2018

White paper series
Issue 2

MANAGING NATIONAL CYBER RISK

OAS More rights for more people

CREDITS

Luis Almagro

Secretary General of the
Organization of American
States (OAS)

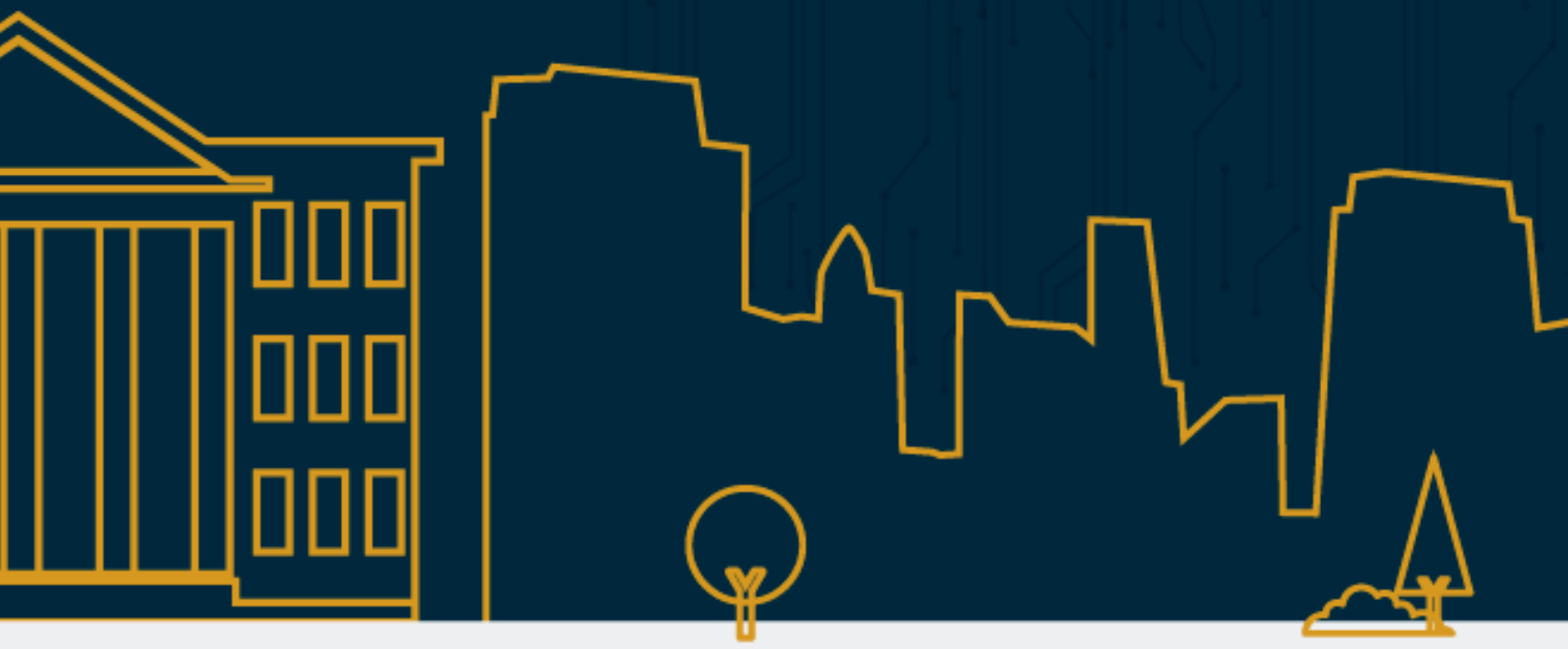
Principal Author

Melissa Hathaway

OAS Technical Team

Claudia Paz y Paz
Alison August Treppel
Belisario Contreras
Kerry-Ann Barrett
Bárbara Marchiori de Assis
Nathalia Foditsch
Gonzalo Garcia-Belenguer

CONTENT



1

INTRODUCTION

Over the last 30 years, governments, companies, and citizens have become critically dependent on the Internet and information communications technologies (ICTs). We assume citizen essential services like power and telecommunications will always operate, and that goods, services, data, and capital will seamlessly cross borders. Yet, many networked systems and infrastructures are vulnerable and being exploited. Organizations of all types are experiencing increased data breaches, criminal activity, service disruption, and property destruction. Collectively our insecurity is growing. More than 100 countries and a rapidly growing number of non-state actors and individuals are capable of causing harm to networked infrastructures of governments and industry. Objectives vary by actor, ranging from political activism; fraud and e-crime; theft of intellectual property (IP); espionage; disruption of service; and destruction of property and assets. Countries and companies are living in a world of *cyber insecurity* — all governments, businesses, and individuals are facing cyber risks and share a level of responsibility in managing them. As recent events underscore, countries and companies must first understand that a disciplined risk management approach must be core to their strategy and digital agenda. The risk of inaction is too big.

Risk is defined in terms of time — when something or someone is exposed to danger, harm, or loss.[1] The condition for risk can change based upon the actions that are taken by at least two actors: the attacker who obtains and uses the capability to cause harm, and the intended target who can take precautions to withstand or thwart the danger intended by the attacker. Every day our digital dependence grows, but the understanding of the risks associated with that dependency remains nascent. Still, cyber risk is increasing because the marketplace for malicious software and tools, illicit services, and sensitive (non-public) data is available, affordable, and being used. For example, malicious software can be purchased for one dollar and distributed denial of services can be launched for less than one thousand dollars. Sophisticated ransomware attacks are available for two-hundred dollars and malicious email spam services are available for approximately four-hundred dollars.[2] Even the most sophisticated weapons from government intelligence services are available for download.[3] Anyone who intends to use and be successful at conducting attacks and causing harm can access these capabilities. As events in 2017 show, governments, companies, and people were harmed by some of the highest profile cyber attacks to date.

In May 2017, ransomware targeted flaws in the Microsoft Windows operating systems and affected millions of computers in 150 countries across every business sector. This global attack — a very simple ransomware named WannaCry — halted manufacturing operations, transportation systems, and telecommunications systems. According to the National Audit Office in the United Kingdom, WannaCry affected at least 81 of the 236 National Health Service trusts — rendering medical equipment inoperable, and significantly affecting public health and safety.[4]

In June 2017, NotPetya — another more destructive malware — was released. NotPetya was launched into the world's networked businesses by way of a software update mechanism for a widely used accounting program (doc.me). Within minutes, the malware infected tens of thousands of Internet connected systems in more than 65 countries, including those belonging to government institutions, banks, energy firms, and other companies. For example, NotPetya's attack on A.P. Moller-Maersk — the world's largest shipping company — encrypted and wiped the company's information technology systems globally. Consequentially, Maersk had to halt operations in most of the company's 76 port terminals around the world, disrupting commerce by sea for weeks. Maersk's financial losses due to NotPetya exceeded $300 million, as it had to rebuild its entire infrastructure, including 4,000 new servers, 45,000 new computers, and 2,500 new applications.[5] It is estimated that NotPetya resulted in billions of dollars of losses due to business disruption and property destruction worldwide.[6] The primary and ancillary losses to the digital economy were significant and the harm (damage) to critical services and infrastructures took months to recover from.

Even more troubling, in August 2017, a Saudi Arabian oil and gas facility was suddenly forced to shut down. It fell victim to Trisis — a well-engineered computer virus designed to sabotage industrial control systems (ICS). Designed to affect the operational components of information technology at industrial sites such as oil and gas and water utilities, this malicious software — or weapon — specifically targets the physical safety mechanisms (emergency shutdown system) of the ICS. While this is only one public example of the successful use of this destructive software, Schneider Electric has warned its customers of critical services and infrastructure owners to ensure their systems are redundant in case one or more systems fail due to future malicious activity.[7]

The malicious cyber activities of 2017 show extraordinary impact in terms of loss and damage, yet the tools used to cause harm were unsophisticated. The number of targeted attacks against power, telecommunication systems, transportation, and financial systems have almost doubled in the last five years, a trend that poses economic and national security risk to everyone. Therefore, there is an urgent need for government and corporate leaders to engage in effective cyber risk management processes and address the digital risks within their strategic planning processes.

2

FRAMEWORKS FOR UNDERSTANDING CYBER RISK

Countries, international organizations, and academic institutions are developing frameworks to help government and corporate leaders diagnose and reduce cyber risk. These frameworks are significantly needed because for the last three decades these same leaders have been persuaded by the features and "benefits" of commercial information technologies, including increased productivity, greater efficiency, lower costs of capital equipment, storage and processing of data, and bottom-line growth — and have deferred investing in the security and resilience of their networked infrastructures and digital businesses. Today's destructive and disruptive cyber activities require these leaders to face the fact that they have inadvertently woven insecurity into the core of society. The losses are accruing; the harm is growing; and the danger is imminent.

Governmental Frameworks

Governments have started to develop frameworks, benchmarks, and broader national strategies to better understand their Internet-infrastructure dependencies and vulnerabilities, and to secure the national networks, infrastructures, and services upon which their digital future and economic wellbeing depend. When it comes to mapping and calling attention to a country's cyber risk, however, the lingering question is: How do you diagnose and reduce a risk that has accrued over 30 years?[8] It is important to start by understanding what a country's 3-5 year strategic plan is and determine what can be done to achieve that goal in the longer term. For example, the Dutch have estimated that by 2020, at least 25 percent of their gross domestic product (GDP) will be comprised by the digital economy (i.e., digital goods and e-services). The Netherlands has affirmed that its future depends on a the ability to secure its digital economy, and is making some of the necessary investments and structural reforms to enable that goal. Other countries, like the United States and Germany, are identifying the top companies that represent more than 2 percent of the country's GDP and working with them to ensure that risk management and resilience are part of their overall business planning processes. Most other countries, however, have taken a broader approach demanding the protection of "critical infrastructures" — those essential assets, systems, and networks perceived to be becoming uniquely vulnerable through increased interconnectedness and reliance on the Internet, and as such, susceptible to equipment failure, human error, weather and other naturally caused outage, and physical and cyber attack.[9] The challenge with this approach is that there is no clear delineation of responsibility between the government and the industry. This makes it difficult to hold someone accountable for inaction. In the meantime, society's insecurity grows with the lack of commitment to reduce risk and increase resilience.

Some governments have determined that it is time to intervene in the marketplace and are using regulations or laws to require certain sectors to identify, assess, and correct deficiencies in their security posture. The sectors being regulated include: electric utilities, financial services,

healthcare, transportation, and telecommunications. Other regulatory measures being adopted by countries involve mandating detailed notification and reporting to the local and/or national authority regarding: a breach that has occurred and the type of data that was exposed or lost; the technique or method used in a breach; and outages or business disruptions (telecommunications) that may have occurred.

The European Union (EU) is imposing these types prescriptive approaches on their critical infrastructures and operators of essential services. In August 2016, the EU adopted a regulation entitled, the *EU Network and Information Security (NIS) Directive*. The regulation established cyber security rules — or sets of security controls — for firms supplying services to society categorized as essential. The services covered under the regulation include energy, transport, banking, finance, water, and health, as well as digital ones, such as online marketplaces (e.g., eBay, Amazon), search engines (e.g., Google), and cloud service providers. EU member states have until May 2018 to transpose the regulation into their national laws. The NIS Directive requires essential services operators in those countries to take appropriate security measures and notify their relevant national authority (e.g. Competent Authority or Computer Security Incident Response Team (CSIRT)) about any serious cyber incident. This approach compels accountability and may reduce cyber risk because it is "forcing" industry to take measures to reduce vulnerabilities and increase resilience.

China has taken a similar approach as Europe and even incorporated elements of the NIS Directive into its new national cyber security law adopted by the Chinese parliament in November 2016 and that became fully effective on 31 December 2017. The law has seven chapters and 79 articles, and is "comprehensive and encompassing" in that it specifies the responsibilities of relevant government agencies, Internet service providers, and Internet users. The law specifies that companies — broadly defined — shall take technical and other necessary measures to ensure the Internet is functioning safely and stably, handle cyber security incidents effectively, prevent cyber criminal activities, and maintain the integrity, secrecy, and usability of Internet data.[10] This regulation compels companies to invest in new safeguards and install a series of controls to guarantee these tenets. It also has an inspection and audit regime to ensure that companies are taking appropriate risk reduction activities and are held accountable if they are found to have insufficient processes in place.

The United States (US) has refrained from taking a regulatory approach in this area, and instead appealed to industry to voluntarily invest in reducing cyber risk to the country's critical infrastructures and services. In February 2013, the President requested the National Institute of Standards and Technology (NIST) to develop a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks. The *Framework for Improving Critical Infrastructure Cybersecurity* was published a year later in February 2014 and contains a set of voluntary standards to help organizations assess, manage, and respond to cyber security risk. The framework directs organizations to evaluate risk under five headings: identify, protect, detect, respond, and recover. According to some industry estimates, the framework is being used by about 30 percent of US organizations (including the government) to help evaluate their risk posture and take a greater responsibility to safeguard their networks and sensitive data from intrusion, damage, or destruction.[11] In addition, the appendix to this document maps various internationally-agreed standards to the NIST Cybersecurity Framework's risk reduction categories. Lessons learned from recent breaches, however, suggest that organizations using the NIST Cybersecurity framework are applying the categories with a view toward compliance rather than evaluating risk on a continuous basis. For example, some organizations evaluated their security and preparedness posture using the NIST Cybersecurity Framework and believed that they had achieved a mature level of cyber security, yet were still significantly harmed by WannaCry and NotPetya.[12]

In September 2017, NIST released revisions to another of its publication on *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*.[13] This framework recommends a process for organizations to identify high-value assets and high-impact systems so that they can better assess operational risk. It also provides a structure to determine and select security and privacy controls and implement and assess control effectiveness. The framework underscores the importance of continuous monitoring of real-time risk vice a point-in-time compliance. It also recognizes that risk management decisions are integral to business functions and mission accomplishment. This framework complements the *Framework for Improving Critical Infrastructure Cybersecurity* and, when taken together, they may provide organizations a more strategic approach to risk management.

International Frameworks

International organizations are voicing their opinions in the cyber risk management discussion as well, and are working to accelerate the adoption of effective cyber security measures using their own frameworks and recommendations. The international risk management debate emerged after the two consecutive phases (2003 and 2005) of the World Summit on the Information Society (WSIS) — a global gathering of the 'ICT for development' community. At that time, at least 170 countries resolved to ensure that everyone would be able to benefit from the opportunities that ICTs can offer by: improving access to information and communication infrastructure and technologies as well as to information and knowledge; increasing confidence and security in the use of ICTs; developing and widening ICT applications; and encouraging international and regional cooperation.[14] From this point on, international institutions embarked on an effort to develop and propagate frameworks to manage risk to ICTs vulnerabilities and increase confidence and participation in the global digital economy.

One of the first international organizations to take up the mantle was the Organization of American States (OAS). In 2004, the OAS through the Inter-American Committee against Terrorism (CICTE) and its Cyber Security Program, began fostering the development of the cyber security agenda in the Americas. The OAS cooperates with a wide range of national and regional entities from the public and private sectors on both policy and technical issues, and seeks to build and strengthen cyber security capacity within its member states through technical assistance and training, policy roundtables, crisis management exercises, and the exchange of best practices related to ICTs. The OAS uses government and academic frameworks to help promote cyber security capacity building and is helping change the national conversation in its member states to recognize that Internet connection—and the ICT infrastructure that underpins it—must be secure. If countries do not invest equally in the security of their core infrastructure and resilience of their systems, the costs imposed by nefarious cyber activities will tax their economic growth

In 2007, the International Telecommunications Union (ITU) — a specialized agency of the United Nations (UN) responsible for ICT issues — announced its *Global Cybersecurity Agenda* (GCA) and published a framework that encourages cooperation and collaboration with and between parties. The GCA contains five strategic pillars to guide countries in building capacity in order to address cyber security responsibly. These include: (1) Legal Measures; (2) Technical and Procedural Measures; (3) Organizational Structures; (4) Capacity Building; and (5) International Cooperation. This framework led to the subsequent development of the ITU National Cybersecurity Guide in 2011, which emphasizes national values, culture, and interests as the basis of any effective national strategy development. It also discusses important questions that every government should tackle when working to transform the topic of cyber security from a mere technical discussion/problem into a strategic national policy area. Building on these initial efforts, in 2014, the ITU launched a Global Cybersecurity Index (GCI) to help countries baseline and measure their cyber security programs vis-a-vis other countries investments and programs. This index is meant to measure a country's development or "wellness" across the five GCA categories: Legal Measures, Technical Measures, Organizational Measures, Capacity Building, and Cooperation.[15] This methodology and index was one of the first international frameworks available to national leaders to inform their national strategy development and provide an approach to measure cyber risk in non-technical terms.

In 2015, the Organisation for Economic Co-operation and Development (OECD) Council adopted and published the OECD Recommendation on Digital Security Risk Management for Economic and Social Prosperity[16] to inform the development of national strategies aimed at managing digital security and optimizing the economic and social benefits expected from digital openness. The framework encourages countries to adopt an approach grounded in risk management and based on a framework of eight interrelated, interdependent, and complementary high-level Principles, including (1) awareness raising, skills acquisition, and empowerment; (2) stakeholders responsibility; (3) human rights and fundamental values; (4) cooperation; (5) risk assessment and treatment cycle; (6) security measures appropriate to and commensurate with the risk and the economic and social activity at stake; (7) innovation; and (8) preparedness and continuity planning. The OECD advocates that if leaders implement these eight principles coupled with other international frameworks, that countries would be positioned to develop better policies (and strategy) grounded in digital security risk management. The eight principles are not a framework per se, rather they are key components where coordination mechanisms within the government and with non-governmental stakeholders can be established or enhanced. OECD recognizes that private-public cooperation is essential to cyber risk reduction.

In 2018, the World Economic Forum's (WEF) published the Cyber Resilience Playbook for Public-Private Collaboration[17] — a tool intended to guide intra-state public-private collaboration on cyber security policy development. Section 4.7 of the Playbook, in particular, addresses the need to establish a clear national cyber governance framework, including roles, responsibilities, and capabilities that should be expected of the public and private sectors. The three-layer framework proposed by WEF aims to help national governments assign responsibilities and better align specific roles and responsibilities with three distinct security capabilities: robustness, resilience, and defense — each strengthening the others. Robustness is defined as "the ability to prevent, repel, and contain threats." Resilience is defined as "the ability to manage and work through successful breaches." And, defense is defined as "the ability to preempt, disrupt, and respond to attacks."[18] This framework builds on the initiatives dating back to the 2014 WEF Global Agenda Council on Risk & Resilience and the 2016 white paper Understanding Systemic Cyber Risk. WEF has advanced to conversation on cyber risk and made direct links to economic impacts and business consequences of cyber insecurity.

3

ACADEMIA AND TECHNICAL COMMUNITY FRAMEWORKS

Academic institutions, think tanks, and the technical community have also started weighing in and have proposed various methodologies to accelerate countries and organizations' cyber preparedness and maturity levels.

The *Cyber Readiness Index 2.0* (CRI 2.0)[19], published by a team of experts at the Potomac Institute for Policy Studies in 2015, builds on the 2013 Cyber Readiness Index 1.0, which provided a methodological framework for assessing cyber readiness. The CRI 2.0 provides a comprehensive, comparative, experience-based methodology to assess countries' commitment and maturity to closing the gap between their current cyber security posture and the national cyber capabilities needed to support their digital future. The CRI 2.0 uses over seventy unique indicators across seven essential elements to discern operationally ready activities and identify areas for improvement in the following categories: (1) national strategy; (2) incident response; (3) e-crime and law enforcement; (4) information sharing; (5) investment in R&D; (6) diplomacy and trade; and (7) defense and crisis response. The resulting actionable blueprint provides a risk-reduction roadmap for countries to follow. Most importantly, the CRI 2.0 links economic growth and development to national security policies. It also recognizes that realizing the full potential of the Internet economy in terms of GDP growth, increased productivity and efficiency, enhanced work force skills, and improved access to business and information, requires aligning economic development strategies with national security priorities. In other words, ICTs can only deliver economic growth if policies, processes, and technologies are put in place to protect and secure the cyber infrastructure and services upon which a country's digital future and growth depend. The CRI 2.0 emphasizes the tools that global leaders can leverage, including policy, legislation, regulations, standards, market incentives, and other initiatives, to protect the value of their digital investments and address the ongoing economic erosion from *cyber insecurity*.

The Oxford *Cyber Security Capacity* Maturity Model (CMM), published in 2016 by the Global Cyber Security Capacity Centre (GCSCC) at Oxford University, depicts varying levels of countries' cyber security maturity across five capacity dimensions: (1) cyber security policy and strategy; (2) cyber culture and society; (3) cyber security, education, training, and skills; (4) legal and regulatory frameworks; and (5) standards, organizations, and technologies. Each of these dimensions is then broken down into more specific factors and indicators, which taken together are emblematic of a more mature state of cyber security capacity. The CMM employs two methods to help diagnose cyber preparedness. The first method uses a survey tool (similar to ITU) where a state can self diagnose its preparedness. Then the survey answers are reviewed and a team engages in a technical exchange workshop with key cyber stakeholders from government, academia, private and public sectors to better assess state level cyber capacity across five levels of cyber maturity (i.e., start-up, formative, established, strategic, and dynamic). The Oxford CMM is an excellent tool for measuring key stakeholders' understanding of the current state of cyber capacity and maturity of the country which provide the foundation for future policy goals and risk reduction outcomes.

Finally, the e-Governance Academy in Estonia launched a National Cyber Security Index (NCSI) during the Tallinn e-Governance Conference in May 2016 and updated/modified the methodology for a new release in January

2018.[20] The methodology incorporates the lessons learned by Estonia as one of the first adopters of e-governance for society as a whole. The NCSI version 2.0 includes twelve capacity areas and 46 indicators to help assess a country's ability, at the national level, to build a "secure" e-state that secure data and transactions while limiting a country's digital risk and exposure. These twelve capacities evaluation areas are: (1) Capacity to develop national cyber security policies; (2) Capacity to analyze national-level cyber threats; (3) Capacity to provide cyber security education; (4) Capacity to ensure baseline cyber security; (5) Capacity to provide secure environment for e-services; (6) Capacity to provide e-identification and e-signatures; (7) Capacity to protect critical information infrastructure; (8) Capacity to detect and respond to cyber incidents 24/7; (9) Capacity to manage large-scale cyber crisis; (10) Capacity to fight against cybercrimes; (11) Capacity to conduct military cyber defense operations; and (12) Capacity to provide international cyber security. The NCSI has many components similar to the other frameworks but has distinct sections that are unique to Estonia's experience for e-governance including how to build a secure environment for e-services and how to provision e-identification and e-signatures.

Framework Summary

Each framework takes a slightly different approach to help strengthen a country's overall cyber security posture and manage national-level cyber risk. These existing frameworks have many commonalities, including: a broad recognition that, in the modern age, countries' national security and economic wellbeing are highly dependent on the ability to secure their national cyber infrastructure and digital economies; a need to promote cyber security at the highest levels of government and corporate leadership; a prerequisite to start by protecting the most critical infrastructures and essential services; a requirement to develop appropriate legal and regulatory frameworks to protect society against cybercrime, service disruption, and property destruction; the necessity for public and private sectors, as well as international and regional communities to collaborate in order to ensure the adoption of effective cyber risk management and resilience strategies; and an obligation to develop the necessary national capabilities to increase confidence and security in the use of ICTs, correct deficiencies, and respond to significant cyber security risks.

4

BECOMING CYBER READY
MANAGING THE RISK

Despite the various models and frameworks now available to national leaders to diagnose, assess, and reduce their countries' cyber risk, and the numerous calls to action by industry professionals and cyber security experts, improving cybersecurity at the national level continues to be a challenge. For example, the Netherlands has recognized that its future economic health is based on a well-functioning, trusted digital economy, and therefore dedicated appropriate funds and established a center to ensure that the country could securely achieve its goals. In July 2015, the National Coordinator for Security and Counterterrorism conducted a "Review of Policy on Critical Infrastructure." In that review, the government defined critical infrastructure "as a set of products, services, and underlying processes that is necessary for the functioning of the country [and that] must be secure and able to withstand and rapidly recover from all hazards."[21] However, when the port of Rotterdam — the largest port in Europe — was significantly affected and its services degraded by NotPetya in 2017, officials began to examine the state of the port's Internet dependencies and discovered that the port infrastructure had actually not been deemed critical in their national cyber security strategy and infrastructure protection policies.

At the same time, even countries like the UK that had identified specific critical sectors, such as healthcare — that must meet a standard of care — did not anticipate that their healthcare providers would not be willing to invest to maintain their software up to date and protect patients' critical services from cyber risk. Therefore, when 81 of the 236 National Health Service trusts fell victim to a simple ransomware — WannaCry — an incident that could have been easily avoided ended up putting lives at risk. As a result, the UK was forced to examine whether its cyber essentials program was sufficient and determine if further government intervention and attention was necessary to manage the risk to the nation and its citizens.

As stated earlier, Germany and the United States have identified the handful of companies that contribute at least 2 percent of the country's GDP and merit further protection and enhanced information sharing/cooperation with government, yet the information exchange between government and industry did not protect these companies from falling prey to the destructive nature of NotPetya. While both countries have processes to share threat and intelligence information — and "warn" industry that they may be vulnerable to attack, in this instance, the imminent warning was not conveyed. As such, companies headquartered in both countries were deeply impacted and global e-commerce faced delays for weeks and months due to the lack of preparedness by these companies and adequate support from their governments. Finally, Saudi Arabia's key energy companies — which deliver nearly 25 percent of the world's liquid-natural-gas and fuel the world's transportations systems — were knocked off-line due to other malicious cyber activities that ultimately affected the world's transportation systems and economy.

As these cases exemplify, no country is cyber ready and preparedness must begin with a disciplined risk management approach. Effective risk management requires a country's leadership to first and foremost understand what it values most, outline what is most important to protect, and demonstrate that it is willing to invest the political capital, executive time, money, and resources needed to protect it.

For example, Colombia initiated a risk management approach to assess its cyber readiness and promote societal confidence in the use of the digital environment. The effort responded to the tasking in the Colombian National Digital Security Policy (national cyber security strategy), that was approved in April 2016 by the National Digital Security Council, through the issuance of Document CONPES 3854 of 2016. Colombia embraced the OECD risk management guidance and used that framework along with recommendations from OAS, ITU, and the North Atlantic Treaty Organization (NATO) to assess the digital threats to the country and understand what critical assets were at risk.[20] The study pushed the country to evaluate the most pressing cyber risks it was facing, identify how cyber incidents are affecting Colombian organizations in both the private sector and the public sectors, and make cybersecurity both a priority and a strong component of its socio-economic development. It also helped raise awareness among the different stakeholders in the country about common and unique types of cyber incidents, threats, and attacks affecting public sector entities and companies and began to quantify the costs to the country's economy. Colombia recognized that managing national-level cyber risks are a fundamental pre-requisite to sector digitalization and digital transformation of the country.

Colombia's experience highlights that risk management begins with leadership and governance. As most of the frameworks, indices, and guides published by the various inter-governmental organizations, academic and technical communities in recent years emphasize, evaluating what is truly at risk and elevating cyber security to the top of a country's national security strategy is fundamental. However, it is not sufficient to make cyber security a priority in a stand alone category and treat it as a predominately national security issue. In fact, ensuring cyber security is also closely intertwined with Internet connectivity and the rapid adoption of ICTs, which – when secure and resilient – can lead to economic growth and prosperity. Therefore, aligning economic initiatives with security, development, and resilience — assessing the value at risk and establishing a national strategy that manages the risk reduction activities — is just as important.

Assess the Risk

National leaders must clearly state their intention to take advantage of the open digital environment for economic and social prosperity by reducing the overall level of digital security risk within and across borders. They must be mindful that risk changes over time based on actions that are taken by at least two actors: the attacker who obtains and uses the capability to cause harm, and the intended target who can take precautions to withstand or thwart the danger intended by the attacker. National leaders need to demonstrate their commitment reduce risk and increase resilience by conducting continuous risk assessments both at the national and sectorial level and adopting appropriate measures, policies, and processes to manage the risks identified.

In order to achieve these overarching goals, national leaders, policy-makers, and other relevant stakeholders in each given country must work together to assess the risk. Strategic planning and reflection can help determine the state of readiness:

- What is the short and long-term strategy for the country, including industrial policies, economic objectives, and national security priorities?

- What could put these objectives at risk? In other words, what weaknesses could be exploited (i.e., unaccounted high value assets) that could disrupt the execution of these objectives?

- Are there clear lines of accountability and responsibility to ensure the execution of the country's objectives and risk reduction measures are implemented?

- Have cyber security and resilience considerations been a core part of the planning process?

This comprehensive and all-encompassing assessment will highlight a country's most critical digital dependencies (e.g., companies, services, infrastructures, and assets) that, if harmed, would have grave economic and national security consequences. Only after properly identifying what is vulnerable, what could jeopardize a country's "crown jewels," and the likelihood of them being exposed to danger, harm, or loss, will the decision-makers be able to take corrective measures to thwart or reduce those risks.

5

REDUCE RISK THROUGH CAREFUL PLANNING

Once a risk assessment has been conducted, a country can devise a risk reduction plan to close the gap between its current cyber security posture and the national cyber capabilities needed to correct deficiencies and support the country's future economic and security priorities. The risk reduction efforts should be led by a dedicated, national competent cyber security authority – a leader (both a person and an entity) who is elevated and strongly anchored at the highest level of government to provide direction, coordinate actions, monitor the plan's implementation, and be accountable for shortcomings and for the results achieved. Given the fact that cyber security intersects many different issue areas (e.g., human rights, economic development, trade, arms control and dual use technologies, security, stability, and peace and conflict resolution), it is important to ensure that the national competent authority has the positional authority, accountability, and empowerment to involve and direct as many stakeholders as necessary.

While guidance on risk reduction activities are abundant, as shown by the various frameworks outlined in previous sections, national leaders should make a stronger effort to understand the cyber risk landscape and specific threats to their networked infrastructures — which should be clearly delineated in their national cyber security strategies and in the national cyber risk assessment(s) — and then work with all relevant stakeholders to better plan their defenses and better allocate human and financial resources to minimize those risks. Common strategies to effectively mitigate cyber risk include:

- Communicating what is at stake and improving overall risk awareness at every level — from government leaders to common citizen. People cannot value security without first understanding how much of their daily activities (not just personal information) are at risk. Therefore, the government should initiate a national public awareness campaign, promote education, training, and skills development, and empower its citizens to become part of the solution in building a strong cyber security culture.

- Identifying, prioritizing, and focusing necessary resources on high-value assets and high-impact systems that require increased levels of protection — the country's most critical digital dependencies (e.g., companies, infrastructures, services, and assets); understanding the vulnerabilities thereof, and prioritizing security measures appropriate to and commensurate with the economic and societal risk.

- Developing appropriate legal and regulatory frameworks to protect society against cyber crime, service disruption, and property destruction.

- Using a wide range of tools including policy, legislation, regulations, standards, market incentives, voluntary compliance schemes, and other initiatives, to increase confidence and security in the use of ICTs, as well as correct deficiencies in the processes and products (e.g., NIS Directive, China Cybersecurity Law, NIST Framework).

- Improving situational awareness, threat indicators, and warnings by continuously monitoring for threats to the networked society and using the latest technologies to detect, repel, and contain such threats.

• Developing the necessary national capabilities to increase preparedness, conduct continuity planning, and respond to and recover from significant cyber security risks when they arise (e.g., large-scale cyber crisis).

• Engaging the international community to improve the overall security, reliability, and resilience of interoperable networks (e.g., financial, telecommunication, energy, etc.) through the development of global security standards and promotion of multi-lateral agreements.

• Anticipating future technology advancements and assessing how they may introduce new vulnerabilities to the country or, on the other hand, how they could be turned into opportunities to build additional security, reliability, and resilience into next generation infrastructures and assets.

Effective implementation of these tasks and other activities will require clearly defining and clarifying roles, responsibilities, processes, decision rights, and accountability mechanisms. Successful outcomes will benefit from establishing performance targets for various ministerial or governmental departments, institutions, or individuals responsible for specific specific tasks in the action plan.

Of course, risk reduction activities also require the allocation of dedicated and appropriate resources for their implementation. Inefficient funding sources and mechanisms can undermine the intended outcomes and reduce accountability of entities tasked with the cyber security of the nation but still left with inadequate resources to carry out their missions. Resources should be defined in terms of money (i.e., dedicated budget), people, materiel, as well as the relationships and partnerships required for successful execution and outcomes of the risk mitigation plans. Resourcing the objectives and tasks within a national cyber security strategy should not be viewed as a one-time initiative. Sufficient, consistent, and continuous funding provides the foundations for an effective national cyber security posture. Resources can be allocated by task or objective, or by governmental entity. The government may also consider the establishment of a central budget for cyber security, managed by a central cyber security governance mechanism. Whether assembling disparate funding sources into a coherent, integrated program or creating a unified intra-governmental budget, the overall program should be managed and tracked by milestones and clearly-defined timeframes to ensure successful implementation of the strategy.

Continuous Evaluation of the Risk

When cyber security efforts turn into a point-in-time assessment (compliance framework) — rather than evaluating risk on a continuous basis — they fail. Risk management requires proactive anticipation of threats to and continuous assessment of vulnerabilities within the country's most critical digital dependencies (e.g., companies, infrastructures, services, and assets). As stated above, there are a number of existing frameworks that underscore the importance of continual risk assessment and remediation of control failures. Monitoring and measuring the performance and successful execution of the cyber security initiatives (risk reduction activities) should be part of the governance mechanisms that a country puts in place in its national cyber security architecture. Continuous assessment of the implementation plan (i.e., what is going well and what is not) helps inform adjustments and further advocacy of the overarching strategy. Good governance mechanisms delineate the accountability and responsibility for ensuring successful execution, and actionable, repeatable, meaningful, and time-dependent metrics or key performance indicators (KPI) should be used to reinforce realistic objectives and timelines. Key performance indicators or metrics should meet the following criteria:

• ***Specific*** – target a specific area for improvement.

• ***Measurable*** – quantify or at least suggest an indicator of progress.

• ***Achievable*** – state what results can realistically be achieved, given available resources.

• ***Actionable*** — there are clear actions to take.

• ***Responsible*** – specify who will do it.

• ***Time-related*** – specify when the result(s) can be achieved.

While no country is fully cyber ready and cyber risks cannot be entirely eliminated, they can and must be managed. Cyber readiness and preparedness begin with an effective risk management approach that encompasses a clear understanding of the country's high-value assets and high-impact systems that require increased levels of protection — the country's most critical digital dependencies (e.g., companies, infrastructures, services, and assets). Once that is understood, a risk analysis and vulnerability assessment can define and prioritize the necessary security measures to correct the deficiencies that are appropriate to and commensurate with the economic and societal risk.

Only with a concerted and coordinated effort across national stakeholders will it be possible to significantly reduce cyber risk and move forward to ensure the future safety and security of a nation.

5 CONCLUSION

Our cyber insecurity is growing. The volume, scope, scale, and sophistication of cyber threats to nations' critical services and infrastructures are outpacing defensive measures. Today's destructive and disruptive cyber activities require governments to urgently address and invest in moving their country from a state of cyber insecurity to cyber readiness. The losses are accruing; the harm is growing; and the danger is imminent.

National leaders must devise comprehensive national cyber security strategies that include a dedicated competent authority responsible for the overall national cyber security posture of the country. A national understanding of the risks faced must be developed at every level — from government leaders to common citizen. Everyone should understand the vulnerabilities of the country's digital environment and know their role in mitigating those risks. This strategic roadmap allows for the adoption of appropriate measures, policies, and processes to correct deficiencies and reduce the risks — to society, the economy, and the nation. This cannot be accomplished without dedicated and appropriate resources that fund initiatives to lower risks and increase resilience. Adopting a national cyber security strategy is one of the most important steps in securing the national cyber infrastructure and services upon which the digital future and economic wellbeing of a modern nation depend.

6

ABOUT THE AUTHOR

Melissa Hathaway is a leading expert in cyberspace policy and cybersecurity. She served in two U.S. presidential administrations, spearheading the Cyberspace Policy Review for President Barack Obama and leading the Comprehensive National Cybersecurity Initiative (CNCI) for President George W. Bush. As President of Hathaway Global Strategies LLC, she advises public and private sector clients and brings a unique combination of policy and technical expertise, as well as board room experience to help others better understand the intersection of government policy, developing technological and industry trends, and economic drivers that impact acquisition and business development strategy in this field. She developed a unique methodology for evaluating and measuring the level of preparedness for certain cybersecurity risks, known as the Cyber Readiness Index. The Cyber Readiness Index 2.0 can be found here: **www.potomacinstitute.org/academic-centers/cyber-readiness-index**.
She publishes regularly on cybersecurity matters affecting companies and countries. Most of her articles can be found at the following websites:
www.belfercenter.ksg.harvard.edu/experts/2132/melissa_hathaway.html and
www.ctm.columbia.edu/people/melissa-hathaway.

5

REFERENCES

1. Oxford dictionary. The NIST SP 800-30 (Rev A) defines risk as: Risk = Threat x Vulnerability. CRM defines risk statements as: Risk = Condition (Probability) + Consequence (Impact).

2. Nicolas Rapp and Robert Hackett, " A Hackers Toolkit." Fortune Magazine 25 October 2017, http://fortune.com/2017/10/25/cybercrime-spyware-marketplace/

3. Eduard Kovaks, "Shadow Brokers Want $20,000 for Weekly Leaks," Security Magazine, 30 May 2017, www.securityweek.com/shadow-brokers-want-20000-monthly-leaks; and
Eduard Kovaks, "Shadow Brokers Promise More Exploits for Monthly Fee," Security Magazine, 16 May 2017, www.securityweek.com/shadow-brokers-promise-more-exploits-monthly-fee; and
Nicole Perloth, "A Cyberattack the 'World Isn't Ready For,'" The New York Times, 22 June 2017, www.nytimes.com/2017/06/22/technology/ransomware-attack-nsa-cyberweapons.html?_r=0

4. National Audit Office, "Investigation: WannaCry cyber attack and the NHS," 27 October 2017, www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/.

5. Richard Chirgwin, "IT 'heroes' saved Maersk from NotPetya with ten-day reinstallation bliz," The Register, 25 January 2018, https://www.theregister.co.uk/2018/01/25/after_notpetya_maersk_replaced_everything/.

6. NotPetya disrupted business and destroyed corporate capital assets globally. Public reporting by A.P. Moller-Maersk, Balersdorf, DHL, DLA Piper, Federal Express, Merck, Mondolez, Nuance, Reckitt Benckiser Group, Rosneft, Saint Gobain, and WPP show losses of at least $2.5 billion. A recent report from Lloyds of London warns that a well executed cyber attack could cause damages around to world ranging from $53.1 billion to $121.4 billion. See: Lloyds of London, "Extreme Cyber-Attack Could Cost as Much as Superstorm Sandy," 17 July 2017, www.lloyds.com/news-and-risk-insight/press-releases/2017/07/cyber-attack-report.

7. Kelly Jackson Higgins, "Schneider Electric: TRITON/TRISIS Attack Used 0-Day Flaw in its Safety Controller System, and a RAT," Dark Reading, 18 January 2018, https://www.darkreading.com/vulnerabilities–threats/schneider-electric-triton-trisis-attack-used-0-day-flaw-in-its-safety-controller-system-and-a-rat/d/d-id/1330845.

8. The top-level-domains (e.g., .mil, .com, .edu, .gov) were introduced in 1985 and enabled the framework for global electronic commerce. Innovation continued introducing new technologies like the creation of hyper-text mark-up language (HTML) in 1990, which enabled expanded and user-friendly information sharing on the Internet—which ultimately became the World Wide Web. Other technological advances emerged including: SMS messaging (1992), voice over Internet protocol (1996), WiFi (1997), wikipedia (2001), the Google search engine (1997), social networking technology (2002), and voice and video over Internet Protocol with Skype (2003). The private sector is driving innovation and adoption of technology with the promise of lower costs, increased productivity, and consumer usability without much discussion of security. See: Melissa Hathaway, "Falling Prey to Cybercrime: Implications for Business and the Economy," in Securing Cyberspace: A New Domain for National Security, February 2012, Aspen Institute Press.

9. Many countries have different definitions of critical infrastructures. For the purposes of this paper a broad definition was used. See: Homeland Security Digital Library, "Presidential Decision Directive 63, PDD/NSC-63," 22 May 1998, https://fas.org/irp/offdocs/pdd/pdd-63.htm.

10. Officials have not yet defined how many sectors will be included within the scope of the law. However, many experts believe that this law include the same sectors as the EU Network Information Security Directive (e.g., energy, transport, banking, financial market infrastructures, digital infrastructures, health, and water). See: Yanqing Hong, "The Cross-border Data Flows Security Assessment: An Important Part of Protecting China's Basic Strategic Resources," 20 June 2017, Yale Law School, Paul Tsai China Center Working Paper,
https://law.yale.edu/system/files/area/center/china/document/dataflowssecurity_final.pdf.

11. NIST, "Cybersecurity 'Rosetta Stone' Celebrates Two Years of Success," 18 February 2016, www.nist.gov/news-events/news/2016/02/cybersecurity-rosetta-stone-celebrates-two-years-success.

12. Hathaway Global Strategies LLC. Insights from engagement with Board of Directors and Management of affected companies.

13. NIST, "NIST Special Publication 800-37 (Rev. 2) DRAFT — Risk Management Framework for Information Systems and Organizations: A System Lifecycle Approach for Security and Privacy (Discussion Draft)," September 2017, www.csrc.nist.gov/CSRC/media/Publications/sp/800-37/rev-2/draft/documents/sp800-37r2-discussion-draft.pdf.

14. WSIS, Geneva 2003 - Tunis 2005, "Tunis Commitment," 18 November 2005, www.itu.int/net/wsis/docs2/tunis/off/7.html.

15. ITU (2014), Global Cybersecurity Index, www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx.

16. OECD (2015), Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, Paris, www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf.

17. WEF (2018), Cyber Resilience Playbook for Public-Private Collaboration, pp. 33-36, https://www.weforum.org/reports/cyber-resilience-playbook-for-public-private-collaboration.

18. Ibid.

19. The Cyber Readiness Index 2.0 builds on the previous Cyber Readiness Index 1.0, which provided a methodological framework for assessing cyber readiness across five essential elements, namely: cyber national strategy, incident response, e-crime and legal capacity, information sharing, and cyber research and development. The Cyber Readiness Index 1.0 applied this methodology to an initial set of thirty- five countries. For more information on Cyber Readiness Index 1.0, see: Melissa Hathaway, "Cyber Readiness Index 1.0," Hathaway Global Strategies LLC (2013), http:// belfercenter. ksg.harvard.edu/ les/ cyber-readiness-index-1point0.pdf.

20. NCSI, "NCSI Methodology," http://ncsi.ega.ee/methodology (1.0) and http://ncsi.ega.ee/ncsi-methodology-2-0-launched/ (2.0).

21. National Coordinator for Security and Counterterrorism, "Review of Policy on Critical Infrastructure," July 2015; and Melissa Hathaway and Francesca Spidalieri, "The Netherlands Cyber Readiness at a Glance," May 2017, Potomac Institute for Policy Studies, http://www.potomacinstitute.org/images/CRI/FinalCRI20NetherlandsWeb.pdf.

22. OAS, MINTIC, IDB (2017), Impact of Digital Security incidents in Colombia 2017, https://publications.iadb.org/handle/11319/8552.

OAS More rights for more people

MANAGING NATIONAL CYBER RISK

White paper series
Issue 2

2018