

Cyber resilience through a risk-based approach

A risk-based approach for implementing effective
cyber governance in an evolving threat landscape



Building a better
working world

WORLD
GOVERNMENT
SUMMIT 2023

Foreword

The World Government Summit analyzes the need for implementing effective cyber governance, risk and compliance programs within government organizations. Today's cyber risks threaten the entire governmental ecosystem and therefore cybersecurity has to be a core-business priority. Next-generation technologies must adopt the best practices and smart solutions with effective methodologies to ensure cyber resilience.

The government and public sector organizations are gearing up for an age of digital transformation that requires an integrated mechanism that considers multiple facets of an organization. It is essential that we move from cybersecurity to cyber resilience to prepare for the complexities faced in today's increasingly unstable geopolitical environment.



Table of contents

Section 1: Executive summary	04
Section 2: Geopolitics and the digital domain: how cyberspace is impacting government and the public sector organizations	06
Section 3: How cybersecurity regulatory environment is evolving to combat the impacts of a fragile geopolitical landscape	10
Section 4: An effective governance approach for managing cyber resilience	16
Section 5: Implementing an agile approach for managing cyber risks and compliance requirements	24
Section 6: Managing business continuity and defining response, recovery strategies	34
Section 7: Conclusion	36
Call to action	38
References	40
Contributors	41

Section 1

Executive summary

An organization's ability to achieve its business objectives depends on its ability to effectively manage the risks it faces, including cyber risk. Unfortunately, executive management is uncertain about how well cyber risk is being managed in their organizations and how resilient their operations are.

“

The Global Information Security Survey (GISS) 2021 further outlined this concern whereby 56.2% of executives surveyed stated that they do not know whether their defenses are strong enough for hackers' new strategies.¹

Despite the growing concern around maintaining cyber resilience, the pressure to deliver digital transformation at speed has led organizations, especially in the government and public sector, to bypass cybersecurity processes. Not coincidentally, it is at a time when cyberattacks, especially from geopolitical threat actors such as state agencies and state-related groups, are on the rise.

At their core, all government and public sector organizations function based on trust. To win and maintain the trust of citizens, such organizations have to demonstrate consistent dedication in preserving confidentiality, confirming the availability of systems and services, and maintaining the integrity of data. As such, cyber attacks pose an unprecedented threat to the government and public sector. It is important that cybersecurity is placed at the heart of any organization's strategy, that is, an effective cyber governance, risk and compliance program, driven by a security-by-design (SbD) approach that embeds risk-based thinking from the onset of all projects.

EY teams' cross-functional knowledge and core competencies in cyber governance, risk and compliance has allowed us to assist several organizations in establishing effective methodologies to ensure cyber resilience. Pioneering organizations are building methodologies that consider not only the business environment, but also the geopolitical risk landscape. As it has become evident that a hybrid warfare, such as cyber attacks is the new reality, and geopolitics and cybersecurity are inextricably linked.

While no organization is immune to cyber attacks, organizations with strong cyber defenses and data protection systems, and those that consider a risk-based approach to cybersecurity, are likely to be more resilient. A risk-based approach to cybersecurity allows organizations to focus on protecting high-value information assets and mitigating

the most impactful risks, thereby reducing the attack surface. Implementing such an approach requires an integrated mechanism that considers multiple facets of an organization (e.g., types of assets, complexity of processes) and a phased methodology that covers the understanding of business and technology environment, classification of technology assets, analysis of risks or threats, assessment of control design, and implementation of risk-treatment options.

This white paper outlines how the government and public sector organizations should focus on cyber resilience capabilities that reduce the impact of a successful cyber attack. It presents the aforementioned risk-based approach to implement a holistic and effective cyber governance, risk and compliance programs that primarily include cyber risk assessments supported by thorough technical assessments, such as vulnerability assessments, penetration testing and critical assets configuration reviews.

“

A risk-based approach to cybersecurity allows organizations to focus on protecting high-value information assets and mitigating the most impactful risks, thereby reducing the attack surface

Section 2

Geopolitics and the digital domain: how cyberspace is impacting the government and public sector organizations



Considering recent technological developments and the interconnected world, we can no longer separate the world of technology from the world of business and neglect the importance of modern technology for critical operations. Information technology (IT) and operational technology (OT) have become essential and indispensable elements in various sectors. Operations, including vital ones in critical sectors or critical network infrastructure (CNI), have become heavily dependent on OT or industrial control systems (ICS) which has resulted in such technologies becoming prime targets for nation-state attackers. While there are many malicious actors in the cyberspace, the state-threat actors are capable of causing the highest degree of damage to government and public sector organizations through the level of sophistication of their attacks. State-threat actors carry out security operations on behalf of the State, and in most cases we are uncertain about their operations.

The propagation of nation-state threat actors can be attributed to the current unstable geopolitical environment. In such a volatile state of international affairs, we expect to observe more cyber operations being driven by geopolitics in the near to mid-term future. Consequently, a destabilized situation and continued threshold exceedance in terms of malicious cyber activity may also lead to more damage. Recently, this has been particularly observed when a number of large CNI companies across the EU were subject to cyber attacks during the war in Ukraine. In the *Microsoft Digital Defense Report 2022*, the software maker said the cyber attacks linked to nation-state activities targeting critical infrastructure around the world jumped from 20% to 40% between 2021 and 2022.²

Over this period, two sophisticated malware programs, namely "Pipedream"(Incontroller) and "Industroyer", were deployed with greatest impact in Ukraine, where they caused significant damage and disruption to CNI in the energy, utilities and telecommunication systems, among others. Furthermore,

state-sponsored organized criminal groups were leveraging vulnerability exploitation (specifically zero- day exploits) to carry out cyber attacks. ProxyLogon, the Fatedier reverse proxy tool, and ProxyShell are among these reported vulnerabilities, according to CrowdStrike's Global Threat Report 2022.³ ProxyShell, for example, was reported in a cyber-espionage operation targeting telecom providers in the Middle East by an advanced persistent threat (APT) group in 2022.⁴

Cyber warfare may also extend to the arms race between countries, which can result in the competitive acquisition of military capability as state actors fight over the best and most powerful technology. In 2022, APT groups harvested technological information and intellectual property (IP) for the benefit of state-owned industries. Winnti Group (APT 41) for example, is a global cyber-espionage campaign that targets manufacturers across North America, Europe and Asia in the defense, energy, aerospace, biotech and pharmaceutical industries (Henriquez, 2022).⁵

It is not possible to escape from cyber warfare in today's world. Global instability, political tension or even cyber attacks in general, oblige countries to reconsider their international strategies and include cyber security as a security against cyber attacks which may otherwise have catastrophic effects in vital sectors.

In April 2022, another major cyber attack was reported in Costa Rica, where hackers breached the Finance Ministry and paralyzed the ministry's network, demanding a ransom of US\$10m to return access to the government (Reed, 2022). In May 2021, an American refined petroleum pipeline which ships refined petroleum products for its customers from Houston, Texas to the eastern portions of the US, suffered from a ransomware attack, disabling computer systems and interfering with pipeline operations. Some affected customers experienced fuel shortages. News of the cyberattack also impacted customers who produce fuel for gas stations.

This resulted in fear of a gas shortage and resulted in panic buying. Long lines at gas stations in many states actually created some real shortages and increases in fuel prices. These attacks could have more dire consequences depending on the extent and scope of the attack.

The concepts of war and politics have changed in the digital era and the complexity of attacks is increasing with the introduction of modern technology, such as quantum computing, internet-of-things (IoT) and blockchain. The nature of these risks requires that governments collaborate with the public sector to develop regulations, policies and procedures to effectively confront and eliminate cyber threats.

“

Additionally, influence operations are on rise in 2022 to enable propaganda influence to erode trust and impact public opinion to propagate narratives through government-backed and influenced media outlets and social media channels.⁶





Section 3

How cybersecurity
regulatory
environment is
evolving to combat
the impacts of a
fragile geopolitical
landscape

In trying times, when the world is making their comeback with lessons learned during the COVID-19 pandemic, we are constantly reminded that the environment is dynamic and daunting. We have seen the unprecedented pace of digital transformation across public and private sectors, and their increased utilization of technologies to achieve strategic objectives. In 2022, we also witnessed how geopolitical tensions brought forth the reality of cyberwarfare as seen in the war in Ukraine and Middle Eastern region, most notable being in the KSA, the UAE and Qatar, where it has had effects on the industries and economies. These scenarios have fueled cybersecurity threats to grow and evolve rapidly, on a national and global stage. This is where the government's role as a policymaker and enforcer has become crucial. The government is challenged to create a secure and resilient environment where the government and public sector, in addition to CNI providers can guarantee the security of our increasingly online way of life.

Regulation vs. emerging threat landscape

With the ever-dynamic threat landscape, traditional guidance on cybersecurity best practices may not be sufficient to address threats. This drives state authorities to conceptualize and implement regulations that would enforce implementation and operation of cybersecurity resilience, to combat next-generation risks. When we talk about cybersecurity resilience, we can envision an environment that facilitates a secure cyber ecosystem to include both core infrastructure and support for industries in sustaining and recovering from attacks. National cybersecurity regulatory frameworks that cover the topics of risk management and threat intelligence can help governments combat emerging threats.

Furthermore, regulations should be able to create an open environment that would allow and encourage information sharing and strong collaboration at both country and industry levels. This was demonstrated by the United Nations (UN) Open-ended Working Group (OEWG), on developments in the field of information and telecommunications, in March 2021. The group endorsed a report containing cybersecurity recommendations and it was adopted by all countries, by consensus.

The war in Ukraine and its contribution to global cyber threats

The war in Ukraine has demonstrated the new 21st century warfare. It gave birth to a number of global implications that has spilled over in the cyberspace. The continued escalation has led to upsurge of "hacktivism", where one hacks into a computer system, for politically or socially motivated purposes, and cyberwarfare, that has threatened those outside the borders of Ukraine. The war in Ukraine serves as a reminder to other countries to bolster their cybersecurity defenses, if the war further expand within their territory and affect their national and foreign policies. In Germany, cybersecurity resilience is promoted among businesses that provide critical services such as transportation, food and utilities to combat any possible threats from war in Ukraine. Finland on the other hand, has been creative in advocating cyber resilience by introducing a voucher scheme that would fund companies in improving their security capabilities in response to the war in Ukraine and the country's bid to join the North Atlantic Treaty Organization (NATO).

“

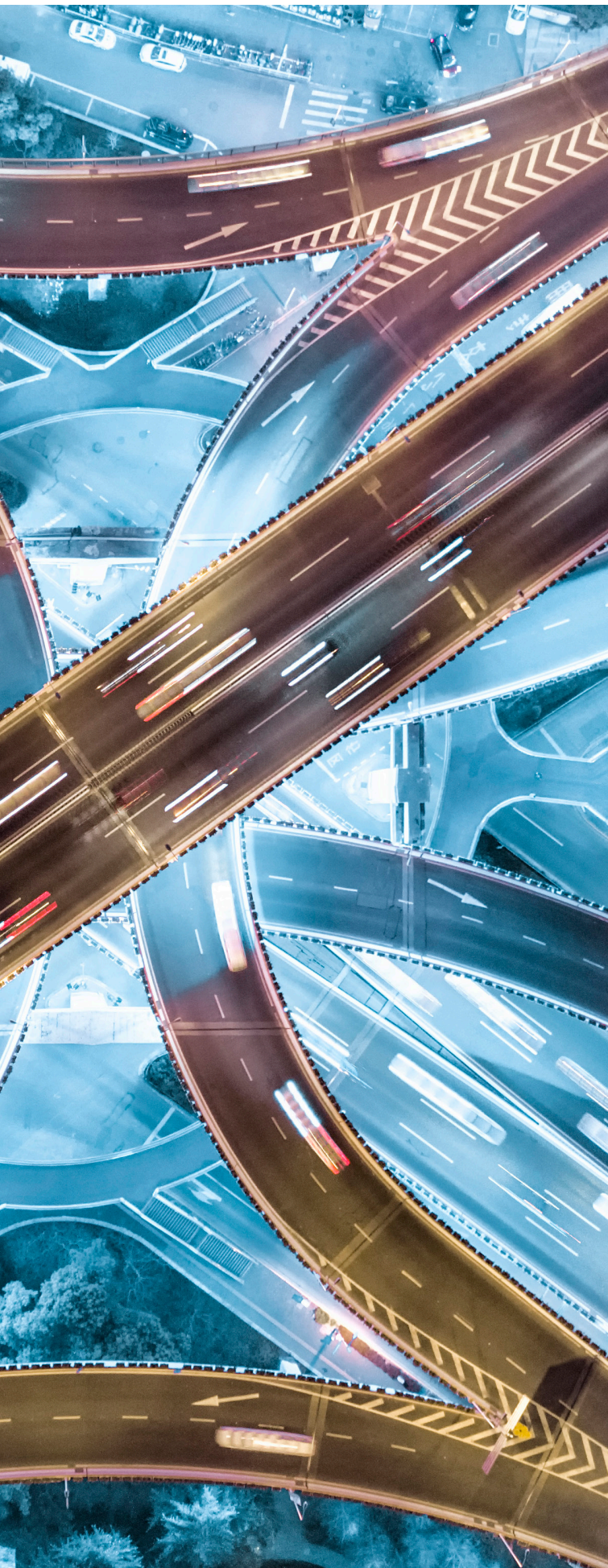
In Germany, cybersecurity resilience is promoted among businesses that provide critical services such as transportation, food, utilities to combat any possible threats from the ongoing war in Ukraine

Risk management as a foundational requirement

The goal of having a cybersecurity resilient environment is to call governments to provide structured methods to measure an organization's ability to defend against attacks. We have seen regulators revisiting their current risk management guidelines to ensure that they are up-to-date, to support industries and organizations in combating cyber threats. National regulators need to consider the following key focus areas as part of the cybersecurity frameworks that are being defined:

- Overall accountability: Resilience is a team sport. Regulations need to mandate organizations to ensure that it is not just the operational or cybersecurity professionals who ensure resilience, but also other internal stakeholders, including the business-line management, vendor management, second-and-third lines, legal and the board, among others. In addition, organizations should be encouraged to develop and implement a cyber resilience strategy that is effectively concerted,





coordinated, multidisciplinary and tested on a periodic basis through simulation exercises.

- ▶ Risk management: Regulations need to provide avenues for organizations to embed cyber resilience requirements into the risk-appetite framework. In this context, the second-line of defense needs to have an effective set of metrics to evaluate the cyber resilience risk. Many of those metrics may come from the first-line, but the second-line needs its own metrics, especially to evaluate enterprise-cyber risk at the aggregate level.
- ▶ Internal audit: The third-line of defense (internal audit) has a key assurance role to play. The approach third-line takes to validate the effectiveness of the cyber framework(s) was adopted by the first-and-second lines for evaluating and managing cyber resilience risk which is essential for ensuring effective resilience capabilities that can withstand cyber attacks.

On 13 May 2022, the Council of the EU and the European Parliament reviewed and updated current Network and Information Security (NIS) directive to NIS2. The new directive sets “a baseline for cybersecurity risk management and reporting obligations across critical sectors.” The agreement will be recognized across all covered regions in hopes of establishing a proactive threat mitigation across industries.

In the US, the National Institute of Standards and Technology (NIST) has released a revised publication of its Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.⁷ The revised publication focuses on helping businesses understand ways to identify, assess and respond to cybersecurity risks throughout the supply chain across their organization. Moreover, the US Department of Commerce published a proposed rule to implement regulations pursuant to the executive order of May 2019, to improve information communication technology services (ICTS) supply chain.⁸ These will address concerns about product's design, development, manufacture, supply, and control of ICTS by foreign adversaries.

Proliferation of ransomware

The threat of ransomware continues to grow in 2022 and it still poses a significant risk to organizations of all sizes across all sectors. The 2022 report from the European Union Agency for Cybersecurity (ENISA) on threat landscape for ransomware shows how organizations are still susceptible to this kind of attack and concluded that it has a devastating impact on organizations, especially if they are not prepared.

The risks imposed by ransomware has pushed regulators and enforcers around the globe to collaborate in fighting ransomware attacks. In July 2021, at the INTERPOL High-Level Forum on Ransomware, it was discussed that effectively preventing and disrupting ransomware would require “adopting the same international collaboration used to fight terrorism, human trafficking, or mafia groups.”⁹ The group called for police agencies worldwide to form a global coalition with industry partners to stop ransomware’s exponential growth. UK’s National Cyber Security Centre (NCSC), Australian Cyber 18 Security Centre (ACSC), Federal Bureau of Investigation (FBI), National Security Agency (NSA), and Cybersecurity and Infrastructure Security Agency (CISA) published a joint alert,¹⁰ urging businesses to take action to protect themselves from attacks.

On the other hand, to further stop proliferation of ransomware attacks, legislations that prohibit ransom payments were enacted in light of the war in Ukraine. For example, in the US Department of Treasury’s Office of Foreign Assets Control (OFAC) has prohibited ransom payments, including payments with cryptocurrency or payments facilitated through third parties, to sanctioned persons or entities.¹¹ As a further attempt to discourage ransom payments to sanctioned entities, the Financial Crimes Enforcement Network released an alert to all financial institutions “to be vigilant against efforts to evade the expansive sanctions and other US-imposed restrictions implemented in connection with the war in Ukraine.”¹²

“

However, governments are also being proactive in combating ransomware. In US again, the FBI has launched the Virtual Asset Exploitation Team(VAXU) to track ransomware and ransomware profits.¹³

Renewed attention on industrial cybersecurity

With the increasing number of OT and IoT devices, the domain of industrial cybersecurity requires renewed attention from the regulators. To combat the ever-growing susceptibility of this area to cyber attacks, countries have introduced technical requirements to enhance security controls over OT or IoT devices. In Europe, the EU has introduced amendments to the EU’s 2014 Radio Equipment Directive (RED), which would ensure all wireless devices are sufficiently safe before being sold. It required manufacturers to follow new cybersecurity safeguards when designing and producing products, and mandated increased protection for personal data.¹⁴ While in the US, a legislation known as the Cyber Shield Act was reintroduced in Congress on 15 March 2021. If passed, the law would¹⁵ create security standards for IoT devices based on the recommendations of an advisory committee made up of cybersecurity experts from the government, academia and the private sector. Devices manufacturers meeting these regulations would be allowed to label their products with a mark indicating they had met the standards and that their products were more secure. Australia is also

considering making mandatory a suite of voluntary regulations that would outline a set of minimum cybersecurity requirements for consumer-grade smart devices.¹⁶

Increased requirements On cyber reporting

To further practice resilience, new regulations are introduced to have better transparency on cybersecurity incidents. Commonly, these requirements are found on data privacy regimes where there are requirements on data breach notifications. Now, governments have realized that cyber attacks go beyond misappropriation of personal data. In the US, the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) was passed in March 2022. It will require critical infrastructure companies, including financial services, to report cybersecurity incidents, such as ransomware attacks, to the Cybersecurity and Infrastructure Security Agency (CISA).¹⁷ Moreover, within the same timeline, the US Securities and Exchange Commission (SEC) proposed a rule requiring publicly listed companies to report to the SEC cybersecurity incidents, their cybersecurity capabilities, and their board's cybersecurity expertise and oversight.¹⁸ In addition, the President of the US has signed into law the "Better Cybercrime Metrics Act" that establishes requirements meant to improve cyber reporting and tracking for increased visibility around attack vectors and attack evolution.¹⁹

The continuous challenge to regulators

As the world further digitalizes and the global geopolitical landscape continues to be dynamic, there is no standard response to all cybersecurity threats. It is imperative for governments to lay down regulations and guidelines that would enable sectors and

organizations to practice cyber resilience within their own environment. The challenge is for regulators to be aware of the changing digital environment, think ahead to prepare for threat actors and create an avenue where industries will be open to collaborations and partnerships.



Section 4

An effective governance approach for managing cyber resilience



With the ever-growing and dynamic threat and geopolitical landscape, it's imperative for the government and public sector organizations to promote cybersecurity resilience as part of its mandates. Revisiting its definition, resilience is the organizational capability to sense, resist and react to disruptive events by adapting and reshaping operations in their environment. Applying this concept in cybersecurity, resilience aims to defend against potential cyber attacks and ensure survival following an attack, without the loss or threat to data.

While defining it may seem easy, the main challenge is to build an ecosystem where the government and its constituents can achieve a sustainable and resilient operation. Of course, it is the government's role as policymaker to enact regulations that would establish cybersecurity resilience across its landscape.

The fast-evolving nature of the cyber risk environment makes it increasingly important that the government and public sector organizations adopt a risk-based approach to cybersecurity. Organizations simply cannot protect everything to the same degree. The first step is getting the cyber governance right. Management understands that cybersecurity is a major risk, perhaps even the number one risk. They know the risk is fast-changing and that it's difficult to keep up with. Yet they struggle to determine how their governance should evolve. In practice, a broader set of trends will influence the future design of cyber risk governance. These include new privacy and data laws, the implementation of the cybersecurity three lines of defense (3LOD), the need to build cybersecurity into innovation, and complying with new regulations and enhanced supervisory expectations. An appreciation of these broader trends is important for better design of governance.

	Who are they?	What are their cybersecurity roles?	What is their challenge?
First-line	Business units and information security teams with direct accountability for owning, understanding and managing cyber risks.	<ul style="list-style-type: none"> ▶ Measure, monitor, manage and mitigate cyber risks and vulnerabilities within the board-approved cyber risk tolerance if front-line business units are working with the information security and cybersecurity teams. ▶ Define the cyber risks and exposures in each line of business. ▶ Develop standards and procedures that implement the second-line cyber risk framework in the context of specific-business risks. 	<ul style="list-style-type: none"> ▶ Getting cybersecurity-thinking embedded in day-to-day operations. ▶ Getting the first-line (not the cybersecurity group) to identify cyber risks properly, and develop and maintain strong controls.
Second-line	Risk managers responsible for aggregate enterprise-wide cyber risks, who are granted independent authority to challenge the first-line's approach to cyber risks effectively	<ul style="list-style-type: none"> ▶ Develop a cyber risk framework and challenge the first-line's implementation of it. ▶ Develop the firm's cyber risk appetite and monitor conformance to it. ▶ Report the aggregate enterprise-wide cyber risks. 	<ul style="list-style-type: none"> ▶ Developing an insightful set of enterprise-wide cybersecurity metrics. ▶ Aligning the cyber risk management framework with the overall risk framework. ▶ Finding talent that knows risk and cybersecurity.
Third-line	Internal audit team providing assurance for the firm's overall cyber risk governance	<ul style="list-style-type: none"> ▶ Audit core elements of cyber, either as separate audits (e.g., on access controls) or with relevant topic-specific audits (e.g., vendor-risk management). ▶ Evaluate overall design and effectiveness of cyber risk management across first-and-second lines. 	<ul style="list-style-type: none"> ▶ Providing insights that improve the quality of cyber controls. ▶ Determining the best approach to independently assess the cybersecurity risk framework.

The second-line risk function has to build its capabilities. Cyber risks should be hardwired into the enterprise-wide risk-appetite framework, so that the management can formally approve its appetite for cyber risk.

The cyber risk management framework should be fully incorporated in the broader enterprise-wide risk management approach, and aligned well with IT, security-risk and operational-risk frameworks. The third-line

(internal audit) will need a stronger focus on cybersecurity, new personnel (or co-sourced capabilities), and a more independent view on how well the board, and first-and-second lines should oversee, evaluate and manage cyber risk. A major challenge for all three-lines is managing cyber risk associated with third parties. Regulators are increasingly pushing for more ongoing, detailed oversight of third parties, particularly as it relates to cybersecurity, resilience and data protection.

Building in cyber resilience from the beginning

Despite the challenges posed by the ever-evolving cyber risk landscape, where the expertise of the bad actors and the threats seem to be multiplying daily, the government and public sector organizations need to discuss a key opportunity, building cyber resilience into the foundation of any organizational change. In addition, building cyber resilience needs to be associated with spreading the practice of trust by design, a top-to-bottom mandate to build in cybersecurity when designing or redesigning all products, processes, applications and services or when contemplating a public-private partnership (PPP). Senior management can support and reinforce this concept by verifying security before initiatives are launched or at the inception of every initiative.

It is important to recognize that the typical IoT devices may pose challenges for the Trust by Design concept. Generally built with speed in mind, these technologies may offer easy access to threat actors. Similarly, many digital transformation programs do not include the security feature until they are implemented, which is a process that almost always creates safety gaps. Thus, it is essential for senior management to support inserting security requirements early in the design-and-conceptualization phases. It is also essential to build trust into everything that is being designed or redesigned. Typically, there may be internal resistance to change as there is

a general misconception that this will cause a slow down in the business side. Thus, the senior management's imperative to ensure early collaboration is critical in a Trust by Design model.

The risk equation

While building security into the design phase of key initiatives enables organizations to mitigate risk, it does not eliminate risk. Companies may need to make tough decisions about where to invest and that is where risk quantification comes into play. It is critical that key stakeholders understand what is at stake, the risk-occurrence probability and an estimate of the financial cost for the damages incurred, if any. The potential magnitude of a given risk can be calculated using this formula: risk = threat (e.g., malware) x vulnerability x impact on the organization (e.g., to its operations, reputation). While numerous assumptions are built into such an equation, the government and public sector organizations seek greater financial quantification to make more informed governance decisions around risk appetite and tolerance.

Independent assessments

Many companies use well-known frameworks and principles to address cybersecurity governance, but using a third party for verification is a key step in linking risks to programs and controls and tying results back to the organization's processes. It is essential that the government and the public sector organizations hire a third party to assess the organization's security program. Some organizations have chosen to have a very simple inquiry and observation with the Chief Information Security Officer (CISO), involving a limited number of hours. For more assurance, others seek additional control testing of relevant frameworks (e.g., NIST). For the highest level of assurance, an attestation

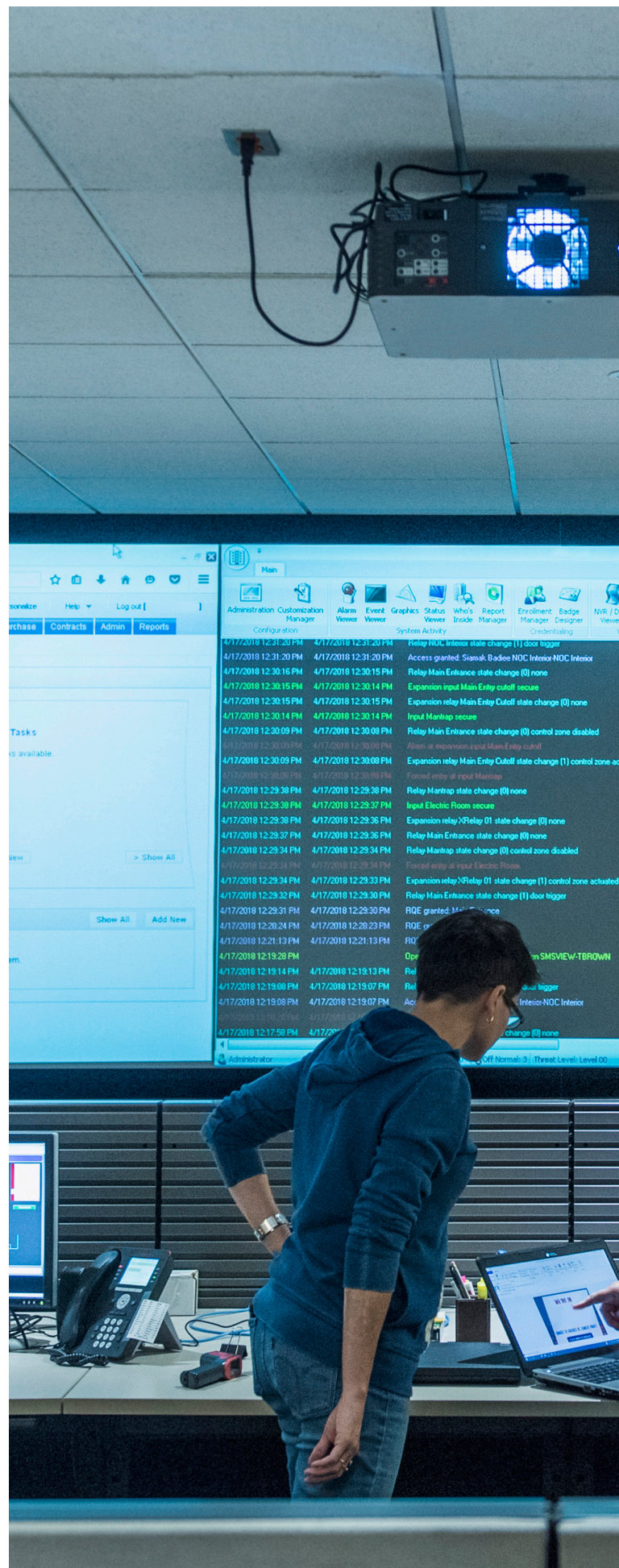
opinion is sought from an independent third party utilizing the American Institute of Certified Public Accountants' (AICPA) System and Organization Controls (SOC) for cybersecurity framework, which provides for an entity-wide evaluation of the organization's cyber risk management program.

We should aim to make cyber resilience a seamless initiation of steps to maintain the ongoing delivery of operations during a disruption. The following approaches can be considered to achieve the same:

Assess risk profile and identify major risks, threats and vulnerabilities

Cyber resilience risk assessment, coupled with the prioritization of criticality, is the fundamental building block for any cyber resilience program. This is the first step in achieving cyber resilience and it can be accomplished by the following:

- ▶ Effective risk-assessment process: Risk identification is a first-and-second line role. How well does the first-line consider cyber and resilience risks, from their perspective? How well does the second-line independently assess these risks to effectively challenge and complement the first-line view?
- ▶ The first-and-second lines' risk analysis will need updating routinely, given the fast-evolving nature of cyber risks.
- ▶ Effective controls: Building controls in the light of the risk assessments is critical. Those controls have to reduce residual risks within the firm's overall risk appetite for resilience. This includes understanding how dependency on third parties impacts the control environment.
- ▶ An enterprise-wide, prioritized view on critical processes and flows: Given finite resources, management time, budget and people, firms inevitably have to prioritize certain resilience activities and determine which processes and systems require a differentiated strategy. This will likely create differing views within each firm about





what can be constituted as critical. The organization's first-line of defense, its risk management committee and regulators may have different definition of criticality. What organizations need to do is manage these stakeholders demands for resilience.

Identify, architect and protect systems

Identifying the most critical systems and assets (including high-value assets) is an essential prerequisite in cyber resilience. Once critical systems have been identified, organizations have to:

- ▶ Identify systems' ecosystem: A number of techniques can be employed in to appropriately identify assets. One of which are business impact analysis (BIA) that can identify cyber components and assets within the organization itself, classify cyber and technology assets based on their confidentiality, integrity, and availability (CIA), and create cyber risk profiles and registers.
- ▶ Evaluate if systems and tools used to monitor infrastructure present major vulnerabilities: Organizations have implemented a growing set of tools to evaluate their networks and systems to detect threats and implement encryption tools to protect sensitive information. However, it is important that organizations validate that those tools do not, in themselves, create additional security threats.
- ▶ Evaluate If systems and tools used to monitor infrastructure present major vulnerabilities: Organizations have implemented a growing set of tools to evaluate their networks and systems to detect threats and implement encryption tools to protect sensitive information. However, it is important that organizations validate that those tools do not, in themselves, create additional security threats.

- Evaluate system obsolescence: Every firm organization has adopted its own strategy for managing system obsolescence, such as the pace at which it moves to new versions of software or hardware, the approach to patching, and the degree to which the firm will depend (or not) on systems that are no longer vendor supported. While the overall strategy may make sense for the firm, it is important that firms show that they have carefully considered a differentiated strategy that is crucial for critical systems. As recent global ransomware attacks have shown, system outages can be traced to dependencies on old versions and bad patching practices. This is unacceptable for critical systems.

Manage critical third parties and other key dependencies

Organizations need to evaluate dependencies on third parties, especially those that support or connect with critical processes and systems. This may include re-evaluating how they identify critical vendors and dependencies. Critical vendors should be evaluated and monitored more than others. Organizations have to:

- Evaluate vendors' resilience and cybersecurity practices: This may be done prior to onboarding vendors, but it will most likely be too cursory and require revisiting, or it might be out of date. Firms will need to determine how quickly vendors can get their systems back up after some disruption and if there is a prolonged outage, how can the vendor support to ensure continuity.
- Manage contract clauses and obligations: Organizations need to build in contractual terms that clarify not only the level of performance but the key risk and performance indicators that the vendor has to provide on a pre-defined frequency.
- Perform ongoing monitoring: Organizations will need to re-evaluate their approach to monitor critical vendors on an ongoing basis. When real-time monitoring is not possible, near-real-time monitoring (that is, within the day) is required.

Cyber resilience

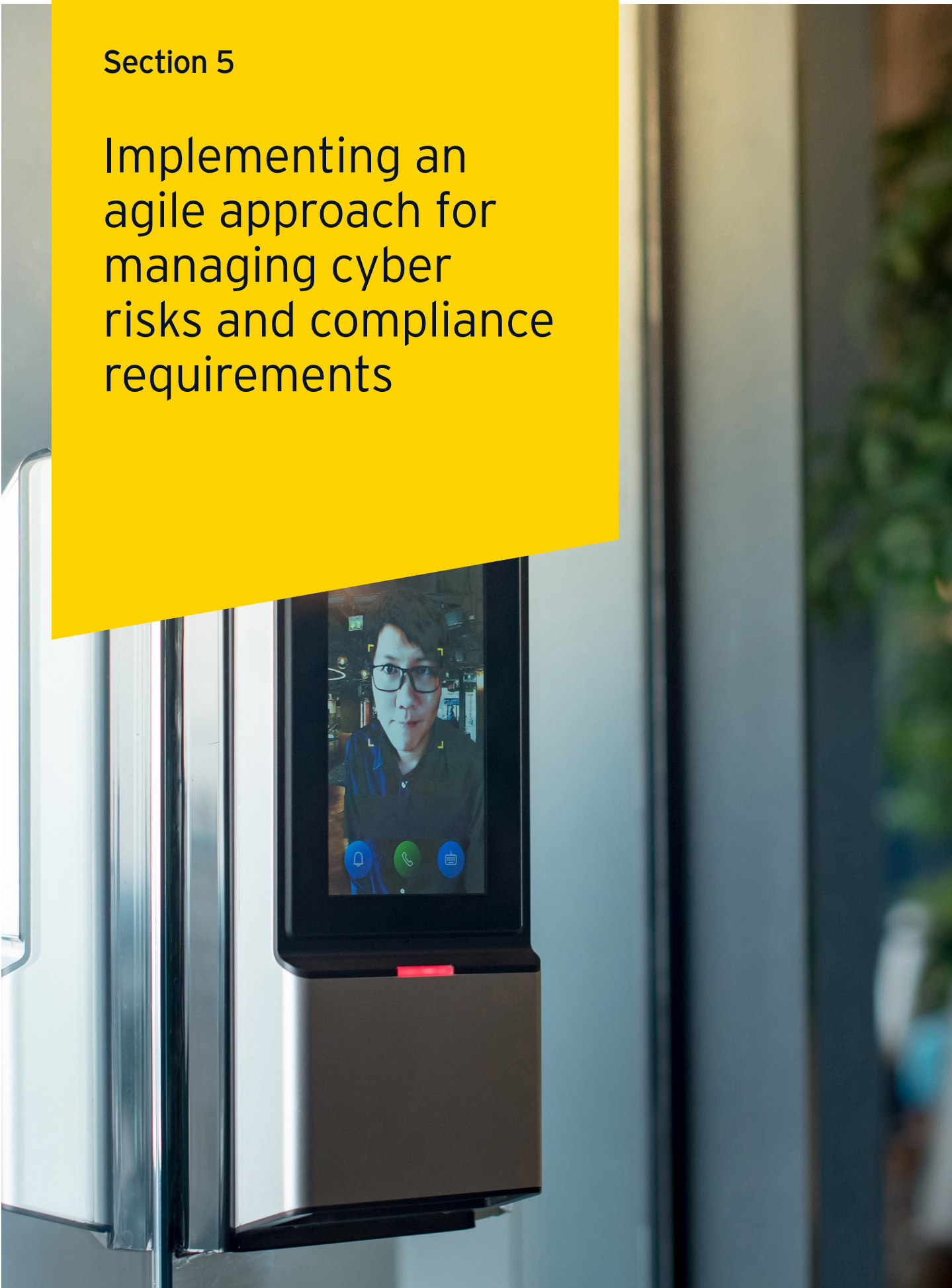
Even with all the best planning in the world, firms still need to conduct their ongoing detection, response and recovery activities. They need to communicate effectively during potential and actual disruptions. When cyber attacks occur, organizations must move quickly to detect and repel them. If those attacks are successful, firms need to know how to react. In the context of resilience, key areas of focus from regulators and organizations include:

- Build capabilities for detection: Detecting problems is essential. It is the lifeblood of resiliency. Organizations should establish a program by collecting intelligence across different sources, analyzing them, and using them to further improve security posture.
- Enhance response capabilities: Being able to respond and operate is a core part of being resilient. This is enabled by having an incident-response program. The program should facilitate effective transition from incident response to crisis management. It is the best practice to regularly test response plan to assess effectiveness and keep key stakeholders adept with their roles and responsibilities.
- Implement recovery capabilities and enhance using testing: Recovering after a disruption remains important. Organizations have to recognize cyber-incidents that present distinct recovery challenges when the systems are down. Recovery sites should be reviewed regularly to ensure high availability of critical systems. Data, as part of recovery, is also important. It helps in validating the integrity and quality of the recovery site while ensuring that it is untampered by an attacker or malicious code.
- Develop escalation and communication plans: Organizations should define an approach to have a speedy and effective escalation during times of disruptions. Communications should be escalated when problem occurs and key stakeholders such as first-line of defense, senior management, regulators and customers must be alerted, if necessary.



Section 5

Implementing an agile approach for managing cyber risks and compliance requirements





Organizations need to take an enormous step to identify and manage the risks associated with their businesses and protect against cyber attacks to minimize any impact on the business operations. Establishing a cyber risk management strategy can assist in making informed risks decisions that are attached to business operations from internal and external perspectives.

Cyber risk management is no longer a choice, it is essential in helping organizations identify the key cyber risks that could affect their businesses. Knowing your risks and associated-risk tolerance and appetite can guide organizations in allocating an effective budget and resources to reduce potential impact by initiating appropriate controls as countermeasures.

The goal of a cybersecurity risk management process is to identify, assess, mitigate and monitor cyber risks of an organization's information assets. This process should be systematic and repeatable so that organizations can be well-informed about the underlying cyber risks and take appropriate actions to protect their assets.

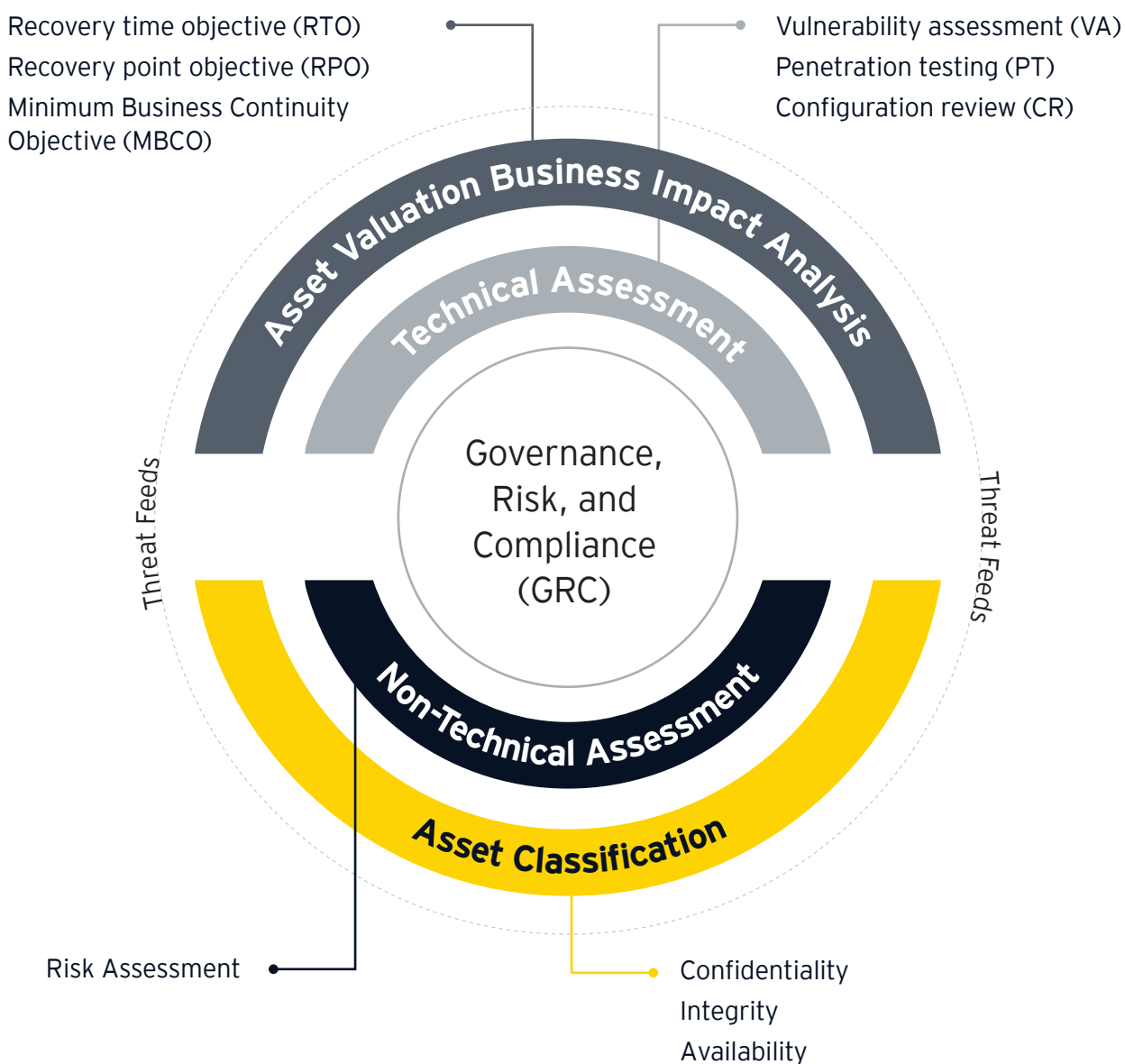
Key components of cyber resilience

Cyber resilience requires an integrated approach to governance, risk and compliance by factoring in the risks and threats along with the resilience capabilities. In order to maintain a resilient ecosystem, it is of utmost importance that cyber governance, risk and compliance functions within organizations are empowered to drive the implementation of key security requirements across the various

business units. The cyber governance, risk and compliance functions can utilize a series of assessments in order to identify the pertinent risk and threat landscape, in addition to leveraging threat intelligence feeds from internal and external sources. We can explain this approach using the diagram below that starts with the identification of asset criticality using the confidentiality, integrity and availability (CIA) triad as well as the traditional business impact analysis (BIA) that considers the impact of disruption to operations.

Figure 1

Cyber resilience integrated approach



Three-pronged approach to identification of risks and threats

We have outlined a three-pronged approach that can assist organizations understand their risk posture, identify its threat landscape and prioritize protection of critical assets, using a series of techniques and assessments that have proved useful for organizations, operating in various sectors, across the globe.

Identifying the organization's "crown jewels"

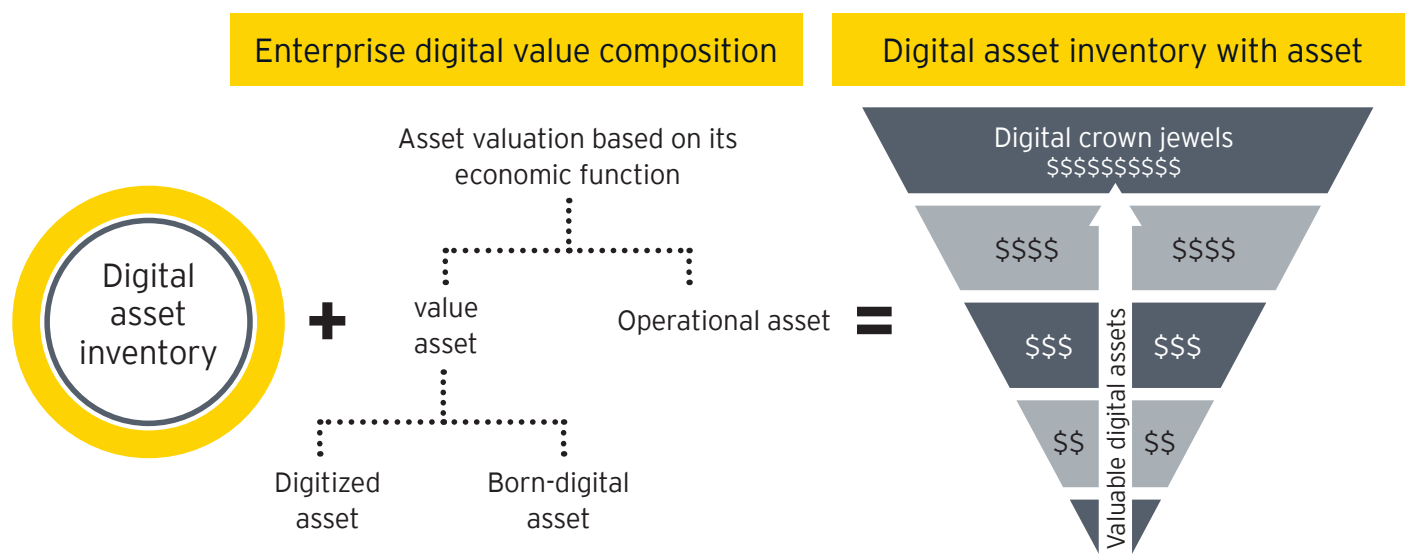
An organization must be willing to spend whatever it takes to safeguard its most valuable assets. Overspending can be avoided through a thorough evaluation using the process outlined in figure 2 below. Organizations can assess the value of their cyber resilience through tailored-economic modeling tools.

Applying a cyber-economic model can help in identifying the most crucial assets that require protection and quantify the economic loss following cybersecurity attacks. For example, what would be the quantified loss to an individual organization if it lost one million customer records, and that loss became public? By employing this model, organizations can plot how the value at risk will start to decline as it increases the defensive controls to prevent the attacks that are relevant to those cyber-economic-loss scenarios.



Figure 2

Three-pronged approach to identification of risks and threats



a. Classification of assets based on CIA

The importance of assets can be identified using the information security model, the CIA triad. Organizations should have a holistic oversight of their information assets, they should be classified by valuating each asset according to the CIA triad. This can be established by identifying the impact rate of each component within the CIA triad according to a predefined scale. For example, impact rate scale can be ranging from low to high. Consequently, organizations can take the maximum rate across the three CIA components of each asset and set the asset criticality accordingly.

This would help organizations separate non-critical assets from unnecessary time-consuming risk assessment activities. This approach supports in having a comprehensive crown jewels repository that reflects its criticality according to the CIA triad which focuses on prioritizing them for the risk assessment step.

b. Integration approach of crown jewels with CIA

Another way of viewing crown jewels is by acknowledging that business processes are considered assets that can be exposed to cyber risks. Thus, a business process becomes an integral factor that organizations should consider while identifying the assets, which aligns with performing the BIA.

Organizations can take their crown jewels repository to the next level by integrating their critical assets with the organization's most critical business processes. Thus, having an integrated approach helps in building resilience and cyber efforts together to come up with robust control over cyber risks within organizations.

Further, integrating business processes adds significant advantage to the crown jewels repository, which enables organizations to efficiently link associated RTO and RPO within each business process. Organizations can have effective oversight over the business impact and amplifications in the event of a successful exploitation, which aids in mitigating risks in a well-informed and proactive manner.

Conduct cybersecurity risk assessment

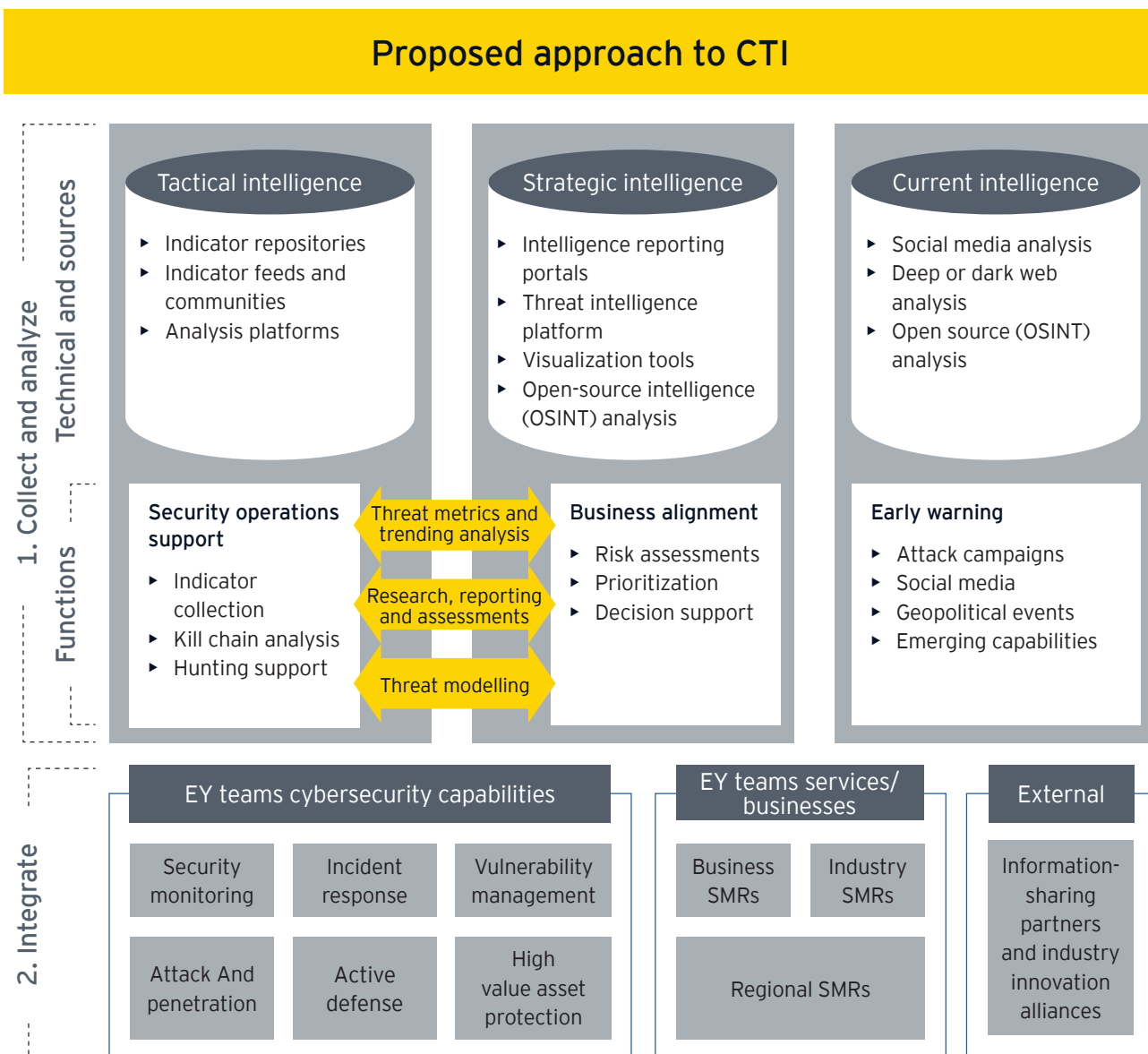
a. Leverage threat intelligence and threat feeds

It is important to invest in cyber threat intelligence (CTI) to understand an organization's risk posture and potential tactics, techniques and procedures (TTPs) and assess how threat agents orchestrate and manage attacks. CTI often goes hand-in-hand with cyber threat hunting (CTH) and provides a view of applicable risks that allow organizations to define their required set of resilience capabilities. CTH is an active cyber defense activity. It is the process of proactively and iteratively searching through networks to detect and isolate advanced threats that evade existing security solutions.

CTI focuses on identifying and analyzing the motivations, methods, capabilities and tools of adversaries who may seek to target an organization by pairing external analysis with data that was once segmented within the organization. While some organizations may choose to define CTI as a component or input-driven service, it is important to note that a process-based intelligence lifecycle within an operational framework is essential to deliver actionable results. Accordingly, a holistic CTI program consisting of processes for collecting, producing and disseminating tactical and strategic intelligence, along with continually augmentation with timely situational awareness updates (also known as "current intelligence"), is required. This helps explain who the relevant adversary is, how and why they may be attacking the organization, what actions could they take following the initial compromise, where could they reside within the organization, and how to detect or respond to an attack.



Figure 3



Collected and produced CTI must be integrated through processes designed to support decision makers, security operations and resilience personnel. The input processes and output products of a CTI program should be designed with the goal of improving cyber threat awareness across the entire organization at a variety of levels. EY teams believe that this can be achieved when CTI is viewed through the lens of "tactical," "strategic," and "current" intelligence components and delivered to relevant stakeholders for defining cyber resilience plans and testing cyber crisis response mechanisms.

b. Identify cyber internal and external risks

The aim of risk identification is to determine what could cause a potential loss and gain insight on how, where and why the loss could occur. Organizations should work on identifying and assessing the possible internal and external cyber risks as an initial step to control risks. Identifying cyber risks can be approached through scenario-based or category-based approach to understand relevant vulnerabilities.

c. Analyze and evaluate cyber risks

When it comes to cyber risk assessment, organizations should consider the impact that a potential cyber risk could cause and the possibility of risk occurrence, which results in understanding the inherent risk rating information such as critical, high, medium and low (impact x probability = inherent risk).

Afterwards, organizations should further analyze the inherent risk rating by identifying and assessing the security controls, implemented currently along with their effectiveness in order to detect weaknesses and vulnerabilities. This also helps to understand the reduced impact and possibility of a successful exploitation, resulting in residual risk rating information, which is considered the final risk rating of a particular cyber risk.

Technical assessments can be employed as part of risks assessment in order to check risk on the components of the technology. Commonly, vulnerability assessment and penetration testing (VAPT) and configuration review, that verifies hardening controls, are performed to complement the usual risk assessment process. However, based on the risk identified and complexity of the implementation, additional review techniques such integration reviews, dynamic code analysis, among others are recommended to ensure that all applicable risks are discovered and assessed.

Types of technical assessments that can be employed in conjunction with risk assessment to accurately detect and discover technical weaknesses and vulnerabilities are.

- **Vulnerability Assessment And Penetration Testing (VAPT):** It is considered to be one of the most popular technical assessments, where based on the scope of assessment it can target the organization's entire technical infrastructure.

- **Configuration Review:** This is considered as an essential aspect of system hardening, which involves secure review of underlying configurations of a particular component within a system.
- **Penetration testing or red teaming:** This is considered as a live demonstration of successful attacks to improve organization's cybersecurity defenses and ensure readiness to protect it against real attacks in an operational environment.

Develop risk-treatment plans and acceptance process

Organizations should consider the management and treatment of cybersecurity risks as a top priority, as a dynamically changing technical environment poses an increased amount of unmanaged cyber risks. Wherever and whenever necessary, efforts should be focused to address critical cyber risks effectively and swiftly, to avoid undesired consequences.

After having structured cyber risk assessment results, organizations can identify their most critical risks based on the residual risk rating and make a well-informed decision on the way forward to treat risks. Should the proposed treatment option indicate mitigation, then, the organization should develop an effective treatment plan that is analyzed and guaranteed to remediate the identified cyber risk and to ultimately protect the organization's CIA.

However, if the proposed treatment option indicates risk acceptance, transfer or avoidance, then, the organization should develop a management process for each treatment option to ensure the risk is well-acknowledged, managed, and treated according to organizational-approved process.

Automation and integration of dashboarding for near-real-time risk monitoring

Organizations should consider implementing an automated risk management dashboard that is integrated with the risk assessment results. This can help in accurately reflecting and propagating the risk ratings and associated information on a holistic executive dashboard. Organizations that deploy this level of mature enablers have more insight and control over their cyber risks, as it enables us to have a comprehensive view to understand which risks pose the greatest threat to an organization's operations and businesses, and manage them accordingly.

The employment of risk management dashboard aids in improving the risk monitoring process by having visual representations of focused statistical references of the risk assessment results. This mainly constitutes monitoring the risk ratings and associated risk remediation progress. Additionally, asset owners can visualize the risk posture in a single consolidated dashboard, which enables an easy yet efficient way of analyzing the overall risk consequences and can help in taking necessary corrective actions.

The risk management dashboard illustrates the status of the organization's risk key performance indicators (KPI) and enables the cybersecurity personnel to monitor the progress of risk remediation activities, the dashboard demonstrates the following components (not limited to):

- ▶ Number of identified threats
- ▶ Percentage of identified risks across rating scale
- ▶ Average of risks per owner
- ▶ Average of treated risks





Automating the risk management dashboard helps in communicating the risk information better among stakeholders, as visualization techniques provide a quick overview of key risk trends and allow cybersecurity personnel to manage and prioritize the identified risks.

Achieving compliance through risk management

A cybersecurity risk management program should align and comply with the applicable national and international standards. The regulations should be considered as a baseline for performing the risk assessment activities. Organizations should identify the necessary compliance requirements based on the organization's applicable legislation and industry-specific mandates.

Relatively, non-compliance with regulated mandates will risk the organizations to being exposed to threats such as financial penalties and reputational damage.

Organizations that follow a cybersecurity risk management in line with compliance requirements can easily identify the mandated controls and assess the risks arising from the missing mandated controls or mandated controls implemented inefficiently. Hence, organizations can effectively monitor and track the compliance status against each control as a result of the risk assessment output. Furthermore, having a risk treatment plan can be leveraged to establish a compliance treatment plan accordingly.

Collaboration invested between cyber risk management and compliance management can propose a unified approach to achieve both aspects while reducing time efforts allocated for each task individually.

Section 6

Managing business continuity and defining response, recovery strategies



With the continuous advancements in digitalization, the current economic landscape is globally dependent on technology-based solutions and digitized or automated processes. Most of these are exposed to the entire world over the internet. This creates a cyber threat surface which compels the governments and public sector organizations to invest in their governance and towards the protection of their services. Accordingly, the concepts of cyber resilience must be incorporated into organizations' business continuity activities to ensure the availability of their core services and to minimize the impact of disruption on services provided to beneficiaries.

One of the leading methods of addressing cyber resilience within the business continuity is by utilizing an enterprise-wide risk approach. This approach seeks to integrate the business continuity risk management activities with the existing risk management activities performed at an organizational level including the cyber domain.

On the other hand, when identifying the cyber risks, business continuity risks must be considered from:

- ▶ An operational perspective such as the safety, wellbeing, and availability of the personnel responsible for managing and performing day-to-day cyber activities. The continuity of cybersecurity management and monitoring activities, such as disruptions, could cause lack of visibility to the organization's threat surface and possible breaches.
- ▶ A cascading and correlated effect perspective. A good example would be a power outage seen as a simple non-intentional disruption, which could in fact be an intentional disruption as part of an advanced cyber-attack to overcome the physical security controls in place, such as surveillance cameras.

The assessment of an organization's risk profile requires identification of risk treatment plans and this serves as the core building

block in identifying appropriate resilience strategies and solutions. Domain 17 of ISO 27001:2013 has provided a good guidance for organizations who want to adopt continuity in their cybersecurity capabilities. Such strategies and solutions must cover several fundamental pillars which include people, technology, site, vital records, operational technologies and operational requirements. Cyber risk profile should be included as an integral part of such activities.

Another area of intersection between cyber resilience and business continuity is response and recovery plans. This plan should define action steps in the resume operation within the defined RTO.

Furthermore, it is of utmost importance that a defined plan is evaluated to ensure validity and effectiveness against adverse situations. Organizations can conduct cybersecurity simulation exercises not only to test the plan but to see how key stakeholders are aware of their responsibilities during disruptions or crisis and build experience.

Finally, adapting post a disruption, whether cyber or non-cyber, is important and could create a new normal for the organization. For example, most organizations implemented remote- working capability as a strategy to address continuity risks during the COVID-19 pandemic. This was seen by many organizations as a more cost-effective solution compared to utilizing a work area recovery (WAR) site or even a primary location which lead to the evolution of new operating models. Since, virtual working is the new normal and this necessitates the implementation of robust cybersecurity controls to ensure resilience.

In the end, resilience is about having the organizational discipline and agility to develop and constantly enhance its capabilities to ensure that key services, including cybersecurity, are delivered continuously. Organizations should foster situational awareness and collaboration that embed resilience in the culture.

Section 7

Conclusion



New technologies are accelerating the pace of digital change and the broad-scale use of automation, data analytics and the cloud. The government and public sector organizations are increasingly concerned about their resilience capabilities and are looking to provide a safer, more secure, yet affordable approach to securing their systems and data. A breach from a supplier or third party could be one of the greatest risks they face.

With a focus on information, communication, and technology (ICT) and other department services and products, the government and public sector organizations require a better understanding of the potential risk that a supplier could pose to the organization, the critical assets that might be targeted, and the cyber risks that may exist across people, processes, and technologies. By understanding the potential risk, leadership or senior management will be able to make risk-informed decisions regarding potential mitigation actions.

If we accept that some form of cyber attack is inevitable, then it becomes even more important for the organization to have systems and strategies in place to reinstate business as usual in the fastest possible way. Organizations must learn from what happened, adapt and reshape the organization to improve cyber resilience, going forward. It is essential for the government and public sector organizations to have a centralized, enterprise-wide cyber breach response program (CBRP) or cyber crisis management plan that can bring together the wide variety of stakeholders, who must collaborate to resolve a breach. The CBRP needs to be led by someone who is experienced with technology, and able to manage the day-to-day operational and tactical response. That leader should also have in-depth legal and compliance experience, as any cyber breach can trigger complex legal and regulatory issues with financial impacts.

When it comes to cybersecurity governance, one of the most important things public sector organizations can do is set the proper tone and align with management on the appropriate risk appetite related to cybersecurity. The senior management of public sector organizations can send that message in part through its own governance and focus on cybersecurity. It is

essential that senior management considers the following questions:


- ▶ How much time are key stakeholders spending on cybersecurity throughout the year?
- ▶ Is cybersecurity on the agenda of meetings once a year or is it part of most meetings?

Senior management are mainly responsible for strategy and risk management, and it is virtually impossible to have those conversations without a thorough discussion of technology and security. Senior management that has the appropriate focus on cybersecurity are the ones that consistently integrate the topic into regular discussions about strategy and risk. They prioritize self-education and seek external advice to enhance the organization's cyber competency. They also have unfiltered discussions with the CISO in executive sessions and consistently send a clear message to management that prioritizing cybersecurity is part of the organization's DNA.

Another critical part of setting the right tone is emphasizing that cyber risk is not just an IT concern but it is an organization-wide issue that cuts across all divisions and functions. Accordingly, management, beyond the security function, needs to be fluent on what controls and processes are protecting its operations, how employees are trained and tested from management down to the front line, and what protocols need to be followed in the event of a cyber incident or breach.

Through an efficient cyber governance and oversight approach, the senior management plays an important role in encouraging functions and divisions to take broader ownership of cyber risk, and it is incumbent on them to understand, if and how the responsibility for cybersecurity is shared across the organization.

Infusing cybersecurity in the overall senior management conversations with all the C-suite executives and division leaders making it evident that cybersecurity is embedded in operations across the organization, and that leaders are accountable for their role in supporting the cybersecurity infrastructure. Giving cybersecurity the same prominence as finance and legal in critical decisions, reinforces the message that it is a critical business issue.



Call to action

Creating a holistic, business-driven approach to combat cyber attacks might feel overwhelming when the organization is already facing disruption on many different fronts. Nevertheless, cybersecurity has to be a core-business priority and it has to be given top priority by modern government and public sector organizations. Here are the top 10 things management needs to consider while implementing cyber resilience plans:

1. Integrate cybersecurity into the talent strategy and create a CISO role that is fit for purpose of the organization. The CISO should have the flexibility to define an organizational structure that considers a broad range of factors and puts resilience at the top of their priority charts.
2. Clearly define the cybersecurity responsibilities of the organization and establish RACI matrices that explain the responsibility, accountability, consulted and informed roles for all stakeholders involved in maintaining cyber resilience during an incident or event.
3. Put cybersecurity at the forefront of a cross-functional business strategy. It must not be viewed as IT's problem and cybersecurity functions should be viewed as an enabler by the supporting business functions. Resilience plans need to be widespread and communicated to all stakeholders.
4. Ensure that cybersecurity is at the heart of digital innovation and aids it, rather than hindering it. Embedding a "Trust by Design" concept is easier said than done. Hence, the need for executive management to provide buy-in into security aspects and requirements while communicating the importance of cyber risk management and cyber resilience across all the business units.
5. Understand how regulation impacts operations, and work with regulators to establish cyber resilience capabilities that address the core requirements. The regulators should be considered as a critical partner,



not only for maintaining compliance, but also to ensure that the critical requirements are implemented in a seamless manner and all challenges are outlined at the initial stages.

6. Risk rate all your key assets and determine a protection approach for each one with a focus on the most critical ones. Identification of the crown jewels is a critical requirement for every organization as this defines the level of protection to be applied to assets. Protecting each and every asset within an organization with the same degree of controls is not a feasible approach, hence, a more pragmatic approach that considers risk as a crucial component is necessary.
7. Develop a dynamic and nimble cybersecurity risk management model to enable the organization to scale if there is an escalation of external risk or a decision to change the organizational risk appetite.
8. Integrate compliance into the cybersecurity strategy, so that any money invested in compliance will return value by providing proper defense for the organization.
9. Strengthen resilience by having a clear crisis action and communication plan for when things do go wrong, crisis and continuity management can be thought through and practiced at all levels of the organization.
10. Collaborate with peers to seek out more intra-sector solutions. Today's cyber risks threaten the entire governmental ecosystem, and the failure of one key player could damage the reputation of the entire industry.

In conclusion, it is no longer sufficient to consider cyber resilience as an afterthought; a next-generation approach to governance, risk, and compliance should be embedded in the government and public sector organizations' immunity system as a shield in a world of uncertainty and rising cyber threats.

References

1. https://www.ey.com/en_vn/ey-global-information-security-survey-2021
2. Tom, Burt, 4 November 2022. "Nation-state cyberattacks become more brazen as authoritarian leaders ramp up aggression," Microsoft Corporate Vice President, Customer Security & Trust (Burt, 2022).
3. Link to reference: <https://www.crowdstrike.com/resources/reports/global-threat-report/>
Direct link to report: <https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2022GTR.pdf>
4. <https://thehackernews.com/2022/12/chinese-hackers-target-middle-east.html>
5. <https://www.securitymagazine.com/articles/97549-winnti-apt-group-stole-trillions-in-intellectual-property>
6. <https://blogs.microsoft.com/on-the-issues/2022/11/04/microsoft-digital-defense-report-2022-ukraine/>
7. <https://www.nist.gov/news-events/news/2022/05/nist-updates-cybersecurity-guidance-supply-chain-risk-management>
8. <https://www.federalregister.gov/documents/2019/11/27/2019-25554/securing-the-information-and-communications-technology-and-services-supply-chain>
9. <https://www.interpol.int/News-and-Events/News/2021/Immediate-action-required-to-avoid-Ransomware-pandemic-INTERPOL>
10. <https://blogs.microsoft.com/on-the-issues/2022/11/04/microsoft-digital-defense-report-2022-ukraine/>
11. https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf, 21 September 2021
12. <https://www.fincen.gov/news/news-releases/fincen-provides-financial-institutions-red-flags-potential-russian-sanctions>, 07 March 2022
13. <https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-remarks-annual-munich-cyber-security>
14. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_5634
15. <https://www.congress.gov/bill/117th-congress/senate-bill/965>
16. <https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/code-of-practice>
17. <https://www.cisa.gov/circia>
18. <https://www.sec.gov/news/press-release/2022-39>
19. <https://www.congress.gov/bill/117th-congress/senate-bill/2629/text>





Contributors

Samer M Omar

Senior Principal, Technology Consulting
Ernst & Young for Systems and Programming WLL (Branch)
samer.m.omar1@sa.ey.com

Salam Shouman

Director, Technology Consulting
Ernst & Young Jordan
salam.shouman@jo.ey.com

Fadi Mousa

Director, Technology Consulting
Ernst & Young for Systems and Programming WLL (Branch)
fadi.mousa1@sa.ey.com

Siddhesh Mudbhatkal

Manager, Technology Consulting
Ernst & Young Ltd, Mauritius
siddhesh.mudbhatkal@mu.ey.com

Eyad A Haddad

Manager, Technology Consulting
Ernst & Young for Systems and Programming WLL (Branch)
eyad.haddad1@sa.ey.com

Edmark M Billones

Manager, Technology Consulting
EY consulting LLC (Abu Dhabi branch)
edmark.m.billones@ae.ey.com

Shatha Almutairi

Manager, Technology Consulting
Ernst & Young for Systems and Programming WLL (Branch)
shatha.almutairi@sa.ey.com

Musab Abutaha

Senior Consultant, Technology Consulting
Ernst & Young Jordan
musab.abutaha@jo.ey.com

Yasmeen H Abdullah

Senior Consultant, Technology Consulting
Ernst & Young Jordan
yasmeen.abdullah@jo.ey.com

Shawkat A Al Nabulsi

Senior Consultant, Technology Consulting
Ernst & Young Jordan
shawkat.alnabulsi@jo.ey.com

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

The MENA practice of EY has been operating in the region since 1923. For over 98 years, we have grown to over 7,500 people united across 26 offices and 15 countries, sharing the same values and an unwavering commitment to quality. As an organization, we continue to develop outstanding leaders who deliver exceptional services to our clients and who contribute to our communities. We are proud of our accomplishments over the years, reaffirming our position as the largest and most established professional services organization in the region.

© 2023 EYGM Limited.

All Rights Reserved.

EYG no. 001913-23GbI

ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com