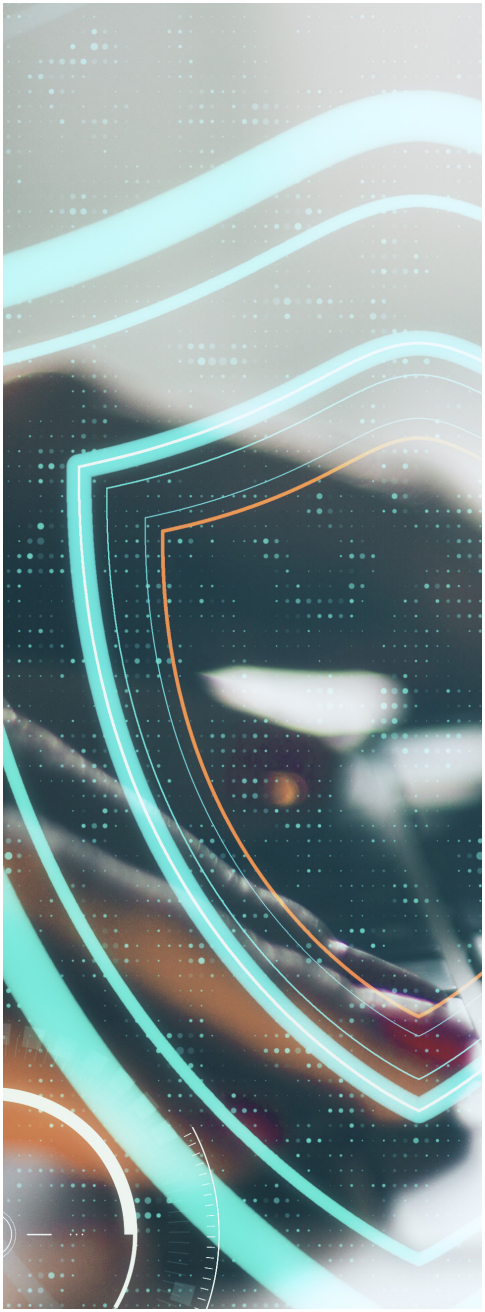
TRUESEC

Nordic CISO Report 2026

Entering an Era Beyond Human Speed



Dear Reader,

The time has come for a new iteration of our CISO Report. This is the third iteration of the report in which we interview Nordic CISOs about how they perceive threats, prioritize and budget for their work, and how they work to defend their respective organizations. The material gathered herein yields a unique and generous insight into the state of cybersecurity in the Nordics through the lens of the people responsible for defending organizations of varying sizes and industries in the region.

So, what are the key takeaways from this report? Well, I think it is fair to conclude that CISOs and their teams have made massive progress over the last two years. This is also reflected in the overall decline in large-scale ransomware attacks, which we also reported earlier this year in our Threat Intelligence Report[1].

In the report, we also conclude that CISOs have continued to mature their conversations with business stakeholders and are now more successful in communicating security posture in terms of actual business risk, such as risks to revenue streams, supply chains, operations, etc.

Is it all good then? Unfortunately, not. One thing that makes the jobs of a CISO or other senior cybersecurity practitioners challenging is the fact that both the threat landscape and technology are constantly evolving. Defending an organization is not like aiming for a fixed target. Today, we are entering an era beyond human speed with the development of AI. This development is not linear, but almost exponential. At the same time, the threat landscape is changing rapidly. As a consequence of a deteriorating geopolitical landscape, we see more nation-state activity hitting not only government organizations but also critical infrastructure in a broad sense. Everyone is part of someone's supply chain.

What does this mean for CISOs? With the new frontier AI models coming out, I believe we are entering a phase of substantial asymmetry in which new vulnerabilities will severely challenge defenders' ability to remediate in a timely manner. It is also our assessment that we will see more attacks on OT systems, which may have a significant business impact.

For CISOs, this means identifying the secret to managing the asymmetry by augmenting your existing capabilities with AI, ensuring your incident response readiness, and preparing for a busy period. Also, communicate to your various stakeholders that even if ransomware has been on the decline, this does not mean we can relax; rather, we should get them ready for the next phase.

And while doing all of this, I have deep admiration for the everyday work you do! Protecting a digitalized organization with substantial outsourcing and multiple partnerships whilst supporting key business outcomes is a very complex task. Doing that in a constantly evolving threat landscape, when new frontier AI models will cause havoc by disrupting our current vulnerability management processes, challenging biometrics with deep fakes, and synthesizing credentials, etc., is even harder. I hope you and your teams get the support and recognition you deserve!

Special thanks to all the CISOs who participated in the interviews. You took time out of your busy calendars to help us develop insights we can share with the community, which in the end will help secure all organizations. Many thanks!

Enjoy your read and do not hesitate to reach out should you want to discuss the report, have a conversation about what to include in the upcoming budget, or volunteer for the next iteration of our report.

I encourage you all to join the CISOs contributing to this report in confidently embracing this new reality beyond human speed and its uncertainty. Together we will prevail!

Rolf Rosenvinge

Rolf Rosenvinge
Chief Strategy Officer, Truesec

1 https://www.truesec.com/threat-intelligence-report-2026

Insights From Top CISOs in the Nordics

About This Report

The CISO Report is an interview-based qualitative study that aims to gather knowledge, render insights, and explore innovative ideas for the security community. The data collection was based on anonymized personal interviews with invited CISOs representing a mix of organizations across the Nordic region, including both public and private-sector entities of varying sizes and industry segments, conducted in April 2026.

We collected insights about the following areas:

- Threat Landscape
- Security Governance
- Security Capabilities
- Security Trends & Investments
- Workforce & Competence

Thank You

First and foremost, Truesec sends our deepest appreciation to all the CISOs who opened their calendars and agreed to share insights and perspectives. Then we extend a special thank you to the main contributors who conducted the interviews, performed the analysis, and wrote the report, all part of Truesec's Cyber Advisory:

Gabriel Winnberg, Principal
Eliza Stoenescu, Associate
Ronny Lundvall, Director

Truesec also gratefully acknowledges the many colleagues and stakeholders who contributed time, valuable perspectives, support, and expertise to this work, in particular *Rolf Rosenvinge, Jennie Mattar, Alexander Axelsson, Humayoun Zaki Dar,* and *Mårten Thomasson*.

Shifting From Protecting Critical Systems to Key Business Processes

Overview

In the 2024 CISO Report, sentiments were expressed that we were closing in on a perfect storm. Bewildered at the dark clouds on the horizon – geopolitics, organized crime, AI – the experts pondered what would ensue as the tempest reached our shores.

But it didn't, at least not in the catastrophic sense. Why, one asks?

Were the predictions off point, was it only hype, or are we still waiting? The clouds at the horizon remain and grow darker. Are we still crying wolf, only louder? The threats certainly didn't diminish. Perhaps we, as a security community, do a good job after all?

The levels of severe incidents reported by the participating CISOs have remained stable, which, in these accelerated times, would equal a net reduction. A remarkable feat. Considering that the complexity and pervasiveness of technology have increased in parallel with the accelerating pace, velocity, and power of attacks, how is it possible that millions of organizations managed to maintain relatively unwavering operations?

Our observations pull in opposing directions; on the one hand, increasing speed and collapsing attack thresholds, while on the other, a net reduction of severe incidents. This contrast likely underpins the impression of an uncertain future that several CISOs expressed. Perhaps this is where we should look for an explanation; complexity and speed are double-edged. Threat actors too face heightened awareness and more efficient controls. And the sheer number of people and organizations collaborating globally exerts an immense force.

Zooming out, we see a pull towards higher-order organization: In 2024, CISOs were being offered "a seat at the decision-makers' table". In 2026, the CISOs interviewed perceived having moved up further in the food chain, not necessarily organizationally, but rather communicationally, where their voices matter more. With few exceptions, CISOs are actively involved in securing buy-in and the necessary funding.

Reasons for this may be attributed to the more challenging threat landscape, as well as to regulations that push accountability towards boards and management teams, where the CISO is many times the messenger and interpreter. So, proximity to executives makes CISOs business-driven. Along with this move comes a shift in objectives, from protecting critical systems to protecting key business processes. There also seems to have been a maturity shift in which the identification and scrutiny of dimensioning threats are being translated into business risks that inform the security program budget.

To the CISO's advantage, as they move up the business ladder, technology also matures, enabling holistic security capabilities across single vector tech stacks. Previously siloed security concepts have become integrated under one hood, where standardization enables interoperability. This decreased entropy enables greater automation with AI serving as a catalyst. All this abstracts and simplifies technical security design and implementation, leaving more room for the CISOs to focus on Identify (business asset value, risk management) and Recover (backup) and business-driven conversations regarding continuity/resilience.

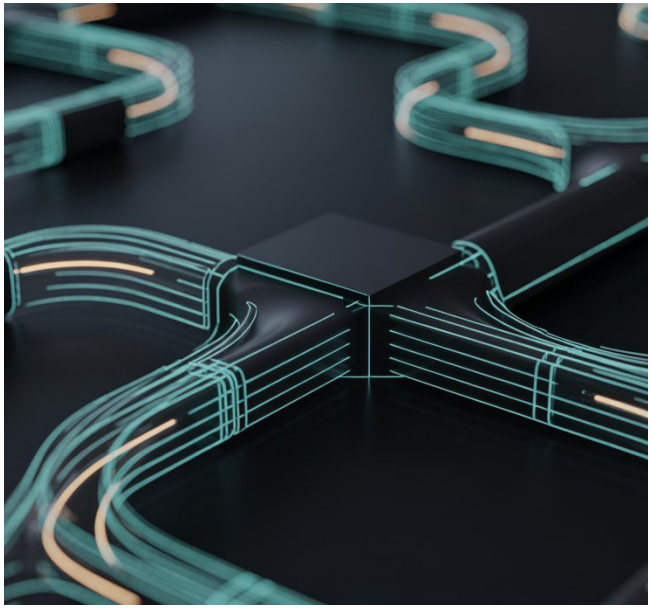
If we instead zoom in on capabilities, while the NIST functions of Protect and Detect, as well as Respond, continue to exhibit a respectable degree of maturity, Identify remains a hard nut to crack. In the last report, we noted increasing investments in Govern and Identify – specifically in Asset Management and Supply Chain Risk Management – but with the supersonic tsunami of zero-day attacks many expect, do we know where the weak links are? As expected, we also note an increasing appetite to revisit Recover due to ransomware's high demands for immutable backups and proper restore procedures.

Another interesting trend-break relates to staffing when security teams are being streamlined. CISOs adapt to strict but realistic budgets, and the fact that senior talent remains difficult to find, expensive to hire, and hard to retain is now a well-established constant. Meanwhile, schools produce juniors with a higher degree of readiness than before. But from the CISO's point of view, staffing issues are increasingly being addressed through capability redesign, automating the people dimension, or sourcing it through other internal functions or outsourcing the entire capability. This automation and outsourcing are yielding smaller teams. Security capabilities become commoditized and are "shifted left," becoming part of the IT operations infrastructure. Outsourcing capabilities such as SOC and TI make more sense given the greater bang for the buck.

Threat actors are better organized and leverage cheaper skills and more advanced AI-powered tooling. Despite this, organizations manage to remain stable. But we are at an inflection point, a new period of asymmetry, the AI-powered wave of zero-day exploitation. Also, there is a new poorly understood exposure: the known-unknown weaknesses of agentic AI, integrated into business processes and actually making decisions. Managing the attack surface and the criticality of assets in terms of business risk is key. Many CISOs believe we will not be able to prevent compromise; as a result, there is a growing shift toward an "assume breach" mindset, with an increased focus on strengthening Data Loss Prevention, Disaster Recovery, and Business Continuity Planning.

To put it succinctly, what we see is the aggregated effects of an ecosystem in successively higher orders of orchestration. This is exactly what the strategists have been saying all along. The idea is hinted at in slogans such as "security must be built-in, not bolted-on". The improvements are emergent properties of interacting bodies in an ecosystem; you cannot bolt on ecological properties, they appear and become effective when the entire system works properly together.

This emergent strength is the result of several mechanisms: CISOs and regulation effectively tying business risk management with security practices on the one hand, and successively more orchestration-enabled tooling across the entire IT estate on the other. This, we argue, is ultimately why the levels of severe incidents remained stable despite the threat actors' increasing speed and capabilities.



Speed, Not Novelty, Defines Risk in 2026

Threats & Severe Incidents

In 2026, a mere 9% of respondents reported an increase in severe cybersecurity incidents, while 91% reported a stable level, and none reported a decrease. At the same time, 55% reported an increase in less severe incidents. This stands in sharp contrast to the 2024 findings, where 53% of respondents reported an increase in severe cybersecurity incidents, 28% reported a stable level, and 19% reported no severe incidents at all, contributing to the narrative of "closing in on a perfect storm."

The relative stabilization of severe incidents suggests that the investments previously made across Protect, Detect, and Respond capabilities are beginning to improve resilience and the ability to contain attacks before they result in major disruptions.

The number of attempted cyberattacks is increasing steadily. Source: Truesec Threat Intelligence Report 2026.

> ***There are just as many serious cyberattacks as last year, but with better detection, fewer have escalated to the worst outcomes.***

However, the 2026 incident-related numbers do not indicate a calmer threat landscape. CISOs are explicit that the threat activity levels are higher than ever: probing is more aggressive, alerts are more frequent, and attacks are more persistent. Incidents being managed earlier may explain the 55% increase in less severe incidents. Improved detection capabilities, faster response, and more effective containment are explanations for this effect. Organizations are not facing fewer attacks than before; they are becoming better at absorbing the pressure.

When describing the threat landscape in 2026, CISOs place little emphasis on new threat categories. Across the interviews, the same core threats and TTPs are repeated: phishing and credential misuse, ransomware, exploitation of exposed systems and vulnerabilities, supply-chain threats, fraud, and insider threats. What consistently differentiates the 2026 landscape is the speed at which the threats are emerging.

Level of Severe Cybersecurity Incidents Over the Past 2 Years	2022	2024	2026
Increasing	69%	53%	9%
Stable	31%	29%	91%
Decreasing	0%	18%	0%

AI as Accelerator

AI is almost universally cited as the dominant accelerator, but not as a standalone threat category. A widely held view by many CISOs is that AI does not change what attackers do; it changes how fast and at what scale they do it. Reconnaissance happens more quickly, phishing campaigns are produced and refined at speed, and tooling is adopted with a level of agility many struggle to match.

Several CISOs note that attackers appear to be faster at adopting AI-assisted techniques than the defending organizations. This indicates an asymmetry worth considering in the systematic defense strategy, where rapid AI adoption and a shift from legacy bureaucratic structures to more agile ones should be included.

This acceleration in the adoption of AI-assisted techniques on the threat actor side of the equation directly reshapes how vulnerability exploitation occurs in practice. In the 2026 data, CISOs rarely describe severe zero-day attacks as isolated incidents with high business impact. Instead, they consistently describe a broader pattern of vulnerabilities being exploited much earlier after disclosure than before. The time window from disclosure to active exploitation is rapidly closing. In 2024, the mean Time to Exploit (TTE) was 53 days, while this year we are already down at 2.4 days.[2] Vulnerabilities that might previously have been assessed, prioritized, and patched in time are now exploited while organizations are still assessing exposure.

2 Time to Exploit (TTE), https://zerodayclock.com.

From Threats & Vulnerabilities to Risk Exposure

Exploited Vulnerabilities & Security Events

An interesting shift in the 2026 interviews is that rather than focusing on vulnerabilities, attacks, and exploits, CISOs now prefer to discuss the exposure of their IT estate. This relates to the maturation of reasoning about threats and business risks mentioned earlier. For example, aware that ransomware threats are targeting OT, CISOs are placing greater emphasis on which production sites are most valuable and therefore pose the highest risk, enabling them to prioritize their defense. This prioritization, based on where we have a higher tolerance for downtime vs. where we must avoid it, is a good manifestation of the resilience concept, which is fundamental to many recent regulatory requirements, such as NIS2 & DORA.

> *No vulnerabilities have been exploited in a way that led to a serious incident.*

> *We see roughly around 100 security incidents per year. None of them has had a serious business impact. We have phishing attempts, third-party-related attacks used for phishing or CEO fraud, but the impact is minimal.*

While vulnerabilities are consistently acknowledged as widespread, the majority of respondents report no instances of successful exploitation resulting in severe incidents. In total, just under three-quarters (73%) either explicitly state that no vulnerabilities have been exploited or are unable to point out concrete cases. Several respondents emphasize the absence of exploit-related incidents even in environments where vulnerabilities are known to exist.

When respondents confirmed vulnerability exploitation, it typically involved opportunistic exploitation linked to a lack of IT hygiene. Even for high-severity vulnerabilities that occur several times a year and spur a global patching race, the impacts are frequently contained or characterized as near-misses rather than realized severe incidents.

> *The zero-day incident was a near miss rather than an exploitation with impact.*

> *The challenge was not detection, but scale... vulnerabilities like Log4Shell affected almost the entire stack.*

People Vulnerabilities & Detection at Machine Speed

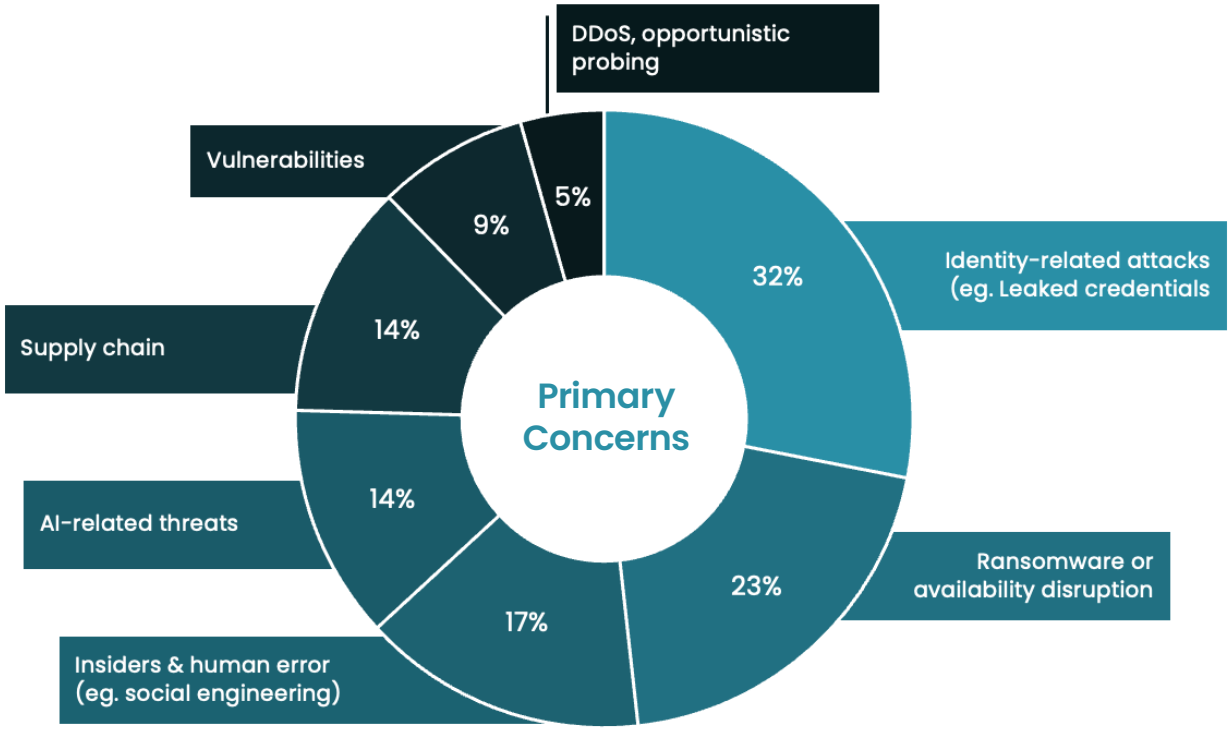
Social engineering and identity-related threats (human error, credential theft, phishing, insider threats, etc.) continue to be the most cited points of entry. People remain a risk even with awareness training. This is due to the sophisticated nature of social engineering, which leverages human psychology and vulnerabilities such as curiosity, greed, and a desire to belong. Due to the complexity of human psychology and individual variation, patching people is much more challenging than patching machines. The effectiveness of security awareness training in addressing social engineering is being questioned because it most often treats a knowledge-based problem rather than a behavioral one.

> *Most incidents we deal with are identity related: account takeover attempts, token theft attempts, phishing-related credential misuse.*

Ransomware remains the most consistently cited threat. Our threat intelligence shows a correlation between exploitation and infection, but over the past couple of years, we've seen threat actors target many SMBs rather than larger enterprises. Despite their larger attack surfaces, apparently, enterprise security exhibits something amounting to resilience.

> *Ransomware is the worst-case scenario for us... anything that threatens availability is critical.*

> *The most significant incident we had was three years ago, when an acquisition was hit by a ransomware attack three days before we took over responsibility.*



Several CISOs describe new problems emerging from AI-enabled development practices. The lowered barrier to producing and deploying code, even outside of engineering, introduces services and integrations without proper vetting. Research has shown that this is not necessarily due to lower quality, but rather to the production of more lines of code, which increases the probability of vulnerabilities. In addition, this new way of developing code undermines assumptions about where security controls should be placed and further emphasizes the need for inventory, permissions, and procedural discipline as critical control points.

Despite the relatively limited role of vulnerabilities in realized incidents, their management cannot be ignored. Automation and DevSecOps alleviate some stress, but the beyond-human speed at which AI models can find zero-day vulnerabilities means it's yet to be seen if our infrastructures will be able to sustain the pressure. Also, some environments remain patching-problematic, such as legacy IT and OT.

Taken together, the 2026 data paint a clear picture. The defining characteristic of today's threat landscape is not novelty, but permanent acceleration. CISOs are less concerned with what new threats might appear next and far more concerned with whether their organizations can detect, decide, and respond fast enough with the capabilities at hand.

Operationalized Trust

Governance effectiveness is increasingly defined by operationalized trust. Trust that the CISO escalates material risk without overreaching. Trust that the reported risk reflects real exposure rather than compliance. Trust that continued investment is justified even when outcomes appear stable.

Compared with 2024, governance in 2026 has moved beyond securing a seat at the table. The central challenge now is whether that seat enables timely, risk-informed decisions in a high-pressure environment.

Reporting Lines & Cadence

Measured purely in structural terms, the CISO's position relative to the CEO has changed only marginally since 2024. In 2026, direct reporting remains rare. Almost half (49%) are two steps away, and the other half (49%) are three steps down. None reported chains longer than three steps. This distribution is broadly consistent with 2024, when no CISOs reported directly to the CEO and the majority were separated by two intermediary layers.

An increase of about 10% with a dotted line to the CEO indicates that the CISO's voice matters more.

In 2026, about 65% of CISOs report through technology leadership (CIO or CTO) with one or two intermediaries to the CEO (half each). 40% of CISOs report to finance, either directly reporting to the CFO or through a CIO.

We still do not observe the CISO evolving into a formal C-suite role. Some suggest that this is not solely a question of organizational maturity. In several cases, CISOs themselves highlight trade-offs associated with proximity to executives, particularly related to independence. They also stress perceived governance effectiveness. Many describe engagement with the CEO, CFO, or board through security committees, audit forums, crisis management teams, or via informal escalation paths. 32% of respondents explicitly state that access, influence, or sponsorship matters more than formal reporting hierarchy.

> *Cybersecurity is presented to the board roughly once per year or more frequently if there are specific concerns or emerging issues.*

> *Formally, I rarely report directly to executive management. Instead, we have an Information Security Council. We meet roughly once a month. All major IT and information security decisions are taken there.*

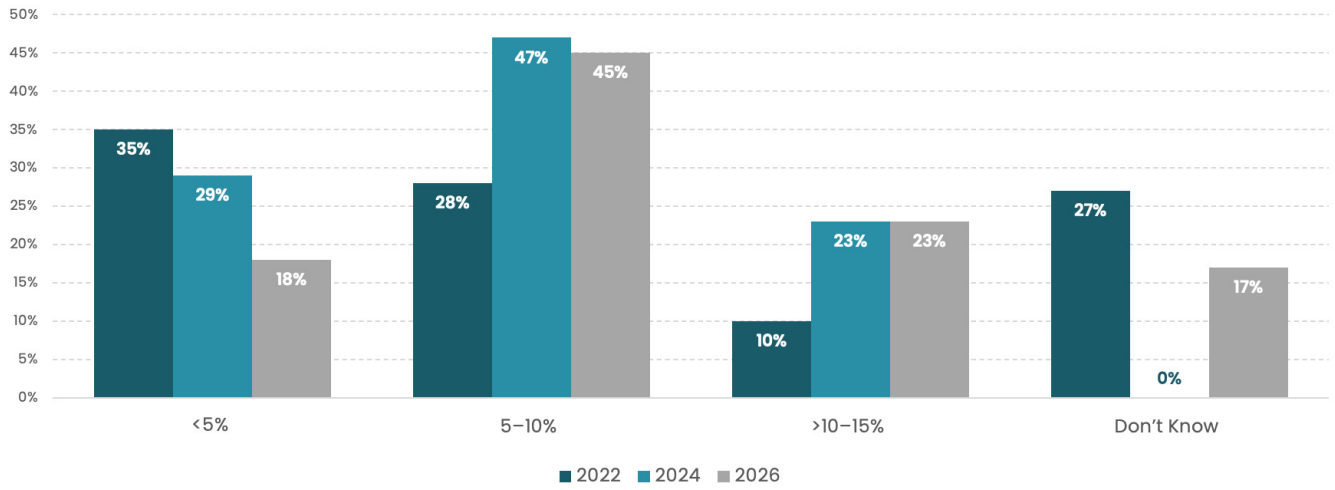
Regarding cadence for formal reporting to the board and executive management, there is no significant change from the 2024 report. Most CISOs report formally to the board once or twice a year, whilst reporting to executive management quarterly. However, we noted one interesting shift: CISOs are having more informal dialogues with executives.

> *We have cyber steering sessions with the Group CFO. We sit down once every few months and look at the numbers.*

> *During the first two years, reporting was more frequent. Since then, formal reporting primarily goes through the audit committee, with occasional direct interaction with the board when required.*

Budget Size Is No Longer the Primary Governance Bottleneck

Security Spend in Relation to IT Budget



From a quantitative perspective, cybersecurity budgets in 2026 remain consistent with the 2024 distribution when measured as a share of IT spend. The dominant range remains approximately 5 to 10% of the IT budget (45% compared to 47% in 2024), with an average of approximately 7%.

A lower bound of around 2% persists in larger or IT-intensive organizations, while an upper bound near 15% is observed in regulated, industrial, or OT-intensive environments.

This distribution closely mirrors the 2024 baseline and shows no evidence of a broad upward shift in relative spending. However, the qualitative interpretation of budgets has changed.

In 2024, CISOs frequently struggled to articulate security spend, questioned its effectiveness, and highlighted that large portions of the budget were locked into long-term contracts. In 2026, many CISOs explicitly state that head-line budget size is no longer the primary governance bottleneck. Security spending is increasingly embedded in enterprise platforms, cloud infrastructure, and identity systems, making strict separation between IT and security both artificial and less meaningful.

What CISOs emphasize instead is budget responsiveness. Governance discussions focus on whether funding can be redirected quickly when exposure shifts, whether tradeoffs are understood and accepted by executives, and whether security priorities survive competition with other strategic initiatives when no crisis is visible. Several CISOs state directly that they do not seek materially larger budgets, but rather predictable funding and executive backing when prioritization decisions become contentious.

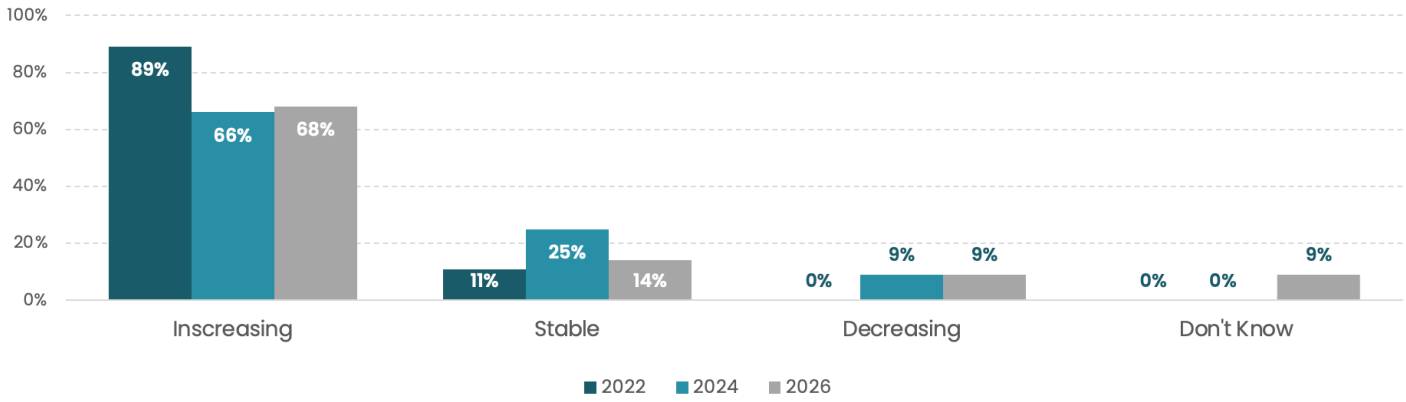
Change to Security Budgets

In terms of changes to security spend, 68% of respondents reported an increase, bringing it to the 2024 level. 14% reported no changes, while a mere 9% reported a decrease in budget. At the same time, some respondents highlight structural transitions, where previously fragmented security spending is being consolidated, making year-on-year comparisons less straightforward. As one CISO notes:

> ***Historically, cybersecurity spending was fragmented, scattered across depart-ments, and is now being rebuilt in a structured way.***

Others emphasize that security is "deeply embedded in everything we do," making clear separation from IT both difficult and increasingly artificial.

Security Budgets Year-On-Year



NIST CSF Capabilities

From "halfway there" in 2022, investments were successfully directed at fundamentals, specifically within Detect and Respond. By 2024, investments shifted from hygiene to more unpredictable issues requiring threat-centric, intelligence-driven, and agile ways of working, primarily within Respond but also Govern[3]. Looking at trends, in 2022, 57% of CISOs reported their greatest strengths to be in Detect and Respond. In 2024, 75% reported the same, and in 2026, the number increased to 81%.

In the 2024 report, respondents stated Govern and Identify as the biggest challenges. However, funds were to be mobilized towards these functions. In 2026, we see substantial improvements, indicating that these investments have paid off. Identify remains the most challenging.

In the previous report, we asked if a bi-modal approach to security, similar to that used in IT, was emerging: on the one hand, managing infrastructure and platforms using waterfall methods, and on the other, managing market-facing services that require rapid adaptation using an agile approach.

In a sense, yes, this is happening. However, again, it is not reflected in organizational changes, but rather in shifts of responsibility and the activation of accountability. We see these changes materialize in different ways:

The ability to make rapid, risk-based decisions is prioritized and kept in-house across all capabilities. Meanwhile, CISO challenges that can be automated are "commoditized" and either outsourced or "shifted left" into IT or development. This is clearly seen in Identify (asset and identity management), Protect (hardening, patching, DevSecOps), Respond (SOAR), and Detect (XDR, SIEM, identity monitoring). Among our respondents in 2026, only 15% maintained an in-house SOC.

When resources are freed, thanks to the above changes, CISOs direct their attention back to basics: Identify and Recover. Among the 2026 respondents, 59% report progression within Identify, and a staggering 82% in Recover.

CISOs are reaping the benefits of investments in Identify started in 2024, though it proves to be an uphill game in a de-perimeterized landscape when shadow IT, shadow AI, IoT, and OT come into play.

Recover is arguably our oldest discipline, still dependent on manual work. Cloud alleviates some of the burden through automation, but all struggle to restore integrations and maintain consistency. Severe or major incident management requires hyper-agility – all hands on deck and crisis escalation – for which we need margins to operate. Therefore, to maximize margins, hyper-preparedness is required, a previously neglected area that is now receiving long-overdue attention.

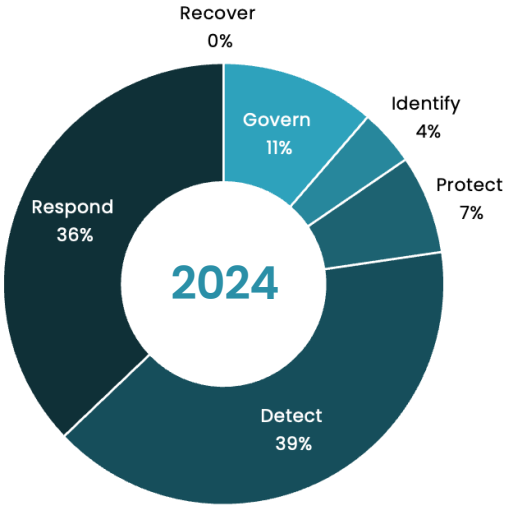
The mother of disaster recovery is business continuity, vital when prioritizing risks and creating playbooks, but also something traditionally not part of the CISO's sphere of influence. As the CISO's chair gets closer to that of the CEO's, we see a fusion of horizons. If business can fail over to a business continuity plan, ensuring at least 20% of business-as-usual capacity without waiting for IT, that is a substantial margin within which the CISO can move. Though some still struggle with the message:

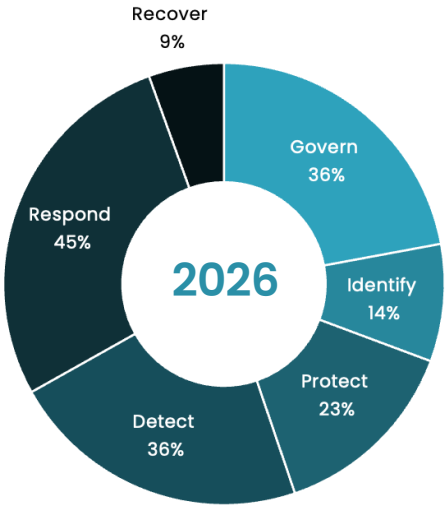
> ***I have a hard time trying to explain to the business that they need to do business continuity planning.***

This new focus on hygiene is expensive but contributes to long-term stability and resilience.

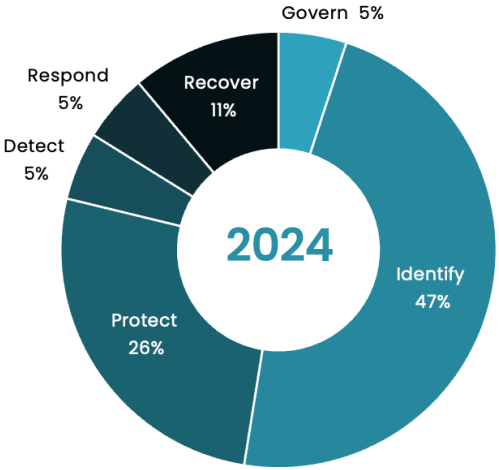
3 During the production of the 2024 report, NIST CSF 2.0 was released which formalized Govern as a new function. Governance concepts had been present before but distributed among other functions.

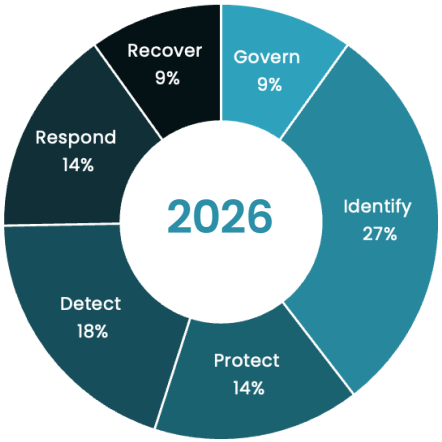
NIST CSF Function Strengths





NIST CSF Function With Most Challenges





Zero Trust

Some of us remember the time without firewalls. Then firewalls came and provided a hard perimeter around a soft center. But trusting everything on the inside soon proved a poor idea. Zero Trust was born; everything should be internet-ready, and de-perimeterization became a thing.

Implementing a Zero Trust in larger organizations requires substantial transformation. It may also prove practically impossible with legacy IT and OT. Comparing data from previous years, there is a noticeable improvement where 60% report a maturity of 3/5 or higher, while in 2024, only 40% estimated the same.

Only a few years back, many SMBs would not consider a Zero Trust journey due to high costs. With gradually improving major vendor software stacks, aspirational Zero Trust support comes standard, making it possible even for smaller organizations.

Zero Trust Maturity (1-5)	2024	2026
1	12%	22%
2	46%	17%
3	24%	33%
4	18%	28%
5	0%	0%

Extended Detect & Response (XDR)

Extended Detect and Response is a category of tools that gather security event data from multiple sources in real time to identify ongoing attacks and enable a rapid response.

All the respondents had some form of XDR service in place, and only one lacked a SOC service. Compared with 2024, 94% of CISOs said their organizations had made at least 3/5 progress on their XDR journey.

This year, 82% had decided to outsource the SOC to an MDR provider, while 14% were operating an in-house SOC. Looking at trends, we see a stable but modest maturity improvement, 71% reported a 4 or 5 in 2024, while 78% reported it in 2026.

XDR Maturity (1-5)	2024	2026
1	6%	0%
2	0%	0%
3	24%	23%
4	59%	64%
5	11%	14%

Zero-Day Attack Resilience

A zero-day attack occurs when attackers exploit a previously unknown software vulnerability before a fix or patch is available. In 2026, capabilities for managing zero-day threats are largely at intermediate maturity levels (50% reported a maturity of 1 or 2).

The big question today is how hard the beyond-human speed zero-day wave of exploitation will hit us. Despite research showing that vulnerability exploitation accounts for up to 32% of intrusions[4], our respondents did not report it as a root cause of *severe* cybersecurity incidents over the past two years. So, speed alone does, of course, not equal high impact:

> ***The zero-day incident was a near miss rather than an exploitation with impact.***

CISOs generally do not consider zero-day vulnerabilities a distinct threat category, but, as with all escalations, it's the speed that is the decisive factor. Since the Time to Exploit (TTE) shrinks by the day, patching is not enough. Thus, greater emphasis is put on Detect and Respond to contain attacks as early in the kill chain as possible.

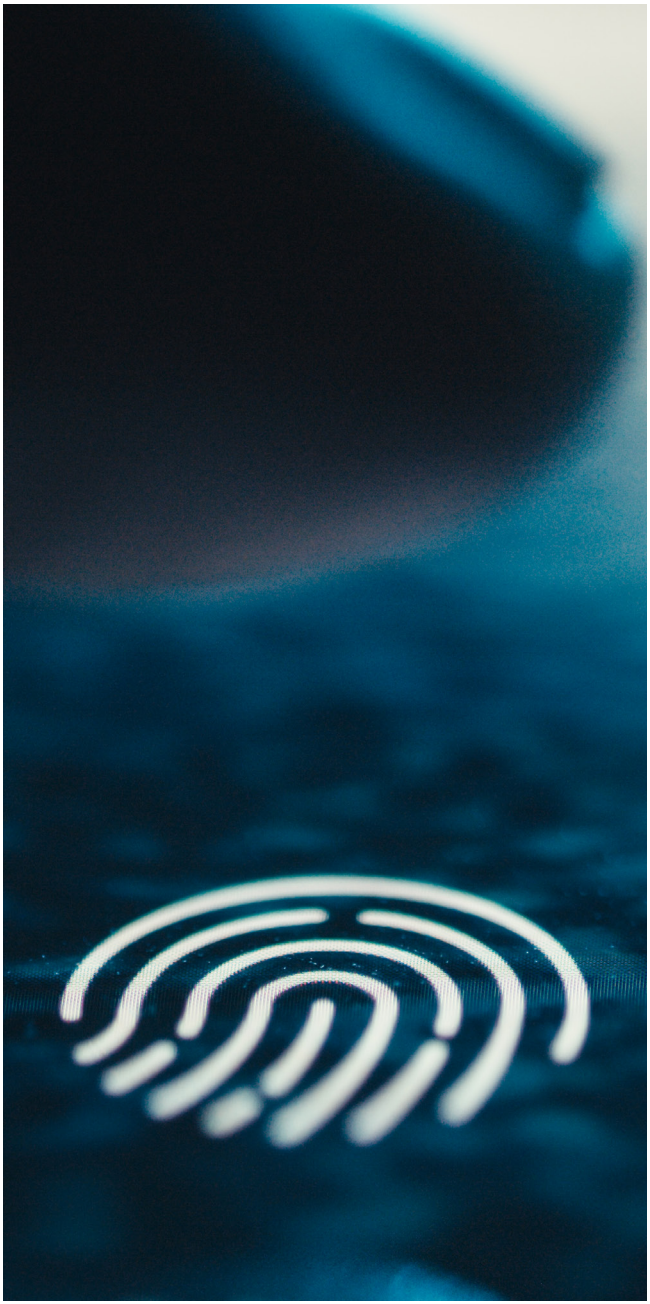
Even so, CISOs first look at reducing the attack surface, explaining investments in Identify. Second, CISOs also assume breach and look at impact mitigation, which explains a new focus on Recover and overall business continuity planning, as well as data loss prevention (Protect). If business on its own can absorb some of the damage, that greatly improves the chances for the security organization, together with IT, to do something meaningful.

As one CISO put it:

> ***We have to be prepared to get back on our feet.***

Zero-Day Attack Resilience (1-5)	2024	2026
1	18%	18%
2	32%	32%
3	41%	27%
4	24%	23%
5	0%	0%

4 https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2026/



Passwordless Authentication

Passwordless authentication allows users to access services without passwords or security questions, instead relying on biometrics, one-time codes, or external tokens/devices.

Throughout the interviews, passwordless authentication is recognized as an important component. While respondents consistently highlight identity-based attacks as the dominant entry points, adoption remains limited: no organization reports full implementation, 49% remain at low to intermediate, and only 23% reach higher maturity.

Passwordless authentication remains one of the least mature identity controls. Organizations have prioritized detecting identity misuse, while structural controls that eliminate credential risk are less mature. This reflects a pattern in which capabilities supporting visibility and response progress faster than those requiring architectural change. While awareness has increased, driven by identity-driven threats and AI-accelerated attack patterns, compared to 2024, the pace of progress has been incremental rather than transformative.

Password Authentication Maturity (1-5)	2024	2026
1	29%	18%
2	12%	32%
3	41%	27%
4	12%	23%
5	6%	0%

Identity Monitoring

Identity monitoring focuses on detecting and managing advanced identity-related threats by analyzing unusual user behavior. It has become an important capability for identifying attacks that, e.g., rely on stolen or leaked credentials, reflecting the growing reality that attackers increasingly gain access by "logging in rather than hacking their way in".

In 2026, identity monitoring reached a higher level of maturity compared to other identity controls. 5% state a fully implemented level, while 71% estimate a 3/5 maturity or higher.

Compared to 2024, the capability appears to have progressed. However, the concentration at intermediate maturity levels also suggests that while monitoring is broadly implemented, for many, it's still a work in progress.

Identity Monitoring Maturity (1-5)	2024	2026
1	18%	5%
2	12%	19%
3	35%	43%
4	24%	29%
5	12%	5%
Grand Total	100%	100%

Regulatory Preparedness

One expression of the pull towards higher-order organization is regulation. The increased threat landscape and need for harmonization and strengthened cyber resilience in the EU have paved the way for regulatory frameworks such as DORA, NIS2, and the CRA.

> *Cyber is now bigger than cyber. It is a whole-of-society problem.*

Regulatory pressure is a constraint, but it also contributes to global resilience, acting as a stimulant for organizational maturity. In part, it pushes our agenda up, directly increasing executive engagement:

> *Due to NIS2 and increased regulatory pressure, I now have more regular direct access to both executive management and the board than before.*

Compliance with these regulatory requirements is a matter for the board and executive management; it is not just a technical or operational concern for the IT department. To achieve compliance, the board and executive management need to work closely with the CISO to ensure that the security program supports risk alignment, operational readiness, and informed governance of cyber risk.

Along with compliance challenges related to new regulatory requirements comes the promise of compliance automation. Even though AI-supported tools from leading market contenders are often viewed as glorified document parsers, this area remains of great interest. To automate compliance, legislation and policies must be consumable by computers. Concepts such as machine readability and rules as code (RaC)[5] are therefore introduced.

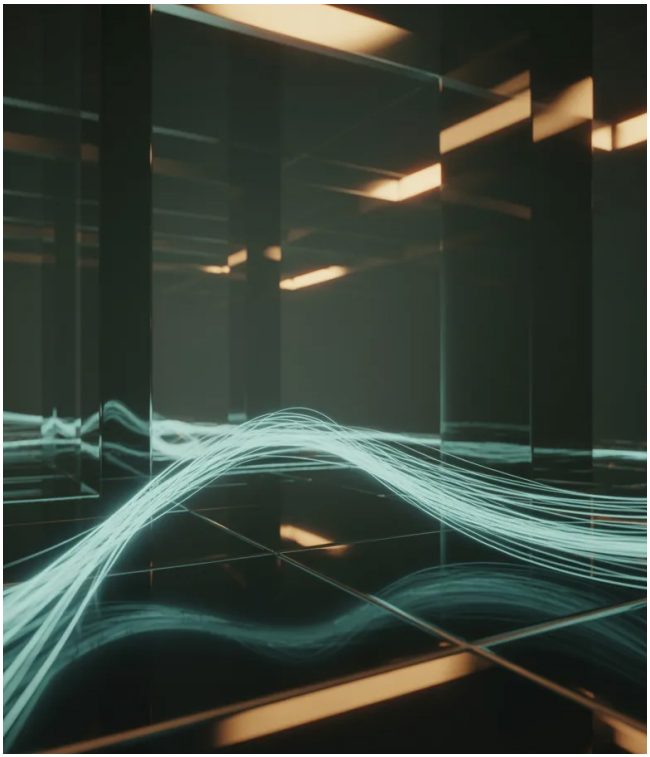
But actual compliance automation is about more than modern tools enabling efficient evidence collection and assessment. Organizations need to make additional efforts in ensuring the design and implementation of compliant processes, including AI augmentation, from the outset, with assurance built in (code, agents, etc.). Just adding AI to evidence collection and assessment will not solve substandard process design; we need to add AI to the entire compliance challenge, as people will not suffice in the era beyond human speed.

Consequently, staffing is also a concern in relation to regulatory ambition. It becomes particularly visible with the ever-growing set of regulations and corresponding demand for specialized roles:

> *I honestly wonder where all the people required for things like NIS2 will come from.*

> *Recruiting compliance specialists has become increasingly difficult.*

In practice, compliance functions often compete for the same limited talent pool. Worst case, regulatory maturity becomes a paper product at the cost of technical controls.



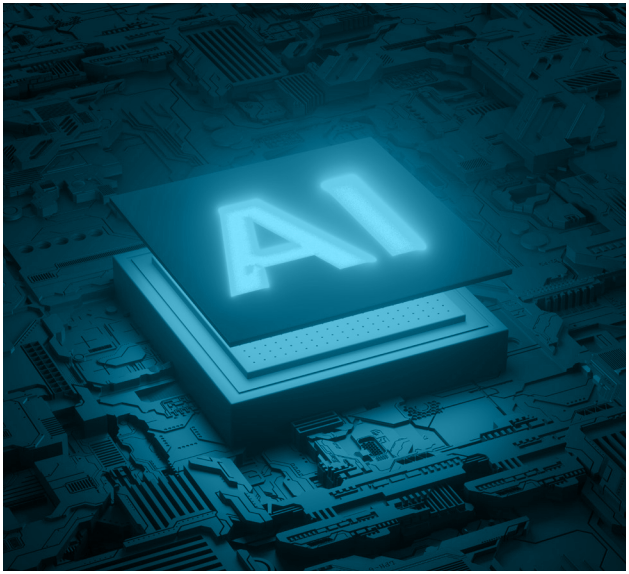
5 https://interoperable-europe.ec.europa.eu/collection/eugovtech/document/rules-code-open-approach

AI Security Governance

The introduction of AI security governance as a new theme in the 2026 report represents many different challenges for CISOs.

One new challenge, yet difficult to manage, is by all practical considerations an insider threat stemming from the AI/ML models themselves. Model security is the practice of protecting models from manipulation or misuse. It ensures the integrity, confidentiality, and availability of models throughout their lifecycle. Example breaches may be a poisoned fraud-detection model approving fraudulent transactions, or a compromised recommendation system exposing sensitive customer data.

Other challenges include the use of non-allowed tools, AI agents running with broad privileges, missing human-in-the-loop controls for high-impact actions, lack of logging, insufficient separation of trusted instructions from untrusted content, lack of validation of outputs and actions before execution, etc.



AI Security Governance Maturity (1-5)	2026
1	18%
2	18%
3	50%
4	14%
5	0%

Most depend on off-the-shelf solutions, but to a growing degree, organizations develop and fine tune models for their own proprietary use. To ensure that the outcome complies with corporate policies, that agentic behavior can be measured and controlled, that only models from trusted sources are used, etc., AI security governance is required.

Of the interviewed organizations, 50% reported having an AI governance function in place, while 36% had a program underway. The remaining were struggling with the concept. None identified themselves as having reached a high level of maturity. A smaller set (14%) estimated they had reached 4/5 maturity, while 50% considered themselves halfway.

AI-Powered Security Tooling

Another new question for 2026 is that of AI-powered security tooling. By that, we mean the use of AI/ML to support cybersecurity regardless of tasks. With the hype, AI is increasingly embedded into existing tools we use to improve efficiency and reduce cognitive load. The vast majority (72%) are at the beginning of this journey, riding along whatever improvements their vendors bring.

In 2026, CISOs mainly describe AI supporting in most of the NIST CSF functions, except Recover.

AI Powered Security Tooling Maturity (1-5)	2026
1	29%
2	43%
3	19%
4	9%
5	0%

Here we list a few examples of AI-Powered Security Tooling for the NIST CSF Functions:

GOVERN

Maturity rating and risk management, policy generation, compliance automation

IDENTIFY

Asset discovery, risk assessment, supply-chain risk scoring, data classification

PROTECT

Awareness training, SAST/SCA remediation assistance

DETECT

MDR, XDR, SIEM, identity monitoring, antivirus, phishing analysis, SAST, SCA, secrets scanning, fraud detection, other forms of anomaly detection, threat intelligence enrichment

RESPOND

SOAR, case summarization

Talent Acquisition Challenge Turned into a Capability Design Solution

Regarding Workforce & Competence, 2026 marks a shift from a talent acquisition challenge to a capability design solution, in which technology advances, automation, and outsourcing are now part of distributed capability design patterns. The difficulty of hiring senior talent persists, but entry-level talent has become more easily accessible, reflecting better cybersecurity education and increased interest in the field.

> *Finding true senior security talent remains extremely difficult. Organizations often undervalue experience by over-emphasizing diplomas and certifications rather than practical capability.*

The increasing regulatory pressure, which we already saw in 2024 and particularly in relation to NIS2 and DORA, intensifies demand for senior GRC professionals.

> *I honestly wonder where all the people required for things like NIS2 will come from?*

Faced with recruitment and budgetary constraints, CISOs identify new ways of building capabilities. One common approach to solving the recruitment challenge is to find talent internally and train them. Another is to remove the need for certain talent in the first place, as stated before. This involves shifting capabilities into IT, potentially automating them, or simply outsourcing them, thus yielding smaller security teams. As one respondent explains:

> *We outsource IAM, SOC, and OpSec because it would be too boring and difficult to retain talent internally, we maintain a small core team focused on architecture and incident response.*

Retention, while still relevant, appears less problematic than recruiting highly specialized profiles. 23% of CISOs claim they can retain staff once hired.

The shift to distributed capability design patterns requires something different from CISOs. Rather than recruiting and managing a centralized security workforce the old-fashioned way, the CISO increasingly acts as a holistic capability designer and orchestrator of distributed capabilities.

From Seeing Threats to Thinking Risks

Closing Statement

We feel both inspired and grateful! It has been a true pleasure conducting the interviews and taking part in your perspectives on the rapidly ever-evolving world of cybersecurity. Your reflections have provided us with rich material, which, after analysis, has resulted in powerful insights being the foundation of this report.

Energized by these insights, we feel emboldened to offer some foresight:

As stated, we see a maturity shift in which the identification and scrutiny of dimensioning threats are being translated into business risks that inform the security program budget.

Cybersecurity is about prioritizations, and they should be based on risk. Enterprise Risk Managers need to leverage strategic threat intelligence to build well-formed threat scenarios, in addition to regulatory compliance, and to have these ingested together with relevant business and incident metrics into the annual enterprise risk management process. The strategic threat scenarios then need to be broken down into tactical scenarios for the CISO to assess risk and identify the security program's budget needs. The broken-down tactical threat scenarios, including TTPs, will also serve as input in the design and prioritization of necessary cybersecurity capabilities, part of the strategic cybersecurity roadmap.

This is how the cyber risk formula is applied pragmatically to result in a risk-based, intelligence-driven approach ready to be augmented by AI to face the accelerating times.

Once you have this systematic approach in place, you may quantify risk and calculate return on investment (ROI), where ROI is calculated in terms of the relationship between security investments and the reduced cost of disturbances in key business processes.

Then a note on recovery. We need to complement the focus on ransomware and immutable backups with a deeper understanding of how to automate the manual art of recovery through "Continuous Disaster Recovery" within the DevSecOps umbrella to improve resilience and decrease business disturbance.

Another area of foresight relates to compliance automation. Despite the benefits, regulation introduces substantial friction. Organizations spend thousands of hours ensuring compliance, reporting, and adapting data processing and operations. In response, there is the emergent field of compliance automation. Though in its early stages, we look forward to sharing experiences on the topic, where we do not only include compliance with regulation (external requirements) but also internal policy. Today, with modern technology, it is possible to render a digital twin of your threat landscape, regulatory requirements, business landscape, and cybersecurity capabilities, and at any given point in time, assess the current posture as well as regularly report this posture to the supervisory authorities, for example, NIS2 and DORA.

Finally, on a more philosophical note, regarding whether CISOs are or are not C-suite. Maybe with the advent of AI and the need to govern both AI and security in tandem, it is time to consider the combined role of "Chief Cybernetics Officer" to manage the higher concept of business decision intelligence.

Thus, we conclude this year's report, bringing us back to the theme: Entering an Era Beyond Human Speed. For this year's edition, we introduced it as a direct question: If you were to provide a slogan for the times we are in, capturing the zeitgeist and summarizing what we see on the horizon, what would it be?

The CISOs shared impressions that together conveyed the same image: speed, unpredictability, uncertainty, trusting nothing and no one, a return to basics, and resilience. The ghost image of an unknown beast appeared, but it didn't inflict despair among you; it inspired confidence.

Audaciously, we summarize,
quoting one of our participating CISOs:

> **This will be the second dot-com thingy, at least this time I'm a little prepared!**

TRUESEC

Prevent Breach & Minimize Impact

Truesec is an international cybersecurity company with a clear mission: to prevent breaches and minimize their impact when they occur. We deliver market-leading Managed Security Services, expert advisory, and rapid incident response to organizations facing today's most advanced cyber threats.

Truesec operates the largest Security Operations Center (SOC) in the Nordics and has completed more than 120,000 hours of incident response. By combining deep expertise with AI-driven methodologies and advanced analytics, we strengthen protection, improve precision, and enable faster, more informed security decisions.

Since 2005, Truesec has protected organizations across both the private and public sectors worldwide, including critical infrastructure and OT environments that require specialized defense. Today, Truesec consists of more than 400 cybersecurity specialists and plays a leading role in strengthening cyber resilience in the Nordics.

Learn more at truesec.com


TRUESEC