

**TEVORA™**

# 2024 CISO Priorities Report

Trends in Cybersecurity  
for the Coming Year

**AUTHORS:**

Christina  
Iodice

Clayton  
Riness

Jeremiah  
Sahlberg

# INTRODUCTION

If 2023 has proven anything, it's the age-old adage that "Change is the only Constant<sup>1</sup>." From the astronomical adoption of AI to an uncertain American economic outlook; from the continued trend toward hybrid work to news-dominating cyber attacks; 2023 was predictably unpredictable. In combination with the past several years, we have all witnessed a rapid transformation in the realm of cybersecurity, with new threats emerging alongside innovative solutions.

As we step into 2024, the need to adapt and anticipate the dynamic shifts in cybersecurity has never been more critical. And as we look to 2024, many CISOs are evaluating an increasingly uncertain cyber threat landscape and evaluating where to allocate efforts and budgets in a way that best solidifies their organizations' security posture.

**As Tevora works with thousands of organizations across a multitude of industries, including public entities, startups, and Fortune 500 companies,**

**our consultants are in a unique position to observe and help guide CISOs and Executives through common upcoming trends.**

In the following pages, we have compiled a guidebook of those trends. From the relentless advancements in artificial intelligence to the escalating prominence of data privacy regulations and the growing threats posed by cybercriminals, this exploration delves into the impending changes poised to impact organizations, governments, and individuals worldwide.

We aim to equip professionals and enthusiasts in the field with a forward-thinking perspective, aiding in the fortification of defenses and preparedness against the ever-shifting cybersecurity landscape. We hope the information included here will serve as a compass, navigating the ever-changing currents of the digital world and illuminating the anticipated trends shaping cybersecurity in the year 2024.

# IN THIS REPORT

<b>PART</b>	<b>01</b>	<b>Compliant and Under Control</b>	<b>4</b>
		• Preparation for PCI 4.0 In Full Force	4
		• Catching up to ISO's Latest Changes	5
		• Watching out for CMMC	5
		• US Privacy Laws Continue to Evolve	6
<b>PART</b>	<b>02</b>	<b>Getting with the Program</b>	<b>7</b>
		• Risk Program Maturity	7
		• Data Governance Program	8
		• AI Security Programs	9
<b>PART</b>	<b>03</b>	<b>Eyes on the Threat Landscape</b>	<b>10</b>
		• Planning Ahead for Identity Resilience	10
		• Looking Inward at Insider Threats	11
		• Testing all Defenses with Adversary Simulation Exercises	11
		• CISO Accountability Makes Headlines	12



## PART 1: COMPLIANT AND UNDER CONTROL

2024 represents a year of change for several compliance frameworks, and CISOs and Compliance Officers are taking note. Remember, PCI, ISO, HITRUST, NIST, and other frameworks all released significant updates to their standards over the last year. It has become apparent that part of the responsibility for compliance professionals is to keep a constant pulse of changing regulations and requirements.

Here are the standards that are creating the most buzz, and dominating CISO, Compliance and Privacy budgets and agendas as we move into 2024.



## Preparation for PCI 4.0 In Full Force

In an attempt to keep up with the rapidly evolving risks surrounding cardholder data, the PCI Council continually evaluates its PCI DSS standards. And while details of the standards have been circulating since early 2022, many organizations are scrambling to ensure their continued compliance before the newest version of PCI DSS - known as PCI DSS 4.0 - goes into effect on March 31, 2024 and has 63 new requirements. Some requirements are effective immediately, but the majority of controls are not effective until March 31, 2025.



PCI DSS version 4.0—published on March 31, 2022—represents a significant upgrade to the previous version (3.2.1). The new version addresses emerging threats to payment data and evolving security and payment technologies.

PCI DSS version 4.0 includes a substantial number of changes. Some are paradigm shifts or significant new or modified requirements. Others are smaller refinements or clarifications to requirements. **And as the March 31, 2024 deadline looms just months away, CISOs and Compliance Officers are now ramping up efforts to ensure they have a handle on the new requirements.**

"The new version of PCI DSS standard means that many organizations need to reassess their internal systems and processes considering the new requirements. This can be a daunting undertaking, but for many of our clients, is resulting in a more secure payment ecosystem," says Christina Iodice, Principal at Tevora.

For more information on PCI DSS, read a [comprehensive blog here](#) or view our [webinar here](#).

## Catching up to ISO's Latest Changes

With 2022 updates to the ISO 27001/ISO 27002 standards, many compliance and security leaders are beginning to assess their organization's ability to meet the newest requirements. All companies that seek to maintain compliance will have to be converted to the new ISO 27001 standard by 2025, and the looming deadline is putting pressure on security and compliance leaders to act quickly. In 2024 any new ISO 27001 Certification must follow the 2022 version of the standard.

ISO 27002:2022 includes several key changes from its 2013 predecessor, including the consolidation of its original 114 controls to 93. While this reduction involves the consolidation of some duplicate controls, the new list includes 11 new controls that compliance leaders will have to consider.

### ISO 27002:2022 CONTROLS COMPARISON

2013: 114 CONTROLS

2022: 93 CONTROLS

"Many security and compliance leaders delayed pursuing compliance efforts this year due to tightened budgets in the middle of 2023. Now, they're looking to pick back up and move quickly to make that 2025 deadline," says Iodice.

For more details on the new merged and introduced controls of ISO 27002-2022, see [our webinar here](#).

## Watching Out for CMMC

While no formal rule-making announcements have been made yet, many experts expect rules around the Cybersecurity Maturity Model Certification, or CMMC 2.0, to be formalized in late 2024, or early 2025. For companies doing business with the US Department of Defense, this will trigger urgent changes to avoid losing valuable contracts.

It is estimated there are approximately 67,000 companies currently categorized as Level 2 CMMC, with many solely relying on DoD contracts for much of their business. "Many CISOs are anxiously awaiting updates," says Jeremiah Sahlberg, Managing Director of Tevora. "As a FedRAMP 3PAO certified assessor and working towards our C3PAO accreditation, Tevora is keeping an eye on developments in this area on behalf of our clients so that we are all ready to act when needed."

## US Privacy Laws Continue to Evolve

In 2023 we saw the following new/updated Privacy Laws become effective

:

- **Virginia's** law was effective and enforceable on January 1, 2023;
- **California's** amendments were effective on January 1, 2023 and enforceable on July 1, 2023;
- **Colorado's** law was effective and enforceable on July 1, 2023;
- **Connecticut's** law was effective and enforceable on July 1, 2023; and
- **Utah's** law was effective and enforceable on December 31, 2023.

Changing aspects of consumer privacy in areas like Applicability, Consumer Rights, updated requirements for Processors and Service Providers, updated Data Protection Assessments (DPAs) and Enforcement criteria.

It doesn't stop there. Organizations should expect the following US privacy laws to be effective between 2024-2026:

- **Montana** – Montana Consumer Data Privacy Act ("MCDPA") takes effect on October 1, 2024
- **Washington** – My Health My Data Act ("MHMDA") takes effect on March 31, 2024, for "regulated entities." and on June 30, 2024, for "small businesses."
- **Texas** – Texas Data Privacy and Security Act ("TDPSA") takes effect on March 1, 2024.
- **Florida** – Florida Digital Bill of Rights ("FDBR") takes effect on July 1, 2024.
- **Iowa** – Senate File 262 ("SF 262") takes effect on January 1, 2025
- **Tennessee** – Tennessee Information Protection Act ("TIPA") takes effect on July 1, 2025
- **Indiana** – Indiana Consumer Data Protection Act ("InCDPA") takes effect on January 1, 2026

Keep in mind that some of these changes include substantive updates to areas like Consent Requirements. Some Attorney Generals have issued rules around a "right to cure period," an altogether new concept in privacy laws.

Privacy is here to stay in the US and Global Market. Organizations should swiftly take this into consideration for their technical, operational and governance programs to ensure consumer satisfaction and compliance.

For more information, view our [Privacy Datasheet](#), or [this recent blog article](#).



## PART 2: GETTING WITH THE PROGRAM

Many cybersecurity experts know that oftentimes, no news is good news. No breaches, no errors, no excitement. But keeping organizations, data, and assets safe means plenty of preventative measures. The myriad of programs and procedures a security team can put into place can make it hard to prioritize the best approach to a secure organization, and many security leaders might wonder how to find the best place to start. Here are some of the preventative risk and security programs we have seen CISOs turn to in Q3 and Q4 of this year.

## Risk Program Maturity

As we approach 2024, more CISOs are asking questions about the maturity of their risk programs. While many have established risk programs in place, changes in technology (think AI) and updates in compliance frameworks (see previous section) have forced a fresh look at existing programs. Those CISOs are turning to formal evaluations of their Risk Program Maturity.

A Risk Program Maturity Evaluation is a comprehensive analysis aimed at assessing and improving an organization's existing risk management program. This evaluation involves a thorough examination of various elements, such as organizational challenges, alignment with the organizational vision, effective program components, and the documentation and reporting of risk management processes and workflows. Key areas include evaluating the methodology and lifecycle of risk, covering aspects like risk intake, profile, risk tolerance or appetite, treatment, and reporting.

"As we approach 2024, the significance of conducting a Risk Program Maturity Evaluation is heightened," says Sahlberg. Evolving regulations, the updated compliance frameworks, and the integration of artificial intelligence into Governance, Risk, and Compliance (GRC) tooling, all put a sense of urgency to the task. "Organizations are assessing their ability to successfully scale their risk management programs by incorporating emerging tools and technologies."

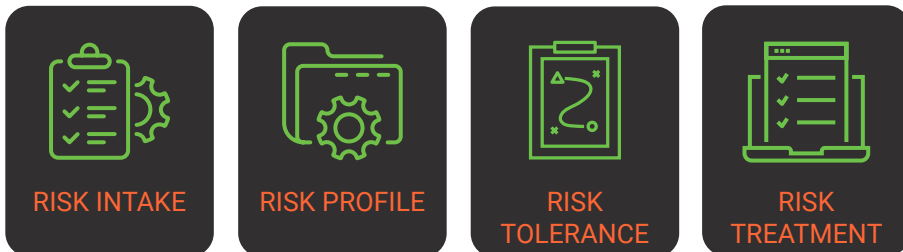
## Data Governance Program

Data Loss Prevention ("DLP") remains a challenging technology for most organizations to successfully implement and operate. Due to the nature of data and DLP operations, organizations frequently stumble with meeting timeline and effectiveness objectives. This often results in DLP being largely bypassed or relegated to disuse within the organizational technology stack in a short amount of time.

Now, more CISOs are questioning the status quo and exploring new DLP strategies for their organization. But concerns over the ability to successfully implement a Data Governance Program hinder many organizations from taking actionable steps.

"We are finding that the best approaches will carefully consider the multitude of factors that play a role in successful plan implementation," says Iodice. "You have to take into account the four key components – Program, People, Process, and Technology – to put you in the best possible position for success."

For more information on implementation and execution of a Data Loss Prevention strategy, access our recent White Paper.



## AI Security Programs

Of course, no look into 2024 would be complete without a comment on AI Security.

“As more and more organizations adopt Generative AI (GenAI) tools en masse, more CISOs are asking how to get in front of any potential threats,” says Iodice. “This has become an increasingly common request.”



According to Gartner, Inc.<sup>2</sup>, by 2025, GenAI is expected to be used by 95% of developers and

According to Gartner, Inc. , by 2025, GenAI is expected to be used by 95% of developers and 60% of marketing departments, among other roles. AI use continues to grow, and cybersecurity professionals are tasked with ensuring a balance between security and strong organizational pressure to adopt new technologies.

“CISOs are discovering the Pandora’s box that AI has opened. Beyond the practical security concerns, there may also be threats to compliance,” says Iodice. For many, this means creating fresh security programs and risk assessments around AI tools and the unique vulnerabilities involved.

Despite the potential risks, the important factor here is for security leaders to understand how they can enable organizations to leverage GenAI rather than prevent them. Creating a comprehensive and effective AI Security Governance Program helps transition this conversation to one of enablement.



## PART 3: EYES ON THE THREAT LANDSCAPE

As cyberattacks increase in frequency and severity, many CISOs consider breaches a matter not of “if,” but of “when” and “how bad.” And while for some, a breach can mean a PR nightmare, for others, it can be business-ending. Threat awareness is always top-of-mind for CISOs, but here is where we see cybersecurity conversations and budgets trending for the coming year.

## CISO Accountability Makes Headlines

The end of 2023 has seen CISOs making the news, and not in a positive way. Most notably, SolarWinds and its CISO were charged by the SEC for misleading investors in connection to a 2020 breach – a breach considered one of the most significant cybersecurity incidents this century. This news – which has shaken many CISOs – was followed by the announcement that Clorox CISO left her position amidst a weeks-long ransomware attack.

“The role of CISO can be unpredictable, but recent incidents have shown that a lack of preparation has consequences.”

Many CISOs understand that the position is highly complex; but consumers, boards of directors, and governing bodies are showing little sympathy when a damaging incident occurs.

“Many of our peers and clients are talking about these incidents,” says Sahlberg. “The role of CISO can be unpredictable, but recent incidents have shown that a lack of preparation has consequences.”

While it may be impossible to prepare for all scenarios, the best course of action is a well-rounded understanding of one’s risk profile, and the implementation of appropriate preventative measures where possible.

“What these recent incidents have shown,” says Sahlberg, “is that these risks are very real. Having the right protective services coupled with well-defined detection and response capabilities are essential against liability – both legal, and otherwise.”

## Planning Ahead for Identity Resilience

2024 saw some headline-making cyberattacks that brought to light the critical and ubiquitous function that IAM systems play in modern businesses. While organizations have implicitly understood the interconnected nature of various applications, many are just beginning to realize the linchpin that IAM systems have become.

“SSO represents an amazing advancement in modern business and technology operations,” says Clayton Riness, Principal at Tevora. “But as businesses have used SSO for more and more critical functions, it becomes a bigger target for threat actors.” As such, identity resilience has been an increasingly trending buzz term.

Identity resilience is generally defined as the ability to protect your identity data and systems from cyberattacks, while ensuring quick recovery if or when disasters hit. More and more cybersecurity experts are prioritizing identity resilience as a top 2024 initiative.

“There are a variety of both technical solutions and practical safeguards that organizations can and should put into place to ensure business continuity,” says Riness. “Identity resilience is increasingly seen as a critical aspect of business continuity planning.”

“Identity resilience is increasingly seen as a critical aspect of business continuity planning.”

## Looking Inward at Insider Threats

Threats can come from anywhere; and based on recent conversations with CISOs, more cybersecurity leaders are turning their attention within as they strengthen their defenses for the coming year.

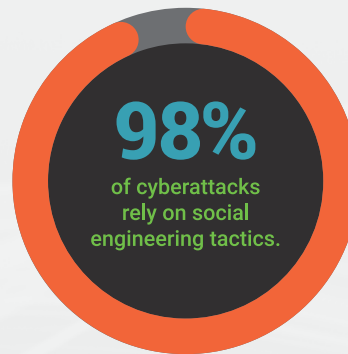
Insider threats in cybersecurity represent a significant challenge, posing risks to organizations by exploiting access privileges held by internal personnel. These threats can arise from various sources, including employees, contractors, or partners who have authorized access to a company's systems, networks, or data.

Not all insider threats are malicious. They can result from inadvertent actions, negligence, or deliberate malicious intent. In many cases, unintentional actions, such as falling victim to phishing attacks or using weak passwords, can lead to compromised security. Malicious insider threats, on the other hand, involve employees or insiders purposefully acting against the interests of the organization, potentially stealing data, intellectual property, or causing intentional harm.

"The challenges of detecting and mitigating insider threats stem from the complexity of distinguishing regular employee behavior from potentially harmful actions," says Riness. "Detecting anomalies that signal a breach in security often requires the ability to key into the details."

When it comes to tackling insider threats, CISOs are evaluating their options. This may include a mix of tools and procedures. Some are turning to monitoring systems capable of recognizing patterns, deviations from typical behavior, or access to sensitive information outside an individual's role. As a best practice, many are establishing effective policies and access controls, implementing regular training and awareness programs, and adopting technologies such as user behavior analytics and data loss prevention tools are crucial steps in preventing and managing insider threats. Moreover, creating

a culture of security consciousness within an organization—where employees understand the importance of cybersecurity and their role in maintaining it—can significantly reduce the likelihood of insider threats and enhance overall cybersecurity resilience.



## Testing all Defenses with Adversary Simulation Exercises

Yes, technology changes constantly. However, as many as 98% of cyberattacks rely on social engineering tactics. And

as big brands find themselves in the headlines for news-cycle-dominating breaches, CISOs are pulling out all the stops to ensure their organizations don't end up famous for the wrong reasons.

This is where we see cybersecurity leaders turning to aggressive adversary simulation testing to ensure proper defenses. "As cyber attacks become more devastating, CISOs are pulling out all the stops to ensure their bases are covered. We've seen an increase in conversations around adversary simulation exercises, and even tactics like on-site penetration testing," says Riness.

The heightened importance of adversary simulation exercises stems from the imperative to stay ahead in the cyber defense game. Organizations can no longer afford to be merely reactive in their security measures; they must adopt a proactive and adaptive stance. These simulations offer a controlled environment for security teams to test, learn, and fortify their defenses by anticipating the latest attack vectors and strategies used by adversaries. Today's adversary simulation tactics use the same sophisticated tools that bad actors have access to, which may include AI-driven phishing techniques or AI voice simulation.

## CHRISTINA IODICE

### Principal Consultant



#### Primary Role

As Tevora's Principal over Privacy, Enterprise Risk and Compliance, Christina's primary role is to assist our clients in aligning their security and privacy programs with their business strategic objectives. With over 20 years of experience in the security and risk space, she helps organizations design, establish, and mature their privacy and security programs and capitalize on efficiency. Christina also mentors junior consultants, manages client relationships, assists with pre-sales and post sales activities, and oversees all projects from inception to the closeout presentation to ensure that every project exceeds our client expectations.

#### Notable Accomplishments

With a diverse background in Education, Finance, Healthcare, Entertainment, Manufacturing, and Hospitality, Christina brings vast knowledge in both business and security to our clients. Her experience in privacy regulations (i.e., GDPR, CCPA, and LGDP), security assessments, security strategy, risk management, compliance, governance, data loss prevention and vendor management adds value to both our practice and to our client's engagements.

Christina holds a Bachelor's degree in Electronic Engineering and Information Technology, a Master's degree in Management Information Systems from NSU, a MBA from MIT and a PhD (ABD) in Information Security and Assurance from NSU. She has been inducted into all notable security and computer science honor societies including Alpha Beta Kappa National Honor Fraternity, Alpha Chi National Honor Fraternity, and Upsilon Pi Epsilon National Honor Fraternity. Christina presents on security, risk and privacy topics at conferences and regional events. Also an Information Security Instructor at University of California Irvine.

#### Certification and Training

Christina holds the following certifications: PCI QSA, PA-DSS QSA, Certified Data Privacy Solutions Engineer (CDPSE), Certified Information Security Manager (CISM), Certified in Risk and Information Systems Control (CRISC), ISO 27001 Lead Auditor, Certificate of Cloud Security Knowledge (CCSK), Cobit, HITRUST Security Assessor (HSA), and a certification from the National Security Agency (NSA) Committee on National Security Systems (CNASS) in Information Security Management (ISO 17799).

#### Tenure

Christina has been with Tevora since 2012.

# CLAYTON RINESS

Principal Consultant



## Primary Role

Practice Lead

## Notable Accomplishments

Clayton leads the lead Tevora’s technical practice delivery spanning Solutions, Threat, Incident Response and Cloud Security. His professional background includes 20 years of information technology and security experience spanning many technologies under the most demanding compliance and uptime requirements. Clayton is able to relate and build rapport and credibility with both executive management and technical personnel alike which contributes greatly to the success of his projects. Clayton is a natural leader that continually inspires and supports fellow consultants.

With more than a decade of experience in IT and security, Clayton delivers/provides clients with extensive knowledge in business and technology His experience in policy reviews, security assessments, security remediation, infrastructure management, and regulatory compliance adds value to both the practice and to client’s engagements.

## Certification and Training

Clayton holds an MBA from the University of California, Irvine, and a Bachelor’s degree in Computer Science from the University of California, Santa Barbara. Clayton has the following certifications: PCI QSA, and the Certified Information Systems Security Professional (CISSP).

## Tenure

Clayton has been with Tevora since November 2011.



# JEREMIAH SAHLBERG

## Managing Director

### Primary Role

As Tevora's Managing Director, Jeremiah oversees several business areas and helps shape their cybersecurity consulting services.

Jeremiah is an executive security consultant and advises clients on establishing security programs and compliance management. His experiences span professional and managed security services and solutions for clients in the payment card processing, entertainment, telecom, healthcare, gaming, energy, transportation, and manufacturing industries.

With over 20 years of experience in the security and risk space, he helps organizations design, establish, and mature their privacy and security programs and capitalize on efficiency. Jeremiah mentors consultants, manages client relationships, assists with pre and post sales activities, and oversees projects from the inception to the closeout presentation to ensure that every project exceeds client expectations.

### Notable Accomplishments

Jeremiah actively contributes to the security community and has presented at Gartner's Evanta, ISACA, NCUA – ISAO, NCTA, SINET, New York State Cyber Security Conference, Nevada Digital Government Summit and also contributed to O'Reilly's Secure Coding: Principles & Practices, Graff and Ken van Wyk.


Since 2012, Mr. Sahlberg regularly guest lectures at NPower, teaching cyber security for young adults from underserved communities. Additionally, he currently sits on the Board of Advisors for Liberty University's School of Engineering and Computational Sciences.

### Certification and Training

Jeremiah holds the following certifications: Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP), HITRUST Security Assessor (HSA), and earned a Bachelor of Science degree in Computer Engineering from Virginia Polytechnic University. Previously, Jeremiah held the PCI QSA certification.

### Tenure

Jeremiah has been with Tevora since 2018.



Founded in 2003, Tevora is a specialized management consultancy focused on cybersecurity, risk, and compliance services. Based in Lake Forest, CA, our experienced consultants are devoted to supporting the CISO in protecting their organization's digital assets. We make it our responsibility to ensure the CISO has the tools and guidance they need to build their departments, so they can prevent and respond to daily threats.

Our expert advisors take the time to learn about each organization's unique pressures and challenges, so we can help identify and execute the best solutions for each case. We take a hands-on approach to each new partnership, and –year after year –apply our cumulative learnings to continually strengthen the company's digital defenses.

# TEVORA™

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

[WWW.TEVORA.COM](http://WWW.TEVORA.COM)

| [SALES@TEVORA.COM](mailto:SALES@TEVORA.COM)

| 833-292-1609



**TEVORA™**