CISO 2.0

NTSC
NATIONAL TECHNOLOGY
SECURITY COALITION

ntsc.org

Jason Witty
Chief Information & Security Officer
USAA

"Over the last decade, the role of the CISO has changed dramatically. While an important and complex role ten years ago, the sophistication, velocity, and volume of cyber-attacks has elevated cyber-security to a Board level topic in recent years. The skills required to be successful in the role have also shifted from needing to understand various policy, governance, frameworks, and oversight practices to deeply understanding international threat intelligence, information sharing networks, public-private operational collaboration processes, and rapidly emerging technologies at a deep technical level. This must all be done while still being an agile organizational leader, thought leader, recruiter, communicator, and coach."

As Jason points out, the role of the CISO has evolved, as has the landscape that surrounds them. These men and women are charged with protecting the enterprise from cyber adversaries, be they nation-states, cyber criminals, or an unwitting employee falling victim to a phishing attempt or committing a non-malicious violation of company policy.

Additionally, today's CISO faces a changing regulatory environment as legislators at both the state and federal levels attempt to address the challenges facing our economy from the proliferation of cyberattacks. Moreover, many legislative initiatives pose serious liability issues for CISOs as legislators seek to hold corporate executives accountable for cyber incidents that impact consumers, making the role even more challenging.

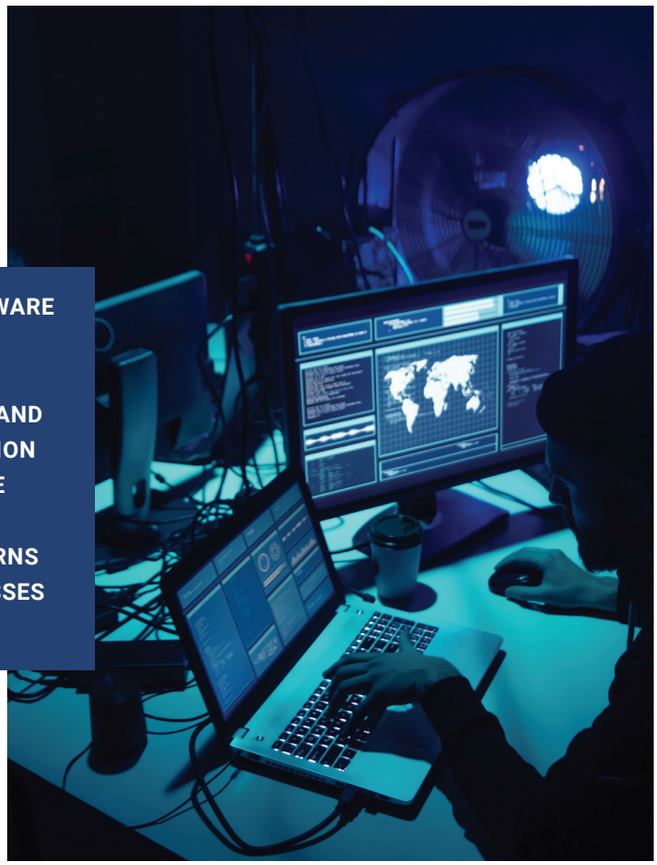
In this paper, we will explore the following:

1. The evolution of the CISO, from a purely technical advisor to that of a "C" Suite business leader.
2. The regulatory environment that surrounds the CISO and how the changes being contemplated in 2022 and beyond could impact the role of the CISO
3. The potential impact items 1 & 2 will have on CISOs and share some thoughts on how both might affect the role in the future

SECTION ONE:

The Changing Role of the CISO

As we navigate 2022, CISOs will face multiple challenges including, but not limited to, the proliferation of ransomware; the challenges that zero day and software supply chain incidents pose; and increased threats from nation-states including China, Russia, North Korea, Iran, and other countries who can easily threaten businesses across the country, but may not have the same expertise as the more advanced adversarial states and therefore are more likely to create a major incident similar to what occurred with Colonial Pipeline. Finally, there is a national cyber workforce shortage that continues to create challenges for businesses across the globe.



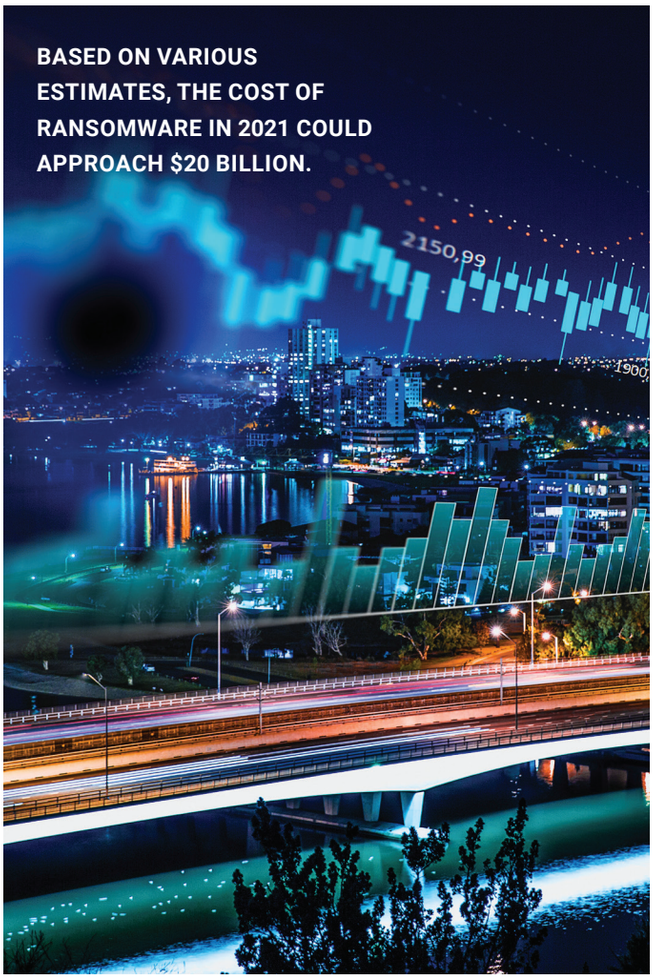
TODAY, RANSOMWARE DOMINATES THE CYBERSECURITY CONVERSATION, AND THE PROLIFERATION OF RANSOMWARE ATTACKS HAVE CREATED CONCERNS ACROSS BUSINESSES OF ALL SIZES.

RANSOMWARE

A recent article published in ***Security Magazine*** notes that "Ransomware will continue to be a significant threat in 2022 and that Ransomware gangs have refined their business models through the use of Ransomware as a Service and are more aggressive in negotiations by doubling down with distributed denial-of-service (DDoS) attacks. The further convergence of IT and Operational Technology (OT) may cause more security issues and lead to ransomware attacks if proper cybersecurity hygiene isn't followed."

Today, ransomware dominates the cybersecurity conversation, and the proliferation of ransomware attacks have created concerns across businesses of all sizes, from small community drycleaners to the Fortune 100. No business is immune to attacks. Because the tools to execute a ransomware attack are easily acquired on the dark web, the attackers range from organized cyber criminals to nation states to lone wolves seeking monetary gain. And because small businesses don't know how to respond or who to contact for assistance, the ransoms are paid without the appropriate agencies obtaining any insight into the attack. This was particularly true in the summer of 2020 when community drycleaners were being attacked across the nation, according to Rear Admiral (Ret.) Mark Montgomery, the former Executive Director of the Cyberspace Solarium Commission.

We asked Jason Witty for his views on ransomware from the CISO's perspective: "Recent successful crypto-ransomware attacks further underpin the need for the CISO to not only remain current in all of the skills of the past, but to simultaneously deepen expertise in geo-politics, international legal frameworks, public relations and communications, and the innerworkings of cryptocurrencies and other blockchain technologies."



Finally, as noted earlier, the economic impact from ransomware remains a major concern for the nation. Based on various estimates, the cost of ransomware in 2021 could approach $20 billion, which keeps ransomware at top of mind for every CISO across the globe.

THIRD-PARTY VENDOR SECURITY

Attacks via third parties are increasing every year as reliance on third-party vendors continue to grow. According to the Wiz Research Team, "82% of companies provide 3rd party vendors highly privileged roles. This is a major risk to sensitive data leakage and may pose both a security risk, as well as serious privacy risk." According to Shir Tamari, Head of Wiz Research, "Security teams need to focus on minimizing the risk of 3rd parties in the cloud environment because it provides room for a supply chain attack and can even lead to compliance risks."

When one considers the number of third-party vendors with which a typical multinational enterprise engages at any given time, it is not surprising that cyber adversaries target these third-party suppliers. Additionally, because the third-party vendor may not have implemented the same security standards as the prime contractor, they are an easier target, especially given the access they often enjoy as noted by the Wiz Research Team.

WORKFORCE CHALLENGES

The ongoing shortages of seasoned cyber professionals, especially those with seven to 10 years of experience, is constantly highlighted by CyberSeek.

Looking at openings versus certification holders for the following, we see significant shortages across the cyber community.

Compounding the workforce shortage is the aging of the current workforce, which is just over 50% Boomers and Generation X. This implies a major retirement window over the next 5 to 7 years, creating even more stress on the workforce shortage issue.

The absence of a holistic national strategy places added pressure on the patchwork of existing programs.

The CyberCorps® Scholarship for Service Program (SFS) was created under the Federal Cyber Service Training and Education Initiative, a component of the National Plan for Information Systems Protection. It is the only major federal education program designed to address cybersecurity workforce challenges. Currently, 90 institutions of higher learning are certified under SFS, including nine Community College Cyber Pilot (C3P) Program Participating Institutions. However, to date, only approximately 3,700 students have graduated from the program over nearly 20 years. According to Admiral Montgomery, this low graduation rate is due largely to limited funding.

SEASONED CYBER PROFESSIONALS SHORTAGES

CISM	CISA	CISSP
45,832 openings	**64,719** openings	**116,984** openings
19,110 certified	**37,653** certified	**93,591** certified

There are private sector programs, but most are narrow and insufficient to achieve the numbers required to meet the needs that will only continue to grow in the coming years.

On a positive note, Microsoft Corporation has announced a major program that could impact the cyber workforce shortage significantly by partnering with community colleges across the nation. Microsoft aims to cut cybersecurity workforce shortage in half by 2025. The program will provide cybersecurity curricula and educator training to community colleges. It will also provide scholarships to "at least" 25,000 students seeking to pursue cybersecurity education.

These programs and other similar initiatives seek to address workforce shortages through the education pipeline. In the short term, however, CISOs will continue to face multiple challenges, including developing the existing workforce while simultaneously developing strategies for retention in the face of ever-increasing competition from other companies seeking to recruit outside talent using higher salaries and other perks.

CYBER INCIDENTS IMPACT THE BUSINESS ACROSS MULTIPLE FACETS, FROM REPUTATIONAL RISKS IMPACTING TRUST AND REVENUE TO POTENTIAL LIABILITIES IMPOSED BY STATE AND FEDERAL LEGISLATORS.

Finally, companies are up against a constant barrage of cyberattacks, with threats coming from multiple directions against varying targets. The increased number of cyberattacks, coupled with the velocity of those attacks, serves to create increased psychological stress across the current workforce, which causes some workers to walk away from the field entirely.

EVOLUTION OF THE CISO

The problems facing CISOs today are as much, if not more, business-related as they are technology-related. Cyber incidents impact the business across multiple facets, from reputational risks impacting trust and revenue to potential liabilities imposed by state and federal legislators. This has created a need for the CISO to engage the board, not only to provide the metrics surrounding the cyber posture of the business, but also to be able to tell the story from a risk-based perspective in a way that can easily be understood by the board members. Board members typically do not absorb the metrics; only a small percentage of today's boards include cyber-savvy executives, so being able to articulate the risks is an imperative for CISOs.

Additionally, many forward-thinking businesses have reevaluated the reporting structure for CISOs within the enterprise. We asked Bruce Brody, Senior Chief Information Security Officer and CISO Advisor at Cisco Secure, for his thoughts on the issue. "In many organizations, and particularly in the U.S. federal government, the CISO is required by legislation to report to the Chief Information Officer (CIO). Much has been written over the years about the feasibility of this organizational construct. Lately, some very progressive organizations in the Fortune 500 and the Global 1000 have elevated the CISO to a reporting relationship under, variously, the Chief Risk Officer, the Chief Security Officer, the Chief Financial Officer, the General Counsel, or even the Chief Executive Officer. Where the CISO belongs organizationally in any enterprise is a function of the roles and responsibilities of the CISO and the way those roles and responsibilities cleave into the critical operations and mission of the enterprise.

According to Heidrick & Struggles 2021 Global CISO Survey, nearly 50% of CISOs report to someone other than the CIO. Additionally, regardless of where the CISO reports, regulatory requirements in many industries require the CISO to make regular reports to the Board of Directors, not filtered through the CIO or other officers.

In the end, whether the CISO reports to the CIO, or to another senior executive, the need for the CISO to be able to articulate the risks in a transparent manner is essential to ensuring businesses are making the right investments in people, technology, and processes, to ensure that they are creating the best possible scenario for engaging cyber incidents and being sufficiently resilient to assure continuity of the business following the incident.

CONCLUSION

As noted earlier, the role of the CISO has changed dramatically. According to Jamil Farshchi, CISO at Equifax, *"The evolution of the CISO role is quite unlike any other in the c-suite. Gone are the days of the CISO being a technical-only contributor. Today's CISO operates in a position that impacts every line item of a company's P&L. As such, the CISO is expected to counsel the CEO and Board in order to contextualize, interpret, and manage technical risk across the entire business. It's a role that requires a greater level of executive presence, business acumen, and strategic communications, than the "traditional" CISO. When looking at the acceleration that's happening right now across business, from digital transformation to M&A, to data security, there's never been a more consequential time to be a CISO."*

It is clear that the cyber world has emerged as the single largest threat facing the nation today. Cyberattacks happen every single minute and the economic impact on our economy has been devasting. The CISO has thus been thrust into the forefront and charged with protecting the enterprise, whether it is a government agency or a Fortune 1000 company. CISOs today must be skilled in building a robust security capability that focuses more on cyber resiliency rather than simply network protection. The functions of as CISO organization involve but not limited to: Strategy and Program Management; Cyber Assurance; Technology Compliance and Governance; Technology Risk Management; Vendor Assessment: Business Continuity/ Resilience; Disaster Recovery; Identity and Access Management; Product Security; Consumer Security; Threat Intelligence and Countermeasures; Security Operations; Vulnerability Management; Application and Development Security; Forensics Investigation; all while ensure proper financial controls and management. The CISO today is a multi-disciplined leader, coach, and business professional that enables profitable enterprises.

The role has evolved beyond the ability to guide the technical decisions required to protect the agency or business and the pressures to succeed are beyond comprehension. Failure not only impacts the bottom line, but also the confidence and psychological wellbeing of the entire security team. The men and women assuming these roles are a special breed and carry immense responsibilities not imagined even a decade ago, in an environment that is constantly changing both technologically and legislatively.

In our next section we will explore the policies and legislation that will impact the CISOs going forward. The NTSC will continue working to represent the voice of the CISO as these policies are crafted by our congressional leaders.

SECTION TWO:

Changing Regulatory and Legislative Landscape

Since the formation of CISA in late 2018, the federal government has grown more attentive to the various cybersecurity challenges that CISOs face daily. A recent slate of severe ransomware attacks such as SolarWinds and the Microsoft Exchange vulnerability have helped focus regulatory and legislative attention on the issue. In response, both Congress and the Executive Branch are working to implement a variety of policy solutions.

ON THE HILL

Incident Reporting Requirements

Industry incident reporting requirements have received most of the legislative focus this Congress. Both the House Committee on Homeland Security and the Senate Committee on Homeland Security and Governmental Affairs have held numerous hearings on the topic.

Additionally, House Committee Chairwoman Yvette Clarke and Ranking Member John Katko introduced H.R. 5440, the Cyber Incident Reporting for Critical Infrastructure Act of 2021. The bill would establish a Cyber Incident Review Office within CISA. The Office would be responsible for receiving, aggregating, and analyzing mandatory incident reports. Under the bill, entities that would be mandated to report cyber incidents would be "critical infrastructure entities" as defined by the CISA director at the time of implementation. The bill specifies that the CISA director may not require incident reporting "earlier than 72 hours after confirmation that a covered cybersecurity incident has occurred."

Senate Committee Chairman Gary Peters and Ranking Member Rob Portman introduced S. 3600, the Strengthening American Cybersecurity Act of 2022. The bill is a compilation of three previous Peters-Portman cybersecurity bills: the Cyber Incident Reporting Act, the Federal Information Security Modernization Act of 2021, and the Federal Secure Cloud Improvement and Jobs Act. Broadly, it would require critical infrastructure operators to and civilian federal agencies to report "substantial" cyberattacks to CISA within 72 hours ("substantial" must be defined by the Director). It also would require critical infrastructure owners and operators to report ransomware payments to CISA within 24 hours. It would also modernize the federal government's cybersecurity posture and authorize the Federal Risk and Authorization Management Program (FedRAMP) to ensure federal agencies can quickly and securely adopt cloud-based technologies. The legislation passed the Senate via unanimous consent in March 2022, and, at time of writing, awaits passage in the House.

INDUSTRY INCIDENT REPORTING REQUIREMENTS HAVE RECEIVED MOST OF THE LEGISLATIVE FOCUS THIS CONGRESS.

Additionally, Senator Mark Warner introduced S. 2407, the Cyber Incident Notification Act of 2021. The bill would require that covered entities report cyber incidents "not later than 24 hours after the confirmation of a cybersecurity intrusion or potential cybersecurity intrusion." Like the Clarke-Katko and Peters-Portman bills, this bill would require the CISA director to define a covered entity but includes a requirement that the federal government be included in that definition.

NATIONAL PRIVACY STANDARDS

Although incident reporting has received the bulk of legislative attention during the 117th Congress, discussion on national privacy standards has not been left by the wayside.

Representative Suzan DelBene and 19 original Democratic cosponsors introduced H.R. 1816, the Information Transparency and Personal Data Control Act. The bill would empower the FTC to regulate the collection, storage, and dissemination of personal consumer data on a national level. Regulatory requirements would include:

- Affirmative, opt-in consent
- Plain language data collection policies
- The requirement that these policies provide contact information, the purpose of the data collection, the categories of data shared with third parties, a consent withdrawal process, access to view what data is collected, categories of sensitive data collected, and how the data is protected

Additionally, data collectors would be subject to audits every two years. Businesses that collect data from fewer than 250,000 individuals per year would be exempt from the regulations.

CRITICAL INFRASTRUCTURE CYBERSECURITY

The Colonial Pipelines attack brought into sharp relief the need to secure critical infrastructure systems. Representatives John Katko (R-NY) and Abigail Spanberger (D-VA) introduced H.R. 5491, the Securing Systemically Important Critical Infrastructure Act. The bill would authorize the CISA Director to establish a "transparent, stakeholder-driven process" to designate systemically important critical infrastructure (SICI) and require CISA to consult with Sector Risk Management Agencies (SRMAs) and stakeholders in establishing a methodology and criteria to define SICI. Additionally, it would require CISA to provide SICI owners and operators with the option to take part in prioritized cybersecurity services, including:

- "Front of the line access" for CISA's key cybersecurity programs, including technical assistance, and voluntary programs to continuously monitor and detect cybersecurity risks;
- Prioritized representation in CISA's newly established Joint Cyber Defense Collaborative (JCDC);
- Prioritized applications of SICI owners and operators for security clearances, as appropriate.

IN MAY 2021, PRESIDENT BIDEN SIGNED THE EXECUTIVE ORDER ON IMPROVING THE NATION'S CYBERSECURITY

NATIONAL DATA SECURITY STANDARDS

In addition to data privacy standards, Congress is attempting to codify national data security standards.

Senators Kirsten Gillibrand and Sherrod Brown introduced S. 2134, the Data Protection Act of 2021. The bill would establish an independent Data Protection Agency (DPA) with a Senate-confirmed director that would serve for five years. The role of the DPA would be to supervise and issue regulations to entities that collect data from consumers. The DPA would also be responsible, in coordination with other agencies, for enforcing federal privacy laws.

Although none of these bills have been signed into law, the energy on the Hill to pass these measures is clear. CISOs should expect to see changes reflecting these legislative efforts within the next few years.

THE EXECUTIVE BRANCH

Since taking office in January 2021, the Biden Administration has shown significant interest in addressing gaps in federal cybersecurity policy. In May 2021, President Biden signed the Executive Order on Improving the Nation's Cybersecurity. The Order declares that the government must "make bold changes and significant investments" in cybersecurity. To achieve this ambitious goal, the Order outlines a series of policy priorities:

- Removing barriers to threat information sharing
- Modernizing federal cybersecurity
- Improving supply chain cybersecurity
- Establishing a Cyber Safety Review Board
- Standardizing federal incident response
- Improving federal network intrusion detection

4

AREAS OF INTERNATIONAL INTEREST

- ✓ **RESILIENCE**
- ✓ **COUNTERING ILLICIT FINANCE**
- ✓ **DISRUPTION AND LAW ENFORCEMENT**
- ✓ **DIPLOMACY**

- Improving federal investigative and remediation capabilities
- Establishing National Security Systems

The White House has also begun working with international partners to address cybersecurity issues as well. In October 2021, the White House hosted 30 other countries for a virtual meeting on ransomware policy. A joint statement posted after the meeting outlines the four areas of international interest:

- **Resilience:** The statement called for "universal cybersecurity best practices" and acknowledged that proper resilience requires proper policy and governance, not just technology.
- **Countering illicit finance:** The statement recognized that uneven implementation of Financial Action Task Force standards and other illicit finance standards is a major factor enabling ransomware profitability.
- **Disruption and law enforcement:** Recognizing ransomware as a transnational threat, the statement declared an intention "to cooperate with each other and with other international partners to enhance the exchange of information and provide requested assistance."
- **Diplomacy:** Finally, the statement promises to leverage diplomatic strategies with states that fail to act against cyber criminals.

The newly created Office of the National Cyber Director inaugurated its first director, Chris Inglis, in July 2021. Director Inglis expressed his priorities during an October 2021 panel discussion hosted by Auburn University. Inglis feel that the federal government "needs to be very proactive, needs to be very coherent, needs to be joined up such that it is the partner that the private sector needs in that collaboration to defend digital infrastructure. At the end of the day, I think that the premise must be we need to make it such that if you're a transgressor in this space, you have to beat all of us to beat any of us."

Additionally, Jen Easterly was unanimously confirmed by the Senate to lead CISA as its first permanent director. During the 2021 NTSC National Policy Conference in September 2021, she described cybersecurity as a "shared responsibility" between the public and private sectors and repeatedly emphasized the need for collaboration between the two.

Chris Inglis
National Cyber Director

Jen Easterly
CISA Director

CISA

Since Director Easterly assumed leadership over CISA, it has established several projects to foster the collaboration about which she spoke. The most prominent among these is the Joint Cyber Defense Collaborative (JCDC), a public-private partnership project. The JCDC brings together federal agencies; state, local, tribal, and territorial (SLTT) governments; ISAOs and ISACs; critical infrastructure operators; and industry and academia. The goal of the JCDC is to "[work] across the public and private sectors to unify deliberate and crisis action planning, while coordinating the integrated execution of these plans."

In addition to creating the JCDC, CISA has established the Cybersecurity Advisory Committee that was created by the FY2021 National Defense Authorization Act in January 2021. The Committee, which was designed at the behest and with the input of the NTSC, now serves as an advisory board to CISA. It is composed of industry and SLTT cybersecurity leaders and "participate[s] in the development, refinement, and implementation of recommendations, policies, programs,

TSA PUBLISHED A SLATE OF NEW CYBERSECURITY DIRECTIVES FOR HIGH-RISK RAILROAD, RAIL TRANSIT, AND AIRLINE OPERATORS.

planning, and training pertaining to CISA's cybersecurity mission." The Committee's current membership includes NTSC board members Ron Green (Vice Chair) and Maureen Allison. The Committee held its first meeting in December, during which NTSC Executive Director Patrick Gaul gave remarks praising the Committee and advocating for increasing CISO presence in its membership.

CISA is also working to streamline its cybersecurity services. In June 2020, it announced CISA Central, a one-stop shop intended to simplify information sharing and situational awareness services by bringing together the National Cybersecurity and Communications Integration Center (NCCIC), National Infrastructure Coordinating Center (NICC), and National Coordinating Center for Communications (NCC) under one umbrella.

OTHER AGENCIES

CISA is not the only federal agency engaging with cybersecurity. The Transportation Security Administration (TSA), in coordination with DHS, issued a security directive in May 2021 for TSA-designated critical liquid and natural gas pipelines and facilities. The directive mandates that these designees report cybersecurity incidents to DHS. It also requires designees to assign a Cybersecurity Coordinator who is available 24/7 to handle cyber incidents. Finally, it requires designees to review their compliance with existing TSA regulations, remediate any gaps in compliance, and report their efforts to TSA and CISA.

Additionally, TSA published a slate of new cybersecurity directives for high-risk railroad, rail transit, and airline operators. The standards include requirements to disclose attacks, establish a cybersecurity point person, and develop continency plans in case of an attack. TSA also published separate, non-mandatory guidelines for lower-risk operators.

To begin enacting the vision put forward by the White House-led international coalition that met in October, the Department of State will create a new bureau focused on cyber and technology diplomacy policy. The bureau would be led by a Senate-confirmed ambassador and would be divided into three units: international cyberspace security, international digital policy, and a cyber envoy.

CONCLUSION

The wide array of legislative and regulatory efforts underway in Congress and the Executive Branch show that energy for cybersecurity policy reform has never been stronger. There has never been a better time for CISOs to lend their voice to the federal government, and the NTSC is proud to represent that voice.

SECTION THREE:

What Should CISOs Expect Going Forward

INCREASED SCRUTINY

As Jason Witty noted at the outset of this paper and as discussed in detail in the first section, the job of CISO has changed dramatically over the past few years. As cybersecurity and privacy have moved up the ladder of executive-level and Board concerns, the CISO role has been elevated from a mainly technical advisor to a peer of other C-suite executives. And with this change in roles comes greater responsibilities, increased scrutiny, and potential liability exposure.

Added responsibilities and elevation to the executive team expand the scope of liability for breach of fiduciary duties inherent in most state corporate codes. Federal laws and regulations that target company executives now also target the CISO. Many of the legislative and regulatory efforts noted in Section Two include possible causes of action that extend to CISO. Further, as noted above, the adjacent areas of responsibility that now increasingly fall within the ambit of a CISO's responsibility, including privacy, business continuity, dealing with regulators and more.

As for exposure, look no further than the prosecution of Joe Sullivan, Uber's former security chief, in connection with the 2016 hack involving approximately 57 million user and driver records. In 2020 he was charged with obstruction of justice and misprision of a felony in connection with an alleged attempted cover-up of the incident. In December of 2021, the Justice Department added allegations of wire fraud.

When considering a CISO position, prospective applicants (or those already in the position) must now consider what other executives have come to know: am I covered under the company's director and officer and other commercial insurance policies, do the companies incorporation documents or bylaws provide indemnification for my acts? And am I being compensated at a level that considers my expanded role and exposure?

Most CISOs come from a technical background, as those skills are still the predominant ones that define the role. But as noted from Section One, and based on the everchanging legislative and regulatory landscape that continues to expand rapidly, it is incumbent upon both current and aspiring CISOs to understand and seek advice and training on areas that were once far beyond the purview of the CISO: legal, regulatory, and corporate governance.

NEW SKILL SETS REQUIRED

Taking into consideration the complexities of the role of the CISO in today's business and security environment, CISOs need to develop a much broader skill set. The information security profession has, over the last decade, expanded into formerly unrelated or less related skills. While not exhaustive, these related skills can generally be broken down into 10 distinct categories, which are as follows:

1. COMPLIANCE
2. AUDITS
3. INFORMATION GOVERNANCE
4. LITIGATION
5. PRIVACY
6. INTELLECTUAL PROPERTY AND TRADE SECRETS
7. CUSTOMER/VENDOR REQUIREMENTS AND SECURITY
8. INTERNAL INVESTIGATIONS AND HUMAN RESOURCES
9. INSURANCE
10. CONTRACTING

Compliance

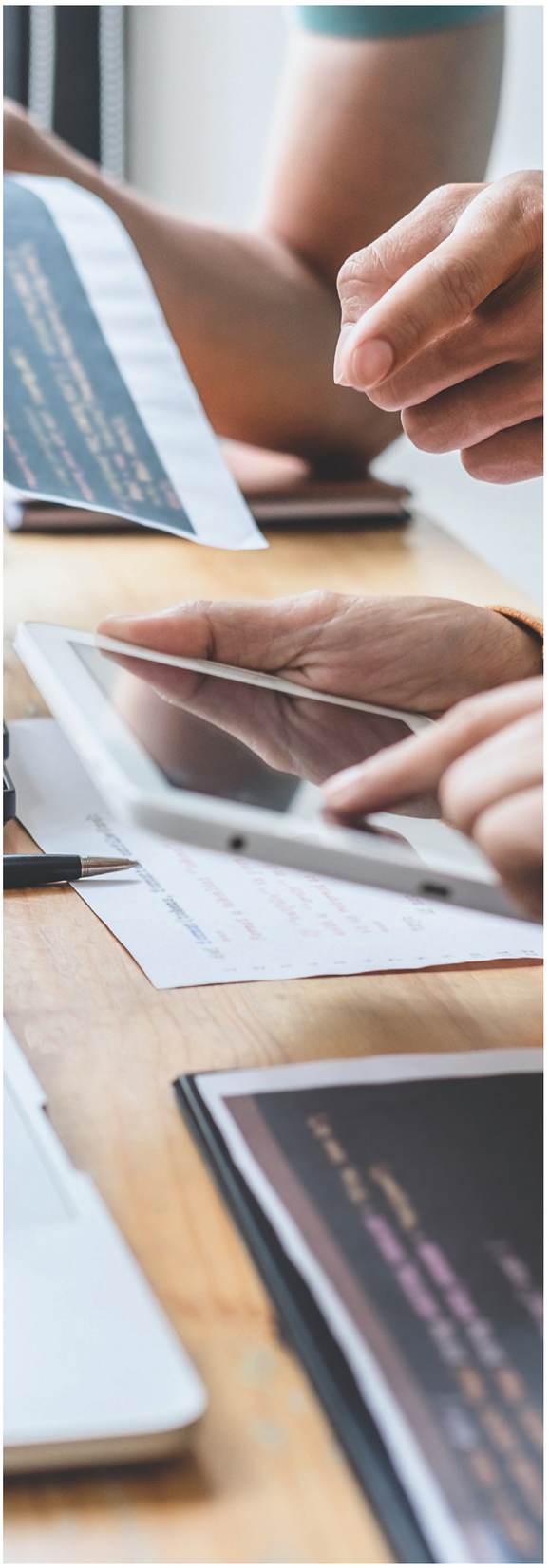
CISOs need to understand a company's responsibilities with respect to certain standards, frameworks, and other guidelines to which the company must comply. These requirements vary across industry and jurisdiction, and a CISO must understand which apply to their company and industry. Some of these might include (without limitation):

- Payment card industry (PCI);
- The Sarbanes–Oxley Act (SOX);
- Cybersecurity Maturity Model Certification (CMMC);
- Defense Federal Acquisition Regulation Supplement (DFARS);
- Health Insurance Portability and Accountability Act (HIPAA);
- The Federal Financial Institutions Examination Council (FFIEC);
- Consolidated Audit Trail (CAT)*;
- The Family Educational Rights and Privacy Act (FERPA);
- Children's Online Privacy Protection Act (COPPA);
- North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP);
- National Institute of Standards and Technology Special Publication (NIST SP 800-37 and 800-53); and
- and many more.

Audits

CISOs are often tasked with assisting with or overseeing internal audits, which might cover the policies, procedures, and controls that an organization puts in place to ensure that compliance and other requirements are met. These might include auditing against (for example):

- Statement on Standards for Attestation Engagements No. 16 (SSAE 16);
- Service Organization Control 2 (SOC 2);
- International Organization for Standardization (ISO 27001);
- Federal Information Security Management Act (FISMA);
- Federal Risk and Authorization Management Program (FedRAMP); and
- National Institute of Standards and Technology Special Publication (NIST SP 800-53A).



*https://www.nytimes.com/2020/08/20/technology/joe-sullivan-uber-charged-hack.html

https://www.justice.gov/usao-ndca/pr/former-uber-chief-security-officer-face-wire-fraud-charges-0

Information Governance

Information is the lifeblood of companies and can be both an asset and liability. Proper records and information management help ensure it remains an asset. CISOs often own responsibility for information governance. But if not, they still must ensure the proper ingestion and management of information. This discipline is responsible for defining retention requirements; developing and implementing rules on indexing and classifying information, system and manual retention; and ensuring appropriate destruction at its end of life. This discipline often works with the security forensics team to conduct discovery, legal and regulatory holds, and bridges the production in legal matters and litigation.

Litigation

CISOs are often asked to assist with litigation, whether it is by the company or against the company. CISOs need to understand how litigation works generally and understand how information and information systems fit into this process. This might include litigations holds, document production, and sometimes participating in depositions or court proceedings.

Privacy

In some companies the CISO is also the designated privacy officer or data protection officer. Regardless, CISOs need to understand and be well versed in privacy related laws and regulations such as:

- Federal, state and local laws regarding privacy and data breech notification;
- European Union General Data Protection Regulation (EU GDPR); and
- Laws regarding opt-in/opt-out and the right to be forgotten.

Intellectual Property and Trade Secrets

Intellectual property and trade secret theft have become big business. CISOs need to understand the basics of intellectual property and trade secrets in addition to understanding how to protect them from bad actors. Knowledge of basic patent and trademark law is a plus, especially in companies that conduct a lot of research and development.

Customer/Vendor Requirements and Security

Customers often ask companies about their security posture and CISOs often are responsible for answering these questions and ensuring compliance. Additionally, CISOs need to understand that their company's security posture is only as good as the security posture of their suppliers and vendors, and CISOs need to be in a position to adequately assess the postures of these third parties.

Internal Investigations and Human Resources

Internal investigations are a key part of the compliance tool kit for companies. CISOs are often asked to help with these investigations from a forensic or IT standpoint. Knowledge of how investigations are conducted, as well as the associated legal and compliance frameworks, will be beneficial for a CISO. Additionally, human resources often must rely upon CISOs for their investigations and for their compliance obligations.

For example, when employees are terminated, information security must be in a position to immediately control access to those employees' accounts to prevent intellectual property theft or other malfeasance.

Insurance

Cyber insurance and other insurance programs often rely on information from the information security governance department or upon representations made by the security department. Cyber and business disruption insurance carriers have begun to do much more rigorous information security assessments to determine the degrees of risk. Central to this process is the role of the CISO. As such, the CISO must be intimately familiar with insurance. This includes in the application process, in ongoing compliance, and should a claim arise. Increasingly, claims are being denied because of misstatements in the application process.

Contracting

CISOs are often in charge of the acquisition of security and other IT services for companies. CISOs need to be knowledgeable with respect to the contracting process, contractor requirements, and other internal procedures regarding the contracting process. CISOs must also have a basic understanding of legal principles with respect to contracts as they often participate in the negotiation process. At a minimum, CISOs must ensure there is appropriate security, security audit, and assessment

language in the contract to ensure ongoing protection.

CLOSING

As can be seen in this whitepaper, the role of a CISO has evolved over the past years and will continue to evolve. Global business, security and political environments have become much more complex and given current events, will continue to do so. The skill sets required for a successful CISO are varied and numerous. That said, a CISO that brings these skill sets and a solid understanding of this new business order to the table will be invaluable both to their company and to themselves going forward.

[I] Top 15 Cybersecurity Predictions for 2022 - Top 15 cybersecurity predictions for 2022 | Security Magazine

[II] 82% of companies give third parties access to all cloud data | 2021-01-26 | Security Magazine

[III] 82% of companies give third parties access to all cloud data | 2021-01-26 | Security Magazine

[IV] Cyberseek

[V] CyberCorps®: Scholarship for Service (opm.gov)

[VI] America faces a cybersecurity skills crisis: Microsoft launches national campaign to help community colleges expand the cybersecurity workforce - The Official Microsoft Blog

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.

NTSC
NATIONAL TECHNOLOGY SECURITY COALITION

4400 North Point Parkway
Suite 155
Alpharetta, GA 30022
ntsc.org