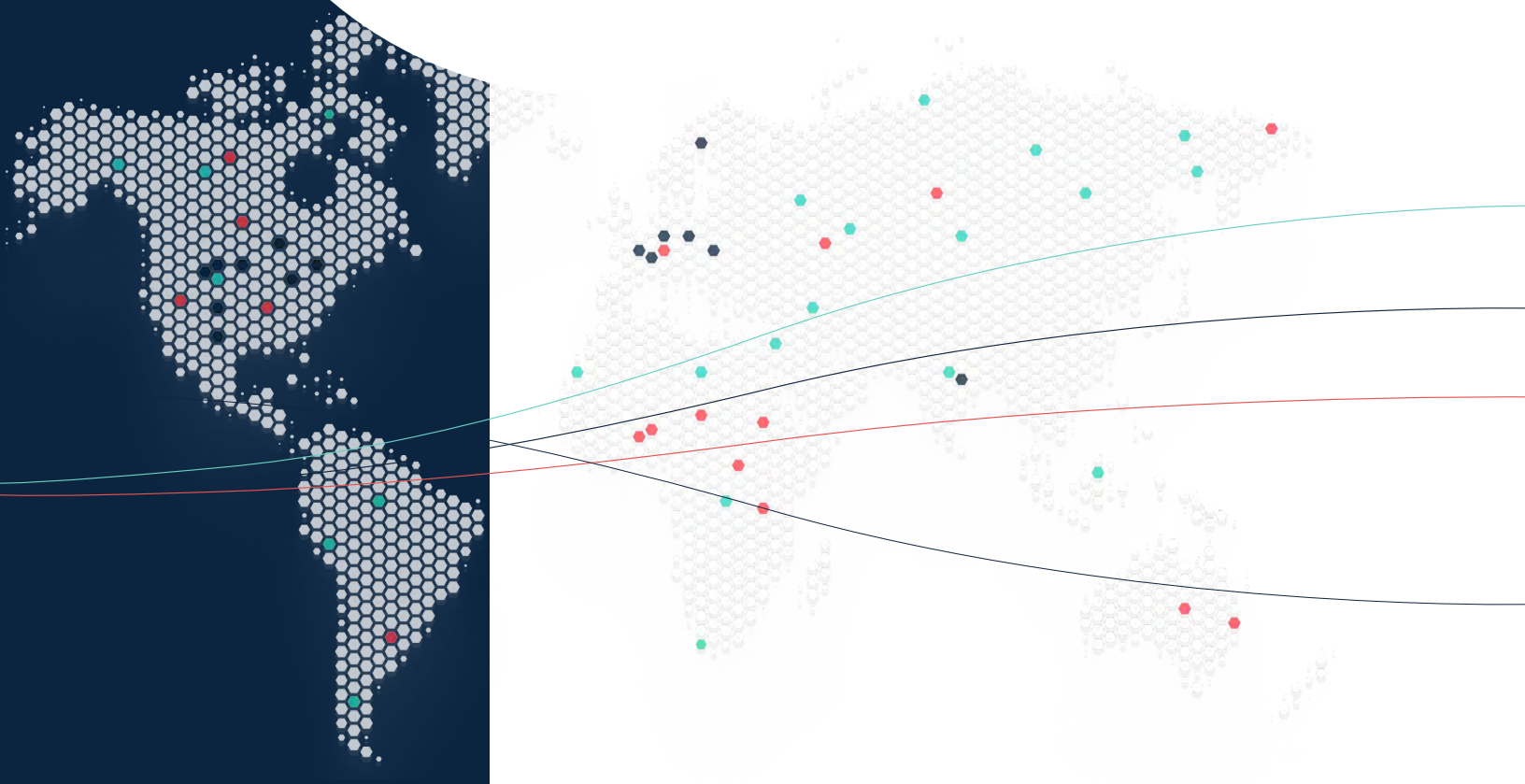
CYE

CYBERSECURITY MATURITY REPORT 2023



Cybersecurity data compiled from hundreds of client assessments across

7	15	11
Cybersecurity Domains	Countries	Industries

Table of contents

INTRODUCTION

Over the last several years, there has been a noticeable increase in corporate security budgets as a result of the sophistication of attacks and the number of cybersecurity solutions introduced into the market. However, vulnerabilities have also proliferated dramatically during the same period. The resulting surge in security breaches has led to substantial business losses including unprecedented financial and reputational damages, highlighting the need for organizations to shift their approach to cybersecurity.

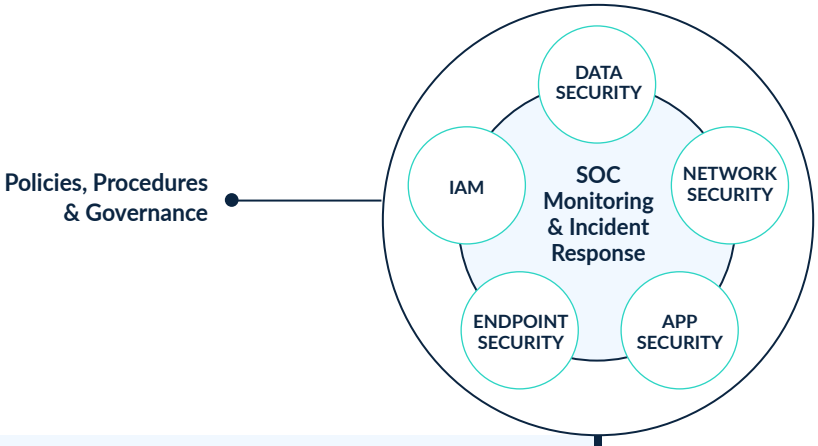
In this report, we highlight which industries and countries have the most robust cyber postures and which are lagging, as well as the most prevalent vulnerabilities. We also examine the scores across different industries, countries, and company sizes and provide recommendations and best practices on how to achieve a better cyber posture.

This report is based on data gathered over two years of cyber assessments, spanning **15 countries** and nearly a **dozen industries**. Each assessment includes an evaluation of the organization across seven different security domains, with a total of 312 data points.

15	11	312
Countries	Industries	Data Points

7 CYBERSECURITY DOMAINS

In this report, each category has been measured for its maturity across seven distinct security domains that make up a holistic cybersecurity strategy. Each domain plays a different role in the protection of critical assets inside of an organization. Here are CYE's definitions.



1

Application Level Security

Security measures at the application level that aim to prevent data or code within the app from being stolen or hijacked.

2

Cross Organization Policies, Procedures, & Governance

IT security governance determines who is authorized to make decisions and ensures that security strategies are aligned with business objectives and regulations.

3

Identity Management & Remote Access

Identity Access Management (IAM) refers to the IT security discipline, framework, and solutions for managing digital identities. The goal of IAM is to make sure that any given identity has access to the right resources (applications, databases, networks, etc.) within the correct context.

4

Network Level Security

Protecting the network from breaches, intrusions, and other threats through the use of access control, virus and antivirus software, network analytics, firewalls, VPN encryption, and more.

5

Security Operations Monitoring & Incident Response

Responsible for ensuring that potential security incidents are correctly identified, analyzed, defended, investigated, and reported.

6

Sensitive Data & Information Management

The classification, encryption, and protection of sensitive information that a person or organization wants to keep from being publicly available.

7

Servers, Network Equipment & Endpoint Security

Security measures taken to address threats faced by network endpoints such as servers, workstations, laptops, and mobile devices.

RESEARCH METHODOLOGY

This report is based on the results of cybersecurity assessments performed by CYE over the course of two years. Each assessment result contained detailed information regarding the overall security status of the organization in seven different security domains. The evaluation included an overall security score, a list of vulnerabilities identified for each of the security domains along with their severity level, detailed descriptions of how each vulnerability was identified and exploited, compromised assets for each vulnerability, and proposed solutions for mitigating the finding.

For the creation of this report, the results of all assessments were automatically parsed, and information regarding the security scores and top findings were extracted. The industry, size, and location of the clients in each assessment were collected as well while maintaining client confidentiality and anonymity. Finally, the data was aggregated according to the collected client characteristics and further processed to identify statistically significant trends and observations. The results were then carefully studied by data scientists and security researchers at CYE to identify and validate the various insights reported.

SCORING SYSTEM

Our scoring system is based on the Capability Maturity Model Integration (CMMI), an improvement model that provides organizations with guidelines for improving their processes and practices. The CMMI framework includes a comprehensive and scalable method for evaluating the implementation of processes and practices associated with the achievement of a cybersecurity maturity level.

The scoring is based on a scale of 1–5, with 1 being the lowest or most vulnerable, and 5 being the highest, most mature level of cybersecurity.

Characteristics of the five levels of the Capability Maturity Model Index (CMMI)

INDUSTRY DEFINITIONS

Communications
Newspapers, book publishers, public relations, and advertising agencies

Consumer
Manufacturers and distributors of consumer products

Energy
Oil and gas companies, utilities, alternative energy producers and suppliers

Financial
Banking, insurance, and investment companies

Healthcare
Hospitals and clinics

Industrial
Chemical process, engineering, and manufacturing companies

Public
Federal, state, and local government agencies and NGOs

Retail
Brick and mortar and eCommerce

Services
Professional services such as legal, accounting, and consulting firms

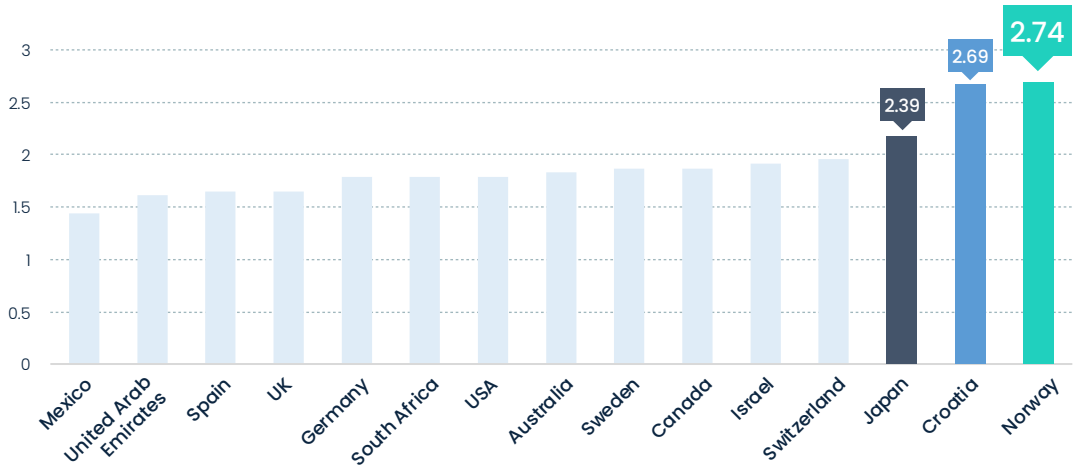
Technology
Software and hardware companies

Transportation
Airlines, railroad, trucking, and delivery companies

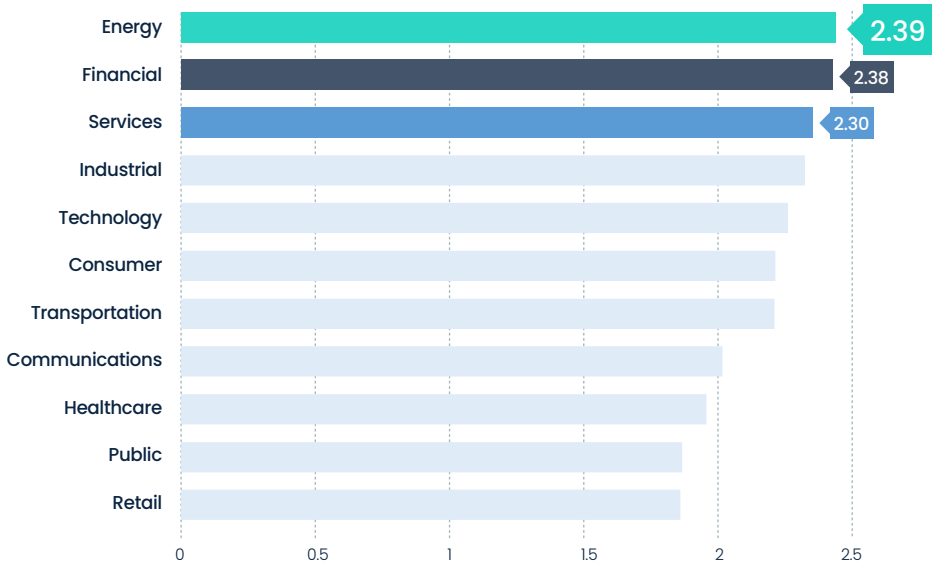
OVERALL RESULTS

The following results represent the average scoring for all organizations across all seven security domains.

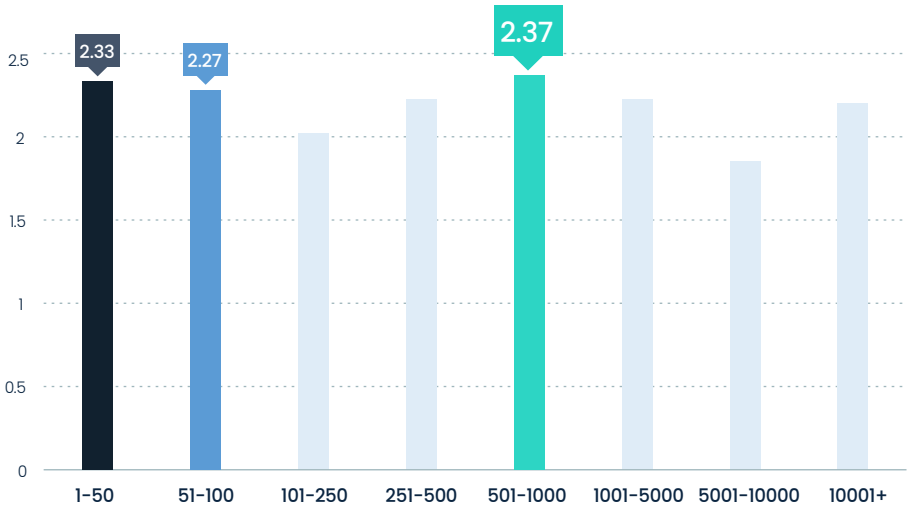
By Country



By Industry



By Size



OVERALL RESULTS

KEY FINDINGS

- The rising number of cyberattacks in the financial sector poses a threat to financial stability and makes cyber risk a key concern for policymakers. Besides that, regulations and concerns of financial loss spur many companies to implement cybersecurity measures. These are the reasons that the financial sector, including banks and fintech, scored well.

- Retail and public industries, on the other hand, scored low on average. This is likely because retailers that have a physical store as well as an online presence may not consider cybersecurity to be a priority in brick-and-mortar stores. Also, many businesses in retail prioritize speed of service over security. The public sector, which relies on its clients, has no other options and thus does not prioritize security. Also, they may have trouble attracting qualified security professionals.

- Both very small and medium organizations achieved the highest cybersecurity maturity scores. Medium organizations know that they have no choice but to make cybersecurity a priority and have the resources to invest in cybersecurity solutions. Small organizations, however, have a small attack surface that can be managed successfully by a small security team. The reason that very large organizations have low maturity is due to the challenges of defending with such a large attack surface.

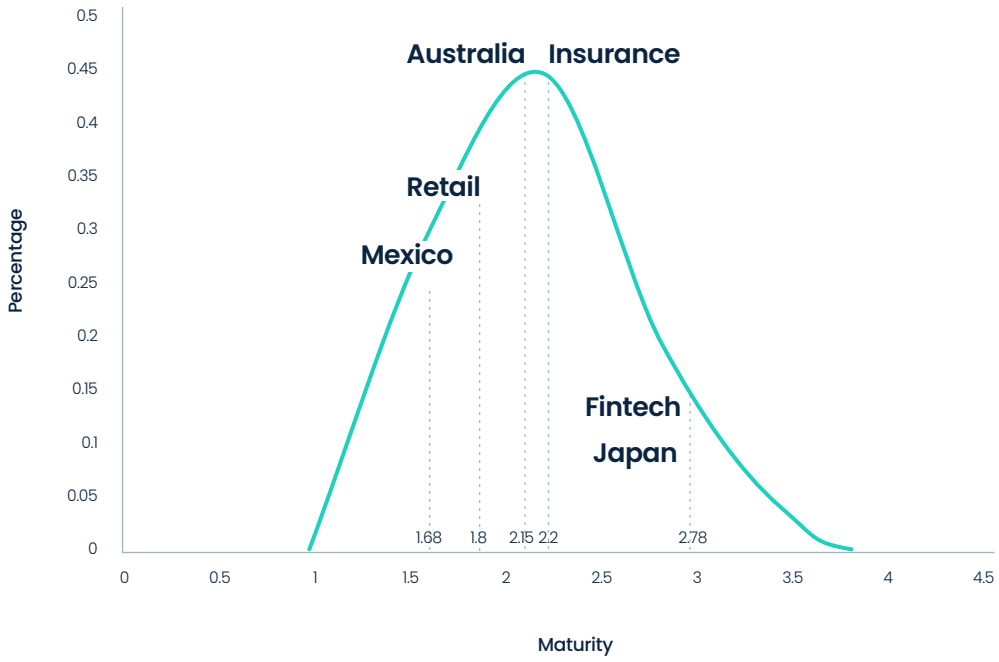
- Although they have generous budgets for cybersecurity spending, the United States, UK, and Germany are not at the top of the rankings, illustrating that a large financial investment does not always translate to a high maturity level. Specific reasons for lower maturity may be a lack of proper cybersecurity risk quantification and strategic planning for maturity. Bottom line: organizations can achieve a superior maturity posture even without a large cybersecurity budget, if they plan and spend it right.

- Norway had the highest scores across most of the domains. The first national Norwegian cybersecurity strategy was introduced in 2003, making Norway one of the first countries in the world to have a national strategy in this particular area. In step with developments in the threat landscape, the national strategy was revised in 2007 and 2012. These scores undoubtedly reflect that.

- Mexican companies scored the most poorly, across half of the domains. Mexico, with no national cybersecurity plan, has encouraged the private sector to independently introduce self-regulatory schemes to try and protect against cyberattacks. Furthermore, according to some studies, Mexico ranks as the Latin American country most targeted by cyberattacks in public and private sectors combined.

OVERALL RESULTS

Maturity Level Distribution over Industries & Countries



The above graph shows the distribution of all maturity scores. The X axis represents the maturity score, and the Y axis represents the distribution of scores in percentages. Maturity scores are distributed as a bell curve, averaging around maturity of 2.2.

We specify some segments of interest on the curve itself. Specifically, we can see that the fintech sub-industry and Japan have the highest maturity score (2.78; only 4% of the research participants have a similar). Insurance and Australia have the mid score (around 2.2; above approximately 50% of the research participants), and Mexico and the retail industry have the lowest score (around 1.7, with around 30% of the research participants).

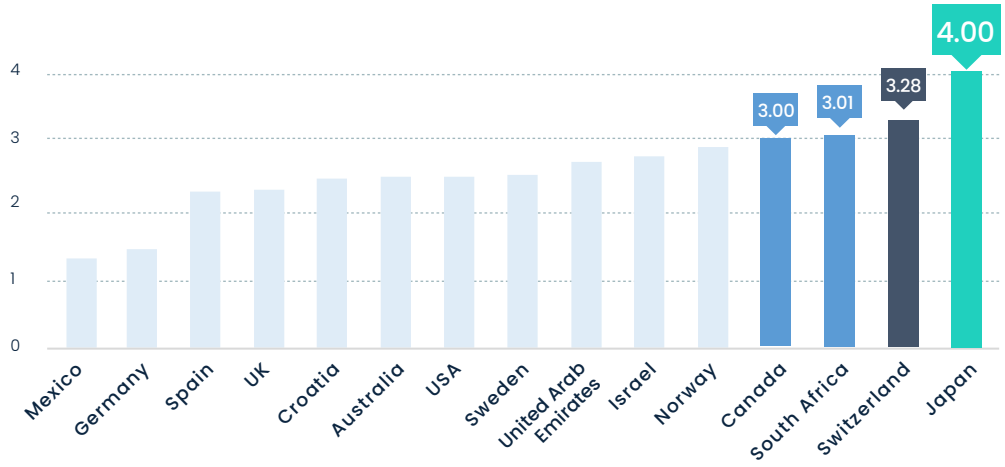
Security Domain:

APPLICATION LEVEL SECURITY

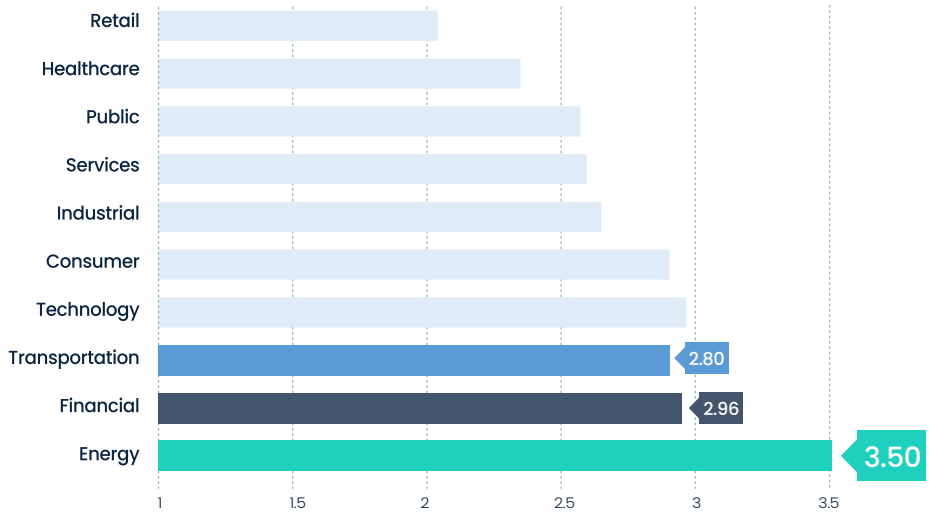
DEFINITION

Application level security describes security measures at the application level that aim to prevent data or code within an app from being stolen or hijacked. This includes security considerations during application development and design, as well as systems and approaches to protect apps after they are deployed. Application level security is the process of developing, adding, and testing security features within applications to prevent security vulnerabilities against threats, such as unauthorized access and modification.

By Country



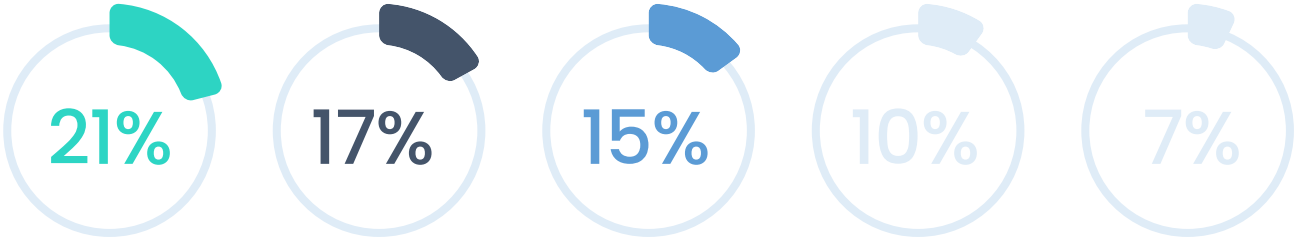
By Industry



Security Domain:

APPLICATION LEVEL SECURITY

Top 5 Frequent Findings by Percentage



Technical information disclosure

No HTTP strict transport security

Missing HTTP security headers

Frameable web content is vulnerable to clickjacking

Data exposure in Robots.txt file

KEY FINDINGS

- It is no surprise that financial companies, in the trading applications they offer to their customers, must maintain the highest level of protection against hacking and theft. Modern financial companies often make use of users' sensitive data and link with users' bank accounts for efficient online transactions. In case of a cyberattack or a security breach, all this sensitive information is at risk.
- Retail companies scored fairly low at 1.45, as they recently received a significant boost, especially in light of COVID-19, and are scrambling to accommodate rapid growth (especially e-commerce). As a result, they have not invested enough time, effort, or resources in the overall security status of their companies or in application level security. Furthermore, to remain competitive, retailers are adopting new payment and digital technologies, exposing them as prime targets for cybercriminals.
- Not surprisingly, technical information disclosure and detailed error messages are prevalent vulnerabilities in this domain. SQL, which used to be a top finding, now ranks lowest, and indeed, hackers have moved on from attempting to exploit this finding. Similarly, while XSS does not rank at the bottom, it is not in the top five, and will likely follow the SQL injection path.
- In terms of geographies, it is interesting to see that many European countries are still scoring relatively low. This is surprising, considering that GDPR compliance is here to stay.

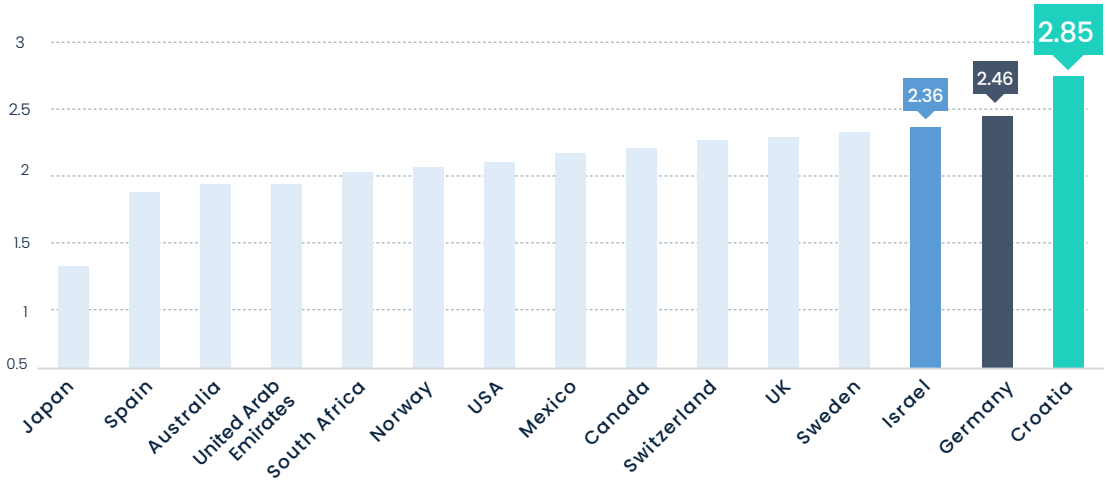
Security Domain:

CROSS ORGANIZATION POLICIES, PROCEDURES, AND GOVERNANCE

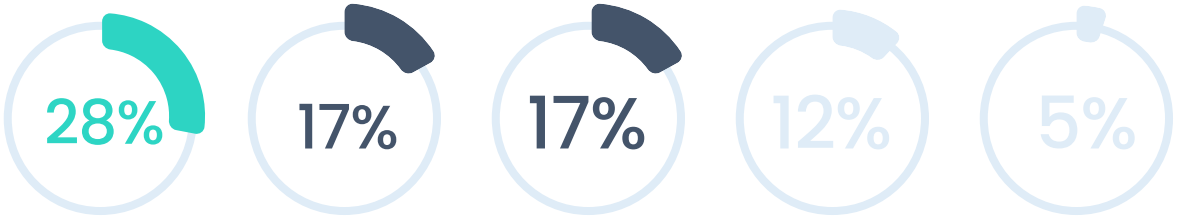
DEFINITION

IT security governance is the system by which an organization directs and controls IT security. It determines who is authorized to make decisions. It provides oversight to ensure that risks are adequately mitigated and that security strategies are aligned with business objectives and consistent with regulations.

By Country



Top 5 Frequent Findings by Percentage



Insufficient global security update policy or mechanism

High risk mainte-nance procedures

Insufficient network segmentation in the corporate network

Ineffective asset management

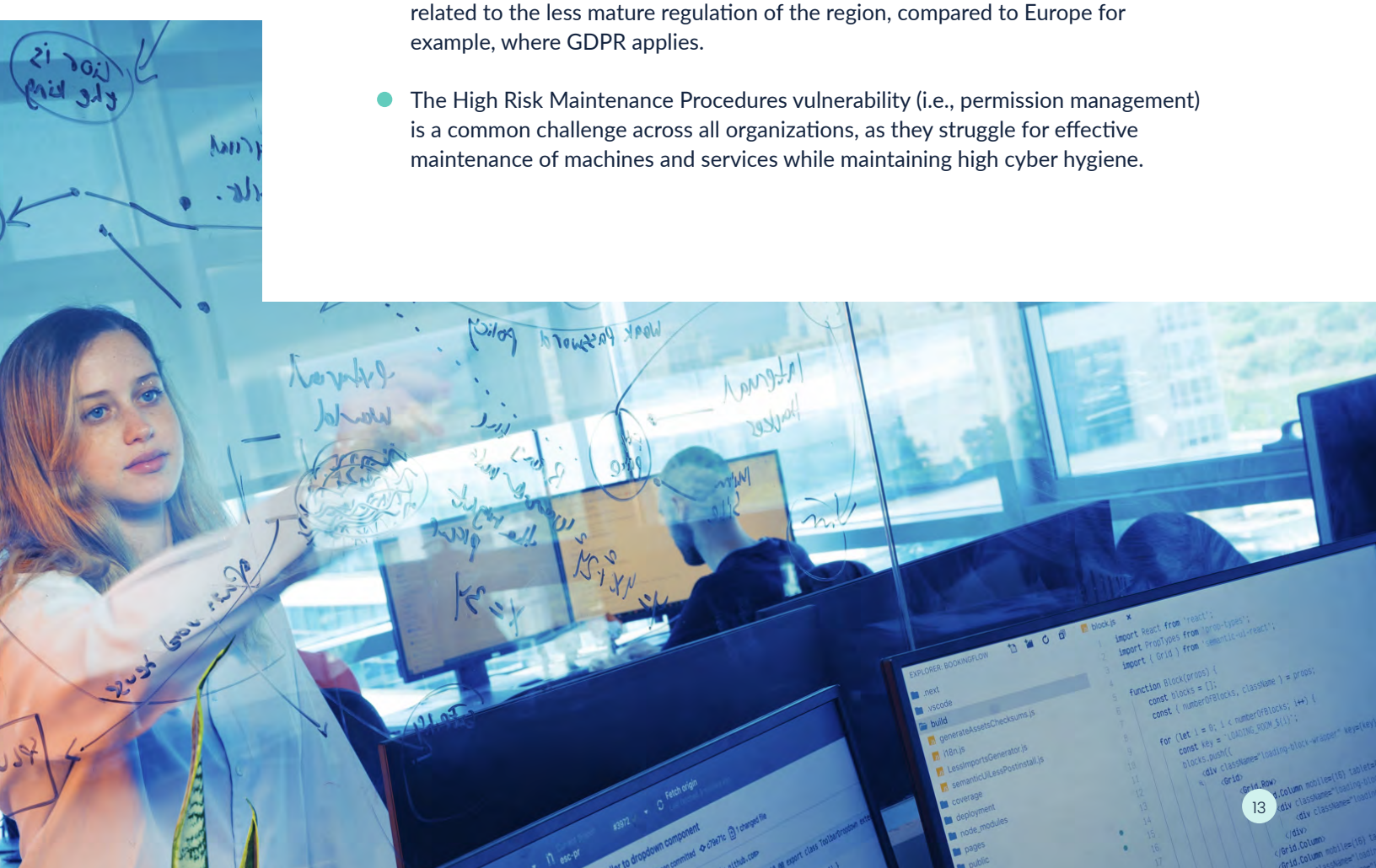
Insufficient security awareness and reporting procedures

Security Domain:

CROSS ORGANIZATION POLICIES, PROCEDURES, AND GOVERNANCE

KEY FINDINGS

- There is a vast correlation between risk and maturity. When an organization has a high level of maturity in its cybersecurity practices, it is better equipped to identify and mitigate potential risks. This translates to a generally low level of risk over time.
- The five top findings are very basic and still relevant, despite some being known as major issues for more than two decades. For example, the “insufficient global security update policy” issue results in reoccurring vulnerabilities and offers a low-hanging fruit for attackers, but organizations often overlook creating and implementing an update policy. By investing in mitigating these top five findings, organizations can increase maturity dramatically.has context menu
- Germany, which usually scores high, received the second highest score in cross organization policies, procedures, and governance, reflecting a top-down approach towards cybersecurity.
- Southeast Asia organizations scored fairly low (1–1.5) in the domain. This is perhaps related to the less mature regulation of the region, compared to Europe for example, where GDPR applies.
- The High Risk Maintenance Procedures vulnerability (i.e., permission management) is a common challenge across all organizations, as they struggle for effective maintenance of machines and services while maintaining high cyber hygiene.



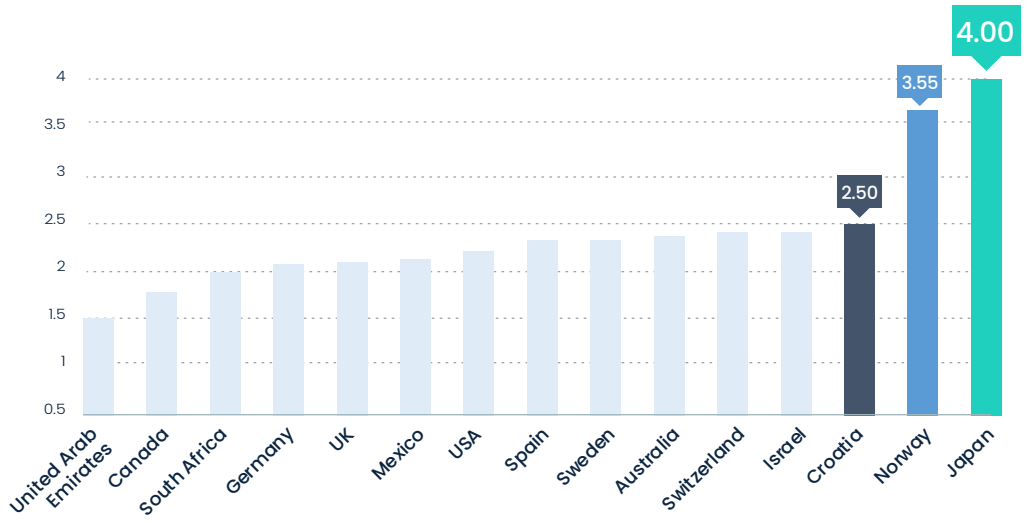
Security Domain:

IDENTITY MANAGEMENT AND REMOTE ACCESS

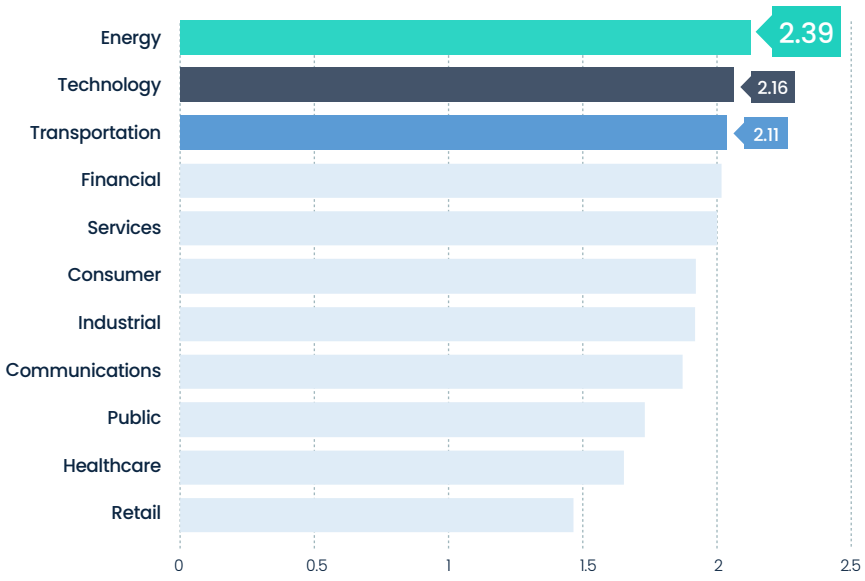
DEFINITION

Identity and Access Management (IAM), also called identity management, refers to the IT security discipline, framework, and solutions for managing digital identities. Identity management encompasses the provisioning and de-provisioning of identities, securing and authentication of identities, and the authorization to access resources and/or perform certain actions. While an individual only has one digital identity, they may have many different accounts. Each account can have different access controls, both per resource and per context. The overarching goal of IAM is to ensure that any given identity has access to the right resources (applications, databases, networks, etc.) and within the correct context.

By Country



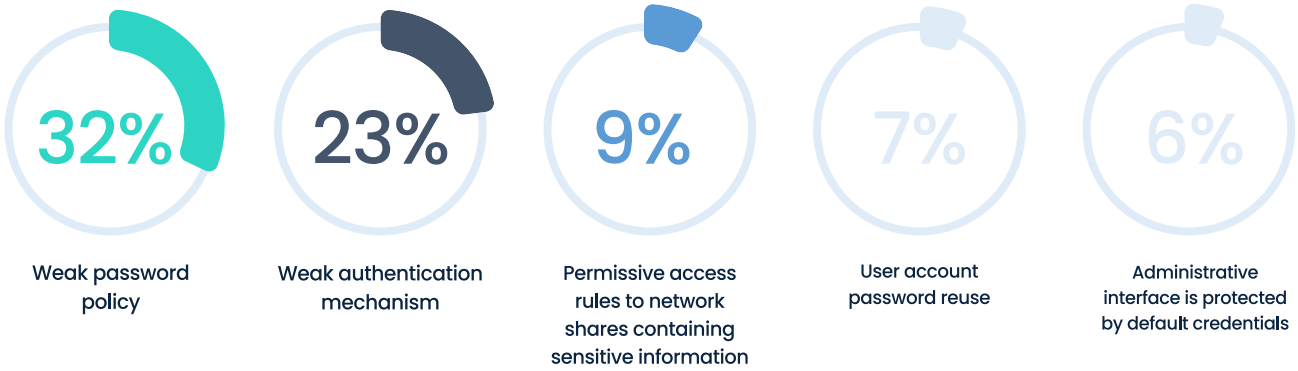
By Industry



Security Domain:

IDENTITY MANAGEMENT AND REMOTE ACCESS

Top 5 Frequent Findings by Percentage



KEY FINDINGS

- The Identity Management and Remote Access security domain addresses the most popular and exploited findings by attackers. Yet it also offers an opportunity to organizations, as it allows for very rapid improvement. In fact, energy and technology are relatively new industries to be leaders here, because they managed to quickly improve maturity in a very significant way.
- The top 5 findings are common and basic, with weak passwords leading the ranking at almost 32% of organizations. A combination of a weak password policy with weak authentication mechanisms empowers hackers, because there's no need to hack; they simply log in. When added to "permissive access rules to network shares containing sensitive information," hackers can access sensitive data with little to no effort.
- The energy sector leads the domain. Oil and gas companies, being a critical infrastructure and subsequently the number one target for cybercriminals sponsored by foreign nation-state powers, had no choice but to improve maturity.
- UAE received the lowest score of 1. The reason could be the lack of awareness of this issue. According to the University of Wollongong in Dubai, the US, UK, and Australia established laws and policies to counter identity theft early (1998) in contrast to the UAE, which only began to look into the issue a few years ago. It was only in 2012 that the Cyber Crime Law was developed in the UAE, which still does not specifically address identity theft and IAM issues.

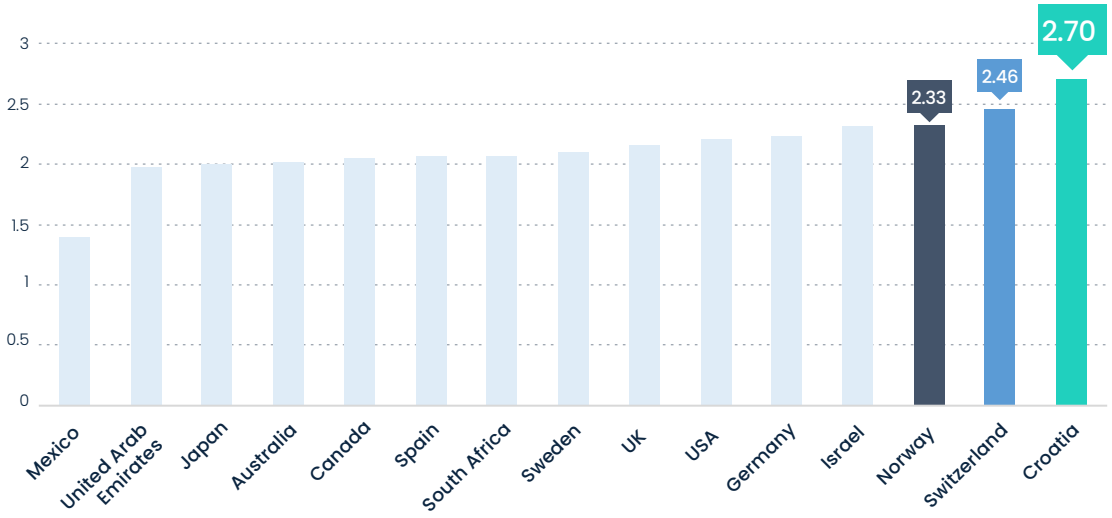
Security Domain:

NETWORK LEVEL SECURITY

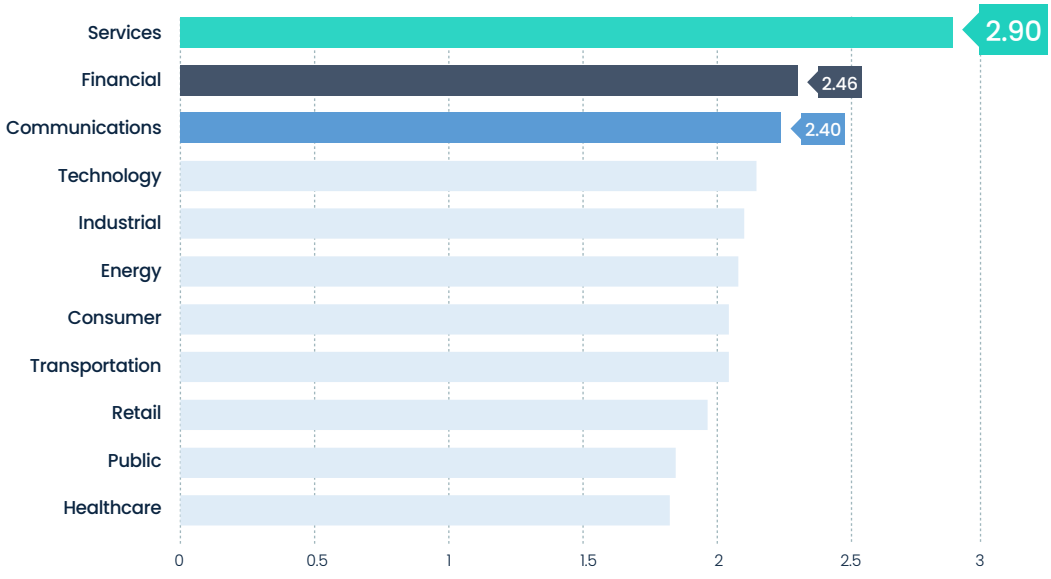
DEFINITION

Network security protects your network and data from breaches, intrusions, and other threats. This is a vast and overarching term that describes hardware and software solutions, as well as processes or rules and configurations relating to network use, accessibility, and overall threat protection. Network security involves access control, virus and antivirus software, application security, network analytics, types of network-related security (endpoint, web, wireless), firewalls, VPN encryption, and more.

By Country



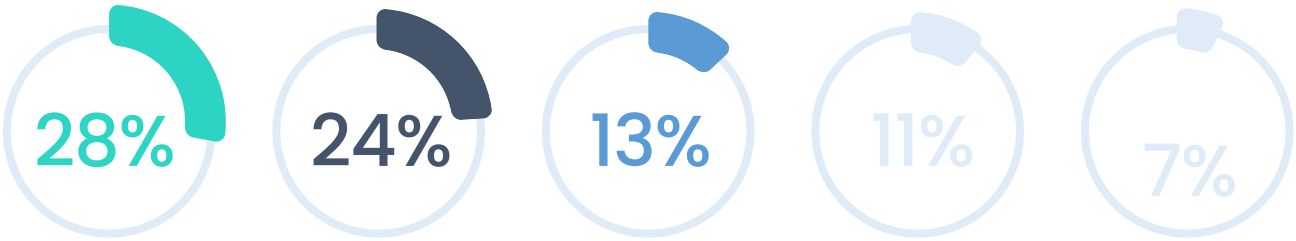
By Industry



Security Domain:

NETWORK LEVEL SECURITY

Top 5 Frequent Findings by Percentage



Administrative and sensitive interfaces are exposed to the Internet

Outdated firewall rule base

Exposed non-production environments

Insufficient network segregation in the corporate network

Administrative and sensitive interfaces are exposed in the corporate network

KEY FINDINGS

- Somewhat surprisingly, technology companies did not perform well in this domain. Although they employ tech-savvy personnel, these employees tend to shy away from handling and maintaining network level security, as it involves low-level, mundane configuration work. Also, they are much more oriented towards reaching development goals, leaving the overall status of network security lacking. The responsibility often falls upon less experienced personnel, resulting in sub-par scoring for the industry. Another factor is that this is a cross-organization, long-term effort. People tend to focus on their specific teams and sub-networks to get the job done quicker, and not through a cross-organization general effort that is required for best results.
- Mexican companies have the lowest score. According to “The State of Cybersecurity in the Mexican Financial System” report, which analyzed cybersecurity in the Mexican financial sector, only 33% of the companies use encryption controls and endpoint security tools and only 54% of the companies use network security tools (VPN, NAC, ISE, IDS/IPS, Web filtering, secure e-mail, etc).
- The services industry leads the ranking, although it is not an expected leader when it comes to cybersecurity. The main reason may be that customers are driving vendors to apply high level security measures as a prerequisite for doing business.
- The top findings in this domain underscore the impact of COVID-19. To allow remote work, COVID forced many environments to become internet-facing.

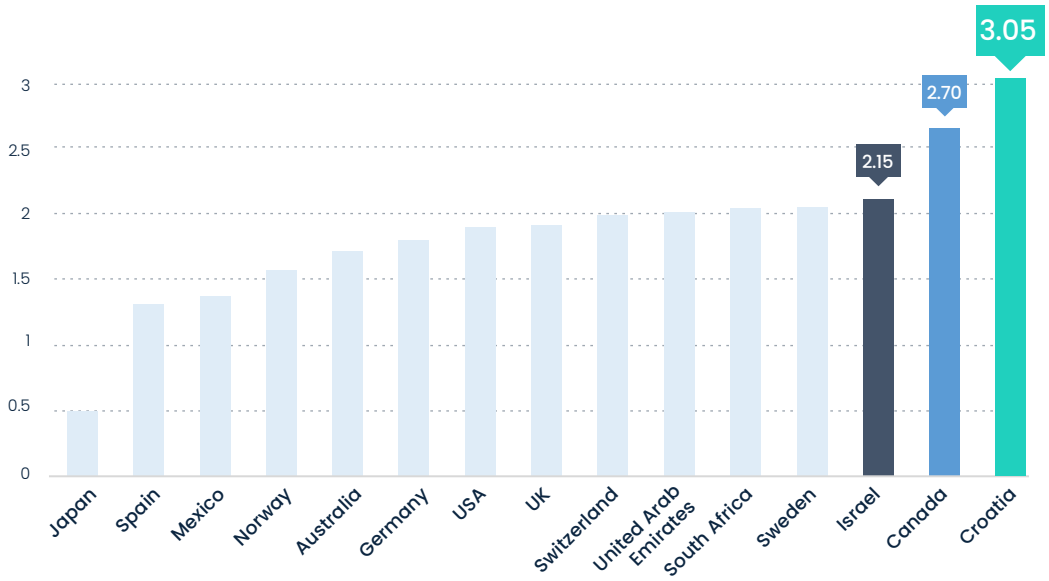
Security Domain:

SECURITY OPERATIONS MONITORING AND INCIDENT RESPONSE

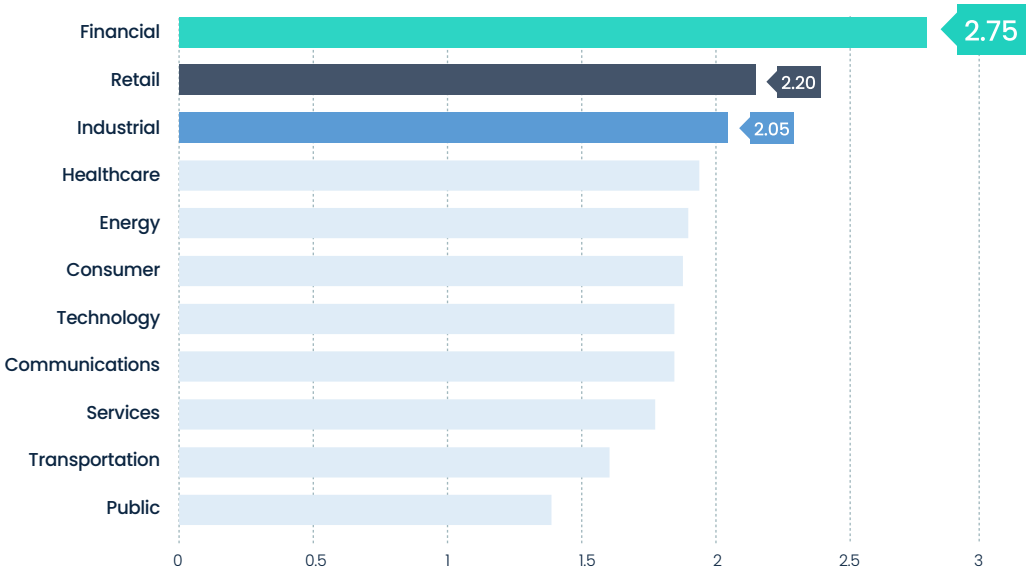
DEFINITION

A security operations center (SOC) is a facility that houses an information security team, which is responsible for monitoring and analyzing an organization's security posture on an ongoing basis. The SOC team's goal is to analyze, detect, and respond to cybersecurity incidents using a combination of technology solutions and a strong set of processes. Security operations centers are typically staffed with security analysts and engineers, as well as managers who oversee security operations. SOC staff work closely with organizational incident response teams to ensure security issues are addressed quickly upon discovery. Security operations centers monitor and analyze activity on networks, servers, endpoints, databases, applications, websites, and other systems, looking for anomalous activity that could be indicative of a security incident or compromise. The SOC is responsible for ensuring that potential security incidents are correctly identified, analyzed, defended, investigated, and reported.

By Country



By Industry



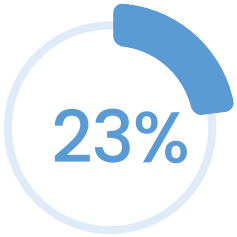
Security Domain:

SECURITY OPERATIONS MONITORING AND INCIDENT RESPONSE

Top 5 Frequent Findings by Percentage

Insufficient monitoring of authentication events

Insufficient monitoring of intrusive activities on endpoints



Insufficient security monitoring procedures

Insufficient monitoring of the corporate network

Insufficient monitoring and protection of assets and services in AWS

KEY FINDINGS

- The Security Operations Monitoring and Incident Response domain cannot be rapidly improved, as it requires a strategic investment over time. Improvement here must come from a combination of tech, personnel, and processes. The finance industry is a clear leader, as they historically invest in reducing response time and containing cyber events—which translate to immediate loss of funds—as soon as possible. As other industries make monitoring a priority, we predict this gap will close in a few years.
- Croatia, surprisingly, was first place in the ratings. In 2020, the U.S. established a new cybersecurity operations center in Zagreb and a mobile cyber incident response team. Furthermore, in 2022, for the first time in U.S. Cyber Command history, a team of elite defensive cyber operators deployed to Croatia to hunt for malicious cyber activity on partner networks. This effort came at a time when countries in Central and Eastern Europe were on high alert for cyberattacks linked to the war between Russia and Ukraine. Therefore, the high awareness, the learning, and the investment in this domain in Croatia in the last years could be the reason for the high score.
- Although monitoring is a second line of defense, organizations mistakenly perceive it as a first line of defense. An example for that is the retail industry, which ranked second here but was much lower in the general ranking. Organizations should be wary of a reactive approach and properly invest in protective policies and tech before they prioritize monitoring.

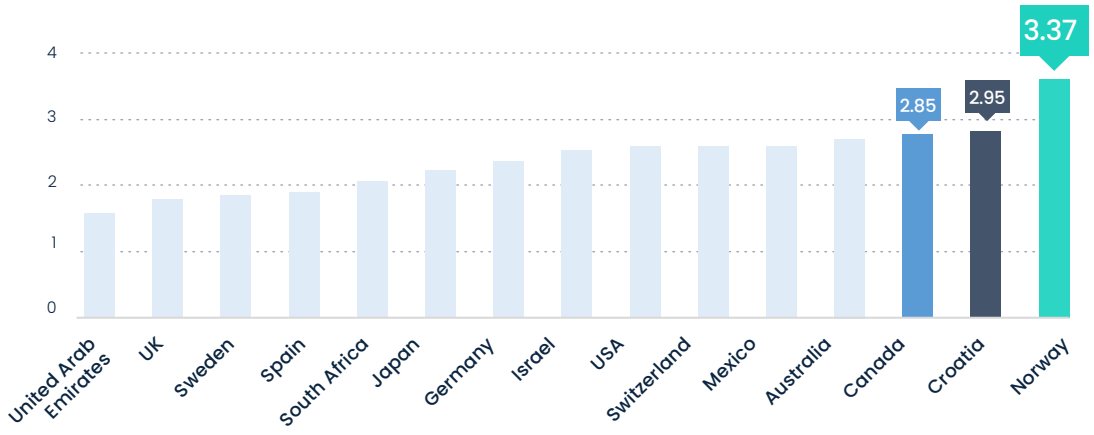
Security Domain:

SENSITIVE DATA AND INFORMATION MANAGEMENT

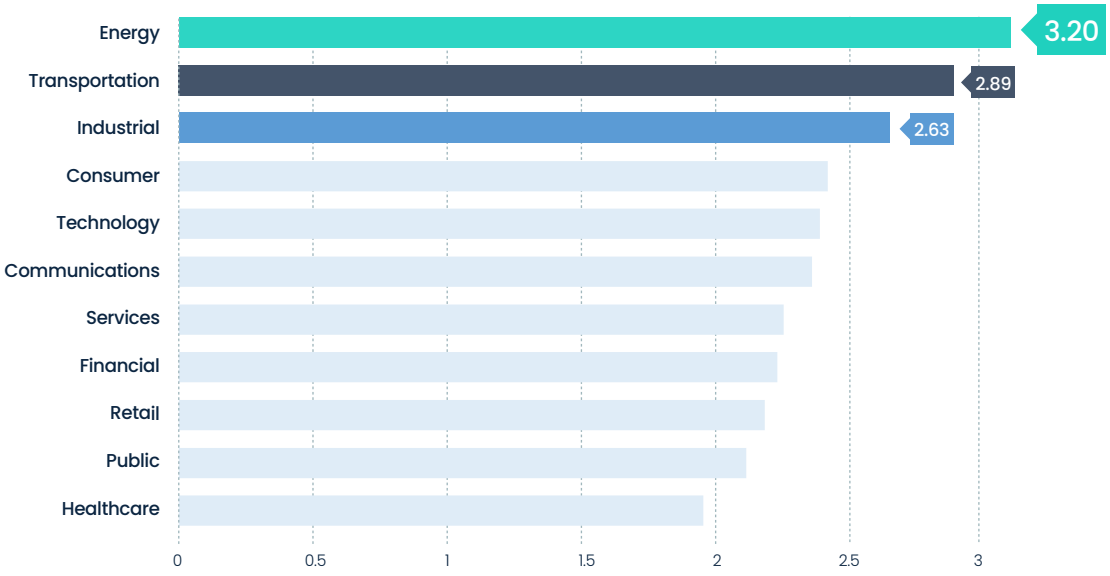
DEFINITION

Sensitive data is information that a person or organization wants to keep from being publicly available because the release of the information could lead to harm, such as identity theft or fraud. In some cases, sensitive data includes individuals' credit card information or medical records. In other cases, sensitive data can be proprietary corporate information. As organizations seek to protect sensitive information, they need continuous visibility into their complex IT ecosystems. This provides an outside-in view across risk factors so that organizations can continuously monitor, remediate, and document their data protection activities. As cybersecurity and privacy become even more important with accelerated digital transformation strategies, gaining real-time visibility into new risks to rapidly mitigate threats and protect sensitive data will become even more critical to businesses.

By Country



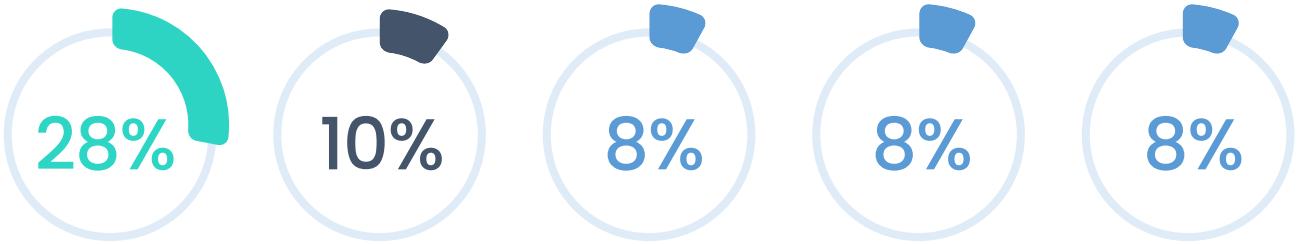
By Industry



Security Domain:

SENSITIVE DATA AND INFORMATION MANAGEMENT

Top 5 Frequent Findings by Percentage



No process for sensitive data removal from file shares

Sensitive technical data stored insecurely on corporate shares

Business-critical data stored insecurely on corporate shares

Insecure storage of credentials in configuration files

Production data in non-production environments

KEY FINDINGS

- It is surprising to see that healthcare—one of the industries most sensitive to personal information—is ranked the lowest. This indicates that awareness of the issue of personal information, even in organizations where we entrust the most sensitive information, is seriously deficient. The fact that "no process for sensitive data removal from file shares" was among the most frequent vulnerabilities indicates that file shares are weak spots across the entire domain.
- With regard to geography, it is surprising that many European countries, which must comply with GDPR, are still not as cyber secure as they should be.
- We note that the maturity scores in the domain are relatively high compared to others. This comes mostly from regulations (GDPR, CISA, etc.), which treats data security as the foundation for all cybersecurity requirements.

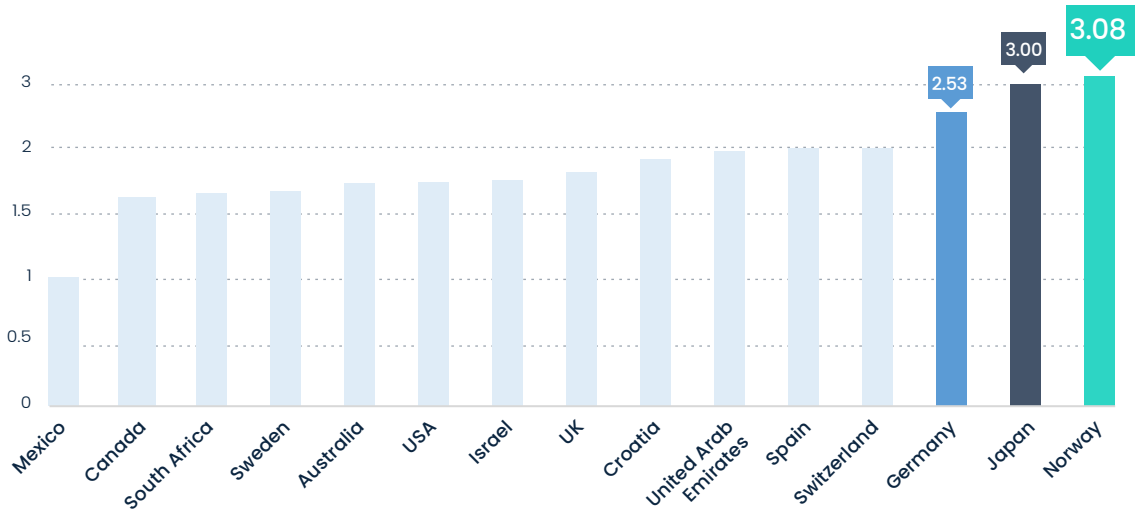
Security Domain:

SERVERS, NETWORK EQUIPMENT, AND ENDPOINT SECURITY

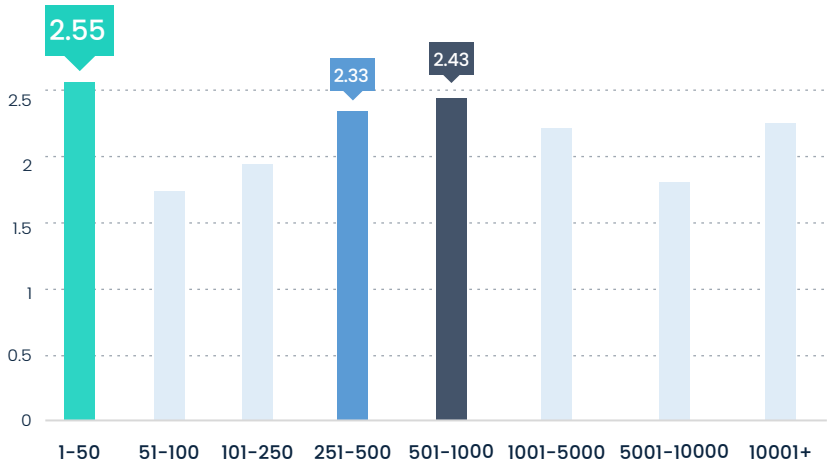
DEFINITION

Endpoint protection, also known as endpoint security, refers to the security measures taken to address threats faced by network endpoints, which are devices such as servers, workstations, laptops, and mobile devices.

By Country



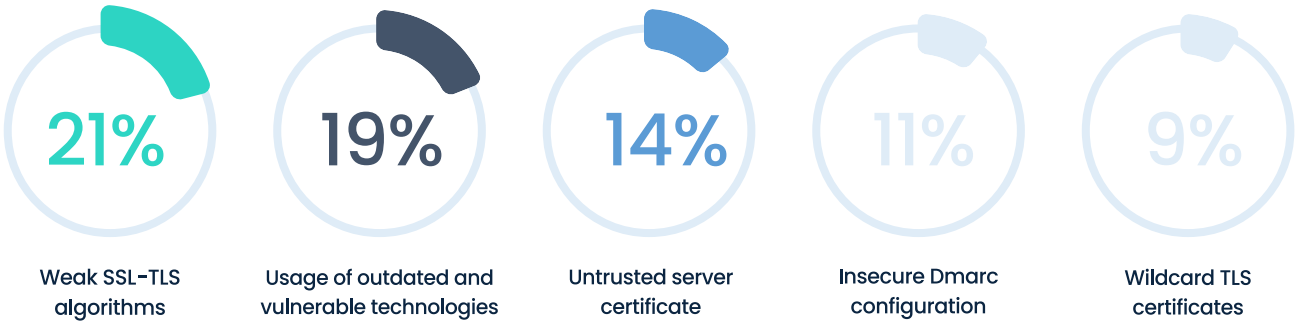
By Size



Security Domain:

SERVERS, NETWORK EQUIPMENT, AND ENDPOINT SECURITY

Top 5 Frequent Findings by Percentage



KEY FINDINGS

- Outdated technology is a major challenge that affects the entire security domain.
- We can see that the small organizations received the highest score (2.55). This is because in endpoint security, it's much easier to apply strict rules and enforce them easily in small businesses.
- Norway received the highest score because it has increased its digital defense spending to protect the country's critical IT infrastructure against a heightened risk of state-sponsored cyberattacks from Russia. The elevated threat level, which followed an uptick in cyberattacks and updated security situational assessments, is linked to Norway's military and trade support for Ukraine.

RECOMMENDATIONS

This report presents the results of our analysis of cybersecurity trends and best practices. Based on this review of the available data, here are recommendations for enhancing the security of systems and data within any organization.

Invest in capabilities and not tools. Build the basic foundations.

Organizations often invest in tools, which result in a larger attack surface, rather than more capabilities. Look for a provider that replaces tools with capabilities by combining technology, people, and processes to manage organizational risk and enable organizations to reclaim control of their cyber resilience.

Develop an integrated approach to cybersecurity with board-level accountability.

The board must be involved in decisions about the company's cyber policy. This is the only way that management will understand the risks and the level of financial investment required to protect the company.

Thoroughly assess your situation, quantify your risk, and prioritize mitigation based on data.

To properly prioritize mitigation and allocate resources, organizations need to understand the risk. Invest in cyber risk quantification by identifying all threats from all attack surfaces, assessing which vulnerabilities and findings are relevant to the organization and how these may compromise business-critical assets. Consider the financial context of critical assets and use statistical data to estimate the likelihood of breach to these assets. Plan mitigation around this data, while investing in comprehensive solutions that address root-cause issues.

ABOUT CYE

CYE's cybersecurity optimization platform, Hyver, enables businesses to assess, quantify, and mitigate cyber risk so they can make better security decisions and invest in effective remediation. CYE combines technology with red team activity to deliver the most comprehensive organizational security assessments and contextual risk analysis and insights. With headquarters in Israel and offices in New York and London, the company serves Fortune 500 and mid-market companies in multiple industries around the world. CYE is funded by EQT Private Equity and 83North. Visit us at cyesec.com.