القمة العالمية للحكومات
WORLD GOVERNMENT SUMMIT

In Collaboration with

EY
Building a better working world

CYBER RESILIENCE IN THE DIGITAL AGE

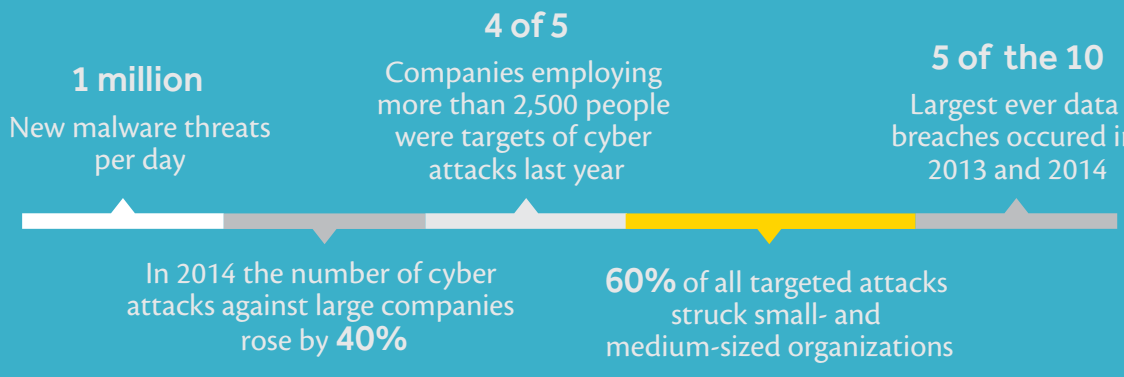
INDEX

EXECUTIVE SUMMARY

The rapid digitization of the global economy is leading to a dramatic increase in the number of cyber security incidents. In 2015, and around the world, four out of five organziations employing over 2,500 people where targets of cyber attacks and the estimated financial impact of all such events exceeded $440b.

As people grow more reliant on technology for their everyday activities, they are also looking to their governments to provide for a and robust environment. One where organizations can leverage technology and information storage with a sense of security and comfort in storing and exchanging information. Citizens and visitors alike demand strong protection against all sorts of threats, including threats to their digital world. Concurrently, governments are relying on digital innovations to help serve stakeholders, contain costs and provide a competitive edge in the global market. These trends point to a growing imperative for cyber threat "resilience" in the digital age. Governments, organizations in the private and public sectors and individuals must all play their part in building an ecosystem that is resilient to cyber threats.

Cyber attacks and their impact



Source: Internet Security Threat Report, Symantec

Source: The Ponemon Institute
2015 Cost of Data Breach Study: Global Analysis

What does resilience mean in the content of a Digital Landscape? **We define resilience to be the organizational capability to sense, resist and react to disruptive cyber events, and to recover from them in a timely fashion.** By definition, a digital economy is borderless and ever changing. Therefore, rather than build a seemingly impregnable fortress around a country's digital presence, the objective, instead, is to create the capability to anticipate threats, to absorb the impacts of such threats and to react in a rapid and flexible way to ensure that a nation's key systems and processes continue operating. With the use of smart technologies, such as artificial intelligence and machine learning, organizations systems will be able to recover from the attack and build stronger defenses against future such events.

Governments have a crucial role to play in helping build a national cyber resilient culture, one where individuals and organizations are educated. Only governments can create the required effective foundation that organizations, citizens and visitors can rely on, leverage and trust.

Cyber threats are real and can be as devastating as risks of terror and catastrophic events. Governments can establish a framework in which organizations collaborate to enhance their resilience against cyber attack, because the former are able to see the bigger picture. When an organization comes under a cyber attack, the target is likely to perceive it as an isolated event, as it attempts to respond. Governments are able to put the event into a national context and to respond on a national or international scale, if need be.

If governments are successful in this endeavor, their residents will feel more secure about the inviolability of their data. Innovation and investment in technology will thrive within an environment nurtured by smart, strong governments.

This reports looks to establish the following themes:

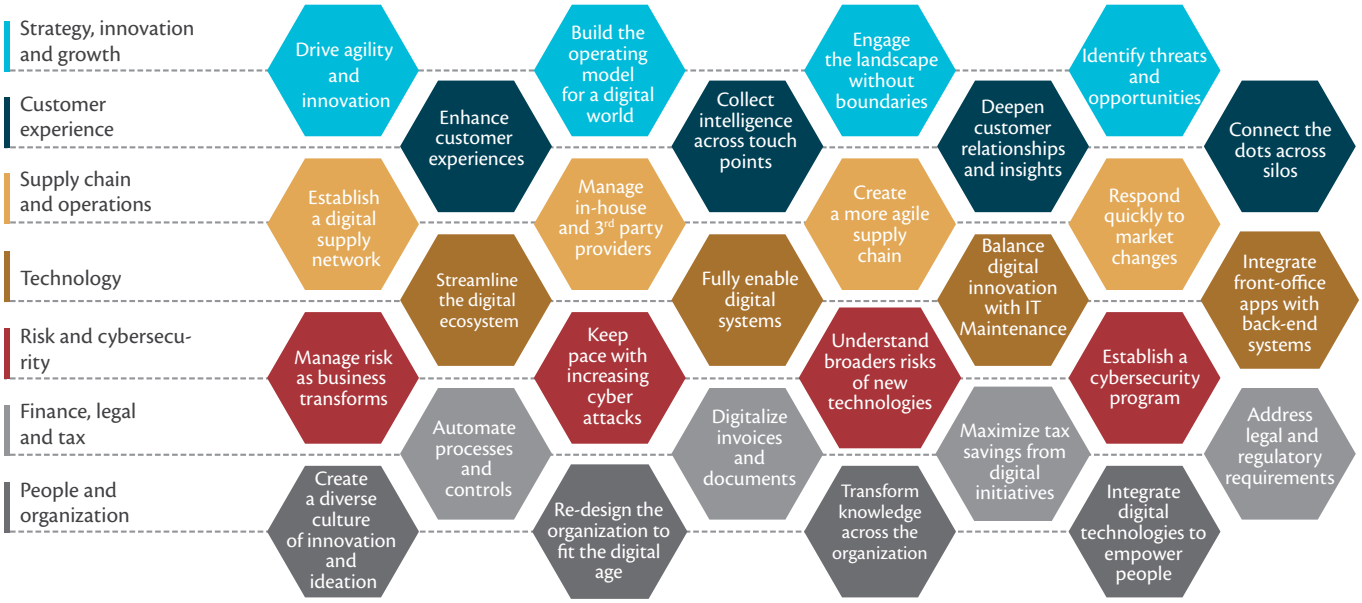
- Governments play a crucial role in creating a strategy for cyber resilience and then implementing it.
- Governments require a clear visibility over the threat landscape, both in its current form, and the changing dynamics. This will serve to protect what is most vital and vulnerable to cyber threats.
- Traditional cyber defense strategies are no longer effective; the emerging threat vectors and speed of change, amplified by a digital revolution, cannot be addressed by traditional methods.

> "We stand on the brink of a technological revolution that will fundamentally alter the way we live, work, and relate to one another. In its scale, scope, and complexity, the transformation will be unlike anything humankind has experienced before"
>
> (World Economic Forum, 2016)

THE ROLE OF GOVERNMENT IN CYBER RESILIENCE STRATEGY

Governments play an important part in shaping the digital future of their countries. There must be a vision of the digital needs of society and of the ecosystem that will achieve it. If the digital economy is to flourish, governments have to create a fertile environment in which innovation and entrepreneurship thrive. Rapid advances in digital technology enable governments to provide services more efficiently and improve users' experience. Governments need to build a sustainable ecosystem that will withstand shocks, both natural and man-made.

Digital ecosystem considerations



Leveraging the opportunities of digital technology requires the government to develop an education policy based on estimates of the digital skills that will be needed by the nation and a plan for how to meet those needs, by educating students who will enter the workforce and retraining those already working who need to adapt to a new culture of cyber awareness.

As more data is collected, stored and exchanged electronically, not only are there new commercial opportunities for the private sector, but also new responsibilities placed on government, such as ensuring data privacy and cybersecurity. Digital transformation requires governments to create the right legal and regulatory framework within which companies and individuals can lawfully operate.

Four distinct digital themes reflecting the holistic set of challenges and opportunities created by digitization

SMART INDUSTRIES AND GOVERNMENTS

- How can digitization help industries and governments redefine service delivery and make citizens happier while reducing cost to serve?
- How can digitization improve industries and government efficiencies?

BUILDING A DIGITAL ECONOMY & SOCIETY

- How can governments build an inclusive digital economy and society?
- How can digitization help the education sector build the right skills & capabilities required in an ever evolving digital environment?

CUSTOMER ENGAGEMENT

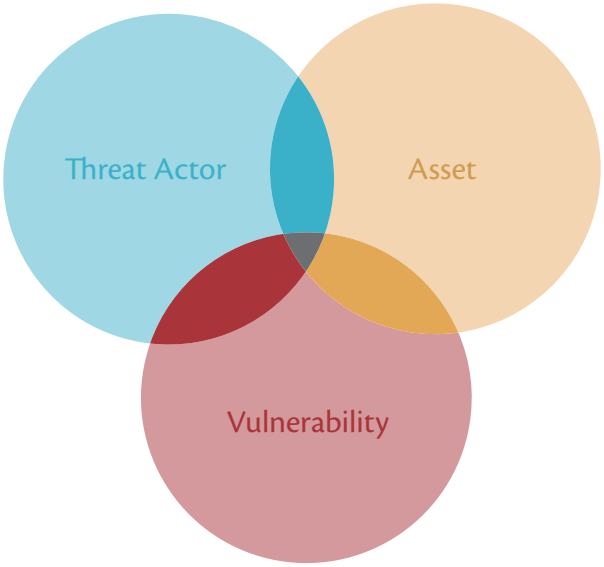
- How does digitization help sectors better relate to customers and become a "trusted brand"?
- How can digitization help industries and governments improve citizens' participation in building an always better economy & society

SMART CITIES

- How can digitization address the issues related to urbanization?
- How can digitization help governments maximize the potential of transportation infrastructure to increase both passenger satisfaction and efficiency?

The rapidly evolving digital landscape opens up a significant new role for a government's chief technology officer (or equivalent). Digital advances are reshaping the function of the chief technology officer to take on a more strategic role than before, as an agent of change and a leader of digital transformation, mindful of the far-reaching effects this will have on the economy. The chief technology officer of the government needs to be an important advocate for a resilient ecosystem and to play a significant role in shaping a policy in creating one.

Attributes of a cyber incident



DIGITIZATION ALTERS CYBER THREAT LANDSCAPE

Digital transformation is opening new investment opportunities every day. It is also creating an array of new cyber threats. Digital innovations expand the target area for a cyber attack, as hackers and other threat actors find new ways to penetrate information networks to steal and disrupt. Governments have to be aware of the emerging areas of vulnerability and to devise a strong strategy to manage cyber risk and help create sustainable conditions for continued digitization.

Attributes of a cyber attack

A successful strategy must be based on a clear understanding of the three elements in a cyber attack (see illustration p6). Governments will need to assess and monitor all three continuously in order to build cyber resilience.

Assets

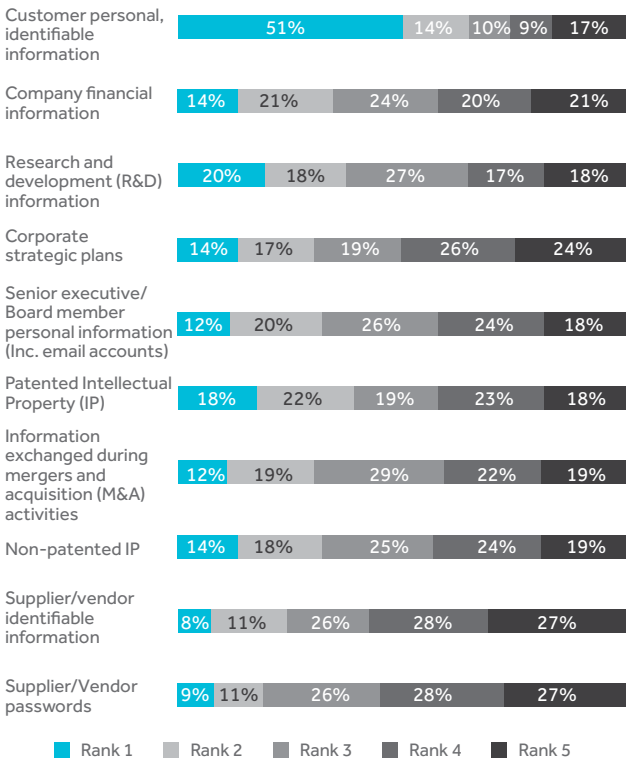
When cyber attacks occur, threat actors can target a nation's assets. These assets can take various forms, including data (such as credit card information, personal health records, privileged user credentials, and intellectual property), money, and systems that control a country's critical national infrastructure (such as telecommunications networks, the power grid, and transport systems). Governments should compile a national asset database that will evolve in step with the digitization of the economy and be flexible enough to align with the cyber resilience strategy. Identifying a country's critical digital assets is an important step in understanding the risks that have to be managed.

Vulnerability

Most governments and organizations approach the protection of vulnerable IT systems by focusing on the various patching cycles, alerts, and automated mechanisms to secure sensitive networks.

EY Global Information Security Survey (GISS) Report 2015

> "What information in your organization do you consider is the most valuable to cyber criminals?"



Threat actors, however, are relying more on social engineering tactics to search for weaknesses. This means they are using tools such as phishing, ransomware, and identity theft to gain access to the crown jewels of a company or a government department. A national campaign sponsored by the government to raise awareness of cyber vulnerabilities would educate people about the risks. The sharing of technical information about cyber security among security practitioners would increase confidence.

Critical national infrastructure, such as the power grid, deserves particularly close attention due to the fact that Operational Technology (OT) and Information Technology (IT) are not linked physically or virtually. Since this infrastructure needs to be operating continuously, updates of OT systems are highly problematic. Exhaustive testing of updates can take up to 18 months, leaving systems vulnerable to cyber attack. Governments need to work closely with specialized OT vendors to optimize the update process.

The Internet of Things deserves special mention, because most connected devices are mass-produced with little regard for cyber security. A lot of devices are being installed that are connected to the Internet, creating a wide-ranging exposure to attack. To ensure that future devices are more secure, some governments have recently published standards for the manufacture of IoT devices in the wake of denial-of-service attacks channeled through such gadgets.

Sidebar: Emerging Standards and approaches to Cyber Resilience

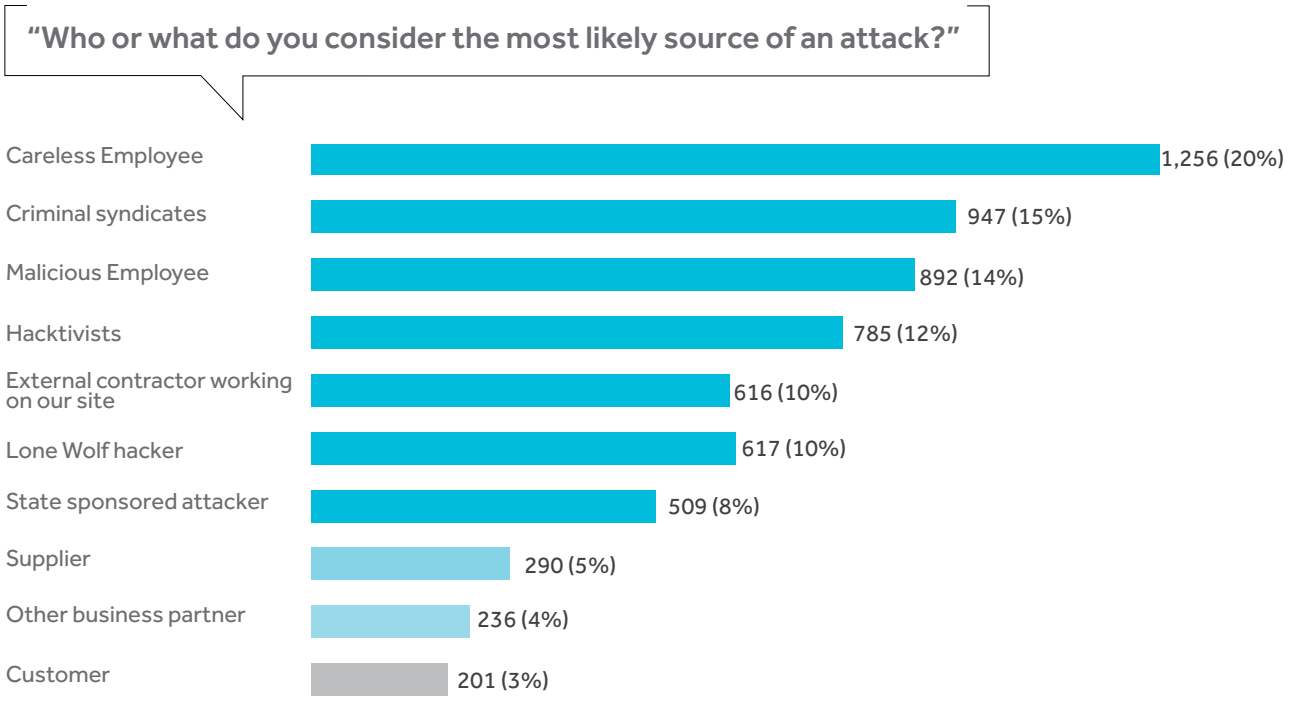
The cyber industry has responded in a number of ways to address the issue of resilience. The International Standards Organization has issued a Draft on ISO 23316 covering the principles and guidelines for organizational resilience. The U.S. National Institute of Standards and Technology has published a report, 800-53, which addresses the resilience of critical national infrastructure. And Carnegie Mellon University has worked with the Software Engineering Institute to develop the Resilience Management Model, which was updated in 2016 (v1.2). Similarly, a number of national and regional entities have developed, and are promoting, various standards and guidance documents on cyber resilience, including the U.S. Department of Homeland Security and the European Union Agency for Network and Information Security.

Threat actors

Governments and the private sector have tended to focus on assets and vulnerability, but it is also vital to make an assessment of threat actors, both actual and potential. After all, an army would not go into battle without an understanding of its opponent. Once humans are added to the mix, governments need to understand the threat actor's motives, intentions, affiliations, tactics, techniques and procedures. These will change over time and in response to alterations in governments' cyber defenses.

Unlike private organizations, governments have the ability to monitor the ecosystem, if need be, by enacting enabling legislation. They have to be mindful of privacy concerns and the risk that too intrusive an approach might deter innovation and investment. They can also monitor the activities of the threat actors themselves, looking for pre-cursors to an attack and changes in a threat actors' tactics, techniques or procedures. The challenge, then, is to disseminate the information about threat actors without alerting the hackers or disclosing their sources. Organizations have to play their part as well. A vigilant government does not obviate the need for organizations to monitor their own environment continuously.

EY GISS Report 2016:



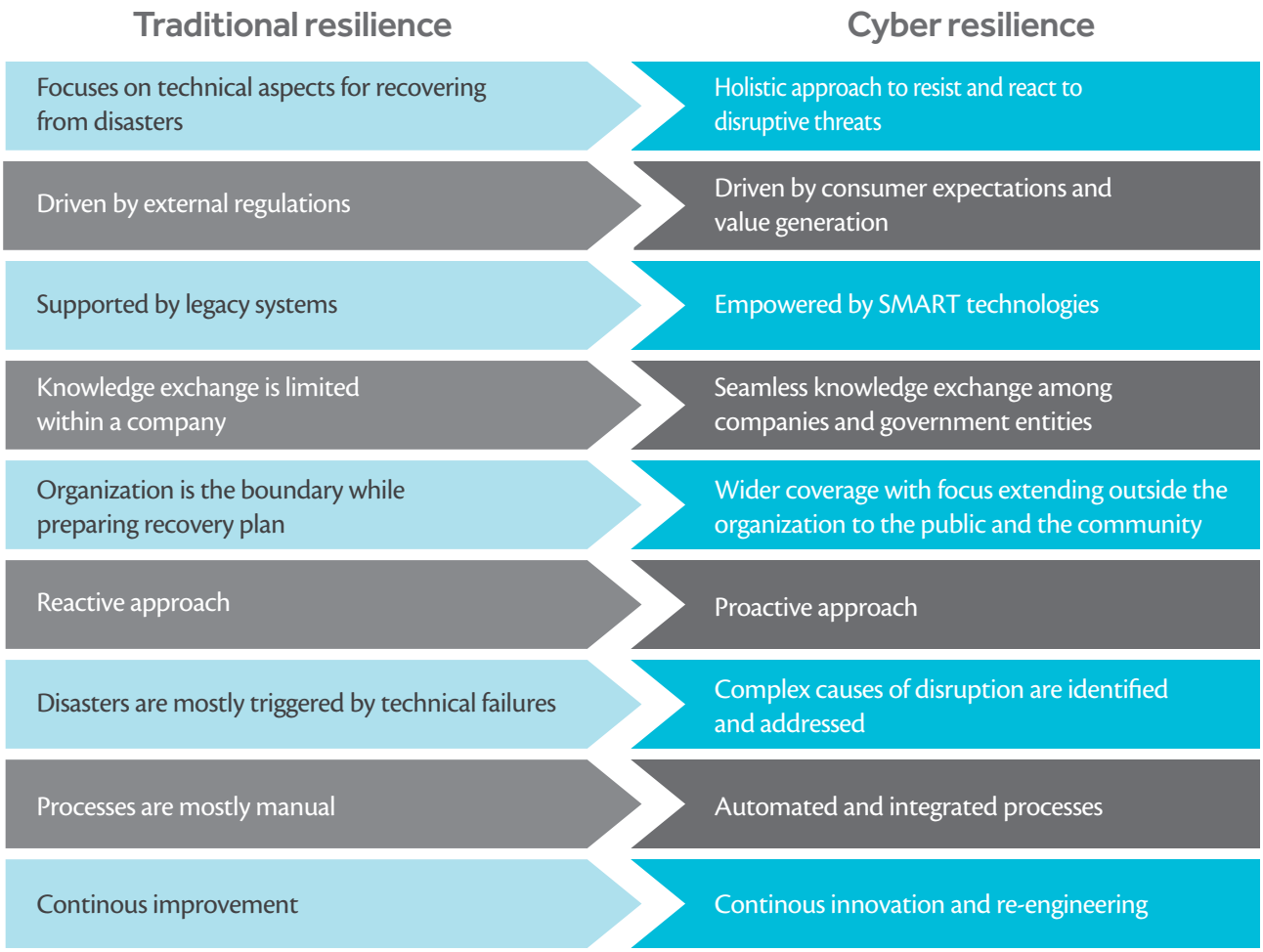
Governments have the means to take counter measures against threat actors, but if these are contemplated, officials should consider setting up communication channels and drafting a memorandum of understanding among governments and organizations to share information before taking counter measures. Governments will also have to update the legal framework with which they would prosecute threat actors. This will include extradition procedures, with the actual punishment in conformity with international legal standards. Government policy will also have to take into account the actions of private organizations, such as companies, and whether they may have failed to comply with relevant regulations. If the policy is too draconian, this may inhibit the commercial development of digital technology.

TRADITIONAL CYBER DEFENSES ARE OBSOLETE

In the recent past, critically important information was stored in-house in stand-alone internal databases and networks, far from prying eyes. Organizations protected the data within the perimeter behind a firewall. As systems became linked with external networks, organizations adopted a "defense-in-depth" security model, so that if the perimeter was breached, there were additional layers of security to protect critical information from falling into the wrong hands.

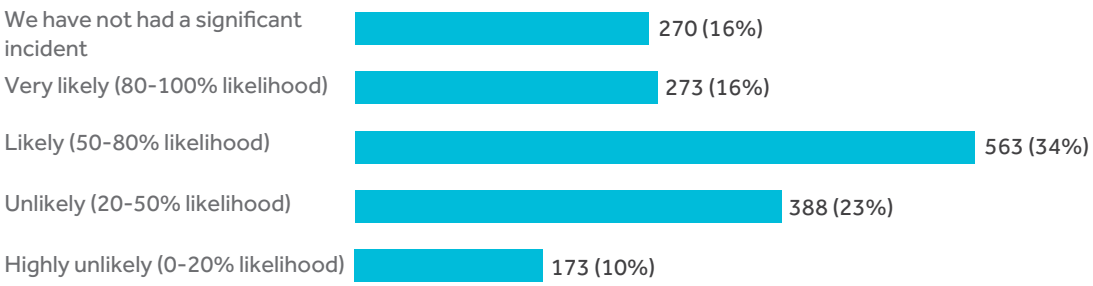
Firewalls continued to be used, along with new methods, such as data loss protection, to track and protect information as it moves across networks. But these measures are no longer sufficient protection against cyber attack. Organizations are beginning to understand that traditional device- and technology-centric security measures such as firewalls fail to provide security in the cyber ecosystem. New, integrated breach-detection programs need to be constituted.

In EY's annual Global Information Security Survey for 2017, of 1,735 C-suite leaders and Information Security and IT executives, we found that the majority of cyber security professionals have not yet adopted more sophisticated breach-detection programs. Similarly, advanced detection technologies, malware detection and so on have still not been adopted widely.



EY GISS Report 2016

"In your opinion, what is the likelihood of your organization being able to detect a sophisticated cyber attack?"



Traditional models of operational continuity are unable to adequately protect digitally transformed governments for a variety of reasons:

- They are not suited to recover information that originates from, and is linked across, multiple sources and reaches multiple users. They may fail to identify the critical data assets or be able to locate them or track how they flow across the digital systems
- They lack the ability to anticipate a cyber security breach
- They are not able to adapt to complex regulations which vary by location
- They unable to cope with the integration of multiple stakeholders and complex supply chains

Rapidly evolving cyber threats require a mechanism to sense emerging risks and resist them, and this can only be achieved through a cyber resilience strategy.

CYBER RESILIENCE IN THE DIGITAL AGE

We define resilience as the organizational capability to sense, resist and react to disruptive events, adapting and reshaping operations in environments where there are both foreseeable and unforeseeable risks. The latter emerge at a time when the pace of technological change is so rapid that it becomes more challenging to predict many of the risks arising in the digital space. Cyber resilience encompasses both cyber security and organizational resilience, and aims to defend against potential cyber attacks and ensure survival following an attack.

Evolution of resilience models

1 Data and Information Backup

As awareness of the potential business disruption that would follow a related disaster, the development of backups took place to come back to best possible state when any disruptive event takes place.

2 Disaster recovery (DR)

The goal of DR was to protect technical systems rather than providing any organizational or business side protection.

3 Crisis Management (CM)

Moving further into the late 1980s and into 1990s the area expanded to take into account external factors by taking its cues more from crisis management. The CM approach differs from the initial, internal and preventative focused and deals with both prevention and recovery.

4 Business Continuity Management (BCM)

Values based mind-set was developed and moved toward BCM where the scope is broadened to include the whole organization, including the employees.

5 Enterprise Resilience

Taking a holistic view of the elements, governance, leadership and capabilities necessary to support high impact, low probability risks with an optimal cost-benefit outcome having four stages as:
- Sense & Anticipate
- Prepare & Plan
- Respond & Recover
- Learn & Adapt, thereby addressing shortcomings of traditional resilience model

National resilience and Sector resilience

Promotion of personal and enterprise resilience together contributes toward the national resilience.

National and Sector resilience can be achieved by deepening government award the national resilience. whole organization,place ith communities and individuals. Cyber resilience is a critical component in the evolution of digital governments into the National and Sector resilience model.

The key question is how organizations can achieve sustainable, resilient operations in the cyber ecosystem. They must decide if, and how, they will achieve their business outcomes within an ecosystem in which individual survival in the digital world cannot be assumed.

An effective cyber resilience strategy will have significant cost implications for the government and the private sector. Organizations may be reluctant to comply with more regulations, but there is agreement among many organizations that more government oversight is needed, especially if a more secure cyber ecosystem lowers costs in the long run. The government can help by ensuring there is a strongly competitive environment for providers of cyber security and by designing education policies to promote the supply of cyber specialists.

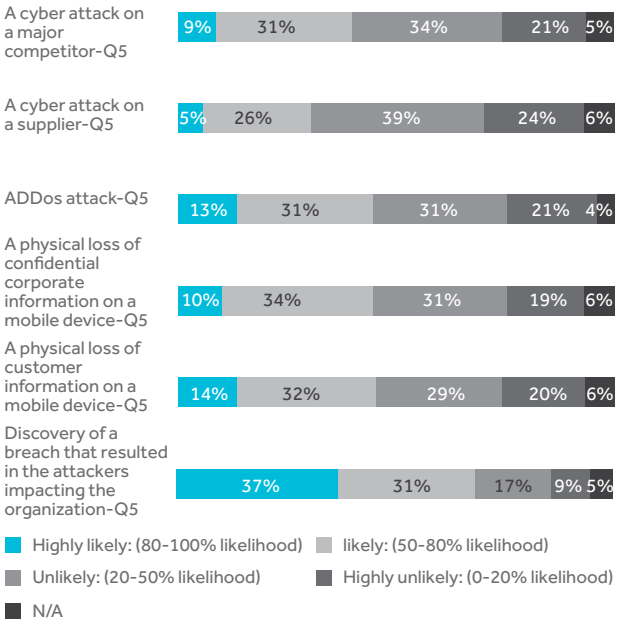
Assuming cyber initiatives are adequately funded, governments can focus on developing a robust cyber resilience strategy. This means the development of the ability to sense and resist as part of pre-disruption mechanisms that enable organizations to detect emerging risks. To address cyber attacks and contribute to cyber resilience, governments need to provide the framework and to facilitate a secure cyber ecosystem to include both core infrastructure and support for industries' resilience. This may include a national framework for cyber risk management, national vulnerability programs, industry collaboration groups, threat intelligence sharing mechanisms.

Some organizations have improved their 'sense' capabilities significantly in recent years. They are using cyber threat intelligence to predict emerging threats, installing continuous monitoring mechanisms (such as security operating centers), identifying and managing vulnerabilities and installing active defenses.

According to EY's GISS survey for 2016, organizations appear to have become more confident they can predict and detect a sophisticated cyber attack: 50% of survey respondents thought it was likely they would be able to do so, the highest level of confidence we have seen since 2013. Despite this, it seems clear that many organizations have not established basic structures and procedures to sense and resist a cyber attack. Forty-four percent say they do not have a security operating center, while 64% say they do not have a formal threat-intelligence program. In addition, 55% do not have the ability to identify their vulnerabilities.

There is further evidence of a lack of preparation for cyber resilience. In the same survey, 62% of organizations say they would not increase their cybersecurity spending after experiencing a breach which did not appear to do any harm. The problem is that cyber criminals often make 'test attacks' or lie dormant after a breach, or they use a breach as a diversionary tactic. Organizations must assume that harm has been done every time there is an attack, and if they have not found it, they should consider the possibility that the damage has not yet emerged.

"How likely is it that any of the following events would encourage your organization to increase your information security budget in the coming 12 months?"



The role of leadership

Executive leadership and support is critical for effective cyber resilience. Unlike the 'sense' and traditional 'resist' activities which can be seen as the domain of the Chief Information Security Officer or the equivalent, in the 'react' phase, cyber resilience requires other senior executives to actively take part and lead. Since 2013, EY's annual GISS survey, have consistently shown that almost a third of responders say there is a lack of executive awareness and support for cybersecurity strategy. This suggests that organizations are not doing enough to ensure that senior executives are taking the lead in building cyber resilience.

Securing the cyber ecosystem

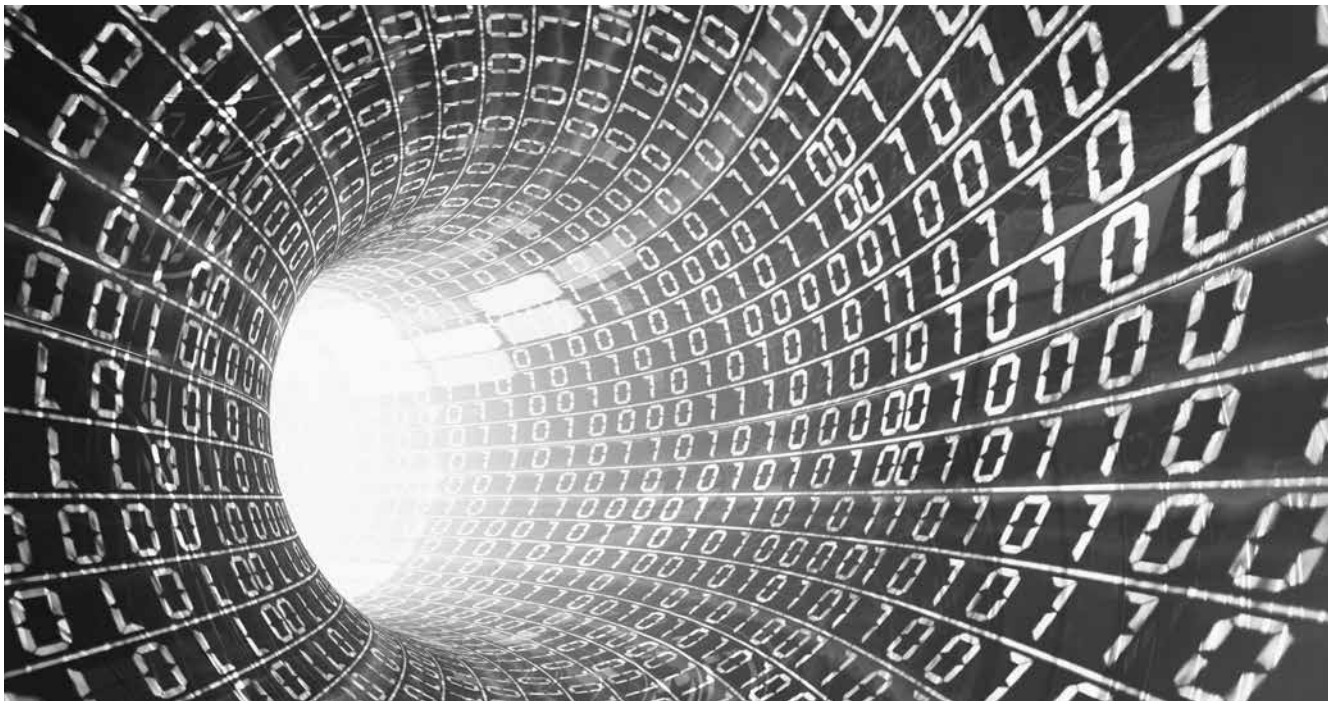
In today's environment, cyber events that occur in the organization's ecosystem of suppliers, customers, and government agencies, can affect the organization itself. This is a major area of risk that are often overlooked, as EY's GISS survey shows. Sixty-eight percent of respondents say they would not increase their information security spending even if a supplier was attacked. Yet such a breach may provide the attacker with a route to penetrate the organization itself. Similarly, 58% would not increase their spending on cyber security if a major competitor was attacked. Yet cybercriminals like to attack organizations that are similar to one another, using techniques they have learnt from previous events.

The impact of Internet of Things

The emergence of the Internet of Things and the rapid growth in the number of connected devices are going to challenge the sensing capabilities of organizations. It will be difficult to identify and track suspicious data traffic in the network and identify who has access to data. It will become harder to identify what part of the environment is going to affect the organization and what part is not.

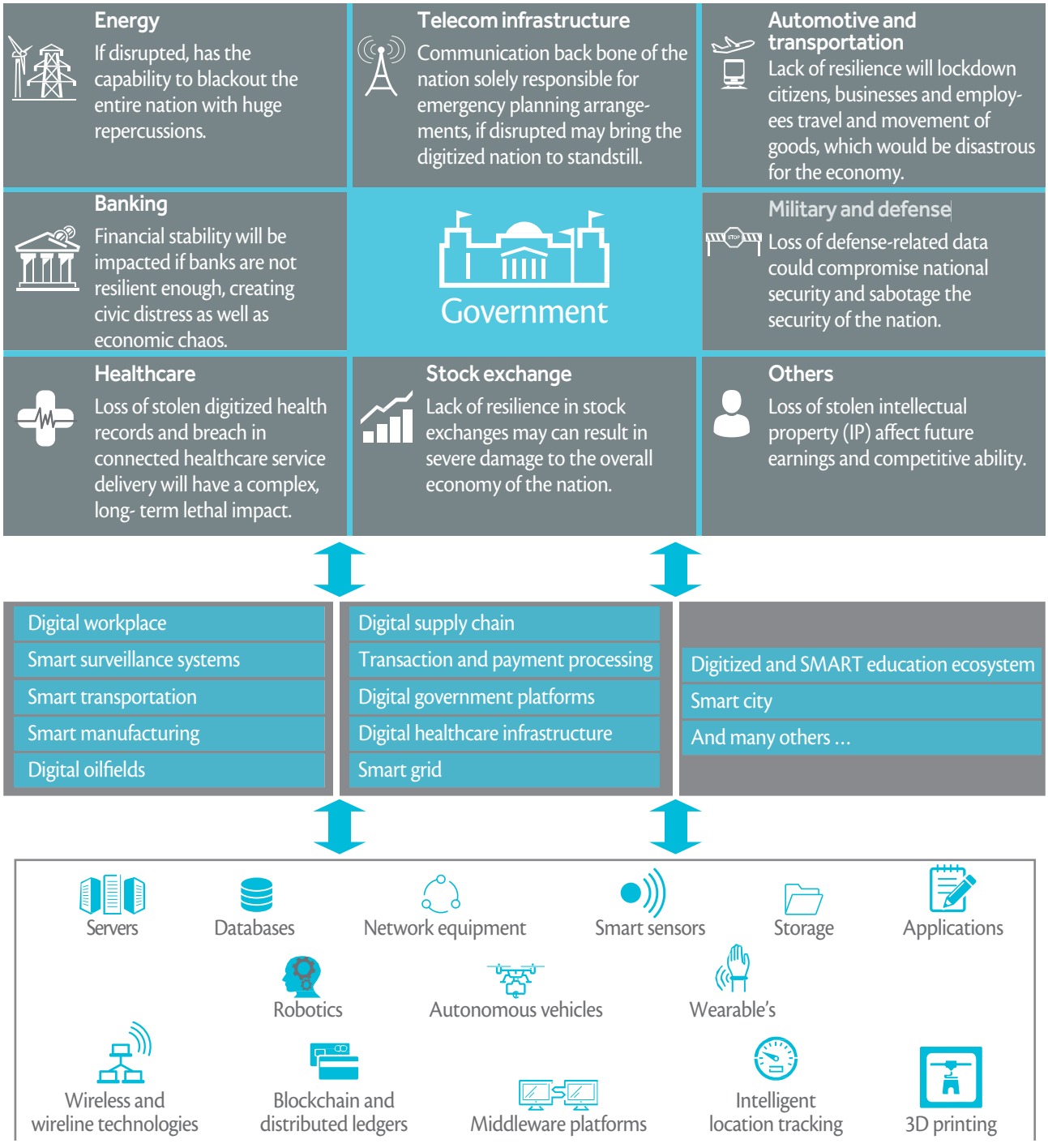
In the future, devices will be able to work together in near real time to anticipate and prevent cyber attacks, limit the spread of attacks across participating devices, minimize the consequences of attacks, and recover to a trusted state. Security capabilities will have to be built into cyber devices to enable preventive and defensive courses of action to be coordinated within and among a range of devices.

In such a cyber ecosystem, system managers will rely on computer applications that automatically detect and report known security vulnerabilities in network nodes. In some cases, system managers will configure their systems to automatically remediate detected security deficiencies.



BUILDING A CYBER RESILIENT ECOSYSTEM

As cyber threats evolve, governments will find that traditional information security approaches will prove increasingly inadequate to the task of protecting organizations. Individual organizations need to establish a base-level of data security, but they also need to recognize that they cannot achieve complete security by themselves. They need to work together with trusted partners to protect their ecosystem. A resilient cyber ecosystem is one in which the organizations operating in it have confidence in the security of their systems and data.



To do this, organizations must look outside their own perimeter to assess the impact of a cyber attack on their business partners, suppliers, vendors and other stakeholders. Good cyber citizens are those that collaborate with third parties to develop healthy, resilient cyber ecosystems, by interacting and sharing data with them. This collaboration requires a strong commitment to cyber resilience and to reinforcing good behavior in the areas of resilience leadership, partnership and change-readiness. Most of all, it requires the unwavering commitment of individuals and leaders to achieve these goals.

Governments and major organizations are leading the way in establishing the policy and practice frameworks to develop resilient cyber ecosystems. But these are early days. The idea of collaborating with partners is gaining momentum slowly, due to the complexity of the undertaking. In the meantime, organizations should ensure they develop their information security capabilities so as to address their own risk environment.

Key characteristics of cyber-resilient organizations

Understand the entire organization: Cyber resilience demands a response that addresses the organization from one end to the other; half measures will not work. It begins with a deep understanding of the operational landscape, to know which workflows must be preserved so the organization can continue to operate in the event of a cyber attack, while safeguarding people and key assets.

Understand the cyber ecosystem: Map and assess the organization's external relationships throughout the cyber ecosystem, identifying the risks and where they exist. Perform a risk assessment of the organization's role in the cyber ecosystem, identifying factors that affect the extent of the organization's control over its ecosystem.

Identify which assets are critical: Most organizations over-protect some assets and under-protect others. EY's survey found that more than half the respondents ranked customer personal identifiable information as the information in their organization most valuable to cyber criminals. Only 11% rated patented intellectual property as the most valuable.

Determine the risk factors

Cybersecurity functions can only achieve limited success if they do not have a complete view of the risk and threat landscape. This requires collaboration with other organizations in the ecosystem.

Manage the human element

In the event of a cyber attack, individuals need to be prepared and educated on how to respond and behave. This requires clear communications inside and outside the organization, while leaders set a strong example of how to respond in a crisis.

Create a culture of change readiness

A rapid response to a cyber attack will minimize the possibility of long-term material impacts. Organizations that react quickly have a well-rehearsed crisis-management plan and the ability to marshal resources from every department. In simulation exercises, organizations can test the existing crisis management, current practices and the risk profile to ensure they are fully aligned with the organization's strategy and risk appetite.

Roadmap to build a cyber resilient ecosystem

While governments prepare for a digital future, they must keep pace with rapidly changing technology. This will help them to adopt and secure architecture that is resilient to system failure, enabling interoperability and openness from beginning to end. Early adopters of advanced design and solutions should be encouraged to share lessons learned and adopt common standards. A harmonized approach needs to be adopted for better content and data to be presented through various channels. This would also ensure privacy and security in a vulnerable digital age. A defined service model has to be deployed across departments, ministries and associated members.

Key resilience attributes of digital government

Resilient leadership

- The visionary, executive-led commitment to establishing resilient government
- Non-routine governance styles are consultative but enable rapid, decisive and compassionate decision making during disruptive circumstances

Resilient culture

- Supports a "one-in, all-in" approach embraced across the government and encourages resilient behaviors of collaboration, vigilance, proactivity, and the preparedness to learn from failure and disruption

Resilient networks

- Establishes and strengthens trust-based relationships with third parties (including business partners, citizens and other stakeholders) to maximize the ability to withstand and recover rapidly from disruptive threats

Resilient change-readiness

- The readiness of departments enabled with training, tools and techniques to rapidly detect, respond to and adapt security responses in an ever-changing security context

Governments need to track and assess resilience attributes throughout the executive branch. These attributes will show how flexible organizations are in their ability to predict security threats. Governments and businesses need to manage high-impact, low-probability risks with an optimal outcome in the digital environment. This can only be achieved by taking a holistic view of the elements, governance, leadership and capabilities required to manage these types of risks. Resilience ensures there is a sustainable capability that adapts to changes within the business and external environment.

The construction of a cyber resilient ecosystem comprises the following five elements:

1. Take a holistic approach

Government decision makers at all levels must strive to educate themselves on the topic of cyber threats. Decision makers can no longer assume that the procurement of a particular cyber security technology or program will solve the challenge. The rising threat of cyber attacks and the complexity and viciousness of such threats require a more holistic approach to protection. A cyber resilience strategy must focus on the behavior of all stakeholders, not just security teams.

Government agencies are beginning to develop national frameworks that aim to provide a legal and policy foundation on which to implement a resilient cyber ecosystem. At the organizational level, a key step forward is to commit government agencies to resilient operations within the cyber ecosystem and to transparency. Governance, risk and compliance tools will help to show where there are security vulnerabilities.

2. Leverage resilient networks

By consolidating, correlating and cross-referencing information across systems, governments can establish a baseline of normal behavior in systems and networks. They can integrate this information with intrusion detection and response technology to identify abnormal or malicious activity. They can leverage automation for real-time detection of attacks, enabling them to respond proactively to security threats. Tightly integrated cloud-based cyber intelligence services can detect advanced persistent threats, while employing trained personnel to act as human sensors.

3. Leverage change-readiness

Governments need techniques and tools that help them respond with speed and agility to emerging threats and cyber-attacks. These include the following:

- Decentralized data protection built into, and as close as possible to, the information itself. An example is information rights management solutions, where security controls are built into data files
- Adaptive and decentralized intrusion detection and response tools incorporated in devices and networks
- Whole-of-system resilience built into devices and networks, enabling them to revert to a "trusted state" when they are the target of an advanced attack
- Automated communications between devices and networks, enabling a programmed and collective response to abnormal or malicious behavior
- System-wide cyber-attack sensors providing automated alerts that security operations centers can share with government computer emergency response teams, intelligence organizations and law enforcement

THE VALUE OF CYBER RESILIENCE

The chief benefit of a cyber resilient ecosystem is that, when attacked and compromised, it can recover to an operational state, because there is visibility across the network and the system can respond quickly. In the event of a cyber attack, a government's cyber resilient system can continue to conduct mission-critical processing, while safeguarding the confidentiality, integrity and availability of data. Even if the system were compromised, data processing would continue.

1 Embeds sense of capabilities to cope up in a crisis

Helps to develop holistic solutions for nation-wide efforts to build, test and improve capabilities to cope up with known disruptions

2 Provides opportunity to enhance and optimize

Helps to follow on engaging approach for nation-wide efforts to continuously test, enhance and optimize the resilience mechanism in place

3 Helps identify areas of inefficiency or risk

Develops a 'one-in, all-in' adaptive, change-ready culture across government entities that enables them to identify inefficiencies in their resilience program

4 Provides seamless continuity capabilities

Leverages people, process and technology opportunities to reshape the cyber environment for sustainable future growth after the occurrence of a disruptive

5 Wider resilience coverage

Cyber resilience unifies multiple disciplines, including risk assessment, technology best practices, knowledge management, risk management, and the coordination of the roles of all departments

RECOMMENDATIONS

Through strategic policy initiatives and action, governments will be able to create the foundation for a national digital transformation in a safe and resilient manner. The recommendations below are intended to provide guidance on the overall policy direction. The actions to be taken by each government will depend on the specific circumstances.

Governments should consider drawing a connection between the National Digital Strategy and their own Cyber Security objectives, where there is a clear purpose to help form a Cyber Resilient ecosystem.

A key aspect is the foundation of a digital-capable workforce that not only improves the nation's employment prospects, but also creates a resilient culture in the digital field.

Cyber resilience must take account of key legal and privacy issues at the national and international level. Each government must aim to achieve a healthy balance between too much and too little regulation, both nationally and globally. Due consideration should be given to international frameworks to enable the country to participate in global organizations that are involved in cyber security.

Governments should establish a framework that supports identification of key assets and asset protection measure (similar to how critical national infrastructure assets are identified). This will help the identification and proper allocation of resources in a prioritized fashion were they are most needed.

The government will have to decide what level of cyber monitoring it will provide and to what entities, and then set standards for the monitoring of those assets not covered. Cyber monitoring will provide an ecosystem that makes cyber attacks visible, thus accelerating the reaction and remediation as well as modifying resilience plans where needed.

A framework should be established for organizations to collaborate over threat intelligence and there should be platforms to enable information about threat actors to be shared quickly. This will allow for a more proactive response than merely cyber monitoring and will raise awareness of the need to enacting any resilience plans.

Comprehensive enterprise cybersecurity metrics, analytics capabilities, enterprise encryption, cloud security and privilege-access compliance are necessary. Government organizations should take the lead in evangelizing and adopting these.

Government should also place a greater emphasis on ensuring organizations develop suitable risk strategies, including definition of risk appetite and tolerances, particularly in response to cyber threats. Operational processes need to be secured as much as possible via internal and external control processes, platforms and services in order to ensure the protection of client and company assets and the continuity of high-value services.

CONCLUSION

Governments face an almost insurmountable challenge to provide a secure and resilient ecosystem for their nation. But the difficulties must not deter them. Action needs to be taken as soon as possible, as the risk of cyber-attacks grows, alongside the rapid expansion of each nation's digital footprint.

The foundation for cyber resilience requires governments to reach beyond their traditional boundaries and establish a strong partnership with the private sector, even as they promote a resilient digital culture among their citizens. For each nation, the building of cyber resilience is a complex and multi-disciplinary process whose requirements will vary depending on social, legal, and economic conditions in each country.

This paper has outlined some of the issues governments will face and recommendations for how to build a cyber resilient nation. The aim is to offer a range of tools that can be adapted to the rapid changes in the digital world. It will hopefully arm governments with a strong framework in which to deal with the unforeseen challenges that lay ahead.

REFERENCES

[1]"Technology and Workforce: Comparison between the Information Revolution and the Industrial Revolution" by Mathias Humbert, University of California, Berkeley

EY Thought Leadership papers referenced:

- "EY Global Information Security Survey 2013-2016" or "GISS" are EY's Global Flahship annual surveys, now in its 19th year, covering topics on Cyber Security, and threat horizons, and emerging topics of relevance and concerns. EY's GISS for 2016 was titled Path to Cyber Resilience: Sense, Resist, React.
- "Agents of change: How government CTOs can drive digital transformation" Government & Public Sector Insights
- "Avoiding a lost generation: Young entrepreneurs identify five imperatives for action" Produced for the G20 Young Entrepreneurs Alliance Summit
- "How will the GCC close the skills gap?" An examination of the challenges and opportunities for governments to address the growing skills gap
- "Citizen today: delivering a Digital future" How policymakers worldwide are using technology to strengthen their public services."
- "Imagining the Digital future" How digital themes are transforming companies across industries
- "Is Digital creating a workforce capability crisis?" Emerging new challenges in the workforce
- "The Power of Three for Smarter, ore Resilient cities"
- "Achieving Resilience in the Cyber Ecosystem"
- "Supply Chain Resilience"
- "EY Protects ® Operations Resilience"
- "Citizen Today — Strengthening public services through technology"
- "Robotics process automations in the Finance function of the future"
- "In a future where data is everywhere, who'll keep it out of the wrong hands?"

AUTHORS

Raddad Ayoub

EY Partner
Resilience Leader - EMEIA Advisory Services
Email: Raddad.Ayoub@ae.ey.com

Clinton M Firth

EY North America Payments Leader
EY Partner
MENA Cyber - Advisory Services
Email: Clinton.Firth@ae.ey.com

Mohamed Nayaz

MENA Leader for IT Risk and Business Resilience Services - Advisory Services
Email: Mohamed.Nayaz@om.ey.com

www.worldgovernmentsummit.org