



**TEVORA™**

# 2025 CISO Trends Report

TRENDS IN CYBERSECURITY  
FOR THE COMING YEAR



# Introduction

## THE EVOLUTION OF ACCOUNTABILITY

The last year has been turbulent for Chief Information Security Officers (CISO). The year was packed with jumbo-sized, headline-making cyberattacks and historic, business-disrupting tech outages that drew the world's attention to the growing importance of digital resilience. The practical implications of these tech and security events have put cybersecurity, risk, and compliance under an unforgiving microscope.

For the CISOs tasked with managing and monitoring these critical functions, the pressures are amplified by hard-to-forget instances where executives have suffered serious consequences for security missteps:

- ▶ [Telco CEO Resigns After 14-Hour Outage After Software Update](#)
- ▶ [Clorox CISO Leaves After Network Breach Causing Production Shortages and Financial Losses](#)
- ▶ [UnitedHealth CEO and CISO draw public ire from Senator in open letter calling the CISO “unsuitable” for his role](#)

## THE UNCERTAIN IMPACT OF LOPER BRIGHT

Just as penalties are becoming more severe, the goal posts are also beginning to waver. In June of 2024, the U.S. Supreme Court overturned a precedent and doctrine called Chevron deference, which had been a cornerstone of administrative law for 40 years. The case overruling Chevron, [Loper Bright Enterprises v. Raimondo](#), determined that courts, rather than federal agencies, will now have the primary role in interpreting ambiguous laws.

This change may lead to more legal challenges to existing cybersecurity regulations enforced by agencies like the FTC, SEC, and [Cybersecurity and Infrastructure Security Agency](#) (CISA). The decision may result in increased scrutiny of regulations, potential delays in enforcement, and varied interpretations of cybersecurity laws across different jurisdictions. To anticipate the expected uncertainties, CISOs should be prepared to work even more closely with General Counsel and their legal teams. Keeping a close watch on case law on the regulation of edge cases may provide a window into precedents as they are set.

## HAVE YOU CHECKED IN ON YOUR CISO FRIENDS LATELY?

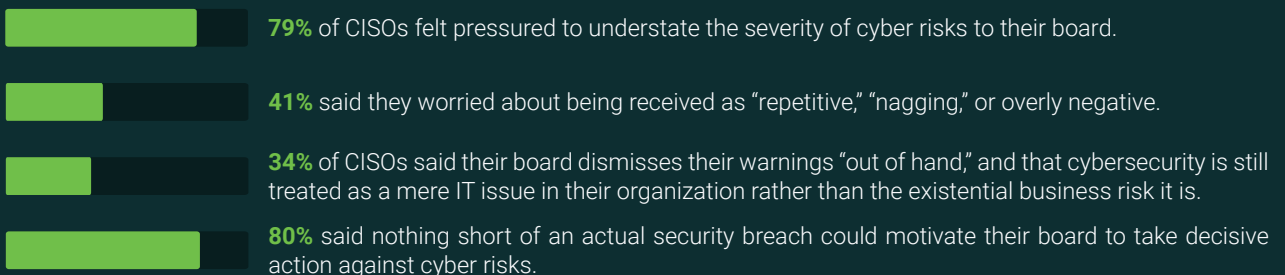
Organizations are more vulnerable than ever to cyberthreats, which can lead to significant financial losses, reputational damage, and legal consequences. As a result, the Chief Information Security Officer's role is increasingly pivotal in guiding organizations toward stronger cybersecurity practices. That hasn't made their job any easier, as CISOs must navigate complex challenges, such as balancing limited resources with the need for comprehensive security measures.

Given the evident risks and pressures, the critical role of the Chief Information Security Officer is both expanding and evolving in opportunistic and reactive ways, depending on the makeup of their particular organization. The role has become highly adaptive as security leaders make adjustments based on the perceived next biggest risk to their organization.

## SECURITY LEADERS ARE UNDER FIRE

More responsibility, more uncertainty, and greater consequences for missteps are pushing CISOs to their limits. Further exacerbating the issue, they aren't always getting the support they need to achieve their security vision.

Trend Micro surveyed 2,600 IT leaders with cybersecurity responsibilities for its report, [The CISO Credibility Gap: How a Communication Breakdown in the Boardroom is Hurting Cyber-Resilience](#). The results were shocking:



# State of the CISO

Tevora's *2025 CISO Trends Report* is a compilation of the insights and trends that our experienced team of consultants have observed through hundreds of client engagements over the past year. The trends captured here aim to give security and technology leaders an idea of where the industry is going in the coming year based on the direction of their peers. This report will inform strategic planning for the coming year and help security and technology leaders feel more prepared to create enhanced cybersecurity in their organizations.

This report is divided into four key categories, each addressing an emerging trend:

1. **Proactive Measures** discusses the importance of anticipating cyberthreats before they occur and outlines strategies that CISOs can implement to stay ahead of potential attacks.
2. **Do More with Less** examines the role of resource optimization, highlighting how organizations can maintain robust cybersecurity defenses even with limited budgets and staffing.
3. **Privacy & Data Governance** outlines the policies and practices essential for protecting sensitive information and ensuring compliance with legal and regulatory requirements.
4. **The Age of AI** explores the impact of artificial intelligence on cybersecurity, emphasizing how organizations can leverage AI technologies to enhance security measures while also navigating the new risks they present.

Together, these trends provide a forward-looking guide for CISOs and other stakeholders to build a more accountable and resilient cybersecurity framework — one that is well positioned to anticipate and respond to the most pressing issues facing digitally-enabled organizations today.



# Category 1:

## PROACTIVE MEASURES

Mitigating risk to the extent possible means anticipating cybersecurity challenges and positioning your organization to defend against – or recover from – as many threats as possible. Organizations looking to fully cover their bases are increasingly leveraging the following proactive measures to best position their organizations:

1. Establishing Cyber Resilience
2. Taking Lessons from Recent Breaches: Analyzing the Threat Landscape
3. Tracking Fourth-party Risk

## Trend 1: ESTABLISHING CYBER RESILIENCE

Cyber resilience of core technical functions has emerged as a fundamental aspect of organizational security. In particular, identity resilience in relation to the ever-critical Identity Access Management environment, has emerged as a particular hot topic among security leaders. With digital identities serving as the gateway to sensitive information and critical systems, protecting them is fundamental to maintaining a secure environment.

### WHAT IS IDENTITY RESILIENCE?

Identity resilience describes the ability of an organization to recover after a disruption prevents or limits access to their Single Sign-On (SSO) via their Identity Access Management (IAM) system. Essentially, identity resilience ensures that even if a breach occurs, the impact is minimized, and recovery is swift.

Most every organization today is now prioritizing strengthening the resilience of their identity systems, and there are several topics of conversation that regularly arise among security and technology leads:

- ▶ **IAM Backup & Restore:** Ensures IAM systems are sufficiently backed up to allow for quick recovery
- ▶ **Identity Provider (IdP) Failover Readiness:** Increasingly, companies are maintaining two parallel IAM tenants in separate IdPs, allowing for a fully functional backup tenant in the event of an emergency
- ▶ **Identity Disruption Response:** The ability to respond to external threats to identity.

**“ITDR is another buzzword that frequently pops up in conversations with security heads. It’s often defined in different ways, but everyone knows they need it as part of their security strategy. In many ways, ITDR is an expansion of SOAR (Security Orchestration and Automated Response) with the added layer of identity.”**

— Ben Dimick, Tevora’s Director of Security Consulting

### ACTIONABLE WAYS TO INCREASE IDENTITY RESILIENCE

As more real-world examples show the dangers of an IAM outage or attack, CISOs are asking tougher questions about the resilience of their identity systems. Some of the steps they’re taking include:

#### 1. Questioning Identity Providers of the availability of backups.

While identity providers sometimes provide basic backups, those backups are often insufficient to be practically usable in an emergency situation. Those backups are often performed infrequently (if at all), and generally do not include the critical configurations that render the data useful. Most IdPs - and many SaaS solutions generally - maintain that it is the client’s responsibility to maintain backups.

#### 2. Testing existing IAM backups for usability.

Even those who maintain regular backups may find that in the case of a disruption of service, the backup data is not functional in a practical sense. Testing backup and restore functionality is the only way to ensure that recovery time (RTO) is kept low if the system were to become unavailable.

#### 3. Preparing a failover scenario.

As mentioned above, companies are increasingly maintaining duplicate IAM environments to serve as a potential failover in the event of an emergency. We have seen an increase in the popularity of this tactic, especially as the fallout of [recent IAM-related breaches](#) have shown to inflict significant damage.

### BETTER SAFE THAN OUT OF LUCK

Beyond IAM solutions, the importance of cyber-resilience extends to all critical IT infrastructure and services. The lack of a functioning business continuity strategy is no longer acceptable, and proactive planning is paramount. We expect this emerging trend to continue to grow as companies allow their business continuity and disaster planning to catch up to today’s realities.

## Trend 2: TAKING LESSONS FROM RECENT BREACHES

### Analyzing the Threat Landscape

The frequency and sophistication of breaches are increasing, underscoring the need for proactive measures to safeguard organizational assets. But there is much to learn from these damaging events. Effective cybersecurity strategies often derive from a deep understanding of breach trends. They reveal vulnerabilities, attacker methodologies, and evolving threat landscapes, enabling organizations to adapt their defenses and stay ahead of emerging risks. This section explores the latest breach trends and outlines how Chief Information Security Officers can take a proactive approach to enhance their cybersecurity planning.

#### ATTACKS GROW IN SCOPE AND SOPHISTICATION

Recent breaches reveal several alarming trends. Advanced phishing attacks have become more prevalent, with targeted techniques such as **spear phishing** and **Business Email Compromise (BEC)** posing significant risks. These attacks exploit human vulnerabilities and are often difficult to detect. Ransomware attacks have also surged, particularly with **double extortion** tactics, where attackers not only encrypt data but also threaten to release it publicly. This trend is a reminder of the invaluable role of penetration testing and vulnerability detection combined with strong data encryption and regular backups.

Concurrently, **supply chain attacks** are increasingly common, as attackers exploit vulnerabilities in third-party vendors to gain access to target organizations. Additionally, insider threats, both malicious and unintentional, are a growing concern, with insiders sometimes providing attackers with unauthorized access. Finally, the rapid exploitation of vulnerabilities in widely used software and platforms, such as in the **XZ Utils backdoor** and the **CrowdStrike outage**, expose the criticality of maintaining up-to-date security measures and the unavoidable interconnectedness of modern digital ecosystems.

These breach trends have significant implications for CISOs. There is an urgent need for advanced threat detection and response capabilities to identify and mitigate sophisticated threats in real time. Managing vendor and third-party risks has also taken on new importance, requiring thorough vetting and continuous monitoring of external partners. As has the job of enhancing security awareness and training programs that equip employees with the knowledge to recognize and respond to phishing and social engineering attacks. Strengthening incident response plans in light of these trends ensures that organizations can swiftly contain and mitigate a breach.

**To address these challenges, CISOs should adopt several proactive cybersecurity planning strategies:**

- ▶ **Implement a Zero Trust Security Model:** Assume no user or system is inherently authorized and require continuous verification of all access requests (**Major federal agencies are required to have implemented a Zero Trust Model as of September, 2024**).
- ▶ **Regularly Update and Patch Systems:** Close vulnerabilities and protect against known exploits.
- ▶ **Utilize Threat Intelligence:** Anticipate potential attack vectors and prepare accordingly.
- ▶ **Automate Security Processes:** Enhance defenses by reducing response times and minimizing human error.
- ▶ **Collaborate Across the Organization:** Foster a security-first culture that ensures that cybersecurity is a shared

## CURRENT THREAT LANDSCAPE: MAJOR CYBERSECURITY INCIDENTS IN 2024

### ***U.S. Social Security Number Data Breach***

A massive data breach in December of 2023 at National Public Data, a background check company, exposed a huge trove of personal financial records. The exact number of affected records is unclear, with estimates ranging from **1.3 million to 2.9 billion**. By April of 2024, the data had begun leaking on criminal message boards. Potentially compromised information includes Social Security Numbers (SSN), names, email addresses, phone numbers, and mailing addresses. Experts recommend freezing credit with all three major credit bureaus as a primary protective measure. But, unfortunately, it seems that millions of Americans can no longer assume their SSN is private.

### ***Microsoft Midnight Blizzard Attack***

On January 12, 2024, Microsoft detected a nation-state cyberattack against corporate email systems. The threat actor was later identified as **Midnight Blizzard** (also known as NOBELIUM), a Russian state-sponsored group. Midnight Blizzard is known to use exfiltrated information to gain or attempt unauthorized access to source code repositories and internal systems, and hence Microsoft notified affected customers whose shared secrets may have been exposed in the exfiltrated emails. In February of 2024, Microsoft determined the attack had intensified, with **password spray** attempts increasing tenfold.

Some Azure Cloud tenants were affected due to the attackers' ability to access development tenant keys, which granted them high-level access to main Azure resources. This incident demonstrates that organizations can become victims simply based on the tools and services they utilize, regardless of their own security practices.

### ***XZ Utils Backdoor***

In February 2024, a sophisticated backdoor was discovered in versions 5.6.0 and 5.6.1 of the Linux utility **xz** within the **liblzma** library. Luckily, a researcher caught the vulnerability before it went into production. The backdoor could have given attackers remote code execution capabilities on affected Linux systems.

The incident sparked discussions about the security of critical open-source infrastructure maintained by volunteers and revealed that many large organizations rely on these resources. It's also an alarming story of a criminal playing the long game and gaining trust with a code maintainer. If undetected, this backdoor could have potentially affected millions of computers worldwide that use Secure Shell (SSH).

It should also serve as a wakeup call for organizations CISOs that have neglected to fully consider supply chain attacks to begin more active threat hunting in that area and to better train defensive teams to address these types of downstream vulnerabilities.

### ***Snowflake and Ticketmaster***

**Snowflake**, a cloud storage firm, revealed in June of 2024 that hackers had breached their security and exfiltrated data. About 165 customer accounts were potentially affected, including Ticketmaster, Santander, Lending Tree, and Advance Auto Parts. The hackers claim they gained access to some Snowflake accounts by first breaching EPAM Systems, a contractor that works with Snowflake customers. The hackers also used old credentials stolen by **infostealer malware** to access some Snowflake accounts. The incident lays bare the security risks associated with third-party contractors and the persistent threat of stolen credentials from infostealer malware.



### **CrowdStrike Outage**

On July 19, 2024, **CrowdStrike** distributed a faulty update to its Falcon Sensor security software. The update caused widespread crashes of Microsoft Windows computers, affecting approximately 8.5 million systems, making it the largest outage in IT history. Affected industries included airlines, banks, hospitals, manufacturing, and stock markets, and the estimated financial damage was pegged at least \$10 billion worldwide.

The outage starkly highlighted the importance of a **DevSecOps** approach to software that integrates security into every phase of the development process, as well as quality assurance, and Continuous Integration and Continuous Delivery (**CI/CD**) practices. CD pipelines often include staging environments that mirror production. Testing in these environments could reveal issues that might not appear in more limited test scenarios.

### **THE BIG PICTURE**

The major cyber incidents of 2024 should remind CISOs that comprehensive Business Continuity and Disaster Recovery (**BCDR**) planning and resilience strategies are their best hope of avoiding seeing their organization on the next headlining security breach.

Organizations must adopt a proactive stance towards threat intelligence, incorporating offensive strategies to identify and address vulnerabilities before they can be exploited. Regular tabletop exercises should be an integral part of business continuity planning, enabling teams to simulate and prepare for various cyber attack scenarios. Furthermore, the increasing reliance on cloud services seen across industries necessitates robust cloud monitoring practices to detect and respond to threats in real-time.

These incidents highlight the need for a holistic approach to cybersecurity through total exposure management, which considers all potential attack vectors, including supply chain vulnerabilities, insider threats, and third-party risks.

### **KnowBe4 Hires a Fake Employee**

In July of 2024, **KnowBe4**, a security training company, discovered and fired an employee who was secretly a North Korean IT worker, despite thorough vetting processes including video interviews and background checks. North Korean workers have become adept at bypassing U.S. hiring practices to illegally obtain remote jobs, using AI tools to alter their voices and images. The incident highlights both the growing threat of insider risks and the challenges faced by even cybersecurity-focused companies in preventing such infiltrations, particularly given increasingly convincing AI tools for image, audio, and video manipulation.

## Trend 3: TRACKING FOURTH-PARTY RISK

Fourth-party risk is increasingly cropping up in conversations with security leaders. In layman's terms, a fourth party is your vendor's vendor. Fourth parties are organizations you do not touch directly, but who may impact your organization through their relationship with your vendors.

### ADDRESSING FOURTH PARTY RISK: VENDOR REVIEW ASSESSMENT

Vendor risk management must extend beyond third-party relationships to include fourth-party vendors, which pose significant risks due to limited visibility. To mitigate these risks, organizations should conduct thorough vendor review assessments, ensuring that security standards and compliance requirements extend to fourth parties. This includes:

- ▶ Reviewing contracts
- ▶ Mandating adherence to security minimums
- ▶ Establishing clear Service Level Agreements (SLA) that cover fourth-party performance
- ▶ Updating and maintaining an accurate SBOM

Strict vendor oversight ensures companies can better manage their total exposure and maintain a more secure vendor ecosystem. To proactively manage fourth-party risk, organizations can implement several strategies:

- ▶ Identify critical vendors
- ▶ Map fourth-party vendor relationships
- ▶ Categorize vendors by risk and include inherent risk as a key factor for establishing control requirements
- ▶ Secure the extended supply chain

### LESSONS FROM CROWDSTRIKE:

#### VENDOR ECOSYSTEMS ARE VAST AND INTERDEPENDENT

Last summer's disastrous [CrowdStrike outage](#) sparked renewed interest in fourth-party risk management among security leaders. The impact of the outage extended beyond CrowdStrike's direct customers, affecting organizations that relied on services provided by CrowdStrike's clients, highlighting the intricate web of dependencies in modern digital ecosystems.

The outage was a wakeup call for CISOs who saw that the efficiency and reliability of their organization's operations could be severely impacted by vulnerabilities in fourth-party relationships they might not even be aware of. This realization has prompted security leaders to reevaluate their approach to risk management, emphasizing the need for deeper visibility into the entire supply chain. CISOs have begun undertaking comprehensive vendor risk assessments that look beyond immediate suppliers.

#### THE CRITICAL NATURE OF THIRD AND FOURTH-PARTY RELATIONSHIPS

While fourth party risk is a current hot topic among security leaders, it cannot be separated from a conversation about third parties. With both the third and fourth parties in the mix, the concept of a carefully maintained SBOM (Software Bill of Materials) continues to be a highly relevant security discussion.

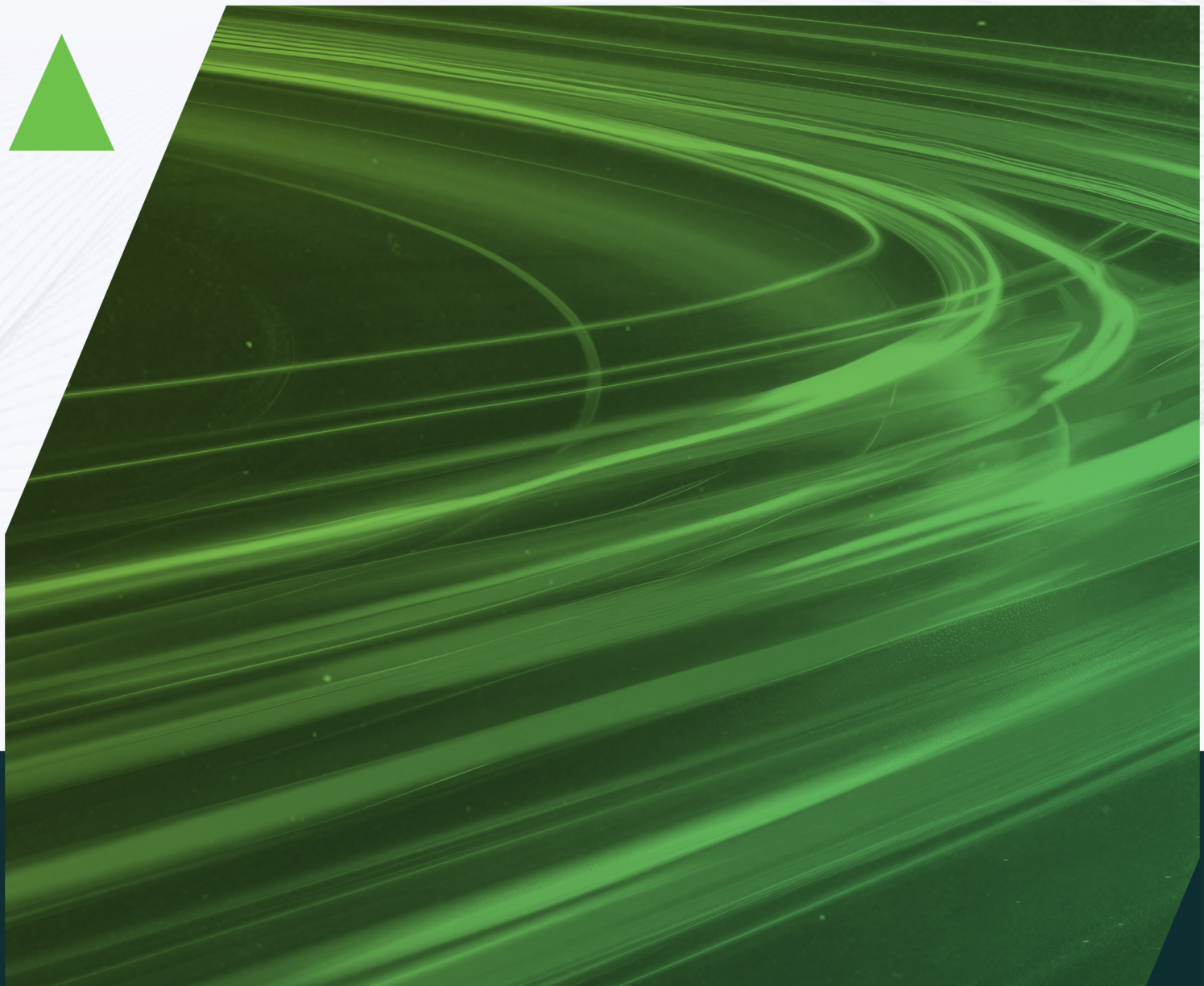
A close inventory of the SBOM continues to be a significant tool in the facilitation of scanning and testing for vulnerabilities. If a breach or incident is to occur, an updated SBOM can also help identify and rectify the source of any issues.



#### ▶ Bonus Tip

#### THE BENEFIT OF CLIENT TRUST PORTALS

For those who find themselves playing the role of a third party, Tevora is finding an increase in the use of Client Trust portals to help communicate security practices to new and existing clients. A Client Trust portal can sometimes circumvent the need for lengthy security questionnaires by publishing the organization's security practices and compliance certifications. Client Trust Portals (also called Trust Centers) may be available publicly on the company's website, or may be password-protected.



# Category 2:

## DO MORE WITH LESS

Many security leaders deal with the challenge of being “budget constrained.” As a continuously evolving and advancing field, resource allocation for security initiatives seems to consistently lag behind need. It’s no surprise that as CISOs prepare for the coming year, many are seeking creative ways to ensure maximum effectiveness of the dollars and resources at hand. And as business confidence in the US has continued to fluctuate, some security leaders are seeing their budgets constrict, despite the onslaught of high-profile cybersecurity incidents. This section will explain how CISOs navigate the tradeoff between what they need and what they have budgeted.

## Trend 1: TOOLS RATIONALIZATION

### Building a **Cybersecurity Platform**

Cybersecurity software and tools are a uniquely complex market. Because the pace of change is so rapid – both in terms of evolving threats and new software entrants – a company’s security tech stack can quickly become outdated or overcomplicated. Oftentimes, the need for a tech stack evaluation is not apparent.

**“We often see the need arise when working with a client on a recommendation for a specific tool, and during in-depth discovery, it comes to light that they have multiple tools capable of closing the use case. The process of finding a solution for a specific need requires understanding of how tools are currently deployed, integrated, and licensed to uncover deficits or shortcomings, thus triggering a larger security posture and tool rationalization conversation.”**

– Mark Broghammer, Tevora’s VP of Architecture

A comprehensive and rigorous tool rationalization process is recommended at least once every three years, but many things can alter that timeline, such as a merger or acquisition.

**“We see a lot of tool rationalization projects when the economy dips or is uncertain. Reducing redundant or unnecessary tools can be an easy win for a security leader.”**

– Ben Dimick, Tevora’s Director of Security Consulting

#### THREE STAGES OF TOOL RATIONALIZATION

A tool rationalization exercise typically progresses through three levels of analysis:

1. Do I have tools that are truly redundant?
2. What capabilities are we actually using, and what is the minimum coverage I really need?
3. Are my tools really effective in these controls?

The ideal outcome is a cybersecurity platform that works optimally for a given organization. That does not always mean best-of-breed, only that it matches all critical requirements at the lowest burden. Vendor consolidation can also help cut costs with adequate coverage from a minimum viable criteria set. Ultimately, the reality in these scenarios is that a 100% perfect platform may not be feasible either due to budget, team constraints, or other factors. The target instead is to get the organization to accomplish 80% of their goals using the resources at hand.

#### ASSESSING THE SECURITY STACK

From the CISO level, the objective is to identify true defense-in-depth and complementary functionality, gaps in security function coverage, and overlaps and redundancy in security function coverage. For example, they might look at how their **HIDS** (Host-based Intrusion Detection System) overlaps with their **NIDS** (Network-based Intrusion Detection System). Together, they provide complementary coverage where HIDS detects local attacks that might not be visible on the network and NIDS scans for broader network-based threats that might affect multiple hosts.

That's a situation where the redundancy is synergistic and beneficial. However, in other cases, such as with antivirus products, overlap can be counterproductive. If an organization is running multiple services to protect endpoints from malware and viruses, each may have unique features, but their core functionalities will have significant overlap. This can sometimes lead to conflicts, reduced system performance, or false positives – not to mention unnecessary expenses.

#### A SHORT-TERM EXERCISE FOR LONG-TERM IMPACT

"The best advice I can give for a tool rationalization project is to get ahead of it!" says Dimick. "If you know budget cuts are coming, start the process early." Because an effective assessment or platform rebuild can take some time, he argues its best to start before a budget cut comes. Dimick also makes the case that there is a valuable return on investment for these practices. "Spend some money to figure out how to save money, and invest time and money into automation. Both will save you a ton later on," he explains.



#### Bonus Tip

#### ELEVATING YOUR CYBER HYGIENE

Did you know that the Federal government offers free Cyber Hygiene services? While not a complete replacement for Web Application Scanning (WAS) solutions, CISA (Cybersecurity & Infrastructure Security Agency) provides free continuous scanning services and reporting to registered organizations. This is a cost-effective way to augment your security toolbox and provide greater coverage than a single solution alone. CISA's WAS service will conduct regular vulnerability scans and web application scanning for your publicly accessible digital properties. Registered organizations receive weekly readout reports, plus immediate alerts regarding critical vulnerabilities. For more information, visit the [CISA Cyber Hygiene Services page](#).

## Trend 2: PURPLE TEAMING

Purple teaming is a collaborative security methodology that combines the efforts of red teams (offensive security professionals) and blue teams (defensive security professionals) to enhance an organization's cybersecurity capabilities. It represents a shift from siloed security operations to a more integrated and adaptive approach, helping organizations stay ahead of evolving cyber threats. While not less expensive than other tactics like red teaming, purple teaming can be more targeted and efficient.

Often more targeted than an extensive red team exercise, some security leaders are postponing the more thorough efforts and turning to purple teaming to sufficiently explore their defensive stances in the short term.

### THE LIMITS OF PEN TESTING

Traditional red team exercises often don't adequately validate security investments on their own. **Penetration tests** and red team exercises focus on finding and exploiting vulnerabilities or creating a specific attack path. This narrow focus may not comprehensively evaluate all security controls and investments.

Most red teams only run a single variation of an attack to show and produce impact. This methodology doesn't test the full range of potential attack vectors or variations that real-world adversaries might use. These traditional methods also often emphasize successful exploitation rather than evaluating an organization's ability to detect and respond to various attack stages, and they frequently focus too heavily on perimeter security, neglecting internal detection and response capabilities.



### SECURITY THROUGH COLLABORATION

The main goal of purple teaming is to improve vulnerability detection, **threat hunting**, and network monitoring through continuous feedback and knowledge transfer between red and blue teams. Unlike traditional approaches where red and blue teams work separately, purple teaming encourages ongoing, cross-team communication to maximize efficiencies and impact.

#### *Purple Team Benefits:*

- ▶ Enhanced security knowledge
- ▶ Improved performance without increasing budget
- ▶ Streamlined security improvements
- ▶ Critical insights into security gaps
- ▶ May have a shorter timeline than other approaches

Purple teaming can be implemented as focused engagements with defined goals and timelines, or as an ongoing conceptual framework throughout an organization.

## TESTING DETECTIVE AND PREVENTIVE CONTROLS

Detective controls identify and alert on potential security incidents or unauthorized activities. Examples include Intrusion Detection Systems (**IDS**), Security Information and Event Management (**SIEM**) systems, and log monitoring tools. Purple Teaming tests these systems by:

- ▶ Simulating various attack techniques and observing if they're detected
- ▶ Evaluating the accuracy and timeliness of alerts
- ▶ Assessing the Blue Team's ability to recognize and respond to these alerts

Preventative controls, by contrast, stop unauthorized actions or access before they occur. Examples include firewalls, access control systems, and endpoint protection platforms. A purple team can test these controls by:

- ▶ Attempting to bypass or circumvent these controls using various attack methods
- ▶ Evaluating if the controls successfully block or prevent unauthorized actions
- ▶ Identifying any weaknesses or gaps in the preventative measures

By testing both types of controls, Purple Teaming provides a holistic view of an organization's security posture. It helps identify where preventative controls might fail and whether detective controls can compensate for those failures. Furthermore, this approach mimics real-world attack scenarios where adversaries might attempt to bypass preventative controls and remain undetected.

## EXPOSING BLINDSPOTS

Because purple teaming can simulate attacks capable of bypassing detection-based security products the way that **Advanced Persistent Threats** (APT) can, it reveals gaps in an organization's security visibility and helps to identify areas where attackers could operate undetected within the network.

It further provides insights into how well the organization can identify and respond to threats when primary detection methods fail, which helps assess the effectiveness of incident response plans and procedures. Purple teaming also encourages the development of proactive threat hunting capabilities and teaches security teams to look for subtle indicators of compromise that automated systems might miss.

## Trend 3: UNIFIED ASSESSMENT

There's no question, the resource burden of a compliance exercise can be significant. This is especially true in highly regulated industries, where five or more compliance standards may be necessary to do business. In these cases, a unified assessment is more commonly used to reduce the time and expense associated with the tedious audit process.

### WHAT IS A UNIFIED ASSESSMENT?

A unified assessment is the act of consolidating multiple compliance audits into a single process.

**“We the assessor are still giving a company the output of multiple reports for compliance framework A, B, and C. Essentially, the burden on the organization’s team is reduced, but you still get all the desired compliance outcomes.”**

— **Ashli Pfeiffer**, Tevora’s Managing Director of Information Security Consulting and SOC Compliance Practice

While unified assessments are not a new invention, CISOs and compliance leaders are considering them more frequently as a “low hanging fruit” tactic to minimize the compliance burden on already overstretched teams. Common frameworks that are included in a Unified Audit:

- ▶ PCI DSS
- ▶ PA-DSS/PCI SSF
- ▶ ISO 27000 Series
- ▶ STAR
- ▶ SOC 1/ SOC 2
- ▶ MPAA
- ▶ FedRAMP
- ▶ FISMA
- ▶ HIPAA
- ▶ HITRUST
- ▶ NIST 800-53
- ▶ NIST 800-171

Generally speaking, companies that move from individual audits to a unified assessment recognize the benefits immediately. This is especially true of teams dealing with audit fatigue. “Often, a team feels like they’ve barely caught their breath with one compliance effort before the next begins. Unified assessment helps with that,” says Pfeiffer.

### HOW NOT TO USE A UNIFIED ASSESSMENT

Despite its many advantages, a unified assessment is not always the answer. Companies undergoing transitions or periods of change — such as mergers and acquisitions or reorganizations — may not reap the same benefits as those with more stable operations. It’s also unwise to attempt it in the middle of a major version change with a framework, or to try and perform it all at once.

An overly ambitious transition to unified assessments can end up causing more issues than it solves. Instead, take a more measured approach that accounts for both the practical aspects of aligning controls and the timing requirements of various certifications.

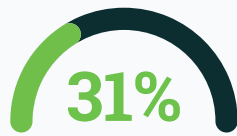
For example, consider moving from five separate audits to three unified ones in the first year, rather than jumping directly to a single unified audit. This gradual transition is more manageable and less risky. That also harmonizes the timing of certifications. Different compliance frameworks may have different certification cycles or renewal periods. Gradually unifying audits allows organizations to align these certification timelines more effectively.



A strategically planned **assessment process** avoids the pitfalls and maximizes the benefits, delivering significant efficiencies:



65% average reduction in staff time spent on audit and compliance efforts



31% average reduction in internal resource costs



10% average reduction in certification costs



100% increase in consistency of collected evidence

### WHY COMPANIES PURSUE A MULTI-STANDARD COMPLIANCE ASSESSMENT

- ▶ **Synchronized Review:** A single assessment covers multiple security standards simultaneously
- ▶ **Enhanced Efficiency:** Leverages common elements across standards to reduce audit fatigue for staff and removes friction from the certification process
- ▶ **Comprehensive Coverage:** Assists with achieving and maintaining compliance across various industry security standards
- ▶ **Client-focused Approach:** Long-term relationship outlook with an emphasis on client satisfaction and continued partnership
- ▶ **Expertise and Customization:** Industry knowledge and security expertise powering solutions tailored to specific needs
- ▶ **Streamlined Services:** Packaged, easy-to-understand services based on extensive experience in the field
- ▶ **Cost and Time Savings:** Consolidating multiple audits into one approach reduces expenses and accelerates compliance

## Trend 4: MANAGED SECURITY PLATFORMS

### Partnering & Outsourcing

As the stakes continue to rise, many CISOs are turning to outsourced managed security programs to bolster their defenses. They may bring experts in for finite, impactful engagements when they have limited staff, or when highly specialized skills make a full-time hire impractical.

More and more often, the use of specialized outsourced support is especially common for tool implementation or management. As cybersecurity tools have gotten increasingly specialized, they may require focused experience and expertise to effectively manage. When resources are limited, outsourcing can be the right answer rather than bringing that specialization in house.

#### TURNING TO OUTSOURCED PROFESSIONALS

There are multiple reasons why many tech leaders are turning to outsourced talent. Finding qualified candidates is time-consuming and expensive, and high demand for skilled professionals leads to turnover, risking knowledge loss. There are also a number of financial advantages associated with choosing the outsourced route instead:

- ▶ **Liquidity:** Outsourcing shifts costs from CapEx to OpEx, reducing upfront expenses, improving cash flow, and increasing flexibility by spreading costs over time.
- ▶ **Economies of Scale:** Managed Security Service Providers (MSSPs) can offer services at a lower cost due to their scale and expertise.
- ▶ **Predictable Budgeting:** Fixed pricing models allow for better financial planning and cost predictability.

More specifically to cybersecurity, CISOs are keenly aware of the shortage of skilled cybersecurity professionals. According to a 2023 report by ISC2, [the global cybersecurity workforce gap has reached over 3 million professionals](#). This talent crunch makes it challenging for organizations to build and maintain in-house security teams capable of addressing current and emerging threats.

#### SUPPLEMENTARY GRC SUPPORT

For the day-to-day task overflow that plagues internal security teams, access to a flexible, skilled Governance Risk and Compliance (GRC) talent can provide significant benefits. Some of the specialized skills that can be outsourced include:

- ▶ General GRC Support for day-to-day GRC Activities
- ▶ Technical writing-policy and procedures
- ▶ Development and implementation of common control framework to meet compliance and regulatory obligations

When evaluating external resources to supplement internal teams, it is important to be clear on evaluation criteria and requirements. Some of the important factors to evaluate include:

- ▶ **Expertise:** Level of qualifications and specific alignment with your requirements
- ▶ **Flexibility:** On-site or remote, full-time or part-time services; hours requirements and contract length
- ▶ **Partnership:** Documented processes and level of collaboration with internal teams
- ▶ **Hands-on approach:** Direct involvement in completing tasks
- ▶ **Goal-oriented:** Emphasis on achieving compliance objectives efficiently

#### EXECUTIVE SUPPORT ON A FRACTIONAL BASIS

In some cases, when more senior security leadership is required, a fractional CISO or CISO "Advisor" can be used to supplement in-house expertise, bring specialized guidance, or set up a strategy for future growth.

This approach is often utilized by smaller or mid-sized organizations, or those whose security leadership is in a phase of transition. Because access to high-level security leadership can be difficult, a virtual CISO (**vCISO**) enables organizations to implement proper security measures without the cost of a full-time executive. It also enables greater flexibility in how companies allocate their security resources.

A fractional CISO can provide comprehensive cybersecurity support, including strategy, governance, program implementation, and education. They can be called upon to fill critical security gaps including:

- ▶ Security Strategy & Roadmap
- ▶ Governance Design
- ▶ Development & Implementation
- ▶ KPI and KRI Development and Regular Reporting
- ▶ Security Program Implementation and Monitoring
- ▶ External Audit Liaison
- ▶ Security Education and Awareness

vCISO experts help their partners implement and manage security solutions, ranging from zero trust architectures, to ERM programs, to secure software development. And when the immediate need lessens, resources can be easily ramped back down with minimal disruption.



# Category 3:

## PRIVACY & DATA GOVERNANCE

Privacy and data governance have become top-of-mind concerns for CISOs in recent years, driven by increasing public awareness and skepticism about data collection practices. A Pew Research Center study found that **62% of Americans believe it's impossible to go through daily life without companies collecting their data**, showing the pervasive nature of data gathering in modern society. This widespread data collection has led to growing unease among consumers, with 81% of users now stating that the potential risks from companies collecting their data outweigh any benefits, according to the same study.

The lack of transparency in data usage practices is also a significant issue, as evidenced by a Tableau survey which revealed that **63% of Internet users believe most companies aren't transparent about how their data is used**. This mistrust has tangible consequences for businesses, with 48% of users reporting they have stopped shopping with a company due to privacy concerns. Furthermore, a Cisco study found that **81% of users believe a company's treatment of their personal data reflects how it views them as customers**. This perception directly ties data governance practices to customer relationships and brand loyalty.

Awareness of the costs of losing private and sensitive data seems only to grow with each year. Cisco also reported that 37% of users have terminated relationships with companies over data issues, an increase from 34% just two years prior. This trend highlights the potential for significant customer churn and revenue loss for companies that fail to prioritize data protection.

In response to these concerns, governments worldwide are implementing stricter data protection regulations, with French tech firm Thales reporting that more than **120 countries have already passed data protection laws** in some form. To add to the complexity, individual states throughout the United States are creating their own privacy laws, as outlined in the following section.

For CISOs, this evolving landscape of consumer expectations and regulatory requirements necessitates a proactive approach to privacy and data governance to maintain customer trust, comply with regulations, and protect their organization's reputation and bottom line.

## Trend 1: PRIVACY IS ON DISPLAY

To match with the increasing public awareness of their own data, security and privacy leaders are becoming more critical of their own compliance with privacy standards. This hyper awareness by public and enterprise has caused an increase of privacy conversations in executive and board rooms.

At its core, data privacy is about giving individuals control over their personal information — how it's collected, used, shared, and stored. It's the right of individuals to keep their personal matters and relationships secret, and to determine for themselves when, how, and to what extent their personal information is communicated to others. The protection of this data involves not just securing it from unauthorized access, but also ensuring its accuracy, integrity, and appropriate use throughout its lifecycle.

### KEEPING UP WITH COMPLIANCE:

#### THE PROLIFERATION OF PRIVACY STANDARDS

Data privacy is heavily influenced by a growing body of regulations worldwide. These laws set standards for how organizations must handle personal data. Key global regulations include:

- ▶ General Data Protection Regulation (**GDPR**) in the European Union
- ▶ California Consumer Privacy Act (**CCPA**) and California Privacy Rights Act (CPRA) in the U.S.
- ▶ Personal Information Protection and Electronic Documents Act (**PIPEDA**) in Canada
- ▶ Lei Geral de Proteção de Dados (**LGPD**) in Brazil

### THE IMPORTANCE OF PRIVACY IMPACT ASSESSMENTS

Many of these data governance frameworks include processes for conducting Privacy Impact Assessments (**PIA**) that help identify and mitigate privacy risks before new projects or systems are implemented. They ensure that privacy considerations are factored into decision-making processes from the outset.

Good data governance promotes transparency in data handling practices with clear communication about how personal data is collected, used, and shared. This transparency builds trust with customers and stakeholders. It also helps organizations meet regulatory requirements for privacy notices and consent management, and it makes it easier for individuals to exercise their privacy rights, such as accessing or correcting their personal data.

### PRIVACY IN REVIEW:

#### TOP-OF-MIND PRIVACY FRAMEWORKS

Despite the waterfall of new rules and regulations across the globe, today's privacy concerns stem from a handful of major compliance frameworks. Of all global privacy frameworks, the GDPR, implemented in 2018, is still considered the gold standard. It applies to all organizations processing personal data of EU residents, regardless of the company's location. GDPR features:

- ▶ Stringent consent requirements
- ▶ Data subject rights (access, rectification, erasure, etc.)
- ▶ 72-hour breach notification
- ▶ Privacy by design and by default
- ▶ Fines of up to 4% of global annual turnover

For example, **Meta (Facebook) was fined \$1.3 billion for GDPR violations** related to data transfers in 2023.

Since GDPR's rise, California has been at the forefront of privacy regulation in the U.S. Effective since 2020, the California Consumer Privacy Act (CCPA) is the first comprehensive consumer privacy law in the U.S., and it was expanded in 2023 by the passage of the California Privacy Protection Agency (**CPRA**) which authorized a new regulator to enforce the law. Under the CPRA, Californians have the right to:

- ▶ Know what personal information is collected
- ▶ Delete personal information
- ▶ Opt-out of the sale of personal information
- ▶ Non-discrimination for exercising rights

While not a recent development, HIPAA remains a top-of-mind privacy concern as technologies expand the reach of sensitive data. On the federal level, **HIPAA** (Health Insurance Portability and Accountability Act) is still considered the most expansive privacy law affecting U.S. companies connected to healthcare. It includes the following privacy and data governance regulations:

- ▶ Privacy standards for individuals' health information protection
- ▶ Security safeguards to protect electronic health information
- ▶ Requires notification of health information breaches

### **RECENT REGULATORY UPDATES**

The growing alarm at mishandled data - and the world's swift adoption of such standards as GDPR and CPRA - has accelerated the passage of new and updated regulations aimed at producing privacy. Some organizations have found themselves unaware and slow to respond to these updates.

Many California companies, for instance, failed to appreciate the effect of a February 2024 decision by the California appellate court which ruled in favor of immediate enforcement of new privacy regulations. This overturned a previous decision that had delayed enforcement until March 29, 2024.

The decision required immediate compliance with new regulations, removed a one-year grace period of compliance that some had expected, and set a precedent for swift enforcement of future regulations.

As privacy concerns grow, new regulations are also emerging across different states:

#### **MONTANA CONSUMER DATA PRIVACY ACT (MCDPA)**

- ▶ Gives Montana consumers rights over personal data
- ▶ Provides guidelines for organizations on how to treat that data
- ▶ Went into effect October 1, 2024

#### **TEXAS DATA PRIVACY AND SECURITY ACT (TDPSA)**

- ▶ Applies to entities conducting business in Texas or serving Texas residents
- ▶ Excludes small businesses (as defined by the U.S. Small Business Administration)
- ▶ Requires consent for selling sensitive personal data
- ▶ Businesses have until January 1, 2025, to recognize **universal opt-out mechanisms**

#### **OREGON CONSUMER PRIVACY ACT (OCPA)**

- ▶ Applies to entities controlling or processing personal data of 100,000+ consumers (or 25,000+ consumers if 25% of revenue comes from selling personal data)
- ▶ Nonprofits are generally not exempt
- ▶ Controllers have until January 1, 2026, to recognize universal opt-out mechanisms

#### **FLORIDA DIGITAL BILL OF RIGHTS (FDBR)**

- ▶ Notable for its narrow applicability
- ▶ Applies to businesses with over \$1 billion in gross annual revenue

As these regulations often share principles like consent requirements, organizations can benefit from adopting a comprehensive privacy program that addresses common **data subject rights** like:

- ▶ Data Deletion or Right To Be Forgotten (**RTBF**)
- ▶ Restrict Processing or **Restriction of Processing** (RofP)
- ▶ Data Access and Export



## Trend 2: DATA AWARENESS

While the importance of data is widely recognized, many organizations struggle with a fundamental issue: they don't truly know their data. Data awareness is the comprehensive understanding of an organization's data assets, including what data you have, where it resides, who has access to it, where it flows, and how sensitive it is.

### THE CHALLENGES OF DATA MANAGEMENT

As organizations continue to accumulate vast amounts of data, they face a growing array of issues in managing this valuable yet complex asset. One significant challenge is the emergence of [data silos](#), where information becomes isolated in different departments or systems, leading to an incomplete view of the organization's data assets. This fragmentation is often exacerbated by [shadow IT](#), as employees may use unauthorized applications or cloud services to store or process data, creating blind spots in the organization's data inventory.

Legacy systems pose another hurdle, as older systems may contain valuable data but lack modern data management capabilities, making it difficult to integrate with newer systems. Additionally, tracking [data lineage](#) — the origin, movement, and transformations of data throughout its lifecycle — can be challenging, especially in complex environments.

These issues collectively contribute to difficulties in risk assessment, as organizations struggle to accurately evaluate and mitigate risks associated with data breaches, non-compliance, or data quality issues without a complete view of their data landscape.

### KEY QUESTIONS FOR DATA AWARENESS

Developing a robust data awareness strategy begins with asking the right questions. By systematically addressing these key areas, organizations can gain a comprehensive understanding of their data landscape and take steps to mitigate risks, improve efficiency, and extract more value from their data assets.

#### *Where is your sensitive data?*

- ▶ **Data Inventory:** Have you cataloged all the types of data your organization collects and processes? Do you know which systems, applications, and databases contain sensitive information?
- ▶ **Data Flow Mapping:** Can you trace how sensitive data moves through your organization? Are you aware of all the touchpoints where sensitive data is accessed, transferred, or stored?
- ▶ **Third-Party Data Handling:** Do you know which third-party vendors or partners have access to your sensitive data? Are you aware of how they store and process this data?
- ▶ **Cloud vs. On-Premises:** Can you distinguish between sensitive data stored in the cloud and on-premises systems? Do you have different protection strategies for each environment?

#### *How secure is your data?*

- ▶ **Access Controls:** Who has access to sensitive data within your organization? Are access rights regularly reviewed and updated based on the [principle of least privilege](#)?
- ▶ **Encryption:** Is sensitive data encrypted both at rest and in transit? Are encryption keys properly managed and protected?
- ▶ **Monitoring and Auditing:** Do you have systems in place to monitor access to sensitive data? Can you detect and alert on unusual data access patterns or potential breaches?
- ▶ **Data Loss Prevention (DLP):** Have you implemented DLP solutions to prevent unauthorized data exfiltration? Are these solutions regularly updated and tested?

#### *Is your data duplicated or obsolete?*

- ▶ **Data Deduplication:** Do you have processes in place to identify and consolidate duplicate data? How do you ensure consistency across multiple instances of the same data?
- ▶ **Data Relevance:** Do you regularly assess the relevance of stored data to current business operations? How do you determine when data has become obsolete?
- ▶ **Version Control:** How do you manage different versions of documents or datasets? Can you easily identify and access the most up-to-date version of any given data?
- ▶ **Data Quality:** Do you have mechanisms to assess and maintain the quality of your data over time? How do you handle data that has become inaccurate or unreliable?

#### *Are you keeping data for too long?*

- ▶ **Data Retention Policies:** Do you have clear, documented policies for how long different types of data should be retained? Are these policies aligned with legal and regulatory requirements?
- ▶ **Automated Retention Management:** Have you implemented systems to automatically archive or delete data based on retention policies? How do you handle exceptions to standard retention rules?
- ▶ **Legal Holds:** Do you have processes in place to identify and preserve data subject to legal holds? How do you manage the lifecycle of data under legal hold once the hold is lifted?
- ▶ **Data Minimization:** Are you actively working to minimize data collection and retention to only what's necessary? How do you balance data retention for potential future value against the risks of over-retention?

### CREATING GREATER DATA AWARENESS

Companies are heightening their data awareness through a series of data mapping processes that help identify, inventory, and track data flow throughout the organization. The data journey often much more complex and fragmented than security leaders like to think. But the exercise can help identify weak points and remediation tactics for a more compliant organization.

## Trend 3: DATA GOVERNANCE

Alongside the increase in privacy concerns, data governance has been a persistent trend emerging from CISO conversations over the last year or more. From collection and storage to processing and disposal, data governance outlines the necessary actions, protocols, and supporting technologies to ensure effective data handling across an organization throughout its lifecycle. It establishes who can access specific types of data, which datasets fall under governance protocols, and how data should be used responsibly.

### EMERGING TRENDS IN DATA GOVERNANCE

Data governance is expanding its scope beyond traditional data management to become a core part of corporate strategy. According to recent data from Gartner, **65% of data leaders now say data governance is a top priority**. But there is also an increased emphasis on demonstrating the return on investment of data governance initiatives. This is partly driven by hefty fines for non-compliance and growing investor interest in companies' data governance practices.

Another emerging trend is the shift towards more decentralized, flexible governance models to balance control with agility. The 2024 State of Data Security Report, commissioned by Immuta and conducted by customer voice platform UserEvidence, reported that **88% of data leaders believe data security will become an even higher priority**, yet there is a simultaneous push to expand data access and streamline distribution to enable business growth. To de-risk that initiative, some data leaders are trying a federated approach that allows each business unit or domain to apply its own methods to meet centralized data governance guidance.

There are also technical factors driving organizations to reconsider their DLP strategies connected to compliance and data leakage:

#### PCI DSS v4.0 Compliance

The release of Payment Card Industry Data Security Standard (**PCI DSS**) version 4.0 has introduced new requirements that compel companies to reassess their data flow and security measures:

- ▶ **Section 12.5.2** mandates organizations to define and validate their data flows
- ▶ Companies must have a clear understanding of how data moves through their systems
- ▶ Organizations need to prove they have appropriate controls in place to protect data

This heightened focus on data flow validation is pushing security executives to modernize their DLP strategies to ensure compliance and enhance data protection.

#### Data Leakage

The unauthorized exposure or access of sensitive information, often due to security vulnerabilities or human error, is becoming a more prevalent issue due to the shift to hybrid and remote work environments and the cross-industry migration to cloud environments. In light of these changes, as well as the steady drumbeat of alarming data breach and cyberattack headlines, regulatory bodies and stakeholders are demanding greater transparency and accountability in data handling practices.

### 5 Phases of Data Governance Transformation

1

#### Strategy & Leadership Alignment:

Unify stakeholders with clear vision and objectives

2

#### Data Discovery & Impact Analysis:

Assess current data landscape and identify improvements

3

#### Data Governance Program Build:

Create scalable data architecture with established standards, compliance measures, tool enhancements

4

#### Data Transformation:

Conduct testing and deploy key data solutions

5

#### Continuous Monitoring & Benchmarking:

Monitoring data flow and making operational efficiencies



**According to recent studies from data leaders:**

- ▶ 65% now say data governance is a top priority
- ▶ 88% believe data security will become an even higher priority

### MANAGING DLP AND DATA GOVERNANCE AT SCALE

As data governance evolves, so too must the strategies and tools used to prevent data loss. Traditional Data Loss Prevention (**DLP**) strategies, while still effective, are increasingly showing their limitations because they often require significant manual effort to manage and enforce policies which makes them prone to human error. To address these challenges, organizations are turning to modern cybersecurity solutions that can enhance both their DLP strategies and overall data governance:

- ▶ **Data Security Posture Management (DSPM)**: Automated scanning of customer data sources and deduplication of data with categorization based on machine learning algorithms or customer-defined policies.
- ▶ **Next-gen DLP**: Prevents data from leaving the organization's defined perimeters based on policy, and offers endpoint protection, blocking actions like uploading to cloud storage, copying to USB devices, and attaching sensitive data to emails.
- ▶ **Cloud Access Security Broker (CASB)**: Also known as cloud DLP, prevents users from accessing unauthorized "shadow applications" and provides visibility and control over data in multi-cloud environments.
- ▶ **SaaS Security Posture Management (SSPM)**: Focuses on the configuration management of SaaS applications (e.g. CRM, ERP, and cloud file storage) by connecting SaaS solutions via APIs and identifying misconfigurations that could allow unauthorized access to stored data.



# Category 4:

## THE AGE OF AI

The rapid rise of artificial intelligence has been a dominant topic in technology and business circles for several years now, capturing imaginations and sparking debates across industries. However, it's only recently that AI security has emerged as a critical concern for security executives.



The growing importance of AI in cybersecurity is reflected in market projections, with the global market for **AI-based cybersecurity products expected to surge from \$15 billion in 2021 to an impressive \$135 billion by 2030**, according to Morgan Stanley.

AI's capabilities in this domain are vast and varied, offering significant advantages in threat detection and response. These systems can identify sophisticated phishing attempts, simulate social engineering attacks, and rapidly analyze vast amounts of incident data. However, AI systems themselves have become new targets, with cybercriminals probing their weaknesses.

## Trend 1: AI SECURITY PROGRAM

As AI permeates every aspect of business operations, it brings with it a new set of security challenges that Chief Information Security Officers must urgently address. The integration of AI systems opens up additional attack surfaces, introduces novel vulnerabilities, and complicates existing security paradigms. CISOs can no longer assume that their current security controls are sufficient to protect against AI-related threats.

Just as the shift to cloud computing required a fundamental rethinking of security strategies, the AI revolution demands that CISOs adapt and evolve their security programs to meet these new challenges head-on. The imperative for CISOs is clear: develop comprehensive AI security programs that not only safeguard against emerging threats but also enable their organizations to harness the full potential of AI safely and responsibly.

### AI SECURITY CHALLENGES:

- ▶ **Data exposure:** Large Language Model (LLM)-based services, when not properly implemented, can expose personal information or organizational intellectual property.
- ▶ **Enhanced social engineering:** Attackers are leveraging AI to create more convincing and effective phishing lures, making traditional user awareness training less effective.
- ▶ **AI-powered attacks:** Malicious actors are using AI capabilities to automate the discovery and exploitation of vulnerabilities, potentially overwhelming existing detection and response systems.
- ▶ **Model manipulation:** There's a growing risk of attackers manipulating input data to cause AI models to generate incorrect or undesirable outputs, potentially leading to flawed decision-making or compromised operations.
- ▶ **Rapid tool proliferation:** The flood of new AI-focused security tools, many still inadequately tested, is straining security teams' ability to effectively evaluate and implement solutions.

The current AI revolution bears striking similarities to the early days of cloud adoption. Many security professionals initially thought that their existing security controls would seamlessly extend to cloud environments. This assumption quickly proved problematic as organizations encountered unique cloud-specific vulnerabilities and compliance challenges that their on-premises security measures were ill-equipped to handle.

## KEY COMPONENTS OF AN AI SECURITY PROGRAM

### *AI-specific risk assessment*

- ▶ Define AI use cases within the organization, identifying where and how AI is being implemented
- ▶ Map out the population affected, including users, data sources, and applications interacting with AI
- ▶ Analyze data flows in and out of AI tools, particularly focusing on sensitive or regulated information

### *Data governance and privacy considerations*

- ▶ Update data classification policies to account for AI-specific data types and usage patterns
- ▶ Implement controls over data used for AI training to prevent inadvertent exposure
- ▶ Prevent and detect the leakage of personally identifiable information (PII) through AI model outputs

### *New attack surface awareness*

- ▶ API integrations: Secure the interfaces between AI systems and other applications or data
- ▶ Model vulnerabilities: Address AI weaknesses, such as adversarial attacks or **data poisoning attempts**
- ▶ Output channels: Protect against the manipulation or misuse of AI-generated content or decisions

### *AI-focused threat modeling*

- ▶ Develop AI-specific attack trees and threat scenarios
- ▶ Model potential misuse of AI systems, including unintended consequences of AI decisions
- ▶ Consider threats to AI model integrity, such as **model inversion** or **membership inference attacks**

**“The world of AI Security has been in ‘wild west’ mode while technology outpaced the security field, but savvy CISOs are catching up. Security leaders are realizing that they need to act fast, and they need to act now.”**

— Jeremiah Sahlberg, Tevora Principal

## Trend 2: ADDRESSING NEW AI THREATS

OpenAI had released its groundbreaking LLM chatbot for less than a year before major security issues started arising, and in 2023, Bloomberg reported that [Samsung banned its workforce of over 250,000 people from using generative AI products after the accidental leak of sensitive internal source code](#) by an engineer who uploaded it to ChatGPT. As organizations rush to harness the power of AI, many are doing so without fully understanding or addressing the associated security risks. This creates a pressing need for CISOs to develop new strategies for cataloging, monitoring, and mitigating AI-related security threats.

### THE EVOLVING AI THREAT LANDSCAPE

In the wake of ChatGPT's public release, security professionals witnessed a staggering [increase in novel social engineering attempts, with a rise of 135% between January and February 2023](#) alone. This surge can be attributed to AI's ability to generate highly convincing and contextually appropriate content at scale. Cybercriminals are now leveraging AI to craft personalized phishing emails, create deepfake voice messages, and even impersonate trusted individuals in video calls. These AI-enhanced tactics make it increasingly difficult for employees to distinguish between legitimate communications and malicious attempts at manipulation. As AI technology advances, so does the sophistication of cyber threats. Attackers are now using AI to:

- ▶ Automate the discovery of software vulnerabilities
- ▶ Generate polymorphic malware that can evade signature-based detection
- ▶ Conduct intelligent, adaptive attacks that learn from defensive responses
- ▶ Create convincing fake websites and social media profiles for large-scale fraud

Moreover, the rise of AI-as-a-Service platforms has democratized access to advanced AI capabilities, lowering the barrier to entry for cybercriminals. This has led to a proliferation of AI-enabled attacks, ranging from advanced persistent threats to ransomware campaigns.

### BEST PRACTICES IN IDENTIFYING LLM THREATS

Launched in response to the surge in LLM integration following the release of mass-market pre-trained chatbots in late 2022, the [Open Web Application Security Project \(OWASP\) Top 10 for Large Language Model \(LLM\) Applications](#) catalogs and organizes the unique security challenges posed by the rapid adoption of LLMs in various applications. These vulnerabilities include prompt injection, where crafted inputs manipulate LLMs into performing unintended actions, and insecure output handling, which can expose backend systems to various attacks. Other critical concerns are training data poisoning, model denial of service attacks, and supply chain vulnerabilities introduced through third-party components. Further complicating the AI security landscape are issues that arise from excessive agency granted to LLM systems, overreliance on these models without proper oversight, and the potential for model theft.

### LAGGING DEFENSES

Legacy security solutions, which rely heavily on historical attack data and known threat signatures, are proving inadequate against the novel and dynamic nature of AI-enabled attack. Traditional security measures often operate on the assumption of recurring attack patterns. However, when novel attacks become the norm rather than the exception, this approach falls short. Signature-based antivirus software, rule-based intrusion detection systems, and static security policies are increasingly outmatched by the adaptability and unpredictability of AI-driven threats.



## Trend 3: AI COMPLIANCE

The potential risks associated with AI— from bias and discrimination to privacy breaches and security vulnerabilities— have prompted governments and international bodies to develop comprehensive regulatory frameworks and standards, notably:

- ▶ [Executive Order 14110](#) on Safe, Secure, and Trustworthy Artificial Intelligence, issued by the U.S. government to promote responsible AI development and use.
- ▶ [NIST-AI-600-1](#), which provides guidance from the National Institute of Standards and Technology for organizations to better manage risks associated with AI systems.
- ▶ [The European Union's AI Act](#), a comprehensive regulation that became law in August 2024, which introduces a risk-based approach to AI governance.
- ▶ [ISO/IEC 42001](#), the world's first AI management system standard, offering a structured approach to managing AI projects responsibly.

The AI-related regulations continue to emerge as regulating bodies catch up with consumer and corporate concerns surrounding AI. Expect this list to grow, and to increasingly impact different facets of AI usage, privacy rules, and more.

### **EXECUTIVE ORDER (EO) 14110: SAFE, SECURE, AND TRUSTWORTHY AI**

Issued on October 30, 2023, EO 14110 aims to ensure that AI development and deployment in the United States are conducted safely, securely, and responsibly. The Executive Order assigns the National Institute of Standards and Technology (NIST) a central role in developing standards and guidelines for AI. Key responsibilities include:

- ▶ Development of companion resources to the NIST AI Risk Management Framework ([NIST AI 100-1](#)) specifically for generative AI and the [NIST Secure Software Development Framework](#) to incorporate secure-development practices for generative AI and [dual-use foundation models](#).
- ▶ Launching a new initiative to create guidance and benchmarks for evaluating AI capabilities, focusing on those that could potentially cause harm, and establishing guidelines and processes for developers of generative AI, especially dual-use foundation models, to conduct AI red-teaming tests.
- ▶ The Executive Order set an ambitious timeline, with most tasks assigned to NIST having a 270-day deadline that expired on Friday, July 26, 2024.

### NIST AI RISK MANAGEMENT FRAMEWORK

Right on schedule in July of 2024, the National Institute of Standards and Technology released NIST-AI-600-1, titled “Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile.” NIST also launched its [Trustworthy and Responsible AI Resource Center](#) to facilitate the implementation of the AI Risk Management Framework (AI RMF) and promote international alignment on AI governance practices.

### EU AI ACT

The European Union’s Artificial Intelligence Act ([EU AI Act](#)) became law on August 1, 2024, marking the beginning of a staggered implementation timeline. The Act’s scope extends beyond EU borders, affecting:

- ▶ Businesses operating within the 27 EU Member States
- ▶ Companies with customers in the EU
- ▶ Organizations whose AI system outputs are used in the EU, even if not intended for EU use
- ▶ Businesses in Norway, Iceland, and Liechtenstein under the European Economic Area (EEA) arrangements

### ISO 42001: AI MANAGEMENT SYSTEM STANDARD

The International Organization for Standardization (ISO), in collaboration with the International Electrotechnical Commission ([IEC](#)), launched the world’s first [Artificial Intelligence Management System](#) (AIMS) standard in late 2023. ISO/IEC 42001 is designed to integrate seamlessly with other management system standards, particularly:

- ▶ [ISO 27001](#): Information Security Management
- ▶ [ISO 27701](#): Privacy Information Management

While ISO/IEC 42001 considers requirements of information security and privacy, it does not require organizations to have these standards as prerequisites. This integration allows organizations to create a cohesive management system that addresses AI, security, and privacy concerns holistically.

This wide-reaching applicability makes the EU AI Act a de facto global standard that businesses worldwide need to consider. It introduced a risk-based approach to AI regulation, with different requirements based on the level of risk associated with AI systems:

- ▶ **Standard Prohibitions:** Banned AI applications include systems using manipulative techniques, exploiting vulnerabilities, [social scoring](#), and certain uses of facial recognition technology.
- ▶ **General-purpose AI Regime:** Applies to AI models with broad functionality (e.g., text, speech, and image generation), and requires transparency about training data and copyright information and includes additional obligations for “systemic risk” models, including evaluation, testing, and risk mitigation.
- ▶ **High-risk AI Regime:** Applies to AI systems in critical areas such as biometric identification, education, employment, and public services, and requires continuous risk management, technical documentation, and human oversight.
- ▶ **Transparency Obligations:** Applies to AI systems interacting with humans, emotion recognition systems, and systems generating synthetic content, and requires clear disclosure of AI use and generated content.



# The Year Ahead


As we prepare for what is unquestionably going to be a dynamic year for cybersecurity, it's clear that CISOs and security leaders face a complex and rapidly changing threat environment. The trends highlighted in this report — from the need for proactive measures and resource optimization to the critical importance of privacy, data governance, and AI security — all speak to the multifaceted challenges that digitally-empowered organizations must navigate.


Ultimately, the success of cybersecurity efforts in 2025 will depend on the ability of CISOs and their teams to stay ahead of the curve, continuously adapting their strategies and leveraging new technologies responsibly. As regulatory frameworks evolve and AI becomes increasingly central to both business operations and security measures, organizations must prioritize not just compliance but also innovation in their approach to cybersecurity.

# TEVORA™

Go forward. **We've got your back.**



 (833) 292-1609

 [sales@tevora.com](mailto:sales@tevora.com)

 sign up for our [newsletter](#)

Dedicated to **Christina Iodice**, who informed many of the pages in this report and who continues to inspire us all.