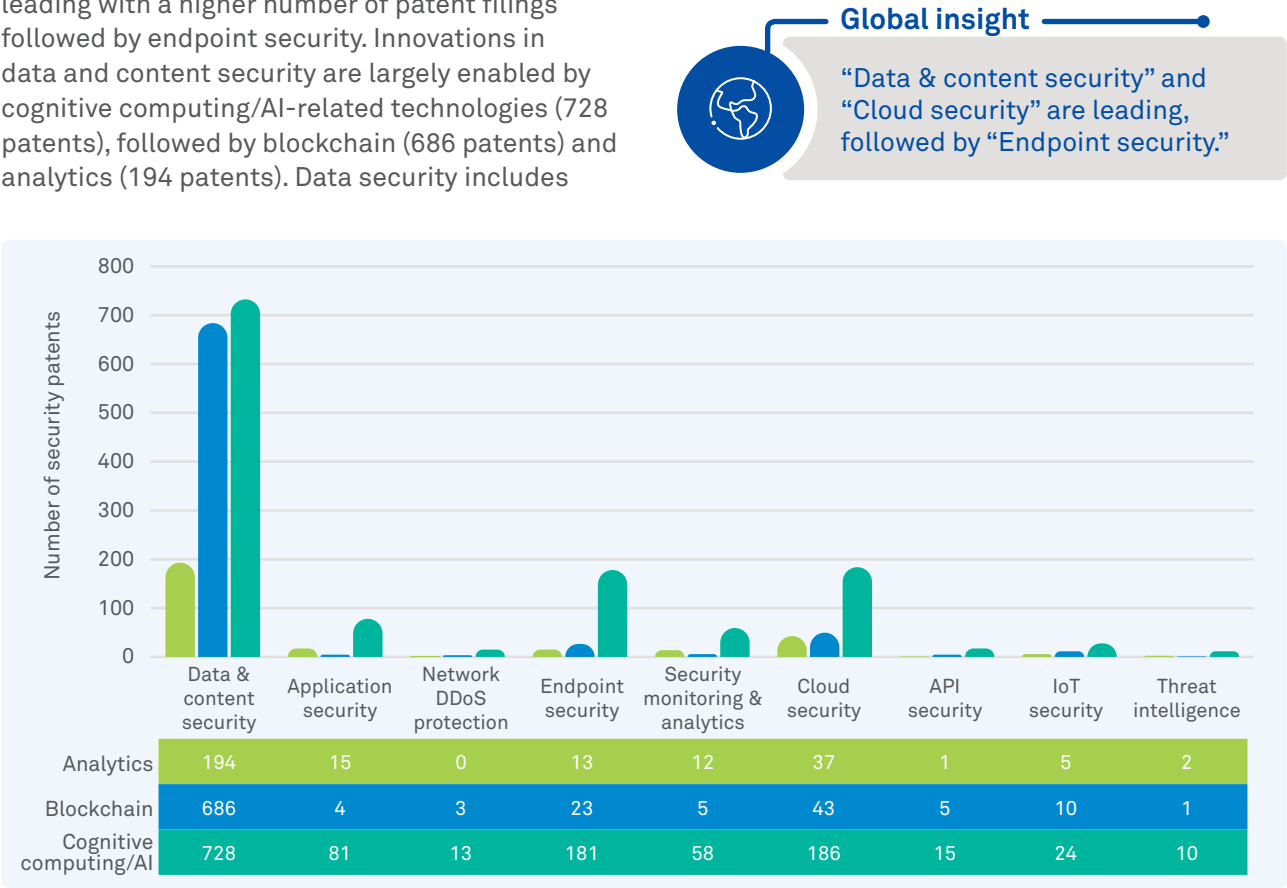


Figure 39: Cross-section of practice areas in cybersecurity and technology implementation

Global insight

Cognitive computing/AI technology dominates the rest of the technologies with more number of patent filings in sub-areas “Data & content security,” “Cloud security,” and “Endpoint security.”

Conclusions

It has been observed that some of the practice areas, such as data & content security and cloud security, have a larger number of patents. While traditional analytics is not registering a positive innovation impact, proliferative growth of cognitive computing/AI in cybersecurity is expected to have a strong impact on how products and solutions innovate in this space, and drive transformation in existing solutions. The use of blockchain in cybersecurity is also rapidly

gaining momentum and is expected to become mainstream within the next five years.

From a practice area standpoint, data and content security continues to be the most significant innovation and growth driver, while we see a stable pace of innovation and implementation in cloud security. Even niche upcoming areas such as API and IoT security are expected to become mainstream in the next two-to-five-year time frame.

Seed investment trends in cybersecurity start-ups

What are the recent cybersecurity areas that have caught the eye of investors?

Seed investment trends in cybersecurity start-ups give an indication of the emerging security domain areas. These areas indicate potential white spaces that enterprises need to watch out for. For the purpose of this

research, Wipro analyzed the start-up funding data received from Tracxn. To arrive at the top security areas that are getting the most seed investment, Wipro classified the start-ups by the security areas they cater to. The research deep-dived into the top 50 start-ups (by total seed funding) founded over the past 3 years, to arrive at the below results.

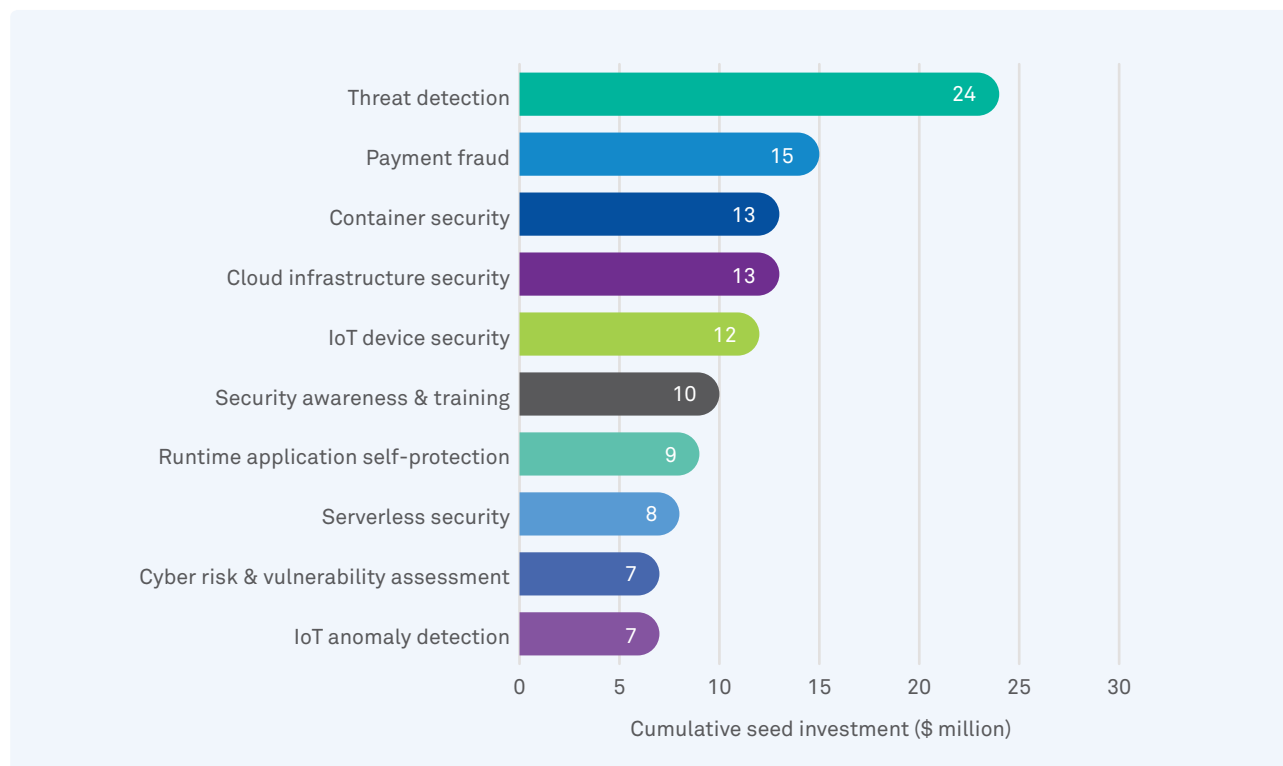


Figure 40: Top 10 security domain areas by total seed funding (2016–2019) [Funding data source: <https://tracxn.com/>]

Areas of Interest

Container security

Microservices exposed through containerized environments are increasingly prone to new threats. Enterprises need to look beyond native security capabilities for securing their container environments.

IoT anomaly detection

IoT assets in enterprise networks come with minimal security functionality. Network behaviour-based anomaly detection solutions are one of the means to fill the gap.

Threat detection

Threat detection start-ups receiving investments are promising AI-driven autonomous threat hunting technology using underlying data sources across the enterprise.

Other notable investment areas

Blockchain technology in fraud detection & serverless security start-ups have seen an upswing in investments.

Another interesting trend noticed is the rise of vertical-specific solution cybersecurity start-ups particularly in medical device security, industrial security and automobile security.

PUF-based authentication for IoT security: An alternative approach

The series of DDoS attacks in recent times on DNS providers have made enterprises realize how vulnerable they are. Some of these attacks were carried out through Mirai botnets hosted over millions of vulnerable IoT devices like digital cameras, smart TVs, printers and baby monitors. One such attack was so enormous that up to 100,000 IoT devices were compromised to inflict a DDoS attack with a strength of 1.2 TBPS.

With the advent of IoT devices, the enterprise perimeter is expanding rapidly. Most IoT devices come with very limited in-built security capabilities. These devices are more difficult to patch and are proving to be the Achilles' heel of the enterprise endpoint ecosystem.

IoT devices are extremely difficult to secure on par with other enterprise systems based on a standard policy baseline because they come with limited computational and battery power. CPU limitations and lack of power prohibits OEMs from implementing classical encryption techniques that are computationally intensive. Additionally, the management overhead of classical security adds to the overall cost of IoT infrastructure. The ones that offer security support traditional authentication protocols where a user presents a set of credentials with supplementary proof such as password or digital certificate-based authentication. However, IoT devices need more advanced methods as these conventional techniques face the persistent

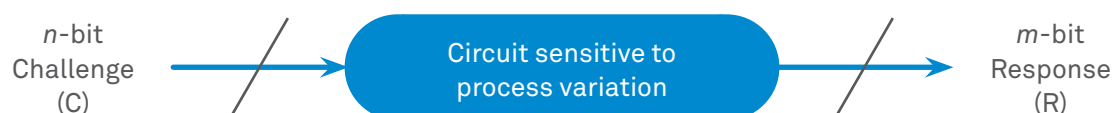
problems of password dependency and not being able to bind the access requests to devices that they originate from. Additionally, the protocols need to be lightweight and heterogeneous for them to work seamlessly.

An alternative way to overcome these problems is through certificate-less authentication and key exchange schemes using lightweight PUF, which addresses the needs of low-powered IoT devices. The PUF-based system acts as a hardware fingerprint generator for the circuit of which it is a part. This facilitates in giving a distinct identity to every device in the IoT framework. PUF-based authentication protocols rely on the “challenge-response authentication” mechanism rather than the conventional password or certificate-based authorization. The response generated on-the-fly by the challenge applied to a PUF instance can be used to authenticate the IoT device and to generate session keys for secure message encryption, thus effectively minimizing the complexity of managing and storing the keys for IoT devices.

PUF is basically a function that maps the input n -bit challenge to the output m -bit response.

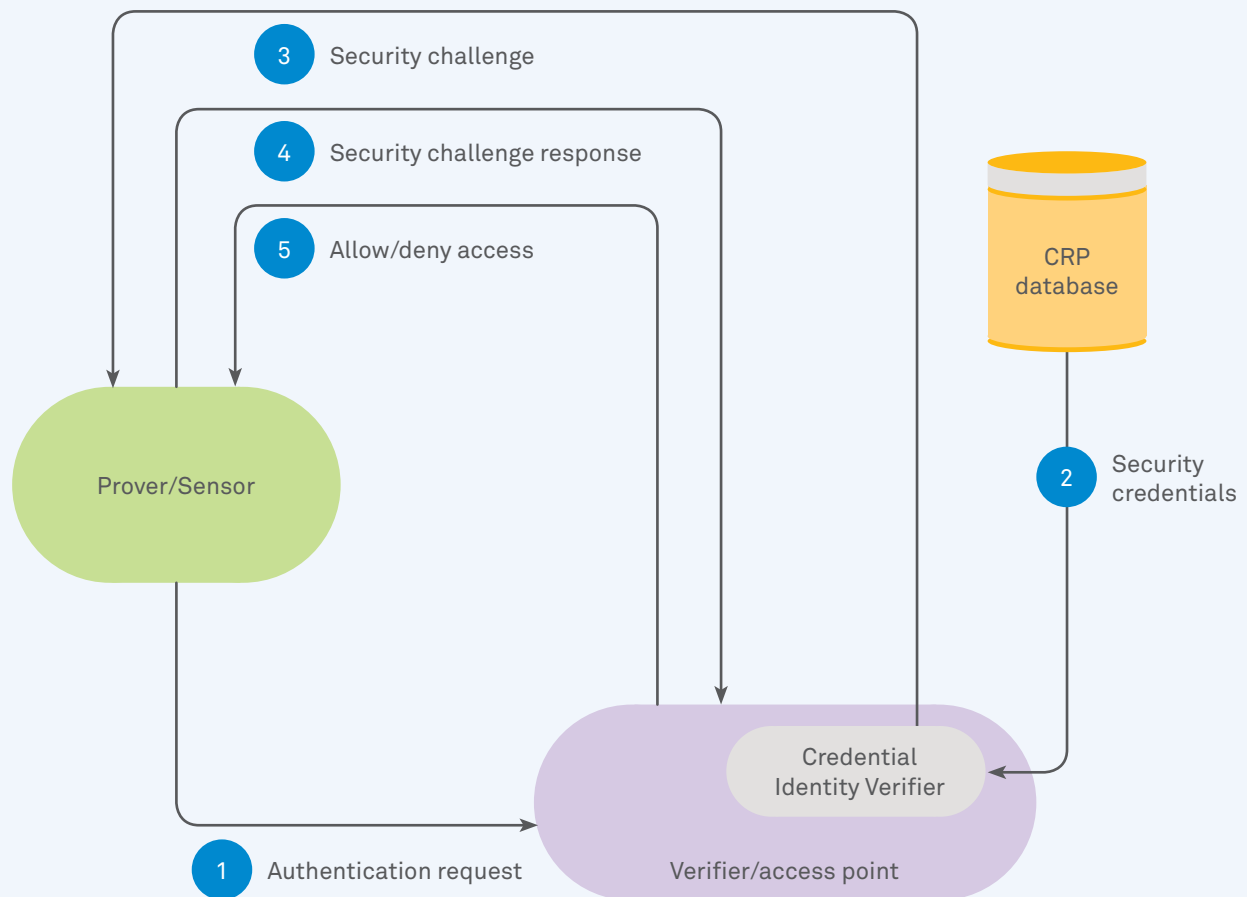
$$\text{PUF}_d : \{0,1\}^n \rightarrow \{0,1\}^m$$

$$\text{PUF}_d : C \rightarrow R$$



The ordered pairs (c_i, r_j) are defined by the hardware variation of the device. As the PUF circuits are designed to be sensitive to manufacturing process variation, each PUF

circuit provides a different response to the challenge provided. The validation is done by comparing the received response to the reference response.



Step 1: The Prover sends an authentication request to the Verifier

Step 2: The Verifier picks a CRP from the CRP database in the public domain

Step 3: The Credential Identity Verifier checks for the sanctity of the CRP picked from the database. Once the CRP is authenticated, the Verifier sends the challenge to the Prover

Step 4: The Prover sends a response corresponding to the challenge sent by the Verifier

Step 5: The Verifier now validates the response from the Prover with the one from the database and if there is a match, access is granted or else denied

Figure 41: PUF architecture

A variety of PUF-based lightweight security protocols have been under development and have, lately, started gaining maturity. Many of these protocols can work with traditional systems that do not have a PUF circuit. An appropriately designed PUF-based security protocol enjoys many advantages including:

1. Unique and abundant built-in keys
2. Unclonable fingerprint of the device
3. No storage required to save secret key
4. Lightweight hardware
5. No requirement of key management infrastructure
6. Hardware–software binding

The major challenge that the PUF technology faces is that of reliability. The PUF can deviate from its ideal response based on the operating conditions (input power, temperature and electromagnetic emanations) and the age of the hardware. Additionally, the PUFs are susceptible to side-channel attacks which occur through the components built around input/output signal interface. The PUFs are also vulnerable to modelling attacks. If an attacker gets hold of a set of Challenge Response Pairs, when the CRP data is exposed as per design/implementation defect/lack of physical security, they can develop a model which can predict the response being generated to the challenge being presented to the device with a very high probability.

Despite the limitations, the PUF-based security approach has the potential to address the security issues between IoT device nodes and the gateways which is absent as of now. Once the challenges of reliability, interoperability with classical security and thorough testing on attack surface are reasonably addressed in the near future, it will be a matter of time before the protocol is widely adopted by the industry. Continuous efforts from the research community are being made to enhance reliability to industry standards, preventing side-channel and machine learning attacks, and designing a protocol that can seamlessly interoperate with classical security.

With the potential of securing the IoT infrastructure through lower computation, minimal management and lesser cost, PUF has applicability in situations where mass deployment and management of the IoT devices are a requirement. Some of the scenarios are:

1. Home-video surveillance systems, where a substantial proportion of cameras are operational with no security. With a suitable software protocol, PUF-based mechanisms can enable authentication and other security requirements on camera devices with negligible user configuration/management.
2. Industrial IoT, where a large number of IoT devices and sensors are deployed within a factory or plant. Existing schemes of securing IoT involves password and setting up keys which results in management overhead. A PUF-based protocol can offer an authentication system which isn't password dependent, which could be a much safer and cost-effective option for the IoT infrastructure.
3. Modern-day hospitals, where there is increasing usage of health sensors. There is a challenge to assign a group of sensors to a particular aggregator that identifies a patient. Currently, this process is manual or semi-automated with password/key-based security setup between sensors and aggregator. PUF-based protocol has the potential to provide password/key/certificate-less security with centralized control.

Wipro is jointly engaged with the Indian Institute of Technology, Kharagpur, for research on PUF-based authentication and key exchange protocols for IoT. The project aims to develop one of the first prototypes on PUF-based authentication and key exchange with promising features of proven high security levels, combined with minimal footprint on power and time.

This section/article has been contributed by Professor [Debdeep Mukhopadhyay](#), Department of Computer Science and Engineering, Indian Institute of Technology, Kharagpur. For more information on the research, refer to: <https://ieeexplore.ieee.org/document/8353301>

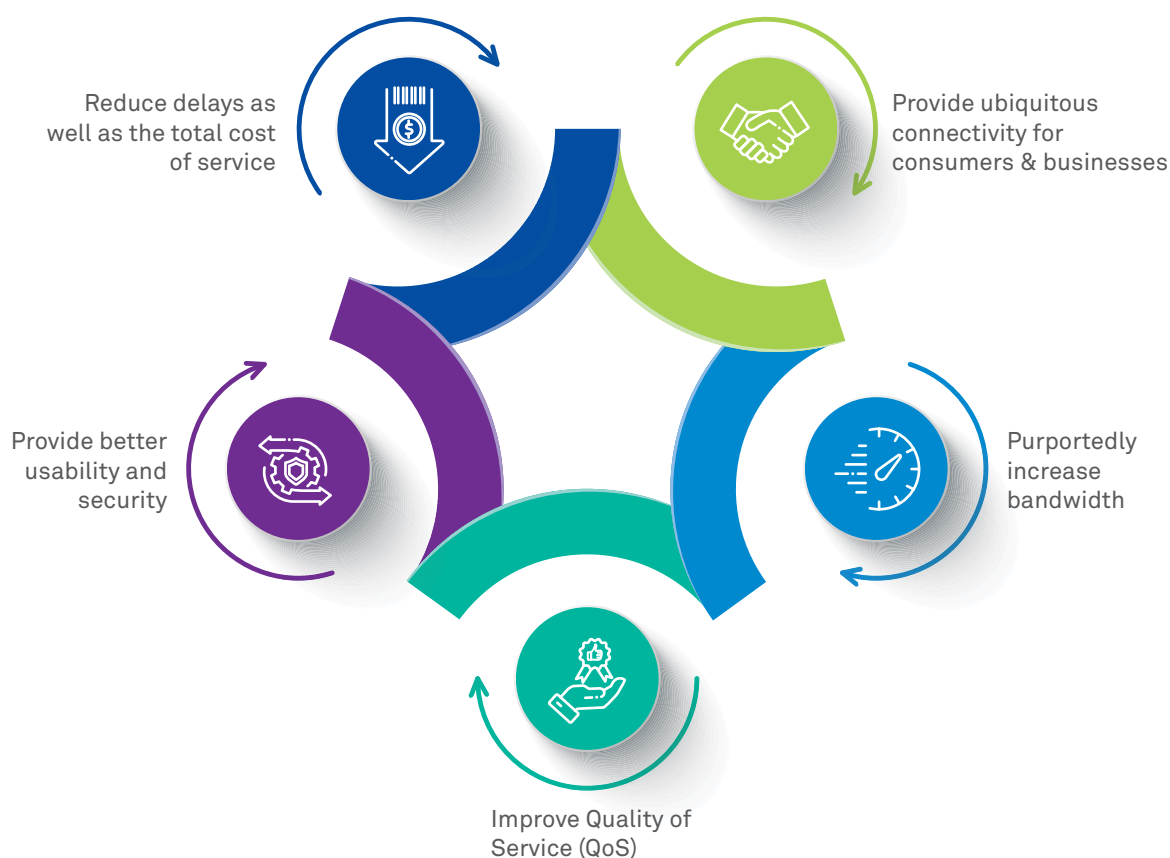
Security pillars of 5G

Fifth-generation(5G) mobile technology is expected to provide a number of improvements compared to its predecessors in terms of higher data rates (up to 1 Gb/s), massive connectivity, flexible service creation and low latency. By virtue of its flexibility and an agile development methodology that uses modular network functions, it supports a wide range of use cases that are both scalable and cost-effective. Software Defined Networking (SDN) and Network Function Virtualization (NFV) play a key role in

providing functional modularity and flexibility in a 5G network.

5G is an enabler of vertical use cases that will transform the way humanity lives, works, and engages with its environment. In the short term, 5G can support exciting use cases like Augmented Reality/Virtual Reality applications, smart cities, smart transportation, eHealth, entertainment services, tactile Internet and holographic interactions.

Benefits of 5G technology



Today, several standard organizations and forums are working on defining the architecture and standardizing various aspects of 5G technologies. These include NGMN (Next Generation Mobile Network), ITU (International Telecommunications Union), GSMA (GSM Association), 3GPP (3rd Generation Partnership Project), WWRF (Wireless World Research Forum), 5G Americas, 5GPPP (5th Generation

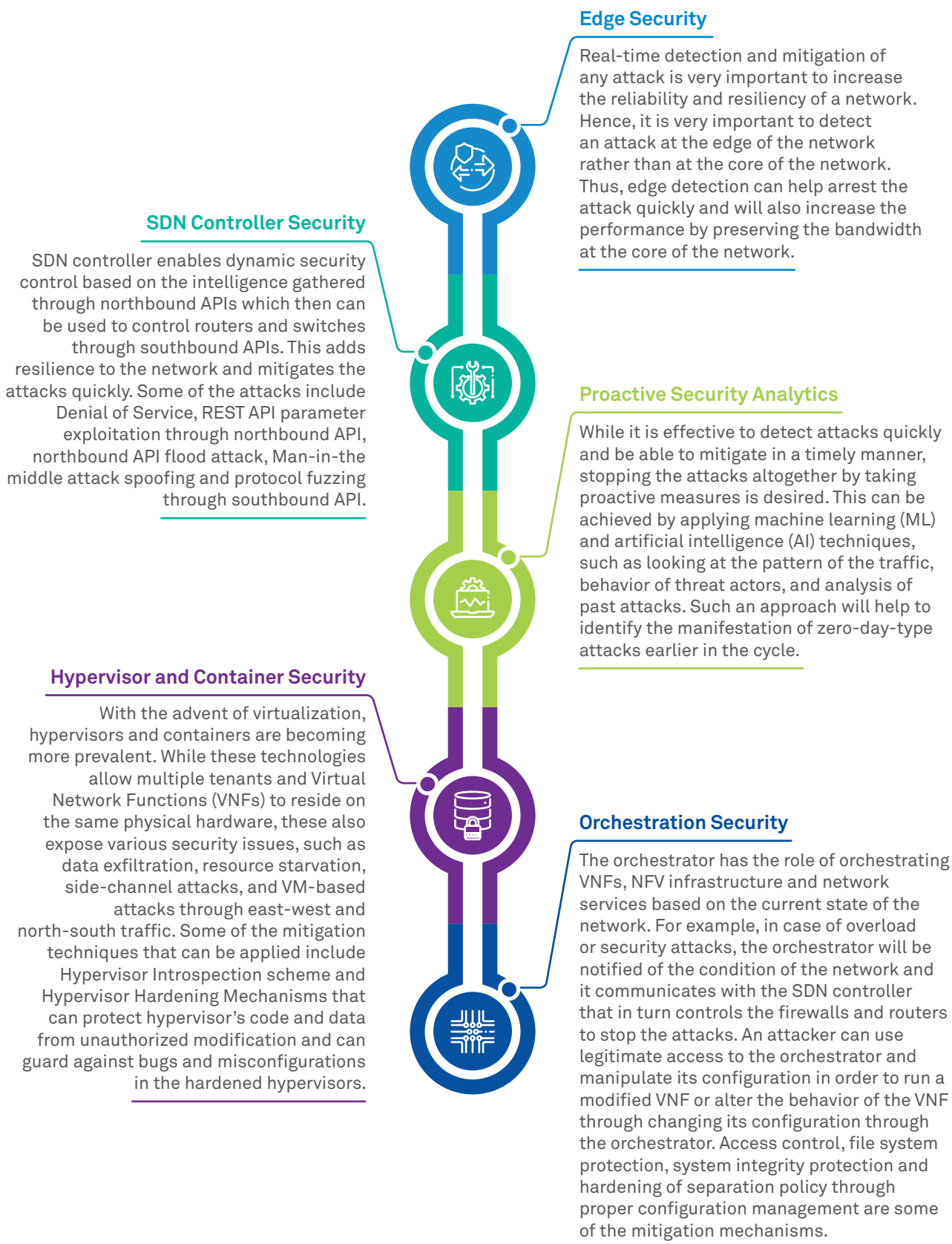
Public Private Partnership), 5GMF (5th Generation Mobile Communications Promotion Forum), 5GForum, and IEEE to name a few.

While the openness and new capabilities in 5G architecture bring new possibilities, they also open up a new threat landscape and the opportunities to deal with them differently.

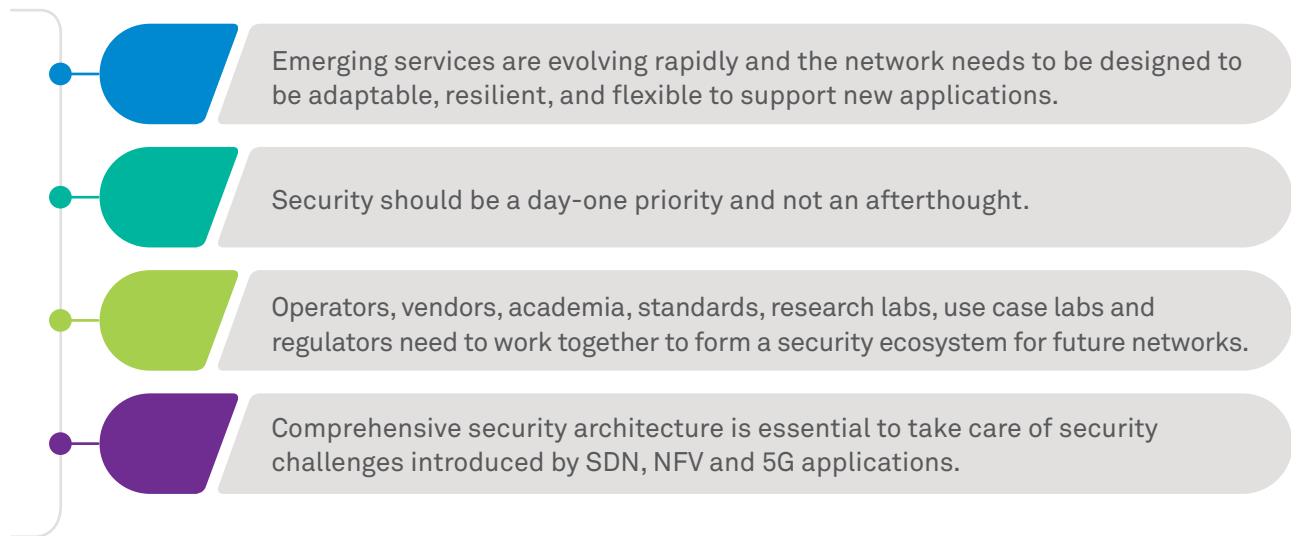
Security components of 5G

Following are the top five components of 5G architecture, from a security standpoint. There are many other aspects of security, such as open source security, network slice security and cloud RAN security that require critical scrutiny. There

is also a need to speed up security processing to support ultra-low latency use cases without compromising security. There is a tradeoff between speed of processing, associated cost and level of security assurance.



Key takeaways



This article has been contributed by [Dr. Ashutosh Dutta](#), Co-Chair IEEE Future Networks Initiative (www.futurenetworks.ieee.org). He is currently employed at Johns Hopkins University Applied Physics Lab. Email: ashutosh.dutta@ieee.org

Methodology & demographics



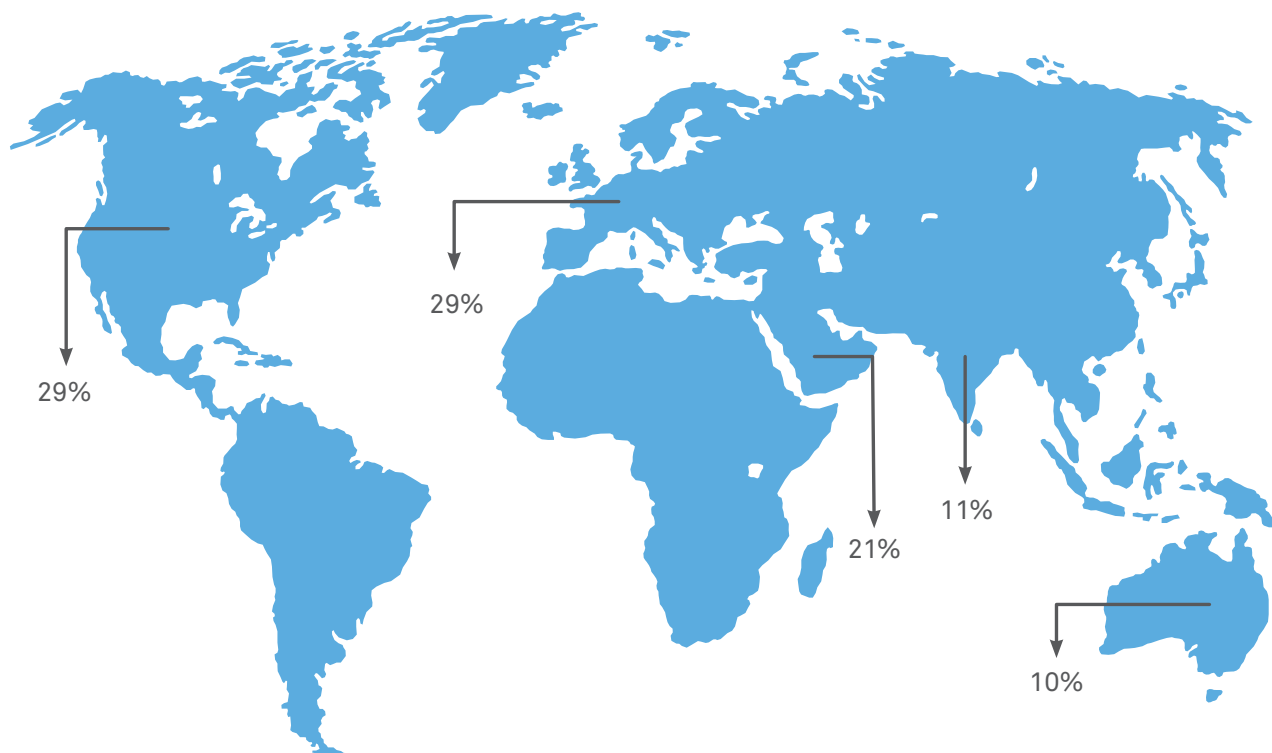
The “State of Cybersecurity Report 2019” from Wipro was developed over a period of three months. The methodology that was followed for developing the report was four-fold:

1. Primary research (external)
2. CDC research (primary research through our Cyber Defense Centers)
3. Secondary research
4. Wipro technology, academia and industry partners

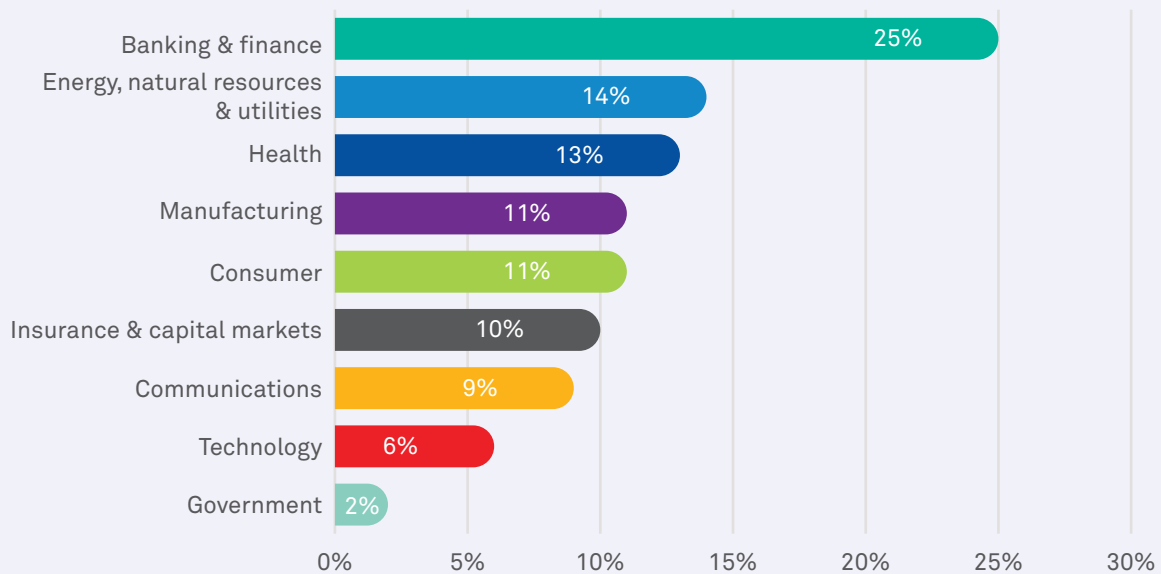
The primary research (external) was driven through surveys of security leadership,

operational analysts and architects in Wipro’s customer base. The research was conducted through direct interviews and Online surveys. The CDC research was conducted on aggregated data from Wipro’s CDCs across North America, Europe, India, Middle-East and the APAC region.

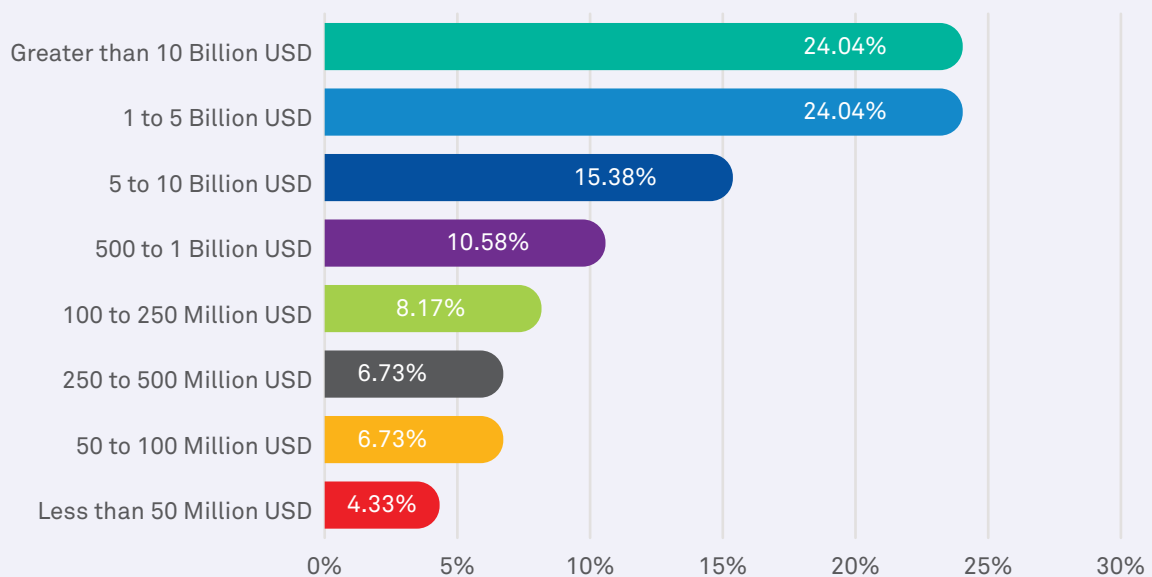
The secondary research was carried out by a core team of Cybersecurity & Risk Services (CRS) Center of Excellence (CoE) analysts who brought in various strategic perspectives from academic, institutional and industry research to supplement the primary and CDC research, and help connect trends in the cybersecurity domain.



Organizations surveyed by vertical



Organizations surveyed by revenue



Classification of industry verticals in the report

Banking, Financial Services & Insurance: Banking, insurance, capital markets & financial institutions

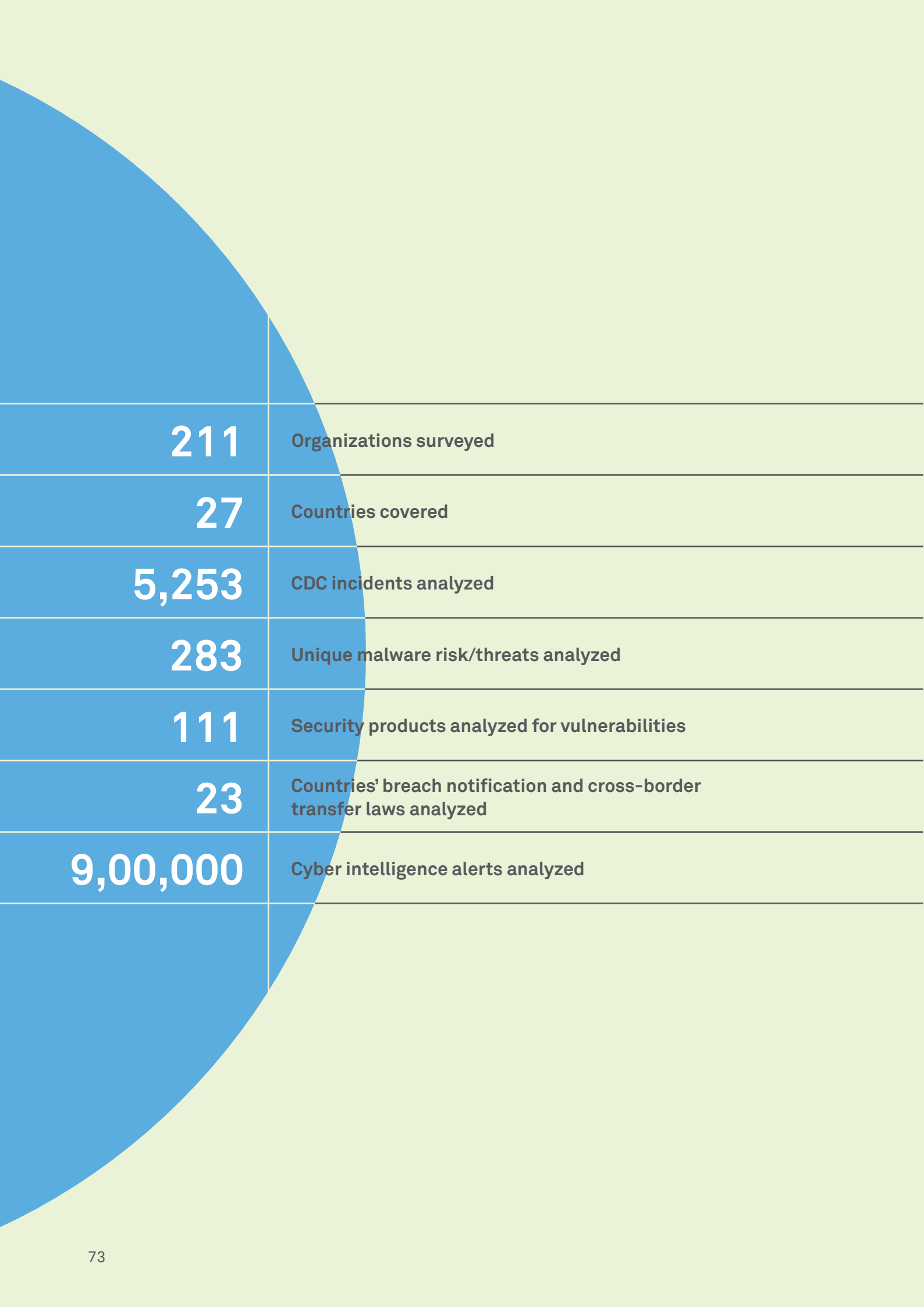
Consumer: Retail, consumer goods, travel & transportation, hospitality

Energy, Natural Resources & Utilities: Natural resources, oil & gas, utility

Manufacturing: Industrial & process manufacturing, engineering, automotive

Health: Healthcare, medical devices, pharmaceutical

Communications: Telecommunications, network equipment providers



211

Organizations surveyed

27

Countries covered

5,253

CDC incidents analyzed

283

Unique malware risk/threats analyzed

111

Security products analyzed for vulnerabilities

23

Countries' breach notification and cross-border transfer laws analyzed

9,00,000

Cyber intelligence alerts analyzed

Contributing partners



www.checkpoint.com



www.paloaltonetworks.com



www.dsci.in



www.futurenetworks.ieee.org



Indian Institute of Technology
Kharagpur

www.iitkgp.ac.in



www.deviceauthority.com



www.fortinet.com



www.denimgroup.com



www.intsights.com



www.cycognito.com



www.rapid7.com



www.tracxn.com

Credits & key contributors



The “State of Cybersecurity Report 2019” would not have been possible had it not been for 200+ of Wipro’s esteemed customers, who extended their support, time and shared practical insights.

Editorial team:

Josey V George

Editor & Distinguished Member of Technical Staff,
Wipro | 2016 Chevening Fellow for Cybersecurity

Kartik Upadhyay

Sub-editor & Security Consultant, CRS, Wipro

Jaiti Vijaywargi

Sub-editor & Security Consultant, CRS, Wipro

Mohona Mukhopadhyay

Security Consultant, CRS, Wipro

Content & research inputs:

Stephane Geyres

Consulting Partner, CRS, Wipro

Sudheesh Babu

General Manager, Head of Strategy and M&A, CRS,
Wipro

Sheetal Sharad Mehta

Senior Vice President, CRS, Wipro

Sridhar Govardhan

CISO, Wipro

Neeti Narang

Global Head, Marketing, CRS, Wipro

Industrial Engineering Services, Wipro

M.M. Prabhu, Debashis Mahata and Mitran Das

Binoy Wilson

Global Brand Lead, Wipro

Consulting Partners/Directors

Mark Brown, Steven Hurst, Graham Francis,
Luke Kennedy Smith, Sanjay Kapoor,
Dinesh Ramasvamy

Subhas Mondal

5G Champion & Distinguished Member of
Technical Staff, Wipro

CTO Office, Wipro

Sudipta Ghosh, Pratik Choudhury, and A. Raju

Deepak Kothari

Lead Architect, Cyber Defense Platform, CRS,
Wipro

Marketing & Content Team, Wipro

Smita Vasudevan and Ushnish Paul

CDC Team, CRS, Wipro

Dhanashekhar Devaraj and Cheshta Batra

Institutional contributors:

Dr. Ashutosh Dutta

Co-Chair IEEE Future Networks, currently
employed at Johns Hopkins University Applied
Physics Lab

Professor Debdeep Mukhopadhyay

Department of Computer Science and
Engineering, Indian Institute of Technology,
Kharagpur

Vinayak Godse

Vice President, Data Security Council of India

Wipro's Cybersecurity & Risk Services



Wipro's Cybersecurity & Risk Services (CRS) enables global enterprises to enhance their business resilience through an integrated risk management approach. Wipro enables customers to define their cybersecurity strategy, envisaging best-recommended practices across people, process and technology. Leveraging a large pool of experienced security professionals located across our global Cyber Defense Centers (CDC), we provide consulting & advisory, system integration and managed services to help customers transform their security posture. Wipro, through its venture arm (Wipro Ventures) has co-invested in multiple cybersecurity start-ups to complement our services with advanced research in emerging technologies. Our close interlock with security technology partners, regulatory bodies and premium academic institutions makes us a leading partner of choice for customers to manage their cyber risks.

Contact



CRS Marketing

crs.marketing1@wipro.com

Editions of State of Cybersecurity Report



<http://bit.ly/SOCR2019>
2019



<http://bit.ly/WiproSOCR2018>
2018



<http://bit.ly/WiproSOCR2017>
2017

Disclaimer:

This document is an informatory report on cybersecurity and cyber risk and should not be misconstrued as professional consultancy. No warranty or representation, expressed or implied, is made by Wipro on the content and information shared in this report. In no event shall Wipro or any of its employees, officers, directors, consultants or agents become liable to users of this report for the use of the data contained herein, or for any loss or damage, consequential or otherwise. Some of the content and data have been contributed by partner companies or collected from third party sources with professional care and diligence, and have been reported herein; nonetheless, Wipro doesn't warrant or represent the accuracy and fitness for purpose of the content and data.

References



- <https://www.forbes.com/sites/oracle/2019/01/17/chief-information-security-officer-priorities-for-2019/#5fa926046937>
- <https://www.securityroundtable.org/whats-the-best-reporting-structure-for-the-ciso/>
- <https://www.privacyrights.org/data-breaches>
- <https://www.breachlevelindex.com/>
- <http://cve.mitre.org>
- <http://www.cvedetails.com>
- <https://www.cvedetails.com/index.php>
- <https://www.us-cert.gov/ncas/alerts/TA18-074A>
- <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>
- [http://www.alrc.gov.au/publications/For%20Your%20Information%3A%20Australian%20Privacy%20Law%20and%20Practice%20\(ALRC%20Report%20108\)%20/51-data-br](http://www.alrc.gov.au/publications/For%20Your%20Information%3A%20Australian%20Privacy%20Law%20and%20Practice%20(ALRC%20Report%20108)%20/51-data-br)
- <https://ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/security-breaches/>
- <https://www.cnil.fr/en/home>
- <https://www.cnil.fr/en/rights-and-obligations>
- <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/>
- <http://www.cert-in.org.in/>
- <https://economictimes.indiatimes.com/wealth/insure/what-to-consider-while-buying-cyber-insurance-plans/articleshow/66445845.cms>
- <https://www.pandasecurity.com/mediacenter/security/memcached-ddos-attack/>
- <https://home.kpmg/xx/en/home/insights/2018/05/global-perspectives-on-cyber-security-in-banking-fs.html>
- <https://www.dlapiperdataprotection.com/>
- www.ngmn.org
- www.futurenetworks.ieee.org
- www.3gpp.org



Wipro Limited

Doddakannelli, Sarjapur Road,
Bangalore-560 035,
India

Tel: +91 (80) 2844 0011

Fax: +91 (80) 2844 0256

wipro.com

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading global information technology, consulting and business process services company. We harness the power of cognitive computing, hyper-automation, robotics, cloud, analytics and emerging technologies to help our clients adapt to the digital world and make them successful.

A company recognized globally for its comprehensive portfolio of services, strong commitment to sustainability and good corporate citizenship, we have over 175,000 dedicated employees serving clients across six continents. Together, we discover ideas and connect the dots to build a better and a bold new future.

For more information,
please write to us at
info@wipro.com