CYE

CYBERSECURITY MATURITY REPORT 2025

17
COUNTRIES

15
INDUSTRIES

1500
DATA POINTS

Table of Contents

03 EXECUTIVE SUMMARY

04 KEY INSIGHTS

07 CYBERSECURITY FUNCTIONS

08 INDUSTRY DEFINITIONS

09 RESULTS BY FUNCTION:
- GOVERN 09
- IDENTIFY 12
- PROTECT 14
- DETECT 16
- RESPOND 18
- RECOVER 20

22 RECOMMENDATIONS

23 RESEARCH METHODOLOGY

SCORING SYSTEM

ABOUT CYE

EXECUTIVE SUMMARY

Understanding and improving cybersecurity maturity has never been more critical.

17
COUNTRIES

15
INDUSTRIES

1500
DATA POINTS

Understanding and improving cybersecurity maturity has never been more critical. In today's age, when it isn't a question of "if" but "when" there is a cyber incident, an organization's resilience and recovery depends on its cybersecurity maturity. An organization that is more mature will likely bounce back quicker with less damage than an organization that is less mature.

Cybersecurity maturity is not the goal. It is a means to measure and evaluate the organization's resilience, both in terms of IT systems and the broader business impact of cyber incidents. The maturity score serves as a foundation to build trust in an environment where digital risk is constant. Organizations leverage maturity assessments to inform and prioritize investments in cybersecurity programs, reduce risk and the potential cost of data breaches, and adapt proactively to change.

This year's report offers an updated global view of cybersecurity maturity, building on our previous findings. It identifies where progress has been made, where gaps remain, and how different sectors, geographies, and organizational sizes are evolving. We also examine the technologies and leadership trends driving change and offer actionable recommendations based on the latest maturity data.

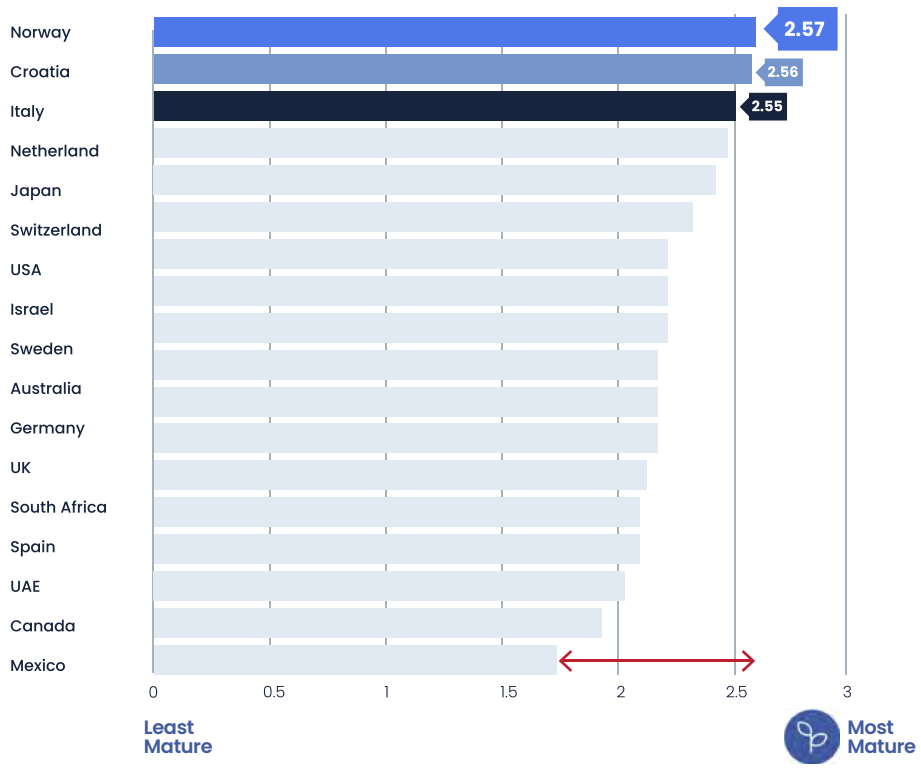
KEY INSIGHTS

The majority of our customers have reported that they are either exploring AI use or actively using it in detection, response, or automation.

Global Cyber Maturity Is Rising, but Unevenly

Between 2023 and 2025, cybersecurity maturity increased globally across most regions, industries, and company sizes. This upward trend is driven by a convergence of regulation, investment, and awareness—but the gains are uneven. Countries like Norway and Japan stand out for rapid progress, while others like Mexico are just beginning to catch up. Smaller nations with strong governance models often outpace larger economies with fragmented or under-enforced security strategies.

Maturity by Country



Adopting AI and Automation in the Cybersecurity Stack Is Improving Organizational Maturity

The adoption of AI and automation tools is democratizing cybersecurity maturity. From automated threat detection to compliance reporting, organizations—especially mid-sized firms—are using AI to close capability gaps and scale operations. The majority of our customers have reported that they are either exploring AI use or actively using it in detection, response, or automation. While attackers also use AI, defenders are increasingly deploying intelligent tools for prevention, monitoring, and rapid response, contributing significantly to the overall rise in cyber resilience.

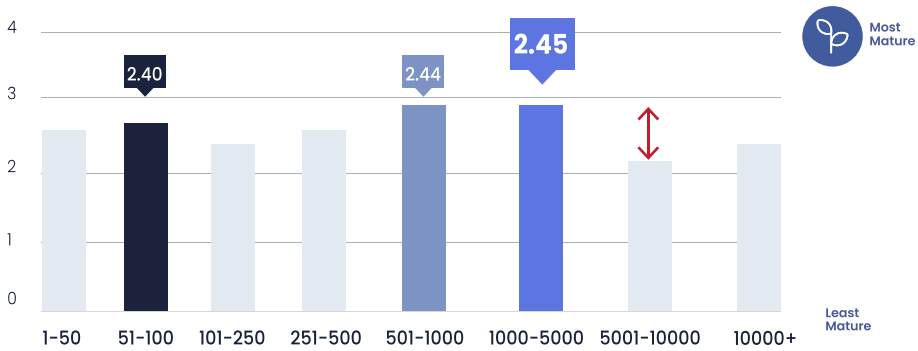
KEY INSIGHTS

Organizations with 250–1000 employees showed the steepest rise in maturity.

Mid-Sized Companies Lead in Cyber Maturity Gains

Organizations with 250–1000 employees showed the steepest rise in maturity. Enabled by cloud-based security tools, virtual CISOs, and manageable attack surfaces, many of these firms now outperform both small and large counterparts. Unlike small businesses constrained by resources or large enterprises slowed by complexity, mid-sized companies have found a sweet spot for agile, cost-effective cybersecurity growth.

Maturity by Company Size



Spending More Doesn't Necessarily Make Organizations Safer

While global cybersecurity spending hit record levels and are expected to exceed $212B in 2025, the report reinforces that how money is spent matters more than how much. Countries like the U.S. and Germany spend heavily but don't always top maturity rankings. In contrast, places like Norway and Japan combine focused investment, cohesive strategy, and execution, proving that strategic alignment is the real differentiator.

CYE's data further supports this, showing a clear connection between higher cybersecurity maturity and a noticeable reduction in both the frequency and severity of breaches. External research echoes this trend: According to Cisco's 2024 Cybersecurity Readiness Index, only 5% of organizations reached the highest level of maturity, yet those in the "Mature" category demonstrated significantly greater resilience and preparedness in the face of cyber threats. This underscores the tangible benefits of advanced cybersecurity practices.

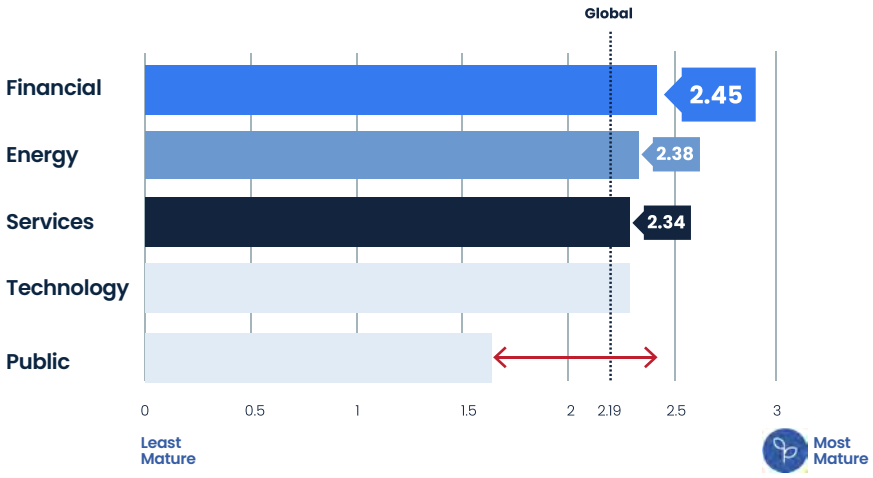
KEY INSIGHTS

Regulatory pressure and systemic risk awareness have made security central to operational continuity.

The Financial Sector Widens Its Lead Over Other Industries

Already a maturity leader, the financial sector doubled down on governance, AI-enhanced fraud detection, and supply chain risk management. Regulatory pressure and systemic risk awareness have made security central to operational continuity. Even fintechs and small banks are aligning with advanced frameworks, widening the gap between finance and other industries.

Maturity by Industry

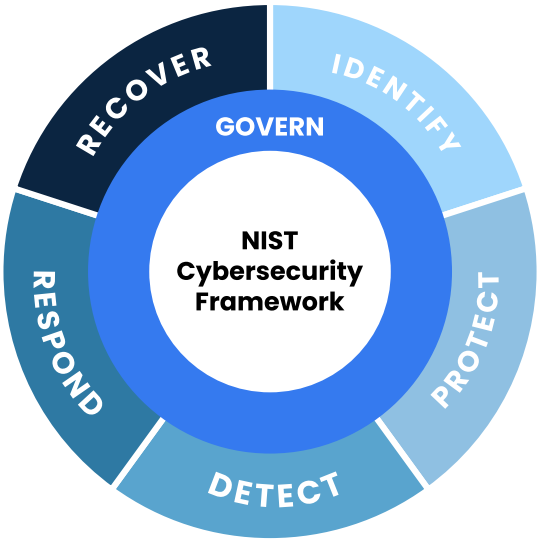


Cybersecurity Has Moved from the Darkroom to the Boardroom.

In 2019, only 16% of S&P 5000 companies had a board member with cybersecurity expertise. Today, that number has risen to over 80%, reflecting the growing recognition of cyber risk as a strategic business issue. This visibility has translated into stronger policies, funding, and organizational accountability, making cybersecurity a strategic priority rather than a technical afterthought.

CYBERSECURITY FUNCTIONS (NIST CSF 2.0)

In this report, we align our cybersecurity maturity assessments with the NIST Cybersecurity Framework 2.0, which introduces six foundational functions. These functions serve as a comprehensive guide to managing cybersecurity risk across an organization's operations and technology ecosystem. Together, they form a continuous cycle of identifying, protecting, detecting, responding to, and recovering from cyber threats—now strengthened by a sixth function, Govern, which emphasizes strategic oversight and accountability.



Note on Framework Adoption

In previous reports, cybersecurity maturity was measured using CYE's seven distinct security domains that reflected core operational and technical areas of cybersecurity strategy. While this model provided valuable insight into organizational posture, CYE has switched to the **NIST Cybersecurity Framework (CSF) 2.0** as the foundation for assessment.

NIST CSF is one of the most widely recognized and adopted cybersecurity frameworks globally. It offers a standardized and holistic structure for managing cyber risk across six integrated functions: Identify, Protect, Detect, Respond, Recover, and Govern. Though the framework is different in form, there is strong conceptual alignment with the original security domains. Each of the domains maps closely to one or more NIST functions, ensuring continuity and comparability in how maturity is evaluated.

However, note that the switch to NIST CSF 2.0 reflects not just a change in structure, but also an evolution in priorities. This is the case with the addition of the Govern function in particular, which emphasizes strategic oversight, risk ownership, and regulatory alignment. As a result, certain shifts and trends in this year's results may be attributable in part to this updated framework.

INDUSTRY DEFINITIONS

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

Consumer
Manufacturers and distributors of consumer products

Education
Public and private universities and colleges, and training and development companies

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

Entertainment
Movie production, sports, gaming, and casinos

Financial
Banking, insurance, and investment companies

Healthcare
Hospitals and clinics

Hospitality
Hotels, restaurant chains, and cruise lines

Industrial
Chemical process, engineering, construction, and manufacturing companies

Pharma
Pharmaceutical and biomedical life sciences companies

Public
Federal, state and local agencies, and non-governmental organizations

Retail
Brick and mortar, and e-commerce

Services
Legal, accounting and consulting firms, and professional services

Technology
Software and hardware companies

Transportation
Airlines, railroad, trucking, and delivery companies

RESULTS BY FUNCTION

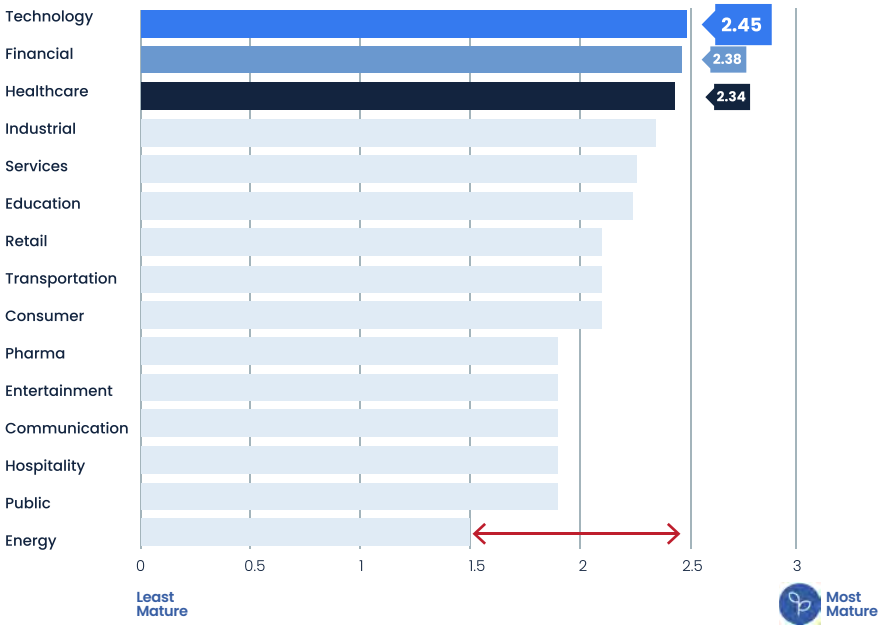
GOVERN

All industries fall short in continuously governing third-party risk across their organization, despite a consistent rise in exploitable threats in the supply chain.

DEFINITION

The Govern function in NIST Cybersecurity Framework (CSF) 2.0 focuses on establishing and overseeing an organization's cybersecurity risk management strategy, policies, and governance processes. Its purpose is to ensure that cybersecurity activities are aligned with business objectives and risk appetite, and that roles, responsibilities, and enforcement mechanisms are in place. In essence, "Govern" emphasizes top-down management of cybersecurity—integrating it into enterprise risk management, setting expectations, and continuously monitoring compliance with those expectations.

Govern Maturity Scores by Sector



Most Frequent Findings

1

Ineffective or Non-Existing Cyber Supply Chain Risk Management Processes

2

Vendors Are Not Continuously Monitored or Assessed

3

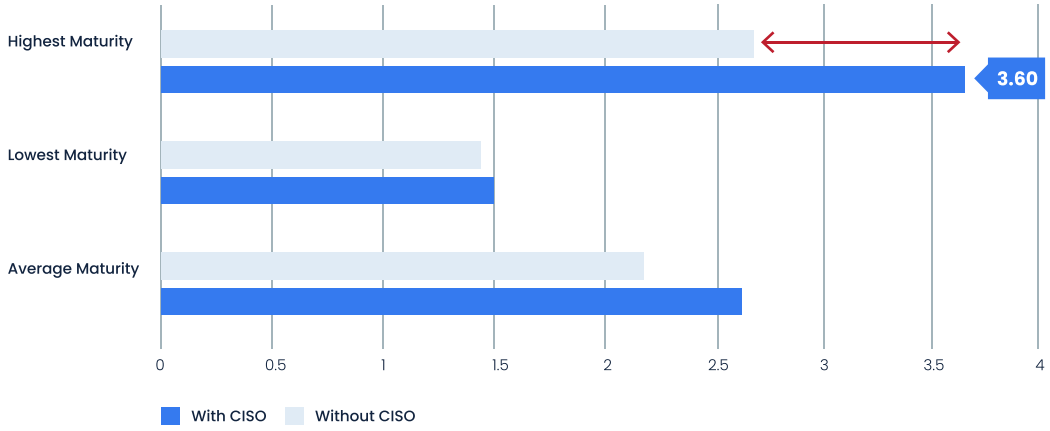
Governance and Risk Management Processes Are Partial or Missing

GOVERN

Organizations with a dedicated CISO consistently achieve higher maturity scores across the board.

The Presence of a CISO Can Make or Break Business Resilience

Organizations with a dedicated CISO consistently achieve higher maturity scores across the board, averaging better outcomes and maintaining stronger posture. The data shows that companies without a CISO not only lag in average maturity but also hit a lower ceiling in overall cyber readiness. While smaller businesses may lack resources for a full-time CISO, even appointing a security lead or external advisor can substantially improve risk oversight, policy enforcement, and strategic alignment.



Industry Drivers of Maturity

Governance maturity varies significantly by industry sector, reflecting external drivers like regulation and risk exposure. For example, organizations in finance or healthcare commonly show higher maturity because they usually must adhere to strict regulatory standards including DORA and HIPAA, which compel them to implement robust cybersecurity governance practices. On the other hand, sectors such as manufacturing, retail, or others with fewer cybersecurity regulations often have lower maturity scores, as they may not be compelled to develop equally rigorous governance. This highlights that regulatory compliance and the increasing cost penalties for non-compliance play a vital role in pushing organizations toward better cybersecurity governance; sectors without that push may need additional incentives or awareness to improve.

Vendors Remain a Blind Spot

A critical weak spot is the absence or ineffectiveness of cybersecurity supply chain risk management processes across organizations. According to Verizon's 2025 Data Breach Investigations Report, third-party involvement in breaches has doubled to 30%. Yet our research indicates that many companies lack formal methods to identify and manage cyber risks posed by vendors and suppliers, leaving a significant blind spot in their overall cyber-security strategy. This gap means third-party risks are not being systematically assessed or mitigated, undermining the organization's security posture from the outside in.

RESULTS BY FUNCTION

GOVERN

Even when organizations perform initial vendor risk assessments, they do not continuously monitor or regularly reassess their vendors' security posture and risk.

Lack of Continuous Vendor Monitoring

Even when organizations perform initial vendor risk assessments, the data shows they often do not continuously monitor or regularly reassess their vendors' security posture and risk. This finding implies that cybersecurity oversight is frequently treated as a one-time checklist item rather than an ongoing process. Without continuous monitoring, changes in a vendor's security posture or new vulnerabilities in the supply chain can go unnoticed, increasing the likelihood of security incidents via third parties, and organizations' overall exposure to supply chain threats.

Partial or Missing Governance Processes

Many organizations have only partial governance of cybersecurity programs, or none at all. This insight indicates that while some may have basic policies or an executive responsible for cybersecurity, they often lack a comprehensive, enforced governance framework. In practice, that means critical activities like regular risk reviews, policy updates, training, and governance of cybersecurity across business units are inconsistent or incomplete, weakening organizations' overall security posture.

RESULTS BY FUNCTION

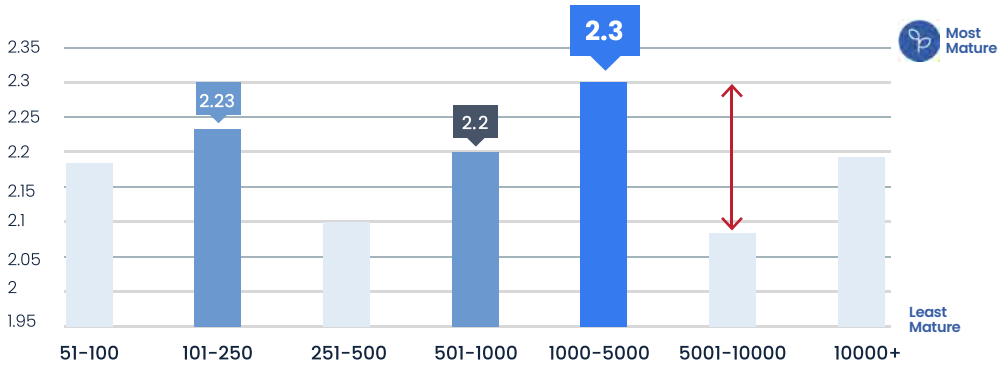
IDENTIFY

Many organizations lack full awareness of their assets and exposures.

DEFINITION

The Identify function in NIST's Cybersecurity Framework (CSF) 2.0 is the foundation of a security program, focused on understanding the organization's environment, assets, and risks. It helps an organization develop a clear inventory of systems, data, and resources and grasp the business context and vulnerabilities associated with them. In essence, Identify sets the stage for all other security activities by determining what needs protection and what risks exist. This function enables companies to prioritize cybersecurity efforts by first pinpointing critical assets and potential threat exposures. By establishing this baseline, an organization can gauge its current security posture and concentrate resources on the weakest links in their cybersecurity program before moving on to protection, detection, and response measures.

Identify Maturity Scores by Company Size



Most Frequent Findings

1

Administrative and Sensitive Interfaces Are Exposed to the Internet

2

Ineffective Asset Management

3

Subdomains Are Susceptible to Subdomain Takeover

RESULTS BY FUNCTION

IDENTIFY

Organizations must treat the Identify function as a continuous, essential practice rather than a periodic task.

The Identify Function is Foundational to Exposure Assessment

NIST CSF's Identify function establishes an organization's baseline cybersecurity posture by cataloging assets, resources, and risks. It is a foundational step—providing clarity on "what's out there" and enabling informed risk management—and it underpins all subsequent security activities. Organizations with a strong Identify function can prioritize protections more effectively, having first determined which systems and data are critical.

Organizations Can't Protect What They Don't Know Needs to Be Protected

The top findings reveal that many organizations lack full awareness of their assets and exposures. Administrative interfaces left publicly accessible, incomplete asset inventories, and dangling subdomains all point to failures in identification processes. These gaps are widespread; for instance, according to Vanta over 75% of companies admit to poor visibility into IT assets, and that directly translates into higher security risks, because attackers can only exploit what you fail to recognize and secure. However, a recent customer survey revealed that the evolving threat landscape is directly shaping cybersecurity maturity planning, driven by factors such as targeted data breaches, ransomware, phishing, AI-driven threats, and geopolitical events like the Russia-Ukraine war.

Need for Continuous Identification and Improvement

Both the data and external research point to a core lesson: Organizations must treat the Identify function as a continuous, essential practice rather than a periodic task. Keeping an up-to-date asset inventory, monitoring new or rogue IT assets, and promptly addressing exposures (like open interfaces or orphaned DNS entries) can dramatically reduce cyber risk. The trends in subdomain takeovers and interface exploits show that attackers will find the things you overlook. Thus, building maturity in the Identify function through automation, clear ownership, and integration with governance is one of the most impactful steps organizations of all sizes and sectors can take to improve their security posture. This is where many need to focus going forward: closing the asset visibility gap so that "unknown" no longer equals "unsafe."

RESULTS BY FUNCTION

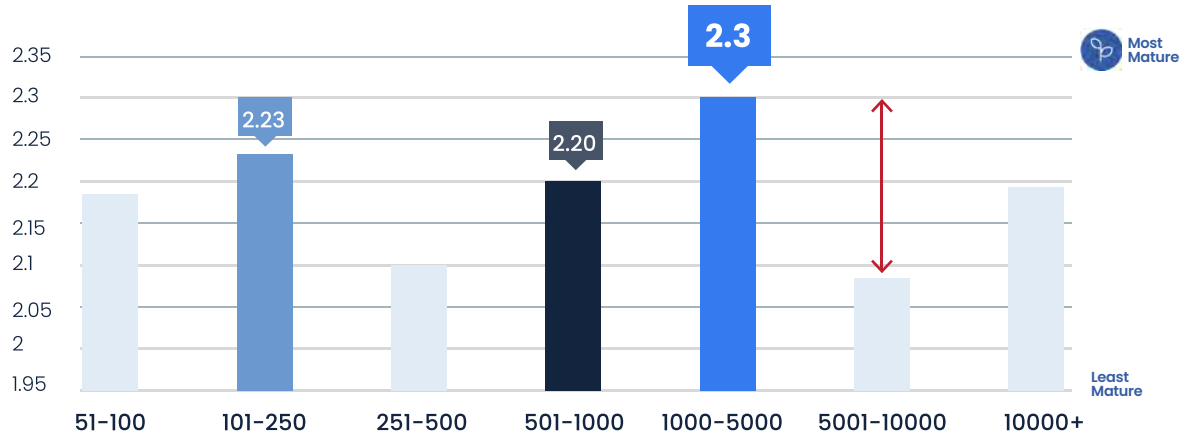
PROTECT

Smart strategy and consistent execution can drive high security maturity, even without the largest budget.

DEFINITION

The Protect function is one of the core components of the NIST Cybersecurity Framework (CSF) 2.0. Its purpose is to outline and implement appropriate safeguards that ensure the delivery of critical services and contain the impact of potential cybersecurity events. In practice, this means establishing controls and processes to prevent or limit damage from cyber incidents. The Protect function covers a range of proactive measures, including identity and access management (e.g. enforcing strong password policies), data security, protective technology maintenance, and awareness and training for personnel. By putting these safeguards in place, organizations build resilience by strengthening their defenses so that even if threats emerge, the likelihood of compromise is reduced and the continuity of operations is maintained.

Protect Maturity Scores by Company Size



Most Frequent Findings

1. **Usage of Outdated and Vulnerable Technologies**
2. **Weak Password Policy**
3. **Insufficient Global Security Update Policy or Mechanism**

PROTECT

An estimated 81% of corporate breaches are linked to stolen or weak passwords.

Legacy Technology & Patching Gaps Remain Widespread

A significant number of organizations still rely on outdated, vulnerable technologies and fail to apply security updates in a timely fashion. Studies show this is a critical issue, as most breaches involve an unpatched vulnerability. These findings underscore that basic maintenance, such as keeping software and systems up-to-date, is often under-prioritized, leaving known weaknesses available for attackers to exploit.

Weak Password Practices Continue to Pose Risks

Nearly one-third of companies lack effective password policies, resulting in weak or reused credentials that undermine security. Poor password hygiene has direct consequences: CYE's Cost of Breach model dataset suggests an estimated 81% of corporate breaches are linked to stolen or weak passwords. Strengthening identity management through strong passwords, multi-factor authentication, and user training is a straightforward, "low-hanging-fruit" improvement that many firms have yet to fully implement but could dramatically enhance their Protect posture.

Protect Maturity Doesn't Scale with Company Size

Small and mid-sized companies often exhibit higher Protect maturity than very large enterprises. With smaller attack surfaces and more agility, they can implement safeguards more comprehensively, whereas extremely large organizations struggle with complex, distributed environments. Surprisingly, some of the largest companies have Protect scores on par with or below much smaller firms, indicating that scaling security is a major challenge and must be addressed through better coordination and risk management in big enterprises. This is because in larger enterprises, there are several factors at play:

- Larger and more complex IT environments across cloud, multi-cloud, and varying scales of tech adoption
- Responsibility for patching and addressing vulnerabilities is dispersed across different teams
- Lack of sufficient and continuous oversight

This complicates the CISO's role, requiring the ability to align and communicate risk mitigation priorities in business terms with executive leadership as well as operationally with different managers. It also requires implementing governance and reporting capabilities on a consistent basis to ensure continuous exposure management.

Strategic Focus with Continuous Exposure Management Outweighs Budget at the Global Level

Some smaller countries (Norway, Japan, etc.) outperformed larger nations (US, UK) in cybersecurity maturity despite presumably lower budgets. Early adoption of national cybersecurity strategies, unified planning, and strong governance contributed to higher Protect function effectiveness in those countries. This underscores that achieving high cybersecurity maturity isn't about the size of the investment, but the precision of it. Tailored risk mitigation strategies, when defined thoughtfully and executed consistently, deliver the most effective results. It's a valuable lesson for both policymakers and organizations around the world.

RESULTS BY FUNCTION

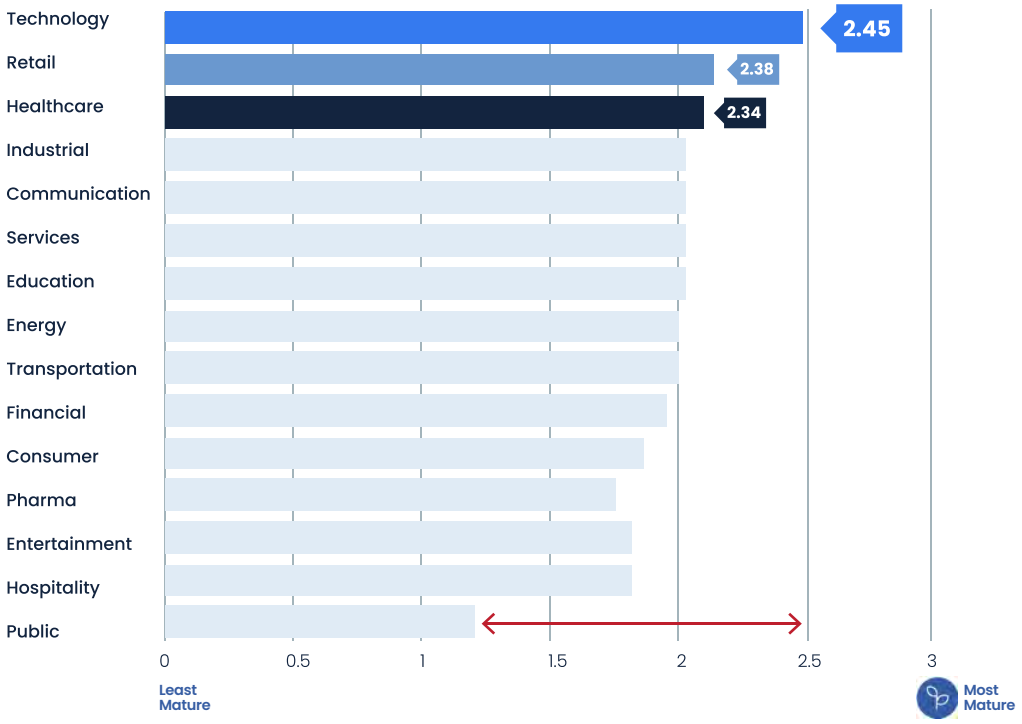
DETECT

Industries with significant lower detection maturity require industry-specific guidance to address disparities.

DEFINITION

The Detect function in NIST's Cybersecurity Framework (CSF 2.0 focuses on establishing capabilities to swiftly discover cybersecurity incidents before they cause extensive damage. According to NIST, Detect "enables the timely discovery and analysis of anomalies, indicators of compromise, and other potentially adverse events that may indicate that cybersecurity attacks and incidents are occurring" (The NIST Cybersecurity Framework (CSF) 2.0). In practice, this means implementing continuous monitoring, anomaly detection, and robust detection processes so that possible threats are found and analyzed early. A strong Detect function is critical for triggering prompt incident response and minimizing an attack's dwell time and impact.

Detect Maturity Scores by Industry



Most Frequent Findings

1

Insufficient Monitoring of the Corporate Network

2

Insufficient Monitoring of Authentication Events

3

Insecure Internet Connectivity Strategy

DETECT

Even the best-prepared industries and countries achieved only modest maturity scores for the Detect function.

Timely Detection Is Critical but Often Weak

The NIST CSF 2.0 Detect function is all about early identification of incidents, yet most organizations have a long way to go. In fact, a recent survey of our customers revealed that the majority had still not transitioned to NIST CSF 2.0. Our data suggests that only a fraction of companies have fully mature threat detection capabilities, highlighting a widespread deficit in the ability to promptly discover attacks. Faster detection enables faster response, so this gap directly contributes to longer breach dwell times and greater damage.

Gaps in Network and Log Monitoring Persist

A top Detect-related challenge is insufficient monitoring of internal networks and security logs. Many enterprises do not adequately watch internal network traffic or device activity, creating blind spots for attackers to hide in. In particular, failure to monitor authentication events such as logins and account use remained a prevalent vulnerability (Cybersecurity Maturity Report 2023 - CYE. This means that signs of compromised credentials or lateral movement often slip by unnoticed. These monitoring failures have real consequences, as seen in breaches like 23andMe where unchecked login attempts led to compromise.

Outbound Traffic Is a Security Blind Spot

Organizations commonly focus on keeping intruders out through ingress filtering, but pay less attention to monitoring outbound connections and data flows. This “insecure internet connectivity strategy” creates a risk where malware already inside can quietly exfiltrate data or beacon out to command-and-control servers. In fact, most corporate firewalls are not configured to sufficiently filter egress traffic, allowing attackers who penetrate the network to communicate externally without resistance. Strengthening outbound traffic monitoring and controls is therefore essential to the Detect function.

Detection Maturity Varies Significantly Across Industries

As with Govern, detection capabilities differ widely across industry sectors because of regulatory pressure and perceived risk. Regulated industries such as finance, telecommunications, and government tend to demonstrate higher detection maturity, driven by compliance mandates, specialized SOC teams, and ongoing investment in monitoring infrastructure. Conversely, less-regulated sectors—including retail, education, and small-scale manufacturing—often lag, hindered by limited resources, fewer skilled personnel, and lower prioritization of proactive monitoring. Addressing these disparities will require industry-specific guidance and broader access to scalable detection technologies, especially for sectors currently underrepresented in advanced security practices.

Even Market Leaders Have Room to Improve

Importantly, the data shows that no group is near perfection in the Detect function. Even the best-prepared industries and countries achieved only modest maturity scores of roughly 2 to 2.5 on a 5-point scale. This means that even organizations that invest heavily in detection are missing pieces of the puzzle, such as coverage gaps or untuned analytics. For the cybersecurity community, this is a call to action: Across all sizes, sectors, and regions, there is substantial room to bolster detection capabilities—from deploying more comprehensive monitoring of network, endpoint, and cloud to improving analysis of alerts—so that threats are found and acted upon before they escalate (The NIST Cybersecurity Framework (CSF) 2.0). Each step up in detection maturity directly reduces the likelihood that adversaries will create significant financial loss or damage to organizations’ systems.

RESULTS BY FUNCTION

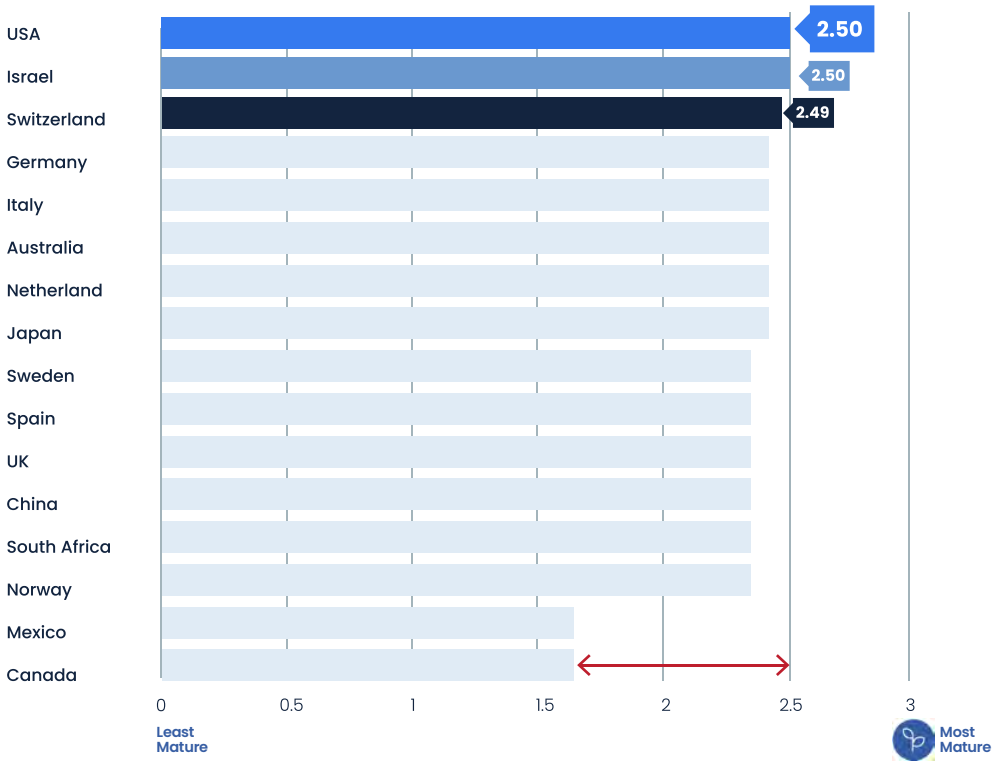
RESPOND

Disclosing breaches to the public is a challenging task, made even more difficult by gaps in informed decision-making.

DEFINITION

The Respond (RS) function in NIST Cybersecurity Framework 2.0 focuses on taking timely and effective action when a cybersecurity incident is detected. Its purpose is to contain and minimize the impact of an incident by executing response plans, analyzing the incident, remediating, and communicating with stakeholders. In essence, Respond bridges the gap between detection and recovery. It ensures that once a threat is identified, organizations can swiftly control the situation, prevent further spread, and initiate appropriate incident handling procedures to limit the impact on the business. This function covers outcomes such as incident management, analysis, remediation, reporting, and communication, making it a critical component of cyber resilience.

Respond Maturity Scores by Country



Most Frequent Findings

1

Missing or Insufficient Incident Response Procedures

2

Missing Incident Information Sharing and Reporting Policies

3

Inadequate Incident Containment Practices

RESPOND

A significant number of organizations have no formal incident response plan in place.

Importance of Preparedness to Reduce Costs

The Respond function is crucial for limiting damage once a cyber incident occurs, yet many organizations remain underprepared. A significant number have no formal incident response plan in place, leading to improvised and slower reactions when attacks happen. This lack of upfront planning directly undermines an organization's ability to contain and manage incidents effectively, often leading to higher, avoidable costs for the business.

Gaps in Communication and Reporting Due to Less Informed Decisions or "Guesstimating"

Beyond technical response, many organizations lack clear policies for incident information sharing, both internally and with external stakeholders. Most companies are hesitant to disclose breaches publicly, which suggests a cultural and policy gap. Companies also do not have the data to inform them when external communication is required, and communicating too early or late can be detrimental to the organizations' reputation and customer retention and can amplify the incident's impact even further. Additionally, this reluctance to report or share details can impede coordinated response from law enforcement or industry CERTs and slows down collective learning from incidents.

Operational Struggles with Incident Containment

Containment—isolating affected systems and stopping an attack's spread—remains a major challenge. Studies show that breaches often go on for months before being fully contained. Such prolonged containment windows give adversaries ample time to inflict damage, highlighting that many companies need to improve technical controls like network segmentation, automated response, and incident response training to shorten the containment phase.

Continuous Response Planning Improves Outcomes in Real Time Worldwide

Some smaller countries (e.g. Norway, Japan) achieved higher cyber readiness than larger nations like the US or UK, underscoring that well-coordinated national strategies and investments in planning can yield better incident response outcomes than budget alone. Overall, the most resilient organizations and nations are those that prioritize incident response planning, regular practice, and continuous improvement as core elements of their cybersecurity strategy.

RESULTS BY FUNCTION

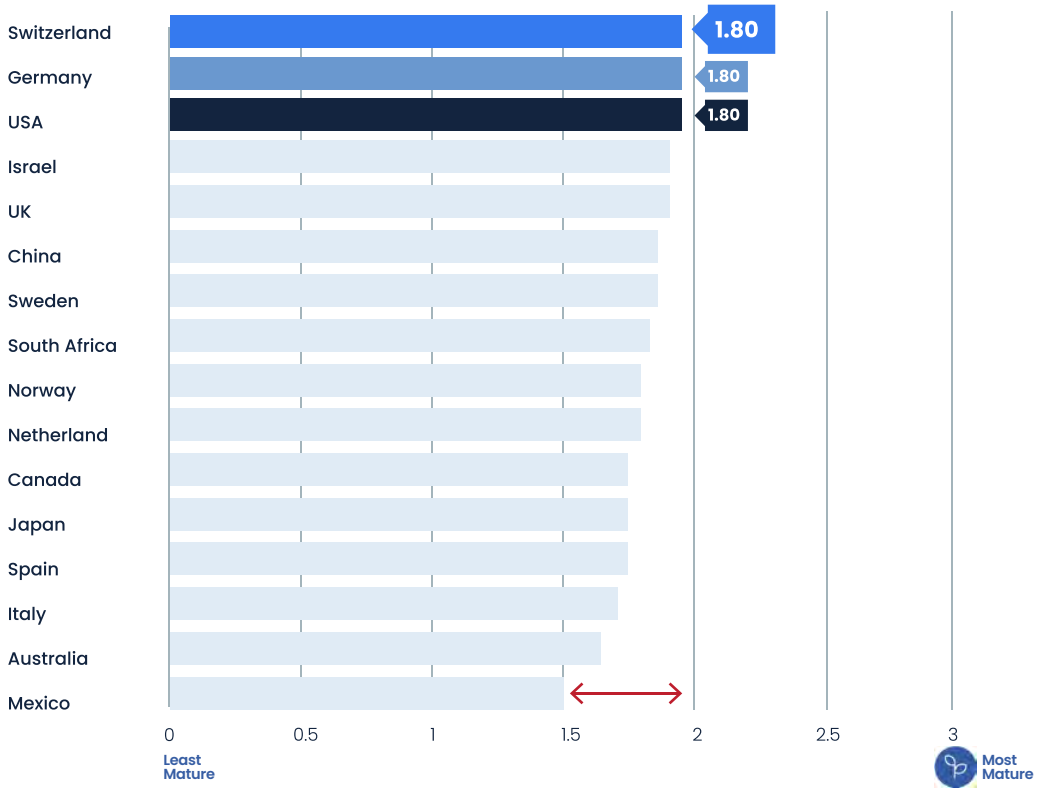
RECOVER

The absence of a formal business continuity and disaster recovery plan continues to be a widespread issue.

DEFINITION

The Recover function in NIST's Cybersecurity Framework (CSF) 2.0 is focused on restoring business as usual operations and reducing the impact of incidents through effective resilience planning. It is defined as the need to "maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event." In practice, this means organizations should have well-developed recovery plans, continually improve those plans based on lessons learned, and communicate effectively during the recovery process. By prioritizing swift restoration of systems and services, the Recover function helps minimize downtime and damage after a breach. It ensures that even if other security controls fail to prevent or detect an incident, the business can bounce back quickly, maintaining critical operations and reducing losses.

Recover Maturity Scores by Country



Most Frequent Findings

1

Missing Dedicated Workstations Set Up for Crisis Recovery

2

Missing Business Continuity Plan

3

Business Continuity Plan Is Not Tested

RECOVER

Building recovery capabilities is a global challenge, and many regions need to elevate their preparedness to match leading practices.

No "Plan B" Infrastructure

A large number of organizations have no dedicated crisis-recovery systems or communication tools ready for use in a major incident. This absence of out-of-band resources like reserve workstations or independent communication channels means that if primary systems go down, teams have no clear way to coordinate recovery, dramatically slowing down efforts. Establishing isolated, secure backup communication and IT resources are essential to enable swift recovery when normal networks are crippled.

A Lack of Business Continuity Plans

Lack of a formal business continuity/disaster recovery plan remains a common weakness. Data indicates that roughly 50% of businesses still do not have a documented business continuity plan (BCP) in place. Budget constraints are part of the challenge: In a recent survey of our customers, most said that investment in recovery planning has been flat, limited, or deprioritized. Organizations without BCP are forced to react on the fly during crises, making them far more exposed to prolonged downtime and higher financial losses.

Plans Are Not Practiced or Updated

Even among companies that do have recovery plans, insufficient testing and maintenance of such plans is a major issue. Many firms have never tested their disaster recovery plan, and many others only dust it off for infrequent annual drills. This leads to outdated or unproven playbooks where organizations learn the hard way that their plan isn't relevant when an actual incident occurs. Regular exercises such as simulations and tabletop exercises are critical to validate recovery procedures, train staff, and keep plans effective.

Uneven Global Resilience

Maturity in the Recover function varies greatly by country and region, reflecting broader disparities in resilience. Some countries—often those with strong regulations or risk awareness—exhibit high maturity scores. For instance, research indexes rank countries like Switzerland and Germany among the most operationally resilient environments. By contrast, organizations in other locales trail behind; countries with minimal continuity culture or resources such as Mexico sit at the bottom of resilience rankings. These differences underscore that building recovery capabilities is a global challenge, and many regions need to elevate their preparedness to match leading practices.

RECOMMENDATIONS

Strengthen Governance and Assign Clear Ownership Across All Cybersecurity Functions.
A common weakness across organizations is the absence of clearly defined accountability, especially around incident response, recovery, and supply chain governance. Organizations should ensure every cybersecurity domain has an executive owner, with governance frameworks that enforce policy compliance and continuously manage cyber exposure to drive business priorities.

Detection and Response Depend on Repetition and Readiness, So Test, Rehearse, and Update Your Plans Continuously.
Incident response and recovery plans are often outdated or untested, leading to poor performance in real-world events, disconnected from an organization's threat exposure. Organizations should regularly conduct tabletop exercises and business continuity drills tailored to their evolving attack surface, business, and cyber threats. These not only validate the effectiveness of current playbooks, but help teams internalize roles and actions, reducing decision delays and costs.

Cybersecurity resilience must be approached as an ongoing cycle of improvement.

Bridge the Gap Between Detection and Protection by Aligning Monitoring with Actual Threats.
Detection maturity remains inconsistent, with many organizations monitoring the wrong signals or lacking visibility into authentication, lateral movement, or outbound traffic. Detection capabilities should be tailored to known risks, particularly around identity and network behavior. Aligning telemetry with attack surfaces increases signal quality and improves response speed.

Secure the Basics Before Chasing Advanced Capabilities.
Many of the most critical findings in this year's report—weak password policies, unpatched systems, missing business continuity plans—are foundational issues. Rather than overinvesting in advanced tooling, organizations should focus on solidifying core controls such as patch management, asset inventory, privileged access, and user awareness training. These remain the most cost-effective paths to improved maturity.

Make Resilience Measurable. Track Maturity, Benchmark Often, and Adjust Based on Performance.
Cybersecurity resilience should be a continuous improvement cycle. Organizations should track their maturity scores by function, benchmark against peers and industries, and use trends to guide investment. This approach ensures that improvements are not just strategic but measurable, and that progress continues year over year.

RESEARCH METHODOLOGY

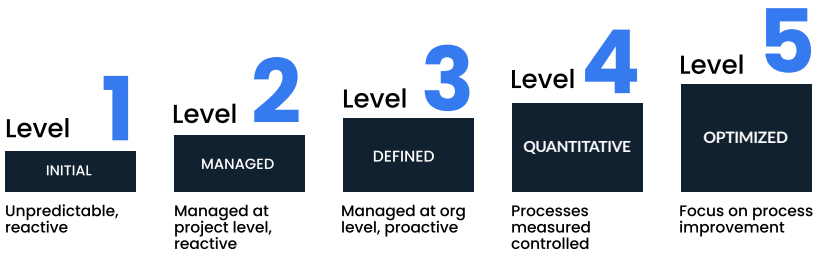
This report is based on the results of cybersecurity maturity assessments performed in CYE's exposure management platform, Hyver. Each assessment result contained detailed information regarding the overall security posture of the organization based on the six functions of NIST CSF 2.0, and each section in this report maps to each specific function. The evaluation included an overall security score, a list of vulnerabilities identified for each of the functions 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 (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)

Want to learn more about how CYE can help you quantify and continuously manage your cyber exposure?
Contact us.

About CYE

CYE's exposure management platform, Hyver, transforms the way security teams protect their organizations. With CRQ at its core, the platform reveals enterprises' exposure in financial terms, visualizes the most exploitable attack routes to critical business assets, and creates mitigation plans tailored to each business. CYE's customized reporting enables the sharing of vital board-level metrics and validating exposure reduction over time. In addition, CYE improves cybersecurity maturity by mapping weaknesses and defining targets based on industry frameworks. Founded in 2012 in Israel with operations around the world, CYE has served hundreds of organizations across industries globally. Visit us at cyesec.com.