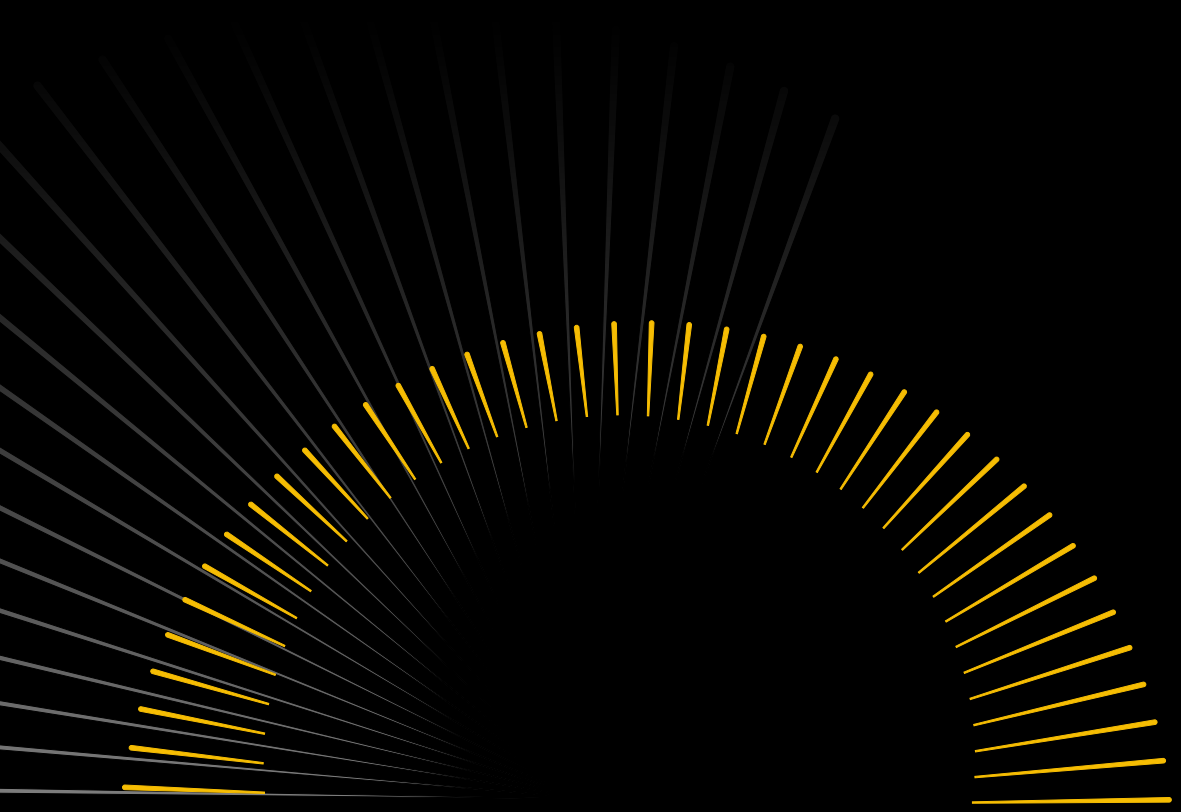

CYBER DEFENDERS COUNCIL

BRIDGING THE CYBER-BUSINESS DIVIDE

Will Regulation Reduce Cyber Risk and Improve Resiliency?

This report paves the way for broader discussion about accountability for cyber risk.

Contents

SPONSORED BY cybereason

ABOUT

The Cyber Defenders Council

The Cyber Defenders Council is an independent group of preeminent cybersecurity leaders from public and private sector organizations around the world. The mission of the Council is to adapt an approach to cyber deterrence, known as *Defend Forward*, for private sector enterprises and to provide prescriptive guidance to help organizations implement *Defend Forward* cybersecurity strategies that increase costs for attackers and improve the efficacy of Defenders.

The Cyber Defenders Council is sponsored by Cybereason.

Executive Summary

During the first Cyber Defenders Council meetings in the Spring of 2022, security leaders from large organizations across North America, EMEA, and Asia-Pacific began adapting for the private sector an aggressive approach to proactive cyber deterrence that originated in the U.S. Department of Defense. This approach is known as Defend Forward.

Driven by a pressing need to better protect their organizations from cybercriminals and nation-state adversaries, Council members worked directly with General Joseph Dunford, the 19th chairman of the U.S. Joint Chiefs of Staff and one of the architects of Defend Forward, to define six principles intended to help security leaders across industries implement this new approach. The Council outlined these six principles in its debut report.

This e-book represents the second report from the Cyber Defenders Council and is based on discussions that took place during the Council's Q2 2022 meetings. This latest report explores the first principle of Defend Forward: Assume You are at Risk - Strengthen the Security and Resiliency of Systems and Networks. This principle may seem obvious, but discussions during Council meetings revealed that many business and cybersecurity leaders continue to make different assumptions about their organizations' cyber risk exposure, with business leaders tending to view cybersecurity as an abstract risk until their company gets attacked, while cybersecurity leaders regard it as imminent and pressing.

The differences in executives' understanding of cyber risk and the measures needed to mitigate it speak to the persistence of the cyber-business divide, a disconnect that heightens organizations' risk exposure and often impedes their ability to meaningfully address it. The need to bridge the cyber-business divide was a common theme across the North America/EMEA and APAC Council meetings. It's an issue that grows ever more pressing in times of economic uncertainty, when cybersecurity budgets inevitably fall under increased scrutiny.

The most provocative question to come out of the North America/EMEA Council meeting centered on whether the principles behind accounting and corporate governance regulations, such as Sarbanes-Oxley (SOX) in the U.S., the E.U. Network and Information Security (NIS) Directive, Australia's CLERP9, Japan's Financial Instruments and Exchange Act, or the new corporate governance regime in the U.K., could be applied to cybersecurity. The intent in applying aspects of these regulations to cybersecurity would be to bridge the cyber-business divide and align leaders around a shared understanding of their organizations' material cybersecurity risks and the actions and investments required to mitigate them. This report explores that question and paves the way for a broader discussion about whether a cybersecurity accountability regulation or standard could help security leaders advance important alignment, risk management, and cyber risk governance objectives without mandating specific cybersecurity controls.

While several Council members from North America made compelling points in favor of a cyber accountability regulation, which are summed up on page 9, support for the idea wasn't unanimous among Council members. Consequently, this report also examines challenges to cyber accountability regulation (see page 17) and whether security leaders could achieve the same objectives through other means, such as through a self-governing industry standard (or some combination thereof).

APAC Council members took a different approach to the first principle of Defend Forward. Where NA/EMEA Council members explored the role of regulation in bridging the cyber-business divide, improving cyber risk governance, and strengthening security and resiliency, APAC Council members shared insights, advice, and best practices for achieving those same goals.

With cyber threats from nation-state actors on the rise and widely expected to increase according to international government cybersecurity authorities, it's going to take bold and decisive action on the part of business and security leaders, grounded in innovative models like Defend Forward, to fundamentally change the calculus of cyber risk and reverse the adversary advantage.

Is It Time for Cybersecurity Accountability Regulation?

In 2001, a wave of accounting scandals swept across several large U.S. businesses including Enron, Worldcom, Tyco, and others.

The scandals–and the enormous corporate bankruptcies they spurred–undermined public trust in the U.S. capital markets and shined an inescapable spotlight on a wide variety of issues that were plaguing many U.S. companies at the time, including conflicts of interest between corporations and their auditors, and fundamental breakdowns in corporate governance.

The financial malfeasance was so egregious, so felonious, and so reckless that it led to the bipartisan passage of the Sarbanes-Oxley (SOX) Act of 2002. As the largest and most comprehensive accounting reform in U.S. history, SOX was designed to protect investors by improving the accuracy and reliability of corporate financial disclosures. Following the enactment of SOX in the U.S., other countries including Australia, China, Japan, and the U.K. passed similar legislation. While initial compliance with SOX and similar regulations was costly and painful for impacted companies, the laws have, by and large, achieved their intended effect of preventing accounting fraud by holding top executives responsible for the accuracy and integrity of their organizations' financial controls and reporting.

The effectiveness of SOX led several U.S. members of the Cyber Defenders Council to suggest that some of the law's language and principles could be applied to cybersecurity. Doing so could align business and cybersecurity leaders around a shared understanding of the material cyber risks and control deficiencies facing their organizations, as well as drive shared accountability for addressing them.

Dave DeWalt, a veteran security industry CEO and investor who has sat on 29 corporate boards and who served as the guest speaker at the North America/EMEA Cyber Defenders Council meeting, suggested that organizations report "significant deficiencies" and "material weaknesses" in their cybersecurity controls and posture in much the same way that SOX requires CEOs and CFOs to report to their organizations' auditors and audit committees all significant deficiencies in their organizations' internal financial controls that could impede their ability to accurately record and report financial data.

"We need something that makes the CEO, CFO, and audit committee chair wake up and take notice," DeWalt said. "I don't want to create a regulatory oversight problem for security leaders, but some kind of requirement for companies to report on significant deficiencies and material weaknesses in their cybersecurity posture could create the board-level visibility and executive-level accountability that security leaders need to make significant improvements in mitigating their organizations' cyber risk."

> We need something that makes the CEO, CFO, and audit committee chair wake up and take notice.

DAVE DeWALT
FOUNDER AND MANAGING DIRECTOR, NIGHTDRAGON

The Argument for Cybersecurity Accountability Regulation

SOX and similar regulations had a very specific purpose and problem to solve when lawmakers drafted them: to prevent willful malfeasance and restore investor trust in public company financial statements. To be effective and avoid over-reach, a cybersecurity accountability regulation or self-governing standard like PCI-DSS (Payment Card Industry Data Security Standard) would arguably need similarly specific and clear objectives.

While cybersecurity isn't plagued by the skullduggery that brought down Enron, Worldcom, and Australia's HIH, as a global economic and national security issue it is unquestionably pressing—especially as geopolitical tensions continue to rise and cyber operations become more centrally strategic.

Yet, despite the risks that potentially catastrophic cyberattacks pose to individual organizations and nations, many public and private sector security leaders still struggle to convince senior leadership to invest adequately in security controls and capabilities. This fundamental disconnect between business and cybersecurity leadership may very well be the problem that cybersecurity accountability regulation needs to solve.

Malcolm Harkins, Chief Security and Trust Officer for Epiphany Systems, believes cybersecurity accountability regulation could address the lack of incentives that prevents many companies from making necessary investments in cybersecurity. "Companies aren't incented to invest in cybersecurity because spending money on cyber doesn't increase revenue," he said. "A 'Cyber Sarbanes-Oxley' is needed to get the C-suite and board to understand the importance of cybersecurity, create the alignments inside organizations around it, and ultimately, move the needle on security in significant ways."

> "Companies aren't incented to invest in cybersecurity..."

MALCOLM HARKINS
CHIEF SECURITY AND TRUST OFFICER, EPIPHANY SYSTEMS

CAUSES OF THE CYBER-BUSINESS DIVIDE

HOW did we get HERE?

U.S. executives rarely welcome government regulation, so the fact that Dave DeWalt and several prominent cybersecurity executives voiced support for cybersecurity accountability regulation speaks volumes about the stubbornness of the challenges facing security leaders. But how did we get to this position where what's normally a last resort—government regulation—is viewed by some security executives as the remedy for getting business and security leaders on the same page regarding cybersecurity? And why are there conflicts between business leaders and the security executives they hire specifically to protect the business? There are several issues at play:

LANGUAGE

- The disconnect between business and security leaders has long been fueled by the arcane, technical nature of cybersecurity. While many cybersecurity leaders have made huge strides in quantifying cyber risk in financial terms and communicating it to the C-suite and board, the technical language that some cybersecurity leaders continue to use perpetuates the disconnect in many organizations.

COMPETING GOALS

- The objectives security leaders are charged with achieving (e.g., mitigating risk, preventing material cyber attacks) are often at odds with growth and profitability objectives. What's more, security is often viewed as a cost center and not as a value driver or business enabler.

THE SECURITY CONUNDRUM

- To get budget funding, security leaders often find themselves in the awkward position of having to prove a negative. In other words, it often takes a major security event (a negative) before money flows to cybersecurity, yet success for a security program means preventing major attacks. If no major attacks take place, it's harder for CISOs to make a case for a budget increase, especially when the global economy is cooling. CISOs need to be able to show the number of attacks the company prevented through measures like security awareness training and detection technologies, as well as assign a realistic monetary value to the costs those measures prevented.

In addition to bridging the cyber-business divide, Cybereason CSO Sam Curry notes that cybersecurity accountability regulation will also eliminate excuses for negligence, ensure organizations have best practices and minimum required cybersecurity capabilities in place, make cybersecurity a manageable and improving practice in companies, and–perhaps most importantly–will prompt action to address significant deficiencies and material weaknesses in security controls.

In the E.U., lawmakers recently agreed to update legislation, known as the NIS Directive, that set cybersecurity standards and requirements for critical infrastructure providers in 2016. Aimed at keeping pace with shifting threats and the rapid rate of technology change, the updates expand the regulation to medium and large organizations across more sectors, address supply chain security, and create accountability for complying with cybersecurity obligations. Cybereason Field CISO for EMEA Greg Day noted that the updates to the NIS Directive take a page from the success the E.U. had with GDPR, where the global data protection regulation drove accountability by enforcing large fines against organizations for noncompliance.

Some external auditors and cyber-savvy corporate directors in the U.S. are already moving in the direction of applying some of the principles of SOX to their governance of cyber risk. Mike Orosz, the Vice President of Information and Product Security at IT infrastructure provider Vertiv, says that his company's external auditor has begun asking questions about corporate IT network security posture to ensure network security around financial systems is aligned with industry best practices.

At organizations where Dave DeWalt sits on the board, he says he's tried to develop "control points" to help him gauge each company's cyber risk exposure and readiness. For example, during board meetings, he asks the CISOs how fast their security organizations can respond to a range of highly specific security incidents, such as a severity level 1 vulnerability with a known zero-day exploit. If the security organization can't respond within a certain amount of time, he considers it a significant deficiency.

> I am seeing more interest in our security posture from our external auditor.

MIKE OROSZ
VP INFORMATION AND PRODUCT SECURITY, VERTIV

Proposals for Cybersecurity Accountability Regulation

Council members who favored applying SOX or similar laws to cybersecurity noted that one of the advantages of SOX that "future-proofed" it and made it effective was that *it did not prescribe the specific financial controls* companies needed to implement. Because it didn't mandate the use of specific controls, the law avoided becoming another "check-box" compliance regulation that so often fails to achieve its intended goals.

Erik Wille, the CISO of auto components supplier American Axle & Manufacturing, has seen the pitfalls of industry policies that push specific prescriptive controls rather than outcome-focused standards. "In automotive manufacturing, upstream customers are trying to get a better handle on supply chain risk, so they push technical controls on their suppliers, but the emphasis on technical controls ends up forcing suppliers into technology decisions rather than into more mature security postures," he said.

Council members agreed that cybersecurity accountability, whether it takes the form of a government regulation or an industry standard, should similarly avoid spelling out the specific cybersecurity controls and activities companies need to implement. After all, plenty of other organizations and laws have done that, including SANS with its Top 20 Critical Security Controls, NIST with its Cybersecurity Framework, and the European Union's GDPR and PSD2 (Payment Services Directive 2) regulations. Council members also pointed out that mandating specific controls can impede innovation and lead to technology lock-in, and they want to be sure that any government regulation or industry standard focuses on mandating better outcomes and spurring innovative security solutions.

To meet the test of time and adapt to rapidly changing threats, a cyber accountability regulation or standard could follow the model of the Budapest Convention, which provided the framework for much of the world's cybercrime laws and which focused on achieving high-level objectives rather than dictating, as many standards do, the technical details of how to achieve those objectives.

If a cybersecurity accountability regulation or standard were to take cues from SOX, it would need to define what constitutes a significant deficiency or a material weakness in an organization's cybersecurity controls or posture. For context, Section 302 of SOX states that a company's "signing officers" have disclosed "all significant deficiencies in the design or operation of internal controls which could adversely affect the issuer's ability to record, process, summarize, and report financial data" and have identified "any material weaknesses in internal controls."

THE QUESTION IS: HOW BEST TO APPLY SECTION 302 FROM SARBANES-OXLEY TO CYBERSECURITY?

- Would a company's signing officers have to identify material weaknesses in their organization's cybersecurity controls and posture?
- Would they then have to disclose all significant deficiencies in the design or operation of those controls that could impede their organization's ability to prevent, detect, or stop a cyber incident from having a material impact on the company?
- What constitutes a material impact?
- To whom or to which authority would organizations need to make these disclosures, and when?
- And what about the cybersecurity controls of issuer's third- and fourth-party partners and other unknowns?

Council members proposed using established risk-ranking criteria and setting significant deficiencies at a threshold of likelihood ***or*** impact and material weaknesses at a threshold of likelihood ***and*** impact. For example, a significant deficiency could be a cyber control weakness or control absence that creates a medium or high impact risk, while a material weakness could be a control gap that increases both the likelihood and impact of the risk to medium or higher. Steve Benton, Vice President of Threat Research at Anomali and former Deputy CISO of BT, suggested reporting deficiencies (and their mitigations) to regulatory authorities six months after identifying them in order to give organizations time to implement mitigations and prevent the disclosure of unremediated deficiencies that attackers could exploit.

Council members also suggested that signing officers acknowledge all risks in the risk registry, along with their related controls and the costs and tradeoffs associated with those controls. They also noted the need to highlight different classifications of data (e.g., intellectual property, PII, medical data, etc.) and to flag the systems holding different types of sensitive data as critical, and therefore requiring attestation that they are securely configured and properly managed, monitored, and audited.

ASSUME you're at RISK

ASSESSING CYBER RISK EXPOSURE

1

Identify the different types of data your organization stores and processes and assign appropriate classifications to them (e.g., IP, PII, etc.)

2

Note the systems holding different types of sensitive data and attest that they are securely configured and properly managed, monitored, and audited.

3

Regularly conduct rigorous and realistic tests of incident response plans, even in production environments, and include cybersecurity vendors and services providers in those tests as needed.

4

Include, prioritize, and acknowledge all known cyber risks in the risk registry, along with related controls and the costs and tradeoffs associated with those controls.

Flipping Board-Level Cyber Risk Reporting on Its Head

Reporting to the board on significant deficiencies and material weaknesses in a company's cybersecurity controls and posture would mark a fairly dramatic change in the way many security executives currently communicate with the board, and in the way many boards currently assess cyber risk. For instance, many boards want to see metrics on the number of vulnerabilities present, number of vulnerabilities remediated, number of attempted attacks, number of attacks mitigated, and whether those numbers are trending up or down on a quarterly basis, and then hear about the measures CISOs and their teams are taking to keep risk in check.

DeWalt believes reporting on significant deficiencies will be far more meaningful to corporate boards and have a far greater impact on improving organizations' cyber resiliency. "I've sat on 29 boards, and during meetings, the only thing the audit committees ask the CISO is, 'Is anything red?' In many cases, the board members haven't grown up with technology, but they understand Sarbanes-Oxley, so they'd presumably better understand cyber risk if it was reported in terms of significant deficiencies and material weaknesses."

The Argument Against Cybersecurity Accountability Regulation

Not all Council members supported regulation. Renee Guttmann, emeritus CISO for Campbell Soup Company, Royal Caribbean Cruises, Coca-Cola, and other large corporations, doesn't think broad-based government regulation is an ideal solution for addressing the challenges of obtaining executive commitment and funding, though she does believe that critical infrastructure—especially systems and services affecting public health and safety—merit greater government oversight.

Guttmann is concerned broad-based regulation will exacerbate the "security poverty line" situation for small and midsize organizations (SMBs) that struggle to fund cybersecurity and lack the resources required to implement complex technology solutions designed for large enterprises. She notes that even SOX has exemptions for some small and midsize public accounting firms and wonders whether cybersecurity accountability regulation should offer exemptions for SMBs or subsidies to help them offset the cost of compliance.

> "Broad-based government regulation is not an ideal solution for addressing the challenges of obtaining executive commitment and funding."

RENEE GUTTMANN
EMERITUS CISO,
CAMPBELL SOUP COMPANY

The SECURITY POVERTY LINE

The security poverty line is a term that Wendy Nather, Head of Advisory CISOs at Cisco, coined in 2011 when she was working as a research director with 451 Research. It refers to **the division between security "haves" and "have nots"**, and principally to organizations that struggle to implement adequate security due to insufficient budget, expertise, capability, or influence.

To address the security poverty line in the U.K., the government introduced **the Cyber Essentials and Cyber Essentials Plus certification programs for SMBs**, according to Cybereason Field CISO Greg Day. The programs allow SMBs to either self-attest or provide third-party attestation that they meet basic cyber hygiene practices. Day says these programs have improved SMB cybersecurity.

Instead of regulation, Guttmann proposes that companies voluntarily commit to following essential cybersecurity controls that organizations like CISA, SANS and the Center for Internet Security have already defined, and then have their CEO and board of directors report and sign off on deviations from those controls. She also believes cybersecurity vendors and services providers must develop offerings that smaller organizations can easily operate.

Even those NA and EMEA Council members who expressed support in spirit for strengthening cybersecurity accountability acknowledged the challenges compliance would pose at the outset, especially as they recalled the headaches associated with SOX compliance when the law first went into effect. They also recognized that many security and business leaders would resist being held legally liable for noncompliance, and may be reluctant to have to attest to their organization's cybersecurity controls.

> "We must be thinking broader than the security risk one single company can 'see' and enhance how we move forward to ensure accountability across the supply chain..."

THERESA PAYTON
CEO, FORTALICE SOLUTIONS

Moreover, they questioned how, exactly, an accountability law or standard for cybersecurity would play out? For example, if a CISO at a new company discovers privileged accounts are not secured with multi-factor authentication, does that constitute a significant deficiency or material weakness that they would need to report? If so, to which bodies would it need to be disclosed: the audit committee, a board-level cybersecurity committee, or regulatory bodies like the U.S. Securities and Exchange Commission or U.K. Financial Conduct Authority through a public filing? If via a public filing, does that then give attackers a treasure trove of information on large publicly traded companies' vulnerabilities? And what if a data breach occurs as a result of inadequate security on privileged accounts? Who's liable and what sorts of penalties might they face?

Theresa Payton, CEO of Fortalice Solutions, observed that a cybersecurity accountability standard does not fix ecosystem-wide security issues unless it offers a holistic approach for reducing risk in global supply chains. "Attack after attack shows how weak visibility is at all levels of assurance. We must be thinking broader than the security risk one single company can 'see' and enhance how we move forward to ensure accountability across the supply chain provides better transparency, resiliency, security, and assurance," she said.

DRIVING ACCOUNTABILITY ACROSS THE SUPPLY CHAIN

Vendor Security and SBOMs

The security risk that both large and small vendors and suppliers create for their customers looms large for Council members. To address it, many companies rely on security provisions in their contracts with vendors and suppliers. The drawback to this approach for vendors is that they need to comply with a range of security controls and requirements as defined by their different customers in these various contracts. For customers, they need to reinvent the wheel each time they ink a new contract with a new vendor.

But a vendor security exchange could deliver efficiencies for both parties while improving ecosystem security, according to Colgate-Palmolive Company CISO Alex Schuchman. Vendors would put their security audits and assessments into the exchange, and there would be controls over who can see that information, but a centralized source for this information would cut down on a lot of redundant work that takes place among vendors and their customers.

> A centralized source for vendor security audits and assessments would cut down on a lot of redundant work.

ALEX SCHUCHMAN
CISO, COLGATE-PALMOLIVE COMPANY

Council members also expressed support for software bill of materials (SBOMs) as a way to address supply chain risk and promote code security. SBOMs provide transparency into the provenance and pedigree of the components that make up a software product, so they can give security teams visibility into vulnerabilities and misconfigurations in software, as well as the security of code below the operating system level. However, Council members questioned whether SBOMs could keep up with the frequency of updates to cloud-based software and 5G infrastructure—and if security teams could realistically consume all those SBOM updates. Philipp Amann, the Head of Strategy for the European Cybercrime Centre (EC3), said having the necessary expertise and resources to audit and report on 5G equipment, software, and every update to that infrastructure presented another significant hurdle. "It's estimated that only a small number of E.U. countries currently have an efficient and effective capability and capacity to do so," he shared.

David Cross, Senior Vice President and CISO of Cloud SaaS Security at Oracle, encourages cloud providers to consider a universal standard for SBOMs that focuses on broad levels of security rather than granular and hard-to-measure levels for every device, component, or IoT asset that might exist in a physical data center.

American Axle & Manufacturing CISO Erik Wille believes SBOMs can also work in manufacturing to certify the security of production processes. "It allows us to shift from declaring something is secure to declaring the process to create the product had security built in," he said.

EXPERT ADVICE

Until SBOMs become an industry standard or regulatory requirement, IT and security leaders alike can lean on their software vendors to sign their software and demonstrate that they've evaluated the provenance of all the code libraries used in their products, scanned their code for vulnerabilities and misconfigurations, remediated those vulnerabilities, and fixed any misconfigurations.

> It allows us to shift from declaring something is secure to declaring the process to create the product had security built in.

ERIK WILLE
CISO, AMERICAN AXLE & MANUFACTURING

The View from APAC

Where the NA/EMEA Council meeting largely focused on the role of an accountability standard in improving security and aligning business and cybersecurity leaders, the APAC Council meeting focused on sharing best practices for building alignment and strengthening security and resiliency.

For example, to build trust with business leaders and promote alignment, Shankar Krishnan, the CISO and Group Head of Information Security for Boost Malaysia, does extensive work on the fintech company's security strategy. He ties it directly to the business strategy and shows Boost's executive team how the security strategy and controls are aligned to business goals and objectives, how cybersecurity will enable the business and help increase revenue, and how adoption of controls will lead to a financially sustainable security model over time.

> "Getting money is one part of the journey. Knowing how to spend it and ensuring the right spend is equally important."

SHANKAR KRISHNAN
CISO, AXIATA DIGITAL SERVICES & BOOST MALAYSIA

The Threat Landscape in APAC

More than 1 in 4 attacks worldwide occurred in Asia in 2021

Top infection methods included unpatched vulnerabilities (43%) and phishing (43%)

Nearly 60% of attacks targeted financial services and manufacturing companies

Only 26% of companies in APAC have a coordinated incident response plan that they apply consistently across all IT assets (cloud-based and on-premises), test environments, and critical systems

20,000
new software vulnerabilities were discovered in 2021

318 days
the amount of time it takes to detect and contain a breach in APAC

150 days
the amount of time it takes to fill vacant cybersecurity positions in APAC

$2.6 million
the average cost of a data breach in APAC

Source: IBM X-Force

While business-cybersecurity alignment is essential, it's also increasingly critical for security leaders to work in lock step with IT and OT leadership. Mel Migriño, Group CISO for Meralco (Manila Electric Company) in the Philippines, said her security organization has been closely tied in with the company's digital transformation and the transformations of its IT and OT architectures from the start. Integrating security into these fundamental business and technology transformations builds security into the fabric of the business and helps to prevent the vulnerabilities that arise when these functions aren't adequately aligned.

John Taylor, Group CIO for Technology and Security at MedHealth in Australia, recommended that cybersecurity organizations strive to be best in class in three areas: governance, connecting with end users, and incident response. "If you're world class in governance, you know what your risks are and where your spend should go, you know what your ROI is, you collaborate more effectively with the business, and the business comes along on the journey," he said.

Connecting with end users is critical to improving security since end users are often an organization's first line of defense. But since some security organizations have a reputation for making end users jump through extra hoops to get their jobs done, Taylor and several other APAC Council members have gone to lengths to win over users and help them appreciate the essential role they play in protecting their organizations from cyberattacks.

For instance, both Taylor and Seng Wei Keng, the CISO at DBS Bank in Singapore, have worked with user experience (UX) design teams to get help designing security controls that end users will embrace rather than ignore or circumvent. Taylor has also worked with external marketing agencies to design internal marketing campaigns that help users understand the importance and value of security–and their role in it. Leonard Ong, APAC CISO for GE Healthcare, recommends removing opportunities for users to make mistakes that lead to security incidents by using controls to automate and enforce cybersecurity policies as much as possible.

> "Security has to be part of a company's digital transformation from the start."

MEL MIGRIÑO
GROUP CISO, MERALCO (MANILA ELECTRIC COMPANY)

With respect to incident response, Hoo Ming Ng, the former Deputy Chief Executive of the Cyber Security Agency of Singapore, recommended having incident response retainers in place so organizations aren't scrambling to find help in the midst of a breach. Incident response retainers ensure organizations have immediate access to experts who can help them quickly identify the root cause of a breach, and to prevent similar attacks from occurring in the future, eliminate any backdoors attackers may have left.

Pei Yuen Wong, ASEAN CTO for IBM Security and former CISO of the Monetary Authority of Singapore, urged companies to go beyond traditional tabletop incident response exercises and instead conduct far more realistic and rigorous tests of their incident response plans and procedures in production environments. He noted the importance of including external stakeholders—especially cybersecurity vendors and partners—in addition to internal stakeholders in these real-world exercises.

A DIFFERENT PERSPECTIVE

While Council members globally underscored the importance of collaborating with business stakeholders and carefully engaging end users in security, Angel Redoble, the Group CISO for PLDT and Smart Communications (the national telecom company in the Philippines), noted there are times when cybersecurity leaders must remove the soft gloves and mandate certain changes and behaviors throughout their enterprises. For example, when Redoble joined PLDT, cybersecurity policy and investment decisions were taking place in silos throughout the company. With the backing of PLDT's Chairman and CEO, Redoble was granted full control over all cybersecurity policy, budget, and implementation decisions across the company so that he could quickly establish an efficient and effective security program. With that program in place, Redoble was then able to focus the cybersecurity organization on partnering with the business.

ANGEL REDOBLE
GROUP CISO, PLDT & SMART COMMUNICATIONS

Spotlight on Cyber Risk in the Crypto Industry

Jason Lau, the CISO of Crypto.com and a member of the Cyber Defenders Council in Hong Kong, said the decentralized finance industry is experiencing unprecedented risk. "We're seeing different types of attacks that we don't have playbooks for." What's more, he noted that the amount of money threat actors have stolen from cryptocurrency exchanges in just the first six months of 2022 exceeds the total amount of money stolen across the industry's entire history.

Compounding the risk that the decentralized finance industry faces is the speed with which attackers are able to exfiltrate funds. "When you're dealing with smart contracts and with the way the blockchain works in cryptocurrency, if you don't react quickly enough to an attack, it's a major issue because hackers immediately start moving funds off to external wallets, then they go to other platforms where they can wash the funds using tornado exchanges or tumblers," Lau said.

One advantage the decentralized finance industry has over other industries, according to Lau, is that the blockchain makes attacks unusually transparent. "It's different from the traditional world where attackers come in, steal data, and disappear," he said. "In the crypto space, you can see attackers' behavior: how they're working and how stolen funds are moving, for example. Based on their behavior, you can identify whether your attackers are nation states or different groups."

> We're seeing different types of attacks that we don't have playbooks for.

JASON LAU
CISO, CRYPTO.COM

Defending Forward and Moving Cybersecurity Forward

The Cyber Defenders Council meetings revealed that business and security leaders continue to make different assumptions about their organizations' cyber risk exposure and the measures needed to address it. APAC Council members showed that driving alignment and awareness at all levels of an organization, from end users to the executive leadership team, takes constant effort and lots of creativity.

To ease some of that effort, a cybersecurity accountability regulation or standard, while controversial, could help companies Defend Forward by compelling them to uncover and understand both the material cyber risks and threats they face, and the significant deficiencies and material weaknesses in their cybersecurity controls and posture that expose them to those risks. It could further help companies Defend Forward by instilling a bias for action and driving accountability for fixing deficiencies. Meanwhile, SBOMs and a vendor security exchange will be invaluable in helping security organizations better manage third-party and software supply chain risk.

Forthcoming reports from the Cyber Defenders Council will focus on each of the remaining principles of Defend Forward. In the meantime, consider what a cybersecurity accountability regulation or standard might look like, think about its objectives, ask yourself if there are other ways to achieve the same goals, and share your thoughts on social media with the hashtags **#CyberDefendersCouncil** and **#DefendForward.**

KEY QUESTIONS to Consider

JOIN THE CONVERSATION ON SOCIAL MEDIA

- Do we need accountability regulation to get cybersecurity the board and C-level attention it deserves?
- What would be the purpose of cybersecurity accountability regulation? What problem do we need to solve?
- What constitutes a significant deficiency or a material weakness in an organization's cybersecurity controls or posture?
- Can we use Section 302 of SOX for cybersecurity? If so, how could we adapt it?
- Which executives should attest?
- What other avenues could we pursue in lieu of regulation to get business and security leaders on the same page regarding cybersecurity?

FOLLOW THE CYBER DEFENDERS COUNCIL ON LINKEDIN

NORTH AMERICA/EMEA COUNCIL MEMBERS

PHILIPP AMANN
HEAD OF STRATEGY - EUROPEAN CYBERCRIME CENTER, EUROPOL

JEEVAN BADIGARI
DIRECTOR OF IT GOVERNANCE AND SECURITY, DAMAC GROUP

STEVE BENTON
BELFAST GM AND VP OF THREAT RESEARCH, ANOMALI

PAUL BIVIAN
DIRECTOR OF INFORMATION SECURITY, KIRKLAND & ELLIS LLP

KEVIN BROWN
CISO, SAIC

BETH-ANNE BYGUM
SVP - CHIEF SECURITY AND COMPLIANCE OFFICER, ACXIOM

ROLAND CLOUTIER
EMERITUS CSO, TIKTOK, ADT AND EMC

DAVID CROSS
SVP AND CISO - SAAS CLOUD SECURITY, ORACLE

GENERAL JOSEPH DUNFORD
19TH CHAIRMAN OF THE JOINT CHIEFS OF STAFF

RENEE GUTTMANN
EMERITUS CISO, TIME WARNER AND THE COCA-COLA COMPANY

MALCOLM HARKINS
CHIEF SECURITY AND TRUST OFFICER, EPIPHANY SYSTEMS

PETER KUNZ
DIVISIONAL CISO, LEICA GEOSYSTEMS

RICARDO LAFOSSE
CISO, THE KRAFT HEINZ COMPANY

JANET LEVESQUE
CISO, ATHENAHEALTH

DAVE LEWIS
GLOBAL ADVISORY CISO, CISCO

DR. YONESY F. NÚÑEZ
CISO, JACK HENRY & ASSOCIATES

MIKE OROSZ
VP INFORMATION AND PRODUCT SECURITY, VERTIV

THERESA PAYTON
CEO, FORTALICE SOLUTIONS, AND FORMER WHITE HOUSE CIO

CHRISTOPHER PETERS
VP AND CSO, ENTERGY

NILS PUHLMANN
CO-FOUNDER, CLOUD SECURITY ALLIANCE

ALEX SCHUCHMAN
CISO, COLGATE-PALMOLIVE COMPANY

KERISSA VARMA
MANAGING EXECUTIVE - CYBERSECURITY, VODACOM

ERIK WILLE
CISO, AMERICAN AXLE & MANUFACTURING

ASIA-PACIFIC COUNCIL MEMBERS

HOO MING NG
FORMER DEPUTY CHIEF EXECUTIVE, CYBER SECURITY AGENCY OF SINGAPORE

CHARLES NG
EVP - INTERNATIONAL BUSINESS & CONSULTING, ENSIGN INFOSECURITY

KEITH LEONG
MANAGING DIRECTOR - GLOBAL DELIVERY, NCS

CHUAN WEI HOO
GROUP CISO, ST ENGINEERING

PEI YUEN WONG
ASEAN CTO, IBM SECURITY

SENG WEI KENG
CISO, DBS BANK

EUGENE TEO
VP AND DEPUTY CSO, ULTIMATE KRONOS GROUP (UKG)

YUEZHONG BAO
CISO, LAZADA GROUP

BORIS HAJDUK
CISO, TOKOPEDIA

MICHAEL BECERRA
CISO, DHL EXPRESS

PAUL LEK
DIRECTOR - IT RISK MANAGEMENT & SECURITY APJ, MSD (MERCK & CO.)

LEONARD ONG
APAC CISO, GE HEALTHCARE

CHRISTOPHER LEK
DIRECTOR CYBER SECURITY, NANYANG TECHNOLOGICAL UNIVERSITY

SHAO FEI HUANG
CISO, SMRT CORPORATION

STEVEN SIM KOK LEONG
PRESIDENT, ISACA SINGAPORE

JOHN LEE
MANAGING DIRECTOR - APAC, GLOBAL RESILIENCE FEDERATION & OT-ISAC

JOHNNY KHO
PRESIDENT, ASSOCIATION OF INFORMATION SECURITY PROFESSIONALS

SHIH HSIEN LIM
CISO AND CSO, CERTIS

JASON WONG
GLOBAL HEAD OF IT SECURITY & COMPLIANCE, DYSON

DATO' TS. DR. HAJI AMIRUDIN ABDUL WAHAB
CEO, CYBERSECURITY MALAYSIA

SHANKAR KRISHNAN
CISO, AXIATA DIGITAL SERVICES & BOOST MALAYSIA

ASIA-PACIFIC COUNCIL MEMBERS

ANGEL REDOBLE
GROUP CISO, PLDT & SMART COMMUNICATIONS

MEL MIGRIÑO
GROUP CISO, MERALCO (MANILA ELECTRIC COMPANY)

YARON SLUTZKY
CSO, AGODA

ROBERT OH
EVP - HEAD OF CORPORATE DIGITAL STRATEGY & COO OF DDI BU HEADQUARTERS, DOOSAN

JOHN TAYLOR
GROUP CIO - TECHNOLOGY & SECURITY, MEDHEALTH

JASON LAU
CISO, CRYPTO.COM

DENNY HUSEN
GLOBAL HEAD OF INCIDENT RESPONSE, CRYPTO.COM

SHUNSUKE UZAKI
CISO AND HEAD OF INFORMATION CYBER SECURITY, COCA-COLA BOTTLERS JAPAN INC.

IVAN NG
GROUP CTO, CITY DEVELOPMENTS LIMITED