CISO 3.0

As cyber threats evolve alongside new technologies, CISOs must become strategic leaders, understanding the changing regulatory landscape and implementing best practices to safeguard their organizations in the future. This white paper explores critical trends and equips CISOs with the knowledge to navigate this complex terrain.

NTSC
NATIONAL TECHNOLOGY SECURITY COALITION
ntsc.org

Jason Witty
Chief Information Security Officer
Fidelity Investments

In the past 10 years, the sophistication, velocity, and volume of cyber-attacks elevated cyber-security to a Board level topic. With explosive growth of Generative Artificial Intelligence, modern CISOs must now double-down on safe business enablement, while still managing risk well. CISOs still require the skills of the past/present including understanding various policy, governance, frameworks, and oversight practices; deeply understanding international threat intelligence, information sharing networks, public-private operational collaboration processes; and advances in modern agile software engineering practices like DevSecOps. They must also remain excellent organizational leaders, thought leaders, recruiters, communicators, and coaches. But deep-knowledge of Generative AI / Large Language Models and broader Model Risk Management and Governance practices has rapidly become skillset table-stakes of the future.

Welcome
[An Introduction]

The digital revolution has irrevocably transformed our world, ushering in an era of unprecedented connectivity and innovation. However, this interconnectedness also presents significant challenges for cybersecurity professionals. Chief Information Security Officers (CISOs) are on the front lines of this ongoing battle, tasked with safeguarding critical data and infrastructure from a constantly evolving threat landscape.

This white paper explores the key trends that will shape the future of cybersecurity and the implications for CISOs. We will delve into the growing importance of cyber-physical security convergence, the vast attack surface created by the ever-expanding Internet of Things (IoT), the potential disruption of quantum computing, and the increasing adoption of artificial intelligence (AI) by both attackers and defenders. We will also examine the regulatory landscape, exploring the potential expansion of existing regulations, the rise of stricter penalties for non-compliance, and the growing consumer demand for transparency and control over their data. Finally, we will peer into the future and discuss the importance of information sharing between organizations and the value of industry best practices in guiding CISOs navigating this complex terrain.

By understanding these trends and embracing new approaches, CISOs can transform themselves from security tacticians into business leaders of a secure digital future. This white paper equips CISOs with the knowledge and insights necessary to stay ahead of the curve, build robust security postures, and protect their organizations from the ever-present threats posed by bad actors.

Table of Contents

[Our Outline]

We have crafted this white paper to have three main elements, all supported by critical insights. The structure is as follows:

Section I

[The Changing Role of the CISO]

The CISO role is evolving into a more strategic and collaborative leadership position, requiring a broader skillset and a deeper understanding of the business and the ever-changing cybersecurity landscape.

1.1

AN EVER-SHIFTING AND EXPANDING FOCUS IS CRITICAL

Over the past several years, the process of fundamentally changing how a business operates by integrating digital technologies across all areas (aka, digital transformation) has continued to expand. That expansion inevitably encompasses elements traditionally outside the normal CISO function, such as risk management, compliance and regulatory adoption, strategic business integration, and crisis management. In short, the CISO role is growing in breadth and scope. Combined with new SEC rules[1], the CISO must primarily serve as a business risk function, prioritizing business acumen over purely technical skills[2]. Research[3] shows that as the CISO role expands into business strategy and enablement, it's increasingly challenging to accomplish core tasks like managing cyber risks, detecting threats, and responding to incidents. All of this points to the reality that a CISO must be able to expand their focus.

Once solely a security tactician, CISOs are evolving into robust business leaders. Research[2] conducted by IANS and Artico cites, as reported by 660+ CISOs, "76% of CISOs come from a mostly technical background, where risk management is often secondary." They assert this will need to change. CISOs can no longer solely focus on technical security measures. They must be more strategic, influencing business decisions and collaborating with other C-suite executives to align security with broader organizational goals. The report states that "the expectations for the CISO role have been elevated to the C-suite level. Yet, we find many CISOs continue to struggle to be viewed as such and/or have not been elevated to that level."

This evolution will be critical as time passes. Several benefits are associated with transitioning the CISO role into one with more alignment with business-centric processes. They include but are not limited to:

1. Fostering better communication between the CISO and other key stakeholders.
2. Lessening the likelihood of critical, timely information being lost or misconstrued.
3. Building trust with CISOs and stakeholders

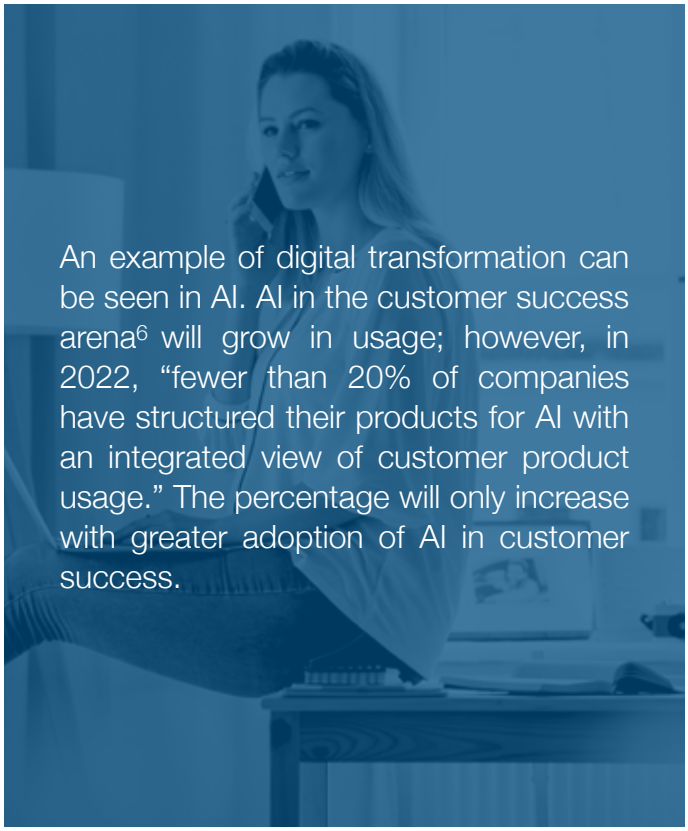
All of these benefits set up the CISO for an expanded scope.

CISOs used to be more narrowly focused on cyber-centric matters, but now they are expanding into other areas. Their focus extends beyond technical solutions and includes proactive risk management, compliance and regulatory adoption, strategic business integration, and crisis management concerns.

When the CISO role emerged in 1995[4] – the responsibilities of the CISO were centered around establishing and maintaining "the security of information and operations contained within the internal technology infrastructures." The role continued to evolve as time passed. By 2000, the CISO's responsibilities extended beyond the corporate boundaries to include e-business partnerships, expanding into a secondary relationship with customers, suppliers, and partners.

The CISO within the corporate structure is still evolving. This evolution will follow emerging trends. Here are some emerging trends impacting CISOs[5] in 2024:

1. **Heightened regulatory compliance and transparency:** We are seeing a shift to obligatory reporting; more reporting means more cyber transparency. If there is more transparency, this will necessitate more cybersecurity measures to ensure stakeholders continue to trust the organization.
2. **The continued expansion of digital transformation:** CISOs must maintain control over asset growth as digital transformation expands. There might be better paths forward than expansion at all costs; thus, CISOs must participate in the critical conversations on whether expanding digital assets can support the business demands or if more time is needed to prepare for such an expansion.



3. **The growing need for cyber resilience spans all parts of an organization:** There's a concerted effort to build a strong security culture and improve detection, prevention, and response capabilities. This includes comprehensive updates to business continuity plans, disaster recovery strategies, and incident response protocols, ensuring a company-wide approach to cyber resilience.

1.2

THE EXPANSION OF FOCUS REQUIRES AN EVOLUTION OF SKILLS

As we have established, the CISO role is expanding. That expansion warrants the evolution of skills that a CISO must embody. These capabilities include leadership skills, business acumen, and communication skills.

CISOs need to have a proven ability to lead. One person cannot solve every cybersecurity issue independently[7]. Whether dealing with a persistent nation-state threat many years and millions of dollars in the making or grappling with a brazen fraudster targeting your less savvy users, no one can do it alone. Success lies in their ability to build a security team[8] of wide-ranging, highly qualified cyber experts.

An article in Harvard Business Review covers[9] six fundamental skills every leader should practice:

1. Shape a vision that is exciting and challenging
2. Translate that vision into a clear strategy
3. Recruit, develop, and reward
4. Focus on measurable results
5. Foster innovation and learning
6. Lead yourself

These leadership skills will aid CISOs in building a program to address their challenges effectively.

CISOs must extend their business acumen to other verticals. CISOs need a strong understanding of the business and its objectives to effectively communicate security risks and propose solutions that align with business strategy.

Previously referenced research by IANS and Artico cite[2], "This comprises the skills that allow CISOs to speak the board's language, including a solid understanding of the corporate strategy and go-to-market; the financial literacy to read and comprehend financial statements; and the ability to frame risks in terms of economic impact and opportunity costs, instead of limited to technical vulnerabilities."

The expansion into addressing other critical business operations will enable the CISO to thoroughly weigh the pros and cons of a business decision that might impact security, such as expanding operations into a new global market or a partnership that requires integrating software systems. Business decisions are not without risk, especially in a digital-first, global economy. The CISO must understand the benefits and if they outweigh the risks.

Understanding the risk isn't enough; they must communicate that risk.

As CISOs continue to grow, they must rely on communication and collaboration to aid them. Building strong relationships across the organization, fostering a culture of security awareness, and effectively communicating risk to non-technical audiences are crucial skills.

The ability to communicate effectively is a critical skill for CISOs. Whether it is with their team, the organization, or C-suite executives, but it is especially true regarding the board of directors.

CISOs need to distill complex technical issues into crisp and meaningful discussions on risk and opportunity in a language the senior business leaders understand and appreciate. Gregory Touhill, Director of the Software Engineering Institute's CERT Division at Carnegie Mellon University, cites[10], "Overwhelming the board and C-suite with 'techno-speak' or an avalanche of PowerPoint slides that don't add value to the running of an effective, efficient, and secure organization erodes trust in the CISO and their organization, often resulting in the CISO being relegated to a smaller role than they ought to have on the corporate leadership team."

Touhill goes on to state that a CISO's ability to negotiate, collaborate, and share information is crucial. He goes as far as to state that "by the end of the decade, the CISO function will subsume all security functions with the CISO role evolving to the broader chief security officer (CSO) role, with responsibility over all security functions: cyber, physical, industrial, and personnel security programs." If his prediction is accurate, the need for a CISO to rely on communication and collaboration will be paramount, especially considering the ever-changing threat and technical landscape.

1.3

AN EVER-CHANGING LANDSCAPE PRESENTS CHALLENGES

As the threat landscape evolves, so must the CISO's role. They must stay ahead of the threats and be able to navigate technological advancements' positive and negative aspects.

CISOs must stay one step ahead of cyber threats. The rise of sophisticated cyber threats, including ransomware and supply chain attacks, demands continuous adaptation and proactive security strategies.

The are several threats that pose a severe risk to organizations. One of these threats is data breaches. According to IBM's Cost of a Data Breach report[11], the top three breaches as grouped by malicious attack are:

1. **Destructive attacks** (rendering systems inoperable and challenging reconstitution) account for 25% of beaches.
2. **Ransomware attacks** - account for 24% of beaches.
3. Attack on the supply chain
    a. **Business partners' supply chain attacks** - account for 15% of beaches.
    b. **Software supply chain attacks** - account for 12% of beaches.

The cost of data breaches is high; on average, IBM estimates that number to be 4.45M USD globally. For the 13th consecutive year, the United States had the highest data breach costs, at 9.48M USD. As a result of a breach, 51% of organizations plan to increase their security investment. The top areas identified for additional investments included incident response (IR) planning and testing, employee training, and threat detection and response technologies. What is quite alarming is that, on average, it takes for an organization to resolve the situation and restore service after the breach has been detected is 277 days.

These high-cost estimates emphasize the importance of staying ahead of the threat actors. Imagine not having to pay or address these complications. To be best prepared to address these threats, CISOs must be up to speed on technological advancements that can aid them.

Technological advancements pose opportunities and challenges to CISOs. They need to stay abreast of emerging technologies like cloud computing, AI, and the IoT and understand their associated security implications.

Let's return to the IBM report to understand these security implications better. The report covers aspects of the mean cost of a data breach. The top five factors that rank most effectively as cost mitigators (those associated with the most significant cost reduction) are the adoption of:

1. A DevSecOps approach
2. Employee training
3. Incident response (IR) planning and testing
4. AI, machine learning-driven insights
5. IR team

In other words, a CISO should consider investing in the areas mentioned above to reduce the cost of a data breach. Those are examples of technological advancements that can aid a CISO.

On the other hand, technological advances pose a challenge to CISOs. The biggest cost amplifiers (those associated with the largest cost increase) include the impact on the IoT or operational technology (OT) environment, security system complexity, noncompliance with regulations, and migration to the cloud.

Collectively, all of these areas should be considered vital areas for an organization's benefit or detriment. One key element is that technology is never constant; the only constant is that it will evolve and change, and a CISO must change with it.

Section II

[Changing Regulatory and Legislative Landscape]

The past two years have seen a whirlwind of changes in the regulatory and legislative landscape, significantly impacting CISOs. There are new regulations to navigate and a growing emphasis on data privacy and consumer rights. More countries are enacting their own data privacy laws on a global scale, adding complexity for multinational organizations. This patchwork of regulations requires CISOs to stay informed and develop strategies for compliance across various jurisdictions.

Furthermore, the growing reliance on cloud computing and interconnected supply chains introduces new security challenges. Regulators are starting to address these concerns, with potential regulations focusing on cloud security posture and vendor risk management. As previously noted, this underscores the need for CISOs to extend their business acumen to other verticals and collaborate with other departments, such as procurement and legal, to ensure a holistic approach to security throughout the entire ecosystem.

2.1

THERE IS A NOTICEABLE INCREASE IN SCRUTINY AND ACCOUNTABILITY

Organizations face more regulatory focus. New regulations are coming from the US, yet there is also constant international pressure. All of this points to the fact that CISOs are experiencing increased legal exposure.

The Securities and Exchange Commission (SEC) has introduced some new cybersecurity rules that warrant

close attention. The SEC's new cybersecurity disclosure and incidents reporting rules require publicly traded companies to disclose details about their cybersecurity risk management programs and report incidents within specific timeframes. To be exact[12]:

- Incidents deemed "material cybersecurity incidents" must be disclosed on Form 8-K within four business days of being deemed material. A registrant may delay filing the Form 8-K if the U.S. Attorney General "determines immediate disclosure would pose a substantial risk to national security or public safety."
- Annual disclosures must be made in Form 10-K and include:
  (1) cybersecurity risk management and strategy,
  (2) "management's role in assessing and managing material risks from cybersecurity threats," and
  (3) "the board of directors' oversight of cybersecurity risks."
- The disclosures must be presented in Inline eXtensible Business Reporting Language (Inline XBRL).

The term material[13] should be interpreted as what the Supreme Court has found to be material: a fact is material if there is a "substantial likelihood that a reasonable investor would consider it important" or if it would have "significantly altered the 'total mix' of information made available." Organizations should be prepared to objectively analyze quantitative and qualitative factors, including evaluating an incident's impact and reasonably likely impacts.

The CISO will be critical in this evaluation process. This requires effective communication among the CISO, finance leader, and legal team to assess materiality. Once materiality is determined, the appropriate response and evaluation of the need for disclosure and the nature of those disclosures can occur. Then, the organization must provide the appropriate information on Form 8-K within four business days.

This puts more pressure on CISOs to ensure robust security practices and transparent communication.

However, this does not stop with the SEC; the **European Union (EU) also flexes its regulatory muscle.** It is widely known that the EU tends to lead on privacy and security regulations. Several measures are being finalized now, including the EU Cyber Resilience Act (CRA) and others.

The CRA[14] aims to safeguard consumers and businesses buying or using "products with digital elements (PDEs)" (including software). The rise in cyber attacks in the EU triggered the CRA. It is designed to introduce mandatory cybersecurity requirements for manufacturers and retailers of PDEs (this protection extends throughout the product lifecycle) to raise the bar regarding cybersecurity practices.

The obligations placed upon manufacturers and retailers of PDEs include:

1. Designing PDEs to meet specific essential cybersecurity requirements through risk assessment and protection against known vulnerabilities
2. Submitting PDEs to conformity assessments
3. Notifying identified vulnerabilities (within 24 hours) to the relevant national cybersecurity authority, the entity that maintains the vulnerable PDE, and, potentially, the European Union Agency for Cybersecurity (ENISA)
4. Notifying severe security incidents to ENISA, the relevant national cybersecurity authority, and users of the PDE
5. Conducting due diligence on imported PDEs

Regarding timing, the CRA will come into force over a phased transition period starting in late 2025.

The CRA is just one of many cybersecurity regulations currently being drafted by the EU. Some of the others are:

- The creation[15] of the European cybersecurity certification scheme (ECCS). The scheme offers EU-wide rules and procedures on certifying information technology (IT) products with security components such as smartphones, bank cards, and routers. It is intended to complement the CRA.
- ENISA is developing[16] the EU Cybersecurity Certification Scheme for Cloud Services (EUCS), a security certification scheme for cloud providers. It might exclude non-EU cloud providers from providing certain ("high" level) services to European companies and preclude EU cloud customers from accessing the services of these non-EU providers. This might have grave consequences for US-based cloud providers.
- The Digital Operational Resilience Act (DORA[17]) aims to strengthen the IT security of financial entities such as banks, insurance companies, and investment firms and ensure that the financial sector in the EU can stay resilient in the event of severe operational disruption, including those related to cyber incidents.
- The NIS2 Directive[18] is the EU-wide legislation on cybersecurity. It provides legal measures to boost cybersecurity in the EU by focusing on preparedness, cooperation, and security

culture.

Failing to comply with these regulations can have severe consequences, including hefty fines and reputational damage. This increased scrutiny necessitates a proactive approach to cybersecurity. CISOs need to invest in technical solid defenses and clear communication plans to keep stakeholders informed in the event of an incident. Building a culture of security awareness within the organization is also essential, as many cyberattacks still leverage human error as an entry point.

Unfortunately, CISOs are experiencing an increase in legal exposure. High-profile breaches and a rise in regulatory enforcement actions have heightened their legal risks. This highlights the need for robust security postures and compliance programs.

Beyond high-profile breaches, CISOs increasingly face personal liability for security lapses. The SEC announced[19] charges against Austin, Texas-based software company SolarWinds Corporation and its chief information security officer, Timothy G. Brown, for "fraud and internal control failures relating to allegedly known cybersecurity risks and vulnerabilities." The complaint alleges that from at least its October 2018 initial public offering through at least its December 2020 announcement, it was the target of a massive, nearly two-year-long cyberattack, dubbed "SUNBURST," SolarWinds and Brown defrauded investors by overstating SolarWinds' cybersecurity

practices and understating or failing to disclose known risks. In its filings with the SEC during this period, SolarWinds allegedly misled investors by disclosing only generic and hypothetical risks at a time when the company and Brown knew of specific deficiencies in SolarWinds' cybersecurity practices as well as the increasingly elevated risks the company faced at the same time. The SEC's action against Brown sets a precedent and sends a clear message: CISOs can be held personally accountable for cybersecurity shortcomings.

THE FOCUS NEEDS TO BE ON PROACTIVE SECURITY AND RISK MANAGEMENT

The only way forward is to be proactive. The fact is that regulations are growing due to governments feeling pressure to address cybersecurity, especially cybersecurity for critical infrastructure.

Data regulations are growing. With growing data breaches and privacy concerns, states like California, Colorado, and Virginia have implemented comprehensive data privacy laws. CISOs must ensure compliance with these regulations, often requiring robust security measures (like zero-trust), data inventorying (known as attack surface management), and user rights management.

How does a CISO prevent a data breach from inception, eliminate any personal responsibility, and stop massive data loss? Simply stop the data breach from happening. It sounds obvious, but it is not that simple. CISOs need to embrace and actively engage in proactive measures to make this a reality. There are several options. Some top approaches are:

1. **Deploy a zero-trust security model:** Zero trust[20] is "an information security model that denies access to applications and data by default. Threat prevention is achieved by only granting access to networks and workloads utilizing policy informed by continuous, contextual, risk-based verification across users and their associated devices." Its three core principles are:
    a. Trust no one at first
    b. Give them access to what they need, nothing else
    c. Always keep an eye on them
2. **Reduce your attack surface:** Businesses increase their likelihood of a cyberattack when they have insecure entry points to the organization's network, known as a weak attack surface. The more users, systems, and networks associated with the organization, the larger the attack surface; thus, the greater your exposure to attack. To counter this, an organization must track all employees and devices; keep records of devices and clear documentation around people, processes, and hierarchies. The CISO must continually map out all relevant assets, label assets accordingly, secure all assets, audit said

The NTSC recognizes that the current state-based privacy law system isn't sustainable. We are encouraging a bipartisan federal bill to be enacted incorporating three crucial elements:

1. **A limited private right of action is needed** to ensure all parties are aware of and bound by a legally established set of guidelines.
2. **The bill should be preemptive**, creating a level playing field for businesses operating in multiple states, leading to cost and resource savings for all affected parties: businesses, shareholders, and consumers.
3. **The Federal Trade Commission (FTC) should enforce the law** with its existing authority.

assets, and monitor everything.

3. **Engage in user rights management:** User rights management, also known as identity and access management, gives individual users within a system access to the tools they need at the right time. It allows an organization to assign users only the minimum access required for their job function. Limiting user access to specific resources and functionalities reduces the overall attack surface for bad actors. Logging user access attempts and activities establishes a clear audit trail. Plus, it facilitates compliance with industry regulations that mandate strict data access controls.
4. **Add a cybersecurity expert to your board of directors:** An expert will help explain the issue, expedite action, and guide executives in the event of a data breach. They can assist in up-leveling the company's collective security posture by helping the executives navigate the evolving threat landscape. In addition, they can provide essential strategic cyber guidance to executives when dealing with complex cyber operations, like digital supply chains[21] or international geo-political cyber processes — many cybersecurity experts are proficient in overseas cyber operations.

These comprehensive measures, deployed in tandem with each other, can significantly reduce the likelihood of cyber attacks.

Critical infrastructure security is top of mind today. The Biden-Harris Administration's focus on securing critical infrastructure will push CISOs to prioritize the security of essential systems.

The Biden-Harris Administration issued an Executive Order to bolster the security of the nation's ports alongside a series of additional actions that will strengthen maritime cybersecurity, fortify our supply chains, and strengthen the United States industrial base. The Executive Order[22] will allow the U.S. Coast Guard to have the express authority to:

1. Respond to malicious cyber activity in the nation's Marine Transportation System (MTS) by requiring vessels and waterfront facilities to mitigate cyber conditions that may endanger the safety of a vessel, facility, or harbor.
2. Institute mandatory reporting of cyber incidents or active cyber threats that endanger any vessel, harbor, port, or waterfront facility.
3. Control the movement of vessels that present a known or suspected cyber threat to U.S. maritime infrastructure and be able to inspect those vessels and facilities that pose a threat to our cybersecurity.

In addition, the U.S. Coast Guard issued a Maritime Security Directive on cyber risk management actions for ship-to-shore cranes manufactured by China at U.S. commercial strategic seaports and a Notice of Proposed Rulemaking on Cybersecurity[23] in the MTS. The Proposed Rule will strengthen digital systems by establishing minimum cybersecurity requirements that best meet international and industry-recognized standards to manage cyber threats.

The Biden-Harris Administration also released the National Cybersecurity Strategy, which aims "to secure the full benefits of a safe and secure digital ecosystem for all Americans."

The strategy highlights[24] the government's commitment to investing in cybersecurity research and new technologies to protect the nation's security and improve critical infrastructure defenses. It outlines five pillars of action, each of which implicates critical infrastructure entities, from strengthening their cybersecurity processes to receiving support from the federal government. The five pillars are:

1. Defend Critical Infrastructure
2. Disrupt and Dismantle Threat Actors
3. Shape Market Forces to Drive Security and Resilience
4. Invest in a Resilient Future
5. Forge International Partnerships to Pursue Shared Goals

The strategy implies that the Biden-Harris Administration is shifting the burden of cybersecurity from smaller players (such as individuals, small businesses, and local government) to the entities with the most significant expertise and resources (such as large operators of critical infrastructure, vendors, and software developers).

The Biden-Harris Administration is making strides to protect the nation's critical infrastructure. Other efforts include:

1. **The 2022 Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA):** Expands the reporting obligations of covered entities.
2. **The 2022 Creating Helpful Incentives to Produce Semiconductors (CHIPS) Act:** Reducs reliance on China-based suppliers of emerging technologies by providing a financial incentive for investment in U.S. semiconductor manufacturing and creating collaborative networks for research and innovation.
3. **President Biden's 2021 Executive Order (on Improving the Nation's Cybersecurity):** Strengthens the nation's cybersecurity defenses by mandating all federal agencies use basic cybersecurity measures (such as multi-factor authentication and requiring new security standards for software makers that contract with the federal government).
4. **President Biden's 2021 national security memorandum:** Directs the Administration to develop cybersecurity performance goals for U.S. critical infrastructure.
5. **President Biden's 2023 Executive Order (on Safe, Secure, and Trustworthy Artificial Intelligence):** Establishes new standards for AI safety and security, protects Americans' privacy, advances equity and civil rights, advocates for consumers and workers, promotes innovation and competition, advances American leadership around the world, and more.
6. **President Biden's 2024 Executive Order (to Protect Americans' Sensitive Personal Data):** Authorizes the Attorney General to prevent the large-scale transfer of Americans' data to countries of concern and provides safeguards around other activities that can give those countries access to Americans' sensitive data.

CISOs must collaborate with the organization's executives to navigate these quickly changing

regulator waters and ensure employees are prepared to help address the challenge.

2.3

THERE IS A GREATER NEED FOR COLLABORATION AND COMMUNICATION

There needs to be more focus on building collaborative relationships and communicating pivotal risks in an understandable manner to those running the organization. This also extends to other stakeholders, including employees.

The CISO must align with business objectives. New regulations often necessitate collaboration between CISOs and other C-suite executives. CISOs must clearly communicate risks and translate them into actionable business decisions to gain support for security initiatives.

As Section One highlighted, collaboration between CISOs, C-suite executives, and the board of directors is no longer optional in today's complex regulatory landscape; it's essential. New regulations often impose strict data privacy and security requirements, demanding a unified approach across the organization. This is where the CISO's ability to translate technical complexities into actionable business terms becomes crucial.

By clearly communicating cyber risks and their potential financial and reputational impact, CISOs can effectively bridge the gap between security and business objectives. Imagine a scenario where a new regulation mandates stricter data protection measures. A CISO, fluent in cybersecurity and business language, can explain the potential consequences of non-compliance – hefty fines, brand damage, and loss of customer trust. This clear articulation of risk allows C-suite executives or the board of directors to understand the security program not as a cost center but as a critical investment in safeguarding the organization's future.

A CISO who can translate cyber risks into tangible

business consequences ultimately empowers informed decision-making. This fosters collaboration, secures buy-in for security initiatives, and ensures the organization navigates the ever-changing regulatory landscape with agility and resilience.

Security awareness and training are more important than ever. Regulations often emphasize accountability and adaption, which can be accomplished through awareness and training. Some explicitly require user education and training. CISOs need to work across departments to build a culture of security awareness and encourage responsible behavior within the organization.

For example, these regulations require training -

- **HIPAA (Health Insurance Portability and Accountability Act):** This US regulation protects the privacy of patients' health information and requires covered entities to implement a security awareness and training program for their workforce.
- **DORA:** This EU regulation requires that the board of directors maintain sufficient knowledge and skill to understand and assess Information and Communications Technology risk and its potential impact on the organization, including by regularly following specific training[25].

While these regulations don't explicitly require training, but emphasize the principle of accountability -

- **GDPR (General Data Protection Regulation):** The EU regulation doesn't explicitly mandate user training but emphasizes accountability. This means organizations are responsible for ensuring that all processing of personal data complies with the regulations. User training on data protection practices is considered a key element in achieving this accountability.
- **California Consumer Privacy Act (CCPA):** California's regulation focuses on consumer data privacy and doesn't explicitly mandate user training. However, organizations that collect and process personal data from California residents are responsible for implementing reasonable security measures, which may include user training on data handling practices.

The emphasis on user education and training within cybersecurity regulations underscores a critical truth: security is a team effort. While technical controls are essential, regulations increasingly recognize that the human element remains a significant vulnerability. This is where CISOs take center stage, not just as technology leaders but as champions of security awareness across the organization.

To effectively address this challenge, CISOs need to collaborate with various departments that span an organization. Here are some specific ways they can do so:

- **Work with human resources** to ensure security awareness training is integrated into onboarding programs and ongoing professional development.
- **Partner with communications teams** to ensure clear, consistent messaging about cybersecurity best practices reaches all employees, regardless of technical background.
- **Engage department heads** to tailor security training programs to address specific departmental needs and risks.
- **Partner with IT and security teams** to develop training content based on the latest security threats and trends.

By fostering a culture of security awareness, CISOs empower employees to become the organization's first line of defense. Regular training equips employees to recognize phishing attempts, avoid suspicious links and attachments, and report potential security incidents promptly. This collaborative approach, driven by the CISO, not only fulfills compliance requirements but also creates a collective responsibility for cybersecurity within the organization.

Section III

[What Should CISOs Expect Going Forward]

The next five years promise an even more dynamic cybersecurity landscape for CISOs. Looking at the evolution of the CISO's role and the regulatory environment, let's use that framework to guide you. We will start with the changing role of the CISO in the near future.

3.1

THE SKILLS THAT WILL BE NEEDED WILL CONTINUE TO EVOLVE

The CISO's role will change to address more than just cybersecurity. With that change, they must evolve to become more business-minded leaders who can communicate with all organizational stakeholders, especially those in the physical security space.

The CISO will become a business translator. The evolving cybersecurity landscape demands a CISO who transcends technical expertise. As cyber threats become more sophisticated and regulations tighten, the CISO's role transforms into that of a skilled business translator. This means effectively communicating the complex world of cybersecurity risks in a language business leaders understand—the language of financial impact and return on investment (ROI).

In an era of ever-increasing cyber threats (such as destructive attacks, ransomware, and supply chain threats), securing necessary resources will be a top priority for CISOs. Gone are the days of relying solely on technical jargon to justify security investments. CISOs must become adept at translating cyber risks into terms that resonate with business leaders. This means quantifying the potential financial impact of security breaches, including lost revenue, operational downtime, and reputational damage. For example, the average

ransomware attack cost in 2023 increased by 13% to 5.13M USD, while the average[26] supply chain attack cost in 2023 increased by 11.8% to 4.76M USD.

Data-driven security reporting is critical to this translation process. Moving beyond technical logs and alerts, CISOs must develop reports demonstrating the effectiveness of existing security measures and the potential ROI for proposed security initiatives. By showcasing the tangible benefits of cybersecurity investments, CISOs can secure the buy-in from budget holders and gain the resources required to build a robust security posture.

Ultimately, the CISO who can articulate the business value of cybersecurity will be well-positioned to navigate the evolving threat landscape. This shift towards business acumen, strong communication skills, and data-driven reporting will ensure that security remains a top organizational priority, not just a technical cost center.

They will also be crisis communication experts. In today's interconnected world, cyberattacks are no longer a matter of "if" but "when." This reality will elevate the CISO's role beyond proactive security. They will also need to be crisis communication experts, prepared to lead the organization through the aftermath of a security incident. Honing these skills is critical for effectively managing public relations, stakeholder expectations, and minimizing reputational damage during a critical time.

A CISO's crisis communication strategy should be developed and well-rehearsed before any incident occurs. This plan should be part of the larger IR plan. The communication plan[27] should:

1. **Define your stakeholders (internal and external)** to include everyone affected by a cyber incident, including employees, management, customers, partners, and regulatory bodies.
2. **Determine notification procedures**, including identifying who will notify stakeholders and what communication channels will be used.
3. **Establish response procedures** such as activating your IR team, containing the incident, and conducting an investigation. It's essential to have a transparent process in place so that your organization can respond quickly and effectively.
4. **Set up communication channels** such as email, text messages, phone calls, and social media. It is vital to ensure that stakeholders are informed promptly and accurately.

By having a well-defined plan, the CISO can ensure a swift and coordinated response, minimizing confusion and fostering stakeholder trust.

By having a well-defined plan, the CISO can ensure a swift and coordinated response, minimizing confusion and fostering stakeholder trust.

Clear and transparent communication is paramount during a crisis. The CISO needs to communicate the nature of the incident, the scope of the impact, and the steps being taken to address the situation in a way that is understandable to both technical and non-technical audiences. Additionally, the CISO needs to manage stakeholder expectations by providing regular updates on the problem without revealing sensitive information that could compromise the investigation or future legal proceedings.

While a cyberattack can be a significant setback, a CISO's adept crisis communication skills can mitigate the damage. By fostering trust through transparency and demonstrating a commitment to resolving the situation, the CISO can help the organization recover its reputation and emerge

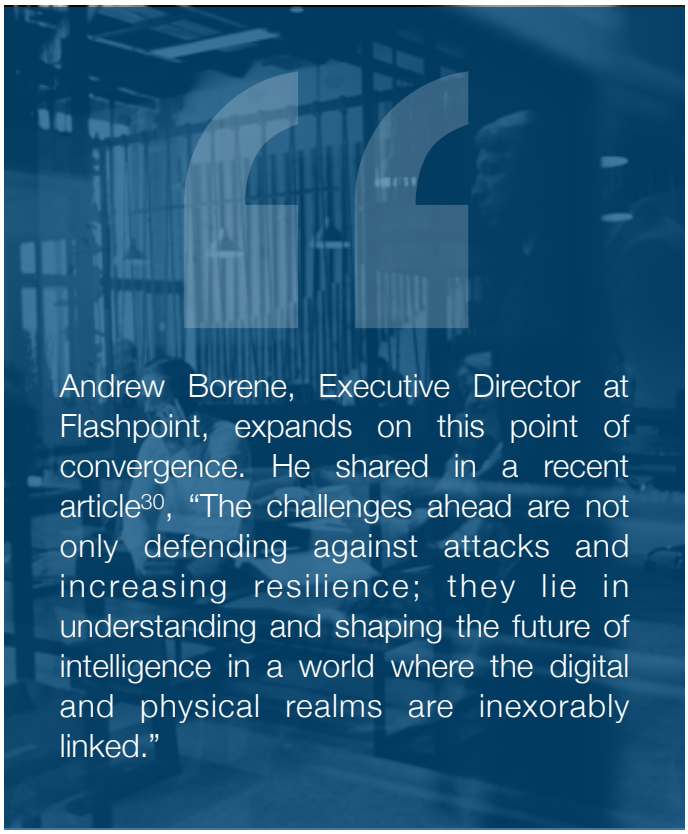
stronger from the ordeal. In essence, the CISO's ability to navigate crisis communication effectively can be the difference between a temporary setback and a long-term public relations disaster.

Cyber-physical security convergence will be a new area that a CISO will occupy. The digital revolution is rapidly blurring the lines between the physical and cyber realms. This convergence has significant implications for cybersecurity, demanding a new approach from security leaders. CISOs, traditionally focused on securing IT systems, will increasingly find themselves at the forefront of a new domain: cyber-physical security.

As operational technology (OT) systems become more interconnected and reliant on digital controls, they become vulnerable to cyberattacks. These attacks can have devastating consequences, potentially disrupting critical infrastructure operations, causing physical harm, and incurring significant financial losses. Traditional physical security measures, like fences and cameras, are no longer enough. A holistic approach that integrates IT security best practices with physical security controls is essential. This convergence necessitates a shift in the CISO's role.

A 2022 report[28] by Fortinet noted that only 15% of respondents say that the CISO holds responsibility for OT security, but 79% say that they expect the function to be rolled under the CISO over the next 12 months. Fortinet conducted another survey[29] in 2023 and found that 95% of respondents plan to roll OT cybersecurity underneath the CISO in the next 12 months.

Expertise in IT security will remain vital; CISOs will also need to broaden their purview to encompass OT security considerations. This might involve collaborating with OT engineers to understand system vulnerabilities, working with physical security teams to integrate cyber controls, and developing incident response plans that address both digital and physical threats. By bridging the gap between IT and physical security, CISOs can ensure a more comprehensive security posture for the entire organization.



Andrew Borene, Executive Director at Flashpoint, expands on this point of convergence. He shared in a recent article[30], "The challenges ahead are not only defending against attacks and increasing resilience; they lie in understanding and shaping the future of intelligence in a world where the digital and physical realms are inexorably linked."

The future of security belongs to those who can navigate this convergence. By embracing cyber-physical security and expanding their skillset, CISOs will become true security leaders capable of safeguarding data and the critical infrastructure that underpins our society.

3.2

THE THREAT LANDSCAPE WILL CONTINUE TO GROW IN NEW AND CHALLENGING WAYS

The threat landscape will evolve as bad actors test and expand their capabilities. Interconnected devices, AI, and quantum computing are just a few areas of concern. The underlying takeaway is that CISOs need countermeasures to guard against these and other threats.

A hyper-connected world will only become more connected. The expanding IoT and interconnected devices will create a vast attack surface for bad actors. CISOs will need to develop strategies for securing these diverse endpoints.

Traditionally, security strategies focused on a well-defined perimeter, protecting a finite number of devices like desktops and servers. However, the explosion of IoT devices creates a vast and constantly evolving network. Each device, with its varying operating systems, security protocols, and potential vulnerabilities, represents a possible entry point for attackers.

This hyper-connected world demands a new approach to security. CISOs need to develop strategies that can adapt to this ever-expanding attack surface. This might involve implementing automated vulnerability management tools to scan and identify connected devices' weaknesses continuously. Additionally, leveraging technologies like microsegmentation can create smaller security zones within the network, limiting the potential damage if a single device is compromised.

CISOs must adopt a proactive and layered security approach to navigate the complexities of the hyper-connected world. By acknowledging the vast attack surface and implementing robust security measures, they can safeguard critical systems and data from the ever-evolving threats lurking within the ever-growing web of interconnected devices.

AI-powered attacks will grow in size and scope. Malicious actors will increasingly leverage AI to automate attacks, personalize them, and bypass traditional security measures. CISOs need to adopt AI-powered security solutions to stay ahead.

Imagine an AI program that analyzes vast amounts of data to identify vulnerabilities in an organization's specific software versions. This AI could then launch a targeted attack campaign, exploiting those vulnerabilities with unprecedented efficiency. Further, AI can be used to personalize phishing emails, mimicking writing styles and tailoring content to specific individuals, making them appear more believable and significantly increasing the chances of success. In addition, AI will increase the volume of these attacks. World

Wide Technology (WWT) recently noted[31] that "Hypothetically, an adversary who was sending 5,000 phishing emails before leveraging AI and automation is now capable of sending 20,000 emails — and it only takes one person to fall for it."

Traditional security solutions, reliant on pre-defined rules and signature-based detection, will struggle to keep pace with this evolving threat landscape. CISOs who remain tethered to outdated methods risk falling behind. To stay ahead of these AI-powered attacks, CISOs need to embrace AI themselves.

By adopting AI-powered security solutions, CISOs can gain a significant advantage. As we noted in Section One, today, one of the top five factors that rank most effectively as cost mitigators is the adoption of AI, machine learning–driven insights. This will continue to grow in effectiveness. AI-powered security solutions can analyze network traffic and user behavior in real time, identifying anomalies and suspicious patterns that might escape traditional detection methods. Additionally, AI-powered security tools can automate IR, allowing organizations to react swiftly and mitigate potential damage before a cyberattack can take hold. That said, it is essential to note that AI alone isn't the answer. WWT cited that "combining human expertise with AI-driven tools creates a more robust and adaptive approach to cyber resilience." A CISO can maximize both by aligning AI objectives with business priorities, establishing an AI center of excellence, and educating users on AI best practices and responsible AI usage.

The future of cybersecurity is a race between offense and defense, and AI is poised to play a pivotal role on both sides. By proactively adopting AI-powered security solutions, CISOs can ensure they have the tools to stay ahead of bad actors and safeguard their organizations from the evolving threats of the intelligent age.

The quantum computing threat might finally see the light of day. While still in its infancy, quantum computing could potentially render current encryption methods obsolete. CISOs need to stay informed and plan for potential security vulnerabilities.

While the timeline for fully functional, commercially available quantum computers remains uncertain, the potential impact is undeniable. These machines harness the bizarre principles of quantum mechanics to perform calculations that would take traditional computers eons to complete. Quantum computers[32], when scaled up, will do things that even today's most powerful supercomputers could never do, including factoring large numbers, a cornerstone of many widely used encryption methods like RSA (Rivest–Shamir–Adleman), a public-key cryptosystem, one of the oldest widely used for secure data transmission. If a powerful enough quantum computer were to become operational, it could crack these codes, rendering vast amounts of sensitive data vulnerable.

The future of cybersecurity in a quantum world is yet to be written. However, proactive CISOs can't afford to wait and see. Staying informed about the latest advancements in quantum computing research is crucial. Additionally, exploring and implementing "quantum-resistant" cryptography algorithms, even if they are in the early stages of development, demonstrates a forward-thinking approach. By acknowledging the potential threat and taking preparatory steps, CISOs can ensure their organizations are not caught flat-footed when the quantum era dawns.

The fight to stay ahead of cyber threats is a continuous race, and the potential disruption of quantum computing demands a proactive approach. By staying informed, exploring new solutions, and planning for possible vulnerabilities, CISOs can ensure their organizations remain secure in the face of this evolving technological landscape.

Emerging technologies and solutions will hold massive value for CISOs. There are several emerging technologies on the horizon. Some that hold a lot of potential. We have listed three areas CISOs should be mindful of. They are:

- **Zero Trust Architecture:** Zero trust principles will become the standard, requiring continuous authentication and verification for all users and devices. This shift from implicit trust within the network perimeter demands focusing on micro-segmentation and least privilege access controls to minimize the attack surface and potential damage, especially in a world with AI. Checkpoint notes[33] that AI-integrated applications disrupt

the clear distinction between users and applications. This reality introduces a new set of security vulnerabilities, such as data leakage, prompt injection, and risky access to online resources (even corporate resources) on behalf of employees. A zero trust AI access approach is needed to address these challenges.

- **Security Mesh Architecture:** Securely connecting and managing distributed cloud environments will be crucial for modern businesses. In Section One, we noted that migration to the cloud is a current challenge for CISO and increases data breach costs. That said, CISOs need to be familiar with these concepts as security mesh architectures offer a dynamic and scalable approach to securing hybrid and multi-cloud deployments, replacing the limitations of traditional, centralized security tools.
- **Advanced Threat Detection and Response (XDR):** CISOs will increasingly rely on AI-powered XDR solutions to automate threat detection, investigation, and response across diverse systems. XDR goes beyond traditional endpoint detection and response (EDR) solutions by collecting and correlating data from a broader range of sources, enabling CISOs to identify and respond to sophisticated attacks that might span multiple systems and user accounts.

3.3

SCRUTINY AND ACCOUNTABILITY WILL CONTINUE TO INCREASE AS SECURITY AND RISK MANAGEMENT CONCERNS GROW

As the threat landscape continues to grow, so will the scrutiny and expectations placed on the CISO. As we move into the coming years, governments will introduce more regulations, fines, and penalties. This heightened awareness will drive consumers to demand greater transparency.

There will be an expansion of existing regulations. Look no further than Europe to see what the future holds. Expect stricter enforcement of current regulations like GDPR, CRA, and DORA. This will also extend to the US.

This expansion of regulations presents both challenges and opportunities for CISOs. On the one hand, complying with a growing patchwork of regulations can be a complex and resource-intensive undertaking. CISOs must stay current on evolving regulations and adapt their security posture accordingly. This will involve implementing new data governance processes, conducting privacy impact assessments, and strengthening data security controls.

However, stricter regulations can also be a catalyst for positive change. By prioritizing compliance, CISOs can foster a culture of data security within their organizations. This can lead to improved data governance practices, more robust access controls, and a heightened awareness of data privacy among employees. Ultimately, focusing on compliance will translate into a more robust overall security posture, better protecting sensitive data and mitigating the risk of cyberattacks and data breaches.

As the regulatory landscape evolves, CISOs who embrace a proactive approach will be well-positioned to navigate the challenges and capitalize on the opportunities. By building a solid foundation of data security practices and staying informed about regulatory changes, CISOs can ensure their organizations are compliant, secure, and prepared for the future.

Organizations will face increased fines and penalties. Be prepared for harsher penalties for data breaches and non-compliance with regulations. This will incentivize organizations to prioritize data privacy.

An interesting aspect that surfaced in IBM's Cost of a Data Breach report is that in environments with high levels of data regulation, 58% of costs continued to accrue after the first year. In low-regulation environments, 64% of the costs associated with a breach were more likely to be resolved within the first year. As more governments adopt regulatory measures, fines will increase after the initial breach.

The potential cost of non-compliance, exceeding millions of dollars sometimes, will force CISOs and executive management to re-evaluate their approach to data security. Investing in robust security measures, implementing comprehensive data governance practices, and prioritizing employee training on data privacy will no longer be seen as optional expenses but as essential investments.

The focus on stricter penalties is not solely about punishment; it's about deterrence. By holding organizations accountable for data breaches and privacy violations, regulators aim to change behavior. The threat of hefty fines compels organizations to prioritize data security to protect their reputation and avoid significant financial repercussions. Ultimately, this shift in enforcement will benefit consumers by encouraging organizations to handle personal data with greater responsibility.

Data privacy is no longer a peripheral concern as non-compliance costs rise but a central pillar of a strong cybersecurity posture. CISOs who embrace this reality and prioritize data security safeguard sensitive information and position their organizations for success in the evolving

regulatory landscape. The future belongs to those who recognize the importance of data privacy and take proactive steps to comply with regulations and mitigate the risk of costly fines.

This will increase consumer demand for transparency and control. Expect consumers to be more proactive about their data privacy. Consumers will demand greater transparency in collecting, using, and sharing data in the coming years.

This shift in consumer behavior will present both challenges and opportunities for organizations. CISOs must develop clear and concise data privacy policies that are easily accessible to all users. These policies should explain what data is collected, why, and how it will be used. Additionally, consumers expect organizations to offer them meaningful control over their data. This might include the ability to request access to their data, opt out of targeted advertising, or have their data deleted upon request.

Meeting these evolving consumer demands presents an opportunity for organizations to build trust and loyalty. By demonstrating a commitment to data privacy through transparent practices and user-friendly control mechanisms, CISOs can foster a positive relationship with consumers. In today's digital age, trust is a valuable asset, and organizations prioritizing data privacy can gain a competitive edge by demonstrating their respect for consumer rights. As consumers become more

empowered, CISOs who embrace transparency and empower user control will be well-positioned to navigate this evolving landscape and build lasting trust with their customers.

3.4

COLLABORATION AND INFORMATION SHARING WILL BE THE ONLY WAY FORWARD

Collaboration and information sharing will be paramount as the threat landscape grows and governments respond with significant control. This future will require more information sharing and reliance on best practices to respond effectively. There will be a convergence in private and public interests, and harmonization of regulation will emerge.

The importance of information sharing between organizations will grow. Collaboration amongst businesses and government agencies will be critical to addressing evolving threats and developing effective regulatory frameworks in the coming years.

By sharing threat intelligence, organizations can gain a broader perspective on the tactics and tools employed by bad actors. Imagine a scenario where a company experiences a sophisticated ransomware attack. By promptly sharing details of the attack method and the malware used with industry peers and government agencies, they can help others identify and mitigate the same threat. This collaborative approach allows organizations to learn from each other's experiences, bolster collective defenses, and ultimately make it more difficult for attackers to succeed.

In addition, information sharing is crucial for developing effective regulatory frameworks. Regulatory bodies need a clear understanding of businesses' challenges in the digital age. By collaborating with industry leaders and security experts, governments can craft regulations that effectively protect consumer data and are practical for businesses to implement. Open communication allows for identifying potential loopholes in proposed regulations, ensuring they achieve their intended purpose without creating unnecessary burdens for organizations.

By fostering information sharing between organizations and government agencies, the cybersecurity community can collectively strengthen its defenses against evolving threats and develop a regulatory landscape that fosters innovation while safeguarding consumer privacy. CISOs who champion collaboration and information sharing are vital in building a more secure digital future for all.

There will be a greater reliance on industry best practices. Industry-specific best practices and standards for data privacy will become more prominent, allowing CISOs to benchmark their security posture.

These industry best practices offer a roadmap for CISOs, outlining recommended security controls, data governance procedures, and incident response protocols specific to their sector. By aligning their security posture with these industry standards, CISOs can gain valuable insights into the data protection expectations within their field. This allows for a more targeted approach to security, ensuring they focus on the most critical controls to mitigate the most relevant threats.

Furthermore, industry best practices provide a benchmark for CISOs to assess their organization's security posture. By comparing their existing controls and procedures with established industry standards, CISOs can identify areas for improvement and prioritize their security investments. This allows them to demonstrate to stakeholders, such as boards of directors and regulators, that they are adhering to the recommended security practices within their industry.

A reliance on industry best practices fosters a collaborative approach to data privacy within a specific sector. By sharing knowledge and best practices, organizations within an industry can collectively elevate their security posture, making it more difficult for bad actors to exploit vulnerabilities. CISOs who embrace industry standards position themselves as leaders in data privacy within their field, building trust with consumers and regulators by demonstrating their commitment to best-in-class security practices.

You will see a convergence of disparate laws and regulations. There will be greater unification of regulatory laws in the US and abroad, driven by the need to reduce cost, risk, and confusion. These changes will be a focus for the public and private sector, alike.

The current global landscape of data privacy regulations is a patchwork of diverse and often conflicting laws. This complexity creates significant challenges for multinational organizations, forcing CISOs to navigate a

labyrinth of regulations that vary by region and industry. However, a trend toward convergence of disparate data privacy laws will gain momentum in years to come.

The push for harmonization will be primarily fueled by the economic realities of operating in a globalized digital world. Complying with a multitude of regulations with unique requirements is a resource-intensive undertaking. Organizations spend vast amounts of time and money deciphering legal nuances, implementing region-specific controls, and managing the administrative burden of compliance. Harmonization towards a more unified set of data privacy principles would significantly reduce these costs, allowing organizations to focus their resources on robust security practices rather than navigating regulatory intricacies.

Furthermore, regulatory convergence would also mitigate risk for both organizations and consumers. The current patchwork of laws creates uncertainty for organizations, as unintentional non-compliance with a specific regulation in a particular region can result in hefty fines and reputational damage. The lack of uniformity makes it difficult for consumers to understand their data privacy rights across different platforms and jurisdictions. A unified set of data privacy principles would provide clarity and consistency, reducing risk for all stakeholders.

While achieving complete global harmonization of data privacy laws might be a distant dream (spanning more than five years), a move towards convergence holds immense promise. By working towards a more standardized approach, regulators can create a more predictable and efficient environment for businesses while fostering stronger data privacy protections for consumers worldwide. CISOs who stay abreast of this convergence trend can proactively adapt their security posture to comply with evolving regulations, ensuring their organizations are prepared to navigate the future of data privacy.

Conclusion
[A Wrap Up]

The digital landscape is a dynamic battleground, and the role of the CISO is transforming to meet the ever-present challenge of cybersecurity. This white paper has explored the key trends shaping the future, from the evolving skillset required of CISOs to the expanding regulatory landscape and the emergence of new threats.

As we look towards the horizon, it's clear that CISOs who embrace change will be best positioned to safeguard their organizations. The future of cybersecurity is undoubtedly complex, but it is also brimming with opportunity. By adopting these trends, honing their skill sets, and fostering a collaborative approach, CISOs can transform themselves from security tacticians into business leaders, building a secure digital future for their organizations.

We hope this white paper has equipped you with the knowledge and insights to navigate the evolving cybersecurity landscape confidently. Stay informed, adapt to change, and embrace collaboration are the cornerstones of success in this ever-changing digital age.

Patrick Gaul
Executive Director
NTSC

The evolving role of the CISO demands a new breed of leader – one who is not only a technical expert but also a strategic business partner. CISOs must translate complex cybersecurity risks into clear business terms, demonstrating the return on investment for cyber threat countermeasures. Data-driven security reporting will be paramount to securing budgets and resources.

Then, when a cyber incident hits, CISOs must address all stakeholder expectations - reinforcing the need for a deep understanding of the organization's business objectives and the ability to communicate with various audiences.

The days of the CISO wholly focusing on pure security are behind us. The evolution of the CISO's role necessitates a broader understanding of cybersecurity and business considerations. In this journey, the entire NTSC and I stand as dedicated resources to help CISOs in this expansion. By fostering a collaborative approach, we ensure CISOs and their companies are not just prepared, but well-equipped for the future.

Endnotes

[1] Deloitte. (2023). *Understanding SEC requirements for cybersecurity disclosures*. Deloitte.com. https://www2.deloitte.com/us/en/pages/risk/articles/SEC-cybersecurity-disclosure-rules.html

[2] Ians. (2024). *State of the CISO, 2023–2024 Benchmark Summary Report*. iansresearch.com. https://www.iansresearch.com/resources/infosec-content-downloads/research-reports/2023-2024-state-of-the-ciso-benchmark-report

[3] Oltsik, J. (2023). *The Life and Times of Cybersecurity Professionals Volume VI, 2023*. techtarget.com. https://www.techtarget.com/esg-global/survey-results/complete-survey-results-the-life-and-times-of-cybersecurity-professionals-volume-vi-2023/

[4] The Institute of World Politics. *Evolution of the Chief Information Security Officer*. cyberintelligence.world. https://cyberintelligence.world/evolution-of-the-chief-information-security-officer/

[5] Nagothu, M. (2024). *The Changing Role of the CISO in 2024 | Navigating New Frontiers in Cybersecurity*. sentinelone.com. https://www.sentinelone.com/blog/the-changing-role-of-the-ciso-in-2024-navigating-new-frontiers-in-cybersecurity/

[6] Bain & Company (2022). *Customer Success: The Next Frontier of AI.* bain.com. https://www.bain.com/insights/customer-success-next-frontier-of-AI-tech-report-2022/

[7] Anaya, M. (2023). *Advice for Leaders—A CISO Needs to be a Leader First*. decodingCyber.com. https://www.decodingcyber.com/articles/advice-for-leaders-be-a-leader-first

[8] Anaya, M. (2023). *Building a Cybersecurity Team Structure: Best Practices*. decodingCyber.com. https://www.decodingcyber.com/articles/building-cybersecurity-team-structure

[9] Ashkenas, R. and Manville, B. (2018). *The 6 Fundamental Skills Every Leader Should Practice*. HBR.com. https://hbr.org/2018/10/the-6-fundamental-skills-every-leader-should-practice

[10] Touhill, G. (2024). *The Top 10 Skills CISOs Need in 2024*. CMU.edu. https://insights.sei.cmu.edu/blog/the-top-10-skills-cisos-need-in-2024/

[11] IBM (2023). *Cost of a Data Breach Report 2023*. IBM.com. https://www.ibm.com/reports/data-breach

[12] Deloitte (2023). *SEC Issues New Requirements for Cybersecurity Disclosures*. Deloitte.com. https://dart.deloitte.com/USDART/home/publications/deloitte/heads-up/2023/sec-rule-cyber-disclosures

[13] PWC (2023). *Making materiality judgments in cybersecurity incident reporting*. PWC.com. https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/sec-final-cybersecurity-disclosure-rules/materiality-sec-cybersecurity-compliance.html

[14] Young, M. and Aleksiev, A. (2023). *The EU's Cyber Resilience Act Has Now Been Agreed*. insideprivacy.com. https://www.insideprivacy.com/cybersecurity-2/the-eus-cyber-resilience-act-has-now-been-agreed/

[15] Covington (2023). *EU cyber regulation wave quietly rolls on – Commission set to finalize new cyber standards*. insideprivacy.com. https://www.insideprivacy.com/cybersecurity-2/eu-cyber-regulation-wave-quietly-rolls-on-commission-set-to-finalize-new-cyber-standards/

[16] Covington (2023). *Implications of the EU Cybersecurity Scheme for Cloud Services*. insideprivacy.com. https://www.insideprivacy.com/cybersecurity-2/implications-of-the-eu-cybersecurity-scheme-for-cloud-services/

[17] EIOPA (2023). *Digital Operational Resilience Act (DORA).* europa.eu. https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

[18] EIOPA (2023). *Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive).* europa.eu. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

[19] SEC (2023). *SEC Charges SolarWinds and Chief Information Security Officer with Fraud, Internal Control Failures.* SEC.gov. https://www.sec.gov/news/press-release/2023-227

[20] Holmes, D. and Burns, J. (2022). *The Definition Of Modern Zero Trust.* Forrester.com. https://www.forrester.com/blogs/the-definition-of-modern-zero-trust/

[21] Schiller, N. (2023). *Understanding and Mitigating Cybersecurity Supply Chain Risks*. decodingCyber.com. https://www.decodingcyber.com/articles/cybersecurity-supply-chain-risks

[22] The White House (2024). *FACT SHEET: Biden-Harris Administration Announces Initiative to Bolster Cybersecurity of U.S. Ports*. Whitehouse.gov. https://www.whitehouse.gov/briefing-room/statements-releases/2024/02/21/fact-sheet-biden-harris-administration-announces-initiative-to-bolster-cybersecurity-of-u-s-ports/

[23] The National Archives (2024). *Cybersecurity in the Marine Transportation System*. FederalRegister.gov. https://www.federalregister.gov/documents/2024/02/22/2024-03075/cybersecurity-in-the-marine-transportation-system

[24] Crowell & Moring LLP (2023). *Biden Administration Releases Comprehensive National Cybersecurity Strategy*. Crowell.com. https://www.crowell.com/en/insights/client-alerts/biden-administration-releases-comprehensive-national-cybersecurity-strategy

[25] Maddox, R. and Lockwood, T. (2023). *EU Digital Operational Resilience Act (DORA): Management Obligations and the Role of the Board*. NYU.edu. https://wp.nyu.edu/compliance_enforcement/2023/04/24/eu-digital-operational-resilience-act-dora-management-obligations-and-the-role-of-the-board/

[26] IBM (2023). *Cost of a Data Breach Report 2023*. IBM.com. https://www.ibm.com/reports/data-breach

[27] Gopalakrishnan, C. (2023). *The Five Steps of a Cyber Incident Response Communication Plan*. TheCyberExpress.com. https://thecyberexpress.com/cyber-incident-response-communication-plan/

[28] Fortinet (2022). *2022 State of Operational Technology and Cybersecurity Report*. Fortinet.com. https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/report-2022-ot-cybersecurity.pdf

[29] Fortinet (2023). *2023 State of Operational Technology and Cybersecurity Report*. Fortinet.com. https://www.fortinet.com/demand/gated/report-state-ot-cybersecurity

[30] Borene, A. (2024. *Beyond Bytes and Bullets: Shaping the Future of Allied Threat Intelligence*. LinkedIn.com. https://www.linkedin.com/pulse/beyond-bytes-bullets-shaping-future-allied-threat-andrew-borene-e17yc/
[31] World Wide Technology (2024). *AI's Role in Cyber Offense and Defense Strategies*. WWT.com. https://www.wwt.com/wwt-research/ais-role-in-cyber-offense-and-defense-strategies
[32] Bell, C. (2023). *Building a quantum-safe future*. Microsoft.com. https://blogs.microsoft.com/blog/2023/05/31/building-a-quantum-safe-future/
[33] Behor, T.. (2024). *Top GenAI Threats – and why Zero Trust AI Access is the Future*. Checkpoint.com. https://blog.checkpoint.com/artificial-intelligence/top-genai-threats-and-why-zero-trust-ai-access-is-the-future/

2625 Piedmont Road NE, Suite 56-370
Atlanta, Georgia 30324
ntsc.org

The National Technology Security Coalition (NTSC) is a non-profit, non-partisan organization that serves as the preeminent advocacy voice for Chief Information Security Officers (CISOs) across the United States. Through dialogue, education, and government relations, we unite both public and private sector stakeholders around policies that improve national cybersecurity standards and awareness.