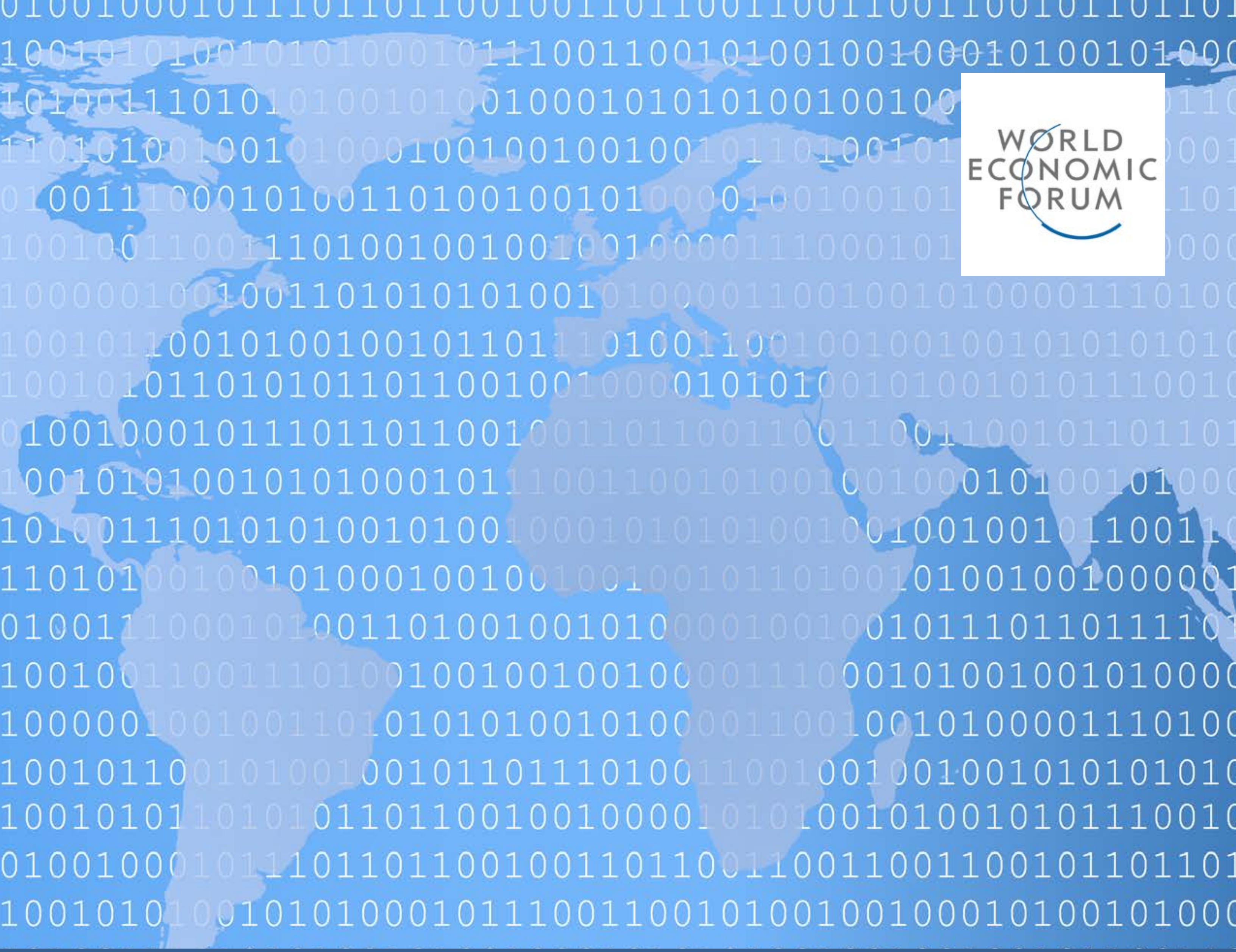


# A FRAMEWORK FOR ASSESSING CYBER RESILIENCE

A Report for the World Economic Forum

Prepared by: Brianna Keys, Aashish Chhajer, Zilong Liu, and Daniel Horner

Dr. Stuart Shapiro, supervising

April 28, 2016

# Executive Summary

Cyber resilience is of growing importance in our hyperconnected world, no longer relegated to simply the concerns of IT Departments. Cyber resilience is more than just about cybersecurity. It incorporates business practices and entails being able to absorb attacks, recover from them, and restore business operations as quickly as possible. At its annual meeting in Davos in 2011, the World Economic Forum (Forum) established a project, Partnering for Cyber Resilience, to promote resilience throughout the global economy. The next phase of this project includes conducting a comparative assessment of resilience across industries and sectors. Our report seeks to set the foundation for that global assessment.

After reviewing frameworks and standards created by public sector organizations and academics, we adapted a comprehensive set of metrics that we believe can effectively measure cyber resilience across industries and sectors. The framework is based on Linkov et al and supplemented with the National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*. The shell of the matrix can be seen below. The columns are the National Academy of Sciences' categories of disaster resilience, with the addition of "Detect" from the NIST framework. The rows are the operational domains of the Network-Centric Warfare doctrine. The cells contain a total of 72 metrics, interrelated and interdependent, that seek to measure different components of cyber resilience.

***Table 1 – Framework Structure***

| | ***Plan & Prepare*** | ***Detect*** | ***Absorb*** | ***Recover from*** | ***Adapt to*** |
|---|---|---|---|---|---|
| ***Physical*** | | | | | |
| ***Information*** | | | | | |
| ***Cognitive*** | | | | | |
| ***Social*** | | | | | |

We developed a set of recommendations for best practices for ten of the metrics from our framework. The metrics were chosen by the Forum and our team as some of the top priorities for becoming cyber resilient. The best practices outlined seek to guide organizations to evaluate existing policies and/or develop new protocols in an effort to become cyber resilient.

PricewaterhouseCoopers' Global State of Information Security Survey (GSISS) is an annual global survey, now in its 18th year, that polls more than 10,000 executives from companies of all sizes and across industries and sectors in 127 countries. We matched the GSISS questions to nearly half of the metrics in our framework, proving the survey to be a potential data source to measure cyber resilience.

The "Physical" and "Information" rows, as well as the "Absorb" and "Adapt to" columns contained the most metrics that could not be measured by the GSISS. Thus, to fill in the gaps left after applying the GSISS to our framework, we developed a supplementary questionnaire that could be used in conjunction with the GSISS to assess resilience.

Our biggest challenge throughout this project was facing limitations on access to the data necessary to assess cyber resilience. While many organizations do collect data on threats and security incidents, they are understandably reluctant to make that data public, which made quantitative analyses impossible. Ideally we would have been able to examine data from a variety of industries across all sectors; however the developing nature of the field coupled with concerns of privacy and propriety regarding risk and incident data ultimately limited the scope of our assessment.

Moving forward, we believe that information sharing will be key to increasing cyber resilience. Of the Forum’s key principles in Partnering for Cyber Resilience, first and foremost is recognition of interdependence. This recognition entails acknowledging that in our hyperconnected world, the system is only as strong as the weakest link. In order to strengthen cybersecurity and increase cyber resilience, data must be made available to those working toward that goal. We also encourage further collection of more varied data through surveys such as the GSISS and our supplementary questionnaire.

# Contents

# 1. Introduction

## Cyber Resilience and the World Economic Forum

Given the global economy's increasing reliance on automated systems, cybersecurity has become a critical component of any business's operations. Attackers are innovative in their approaches and their targets typically must adopt a defensive posture. Private information that can be used to identify consumers is constantly at risk, as attackers seek out information such as credit card numbers, passwords, and login information. Additionally, security researchers must now confront vulnerabilities in the emerging field of operational technology (OT), which seeks to safeguard the "Internet of Things". OT differs from the traditional concerns of information technology (IT), as its focus on automated technologies removes the human interaction, but introduces a reliance on a more distributed network of connected devices.

But more important than cybersecurity is cyber resilience. Resilience is about the "ability to withstand and recover quickly from unknown and known threats."[1] Becoming cyber resilient means being able to absorb attacks and maintain or quickly restore necessary organizational functions. As cyber threats become increasingly sophisticated, organizations must focus not only on addressing cybersecurity, but becoming cyber resilient in order to remain successful in our hyperconnected world.

Recognizing the growing importance of technology in the global economy, the World Economic Forum (Forum) established the Partnering for Cyber Resilience project at its Annual Meeting at Davos in 2011. One of the first objectives of the project was to garner support from business leaders for the four core principles:[2]

1. Recognition of interdependence: there is a shared interest to promote cyber resilience and the system is only as strong as its weakest link;
2. Role of leadership: executive-level awareness and leadership should be encouraged to recognize the importance of their roles in setting the tone and structure for promoting cyber resilience;
3. Integrated risk management: Practical and effective implementation of cyber risk practices should be seamlessly weaved into existing risk management practices; understanding that constantly actively pursuing cyber resilience protects the organization, contributes to the greater good and demonstrates good corporate leadership;
4. Promoting uptake: Understanding the implications of our hyperconnected world, encourage all others in the supply chain to become aware and promote preparedness and resilience themselves.

[1] Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P, Allen, J. & Kott, A. (2013). Resilience Metrics for Cyber Systems. *Environment Systems and Decisions, 33(4)*, 471.

[2] World Economic Forum. (2012). Partnering for Cyber Resilience. Retrieved from http://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf.

The current stage of the project is “Advancing Cyber Resilience” and seeks to conduct three interrelated examinations: *industry-specific assessments*, to assess potential differences in threats faced and challenges presented; *risk normalization*, in an effort to incorporate cybersecurity risks into normal business risk infrastructures for more effective and efficient risk management; and the *security concerns in the Internet of Things*, acknowledging the evolving technological landscape and addressing the concern that most security and resilience assessments tend to focus on IT alone.[3]

We were tasked with a project that would supplement the work being carried out in the current stage of the Forum’s overarching project. The central task was to create a framework that could be used to evaluate an organization’s cyber resiliency, which could then be used in conjunction with case studies to understand and examine differentiations across sectors, or industries, in the types of policies in place or the threats they faced. The framework and case studies were to be based on existing cyber policies and strategies, successful public-private partnerships and governmental policies that promoted cyber resilience.

This report proceeds as follows. First we discuss the existing frameworks and guidelines that provided the structure and background to our comprehensive framework. Then we describe our recommended cyber resilience framework. This framework meets the requirements of the World Economic Forum and is designed to be flexible enough to be able to evolve with the ever-changing nature of this field. We then review assessments of the current state of cyber resilience at the state and federal agencies of the United States, as well as other international governing bodies.

In the second section of the paper we discuss the possible applications of our framework to real world data, and the limitations to the available data that resulted in a change in direction of our project from the initially planned analytical aspects to establishing guidelines for the best practices of ten fundamental metrics of our framework. We also present a questionnaire that can be used to populate the portions of the framework that are not available from current data. The best practices are outlined in the following section. We then offer our concluding thoughts.

[3] World Economic Forum. (2015). Advancing Cyber Resilience: Project Scoping Workshop. Retrieved from http://www3.weforum.org/docs/IP/2015/ICT/19Nov_CyberResilience_PreRead.pdf.

# 2. Background on Framework Development

The Forum's current project aims to provide insights for business leaders and policymakers so they may better understand and more effectively advance cyber resilience. As a central component of this project, we were asked to create a set of metrics to measure the effectiveness of cyber resilience practices and policies set forth by both business leaders and policymakers. With these metrics, we aim to provide improved methods by which organizations can identify and prioritize needs, monitor threats, and distribute resources. Many leaders have already recognized the importance of establishing metrics to inform the extent to which their networks are resilient, but challenges to advancing a globally accepted framework still exist. Currently, no standardized framework that measures cyber resilience has been adopted across different organizations. The usage of metrics for an aggregated assessment is significantly impeded, because different organizations use their own specific approaches and means of measuring resilience.[4] In an increasingly connected world, it is critical that organizations utilize a common understanding and standardized framework to assess cyber resilience.

We now provide an overview of the existing frameworks and guidelines that we examined throughout the development of our framework. Ultimately, through a combination of academic and governmental assessments, supported by governing standards and insights, we were able to develop a framework that we believe can be effectively utilized to assess cyber resilience across industries and sectors.

### 2.1 European Union Agency for Network and Information Security (ENISA) Standards

In order to define a framework that is based on good metrics, the European Union Agency for Network and Information Security (ENISA) identified several key principles that should be considered during the development and implementation of a program designed to measure cyber resilience.[5] Good metrics must possess technical characteristics: they should be quantifiable, repeatable, and comparable to allow for viable and accurate comparison of different measurements. Good metrics should also possess some non-technical business characteristics. They should be easily obtainable, relevant to the business mission, and work toward the continuous improvement of resilience.

[4] ENISA. (2011). Measurement Frameworks and Metrics for Resilient Networks and Services: Challenges and Recommendations. Retrieved from https://www.enisa.europa.eu/publications/metrics-tech-report/at_download/fullReport.

[5] Ibid.

## 2.2 The Local Government Research Center Framework [6]

In November 2015, the Bloustein Local Government Research Center at Rutgers University published a report entitled *Managing Technology Risks Through Technological Proficiency*. The study defines risks as events that stem from the things that people do (or do not do), the failure of technology systems, the failure of management and operational processes, and the disruptions created by external events. These risks can be categorized into six interrelated areas: cyber security, legal, operational, financial, reputational, and societal.

The Rutgers study provides a framework that suggests that organizations manage these risks through technological proficiency. The framework's focus is on achieving technological proficiency by establishing and institutionalizing four essential practices: governance (the governing/managing body should provide overall technology policy goals and guidance, make risk management decisions, and monitor activities); planning (government officials and technology managers combine to establish the long- and short-term goals of the organization, establish a technology plan, and recommend risk management strategies); cyber hygiene (employees are trained to understand and practice the safe use of technology to prevent technology compromise); and technical competence (maintaining human, technical and financial resources that are necessary to ensure sound technology practices are properly and adequately deployed). Achieving technological proficiency is an ongoing process, which requires an organization to efficiently use its three most valuable resources: time, attention, and money.

## 2.3 The Linkov Framework[7]

Linkov et al combine the National Academy of Sciences (NAS) definition[8] of disaster resilience with the Network-Centric Warfare (NCW) doctrine,[9] which defines operational domains (i.e., physical, information, cognitive, and social), to develop a set of resilience metrics.[10] NAS defines resilience as encompassing four categories: plan/prepare (foundation for keeping services available and assets functioning during a malfunction or attack); absorb (continuing to function during attack and repel or isolate the attack); recover (get back all functions and services to pre-attack levels); and adapt (utilizing knowledge and experience gained to become more resilient). The NCW doctrine defines four interrelated operational domains: physical (physical resources and design and capabilities of those resources); information (information development regarding

[6] Pfeiffer, M. (2015). Managing Technology Risks Through Technological Proficiency. Retrieved from http://blousteinlocal.rutgers.edu/managing-technology-risk/

[7] Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P, Allen, J. & Kott, A. (2013). Resilience Metrics for Cyber Systems. *Environment Systems and Decisions, 33(4),* 471.

[8] National Research Council. (2012). Disaster Resilience: A National Imperative. *The National Academies Press*. Retrieved from http://nap.edu/13457

[9] Alberts, D. (2002). Information age transformation, getting to a 21st century military. *DOD Command and Control Research Program*. Retrieved from http://www.dtic.mil/get-tr-doc/pdf?AD=ADA457904

[10] Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P, Allen, J. & Kott, A. (2013). Resilience Metrics for Cyber Systems. *Environment Systems and Decisions, 33(4),* 471.

the physical domain); cognitive (use of physical and information to make decisions); social (organization structure and communication to make cognitive decisions).

By combining the two frameworks, Linkov et al was able to create a matrix that measures the ability of the systems to handle attacks and provide metrics to assess resiliency. All metrics are interrelated and each have implications on each other, especially as you move across the columns and down the rows. This matrix is intended to be a general framework and Linkov et al note that it should be adapted to individualized needs of each system.

### 2.4 The National Institute of Standards and Technology's (NIST) Framework[11]

The National Institute of Standards and Technology (NIST) published their *Framework for Improving Critical Infrastructure Cybersecurity* in 2014;[12] the framework's focus is on utilizing an organization business processes to guide its cybersecurity activities and internalizing cybersecurity within the organization's risk management processes. Somewhat uniquely among the frameworks studied, protecting civil liberties is a stated goal for this framework. The authors noted that the framework is not intended to be a "one size fits all," solution, and that it should be adapted as needed to unique threats. While it was written with critical infrastructure in mind, it can be adapted to a wide variety of scenarios.

The NIST framework identifies five key functions of cybersecurity which are similar to the Network Centric Warfare doctrine. These functions organize cybersecurity at the highest levels. They are identify (develop understanding of and manage risk to systems, assets, data, and capabilities), protect (develop and implement appropriate safeguards to ensure delivery of critical infrastructure services), detect (identify the occurrence of a cybersecurity event), respond (take action regarding a detected cybersecurity event), and recover (maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event).

### 2.5 Operational Security, "The Internet of Things"

As more devices become networked, from thermostats and refrigerators to vehicles and medical devices, the opportunities for attackers to do physical damage through a cyber-attack are increasing rapidly. Hackers have demonstrated that it is possible to take control of a late model Jeep's functions (windshield wipers, engine, power steering) through software vulnerabilities and the car's GPS.[13] As medical devices become linked to smartphones, it is possible that hackers

[11] National Institute of Standards and Technology. (2014). Framework for Improving Critical Infrastructure Cybersecurity. Retrieved from http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf
[12] Ibid.
[13] Greenberg, A. (2015, July 21). Hackers Remotely Kill A Jeep on the Highway. *Wired*. Retrieved from http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

could interfere with pacemakers.[14] While there is a relatively shallow body of academic research on this topic, private companies have been releasing white papers at an increasing rate over the last two years.

Operational security, while ambiguously defined, is used in this document to refer to the protection of the Internet of Things. While this is typically viewed in the lens of “smart home” devices and self-driving cars, there is a growing public-sector component as well, as cities move towards providing more access to services electronically; Barcelona, for example, is working to connect citizens virtually to waste management, smart parking, and the city bus service.[15] The public sector’s investments in IoT highlight the scale of some security and maintenance challenges. Power plants are increasingly networked and automated, creating challenges not only security the systems themselves, but also ensuring safety in the event of software updates.

The frameworks above do not explicitly mention the “Internet of Things” (IoT), the “network of physical objects that contains embedded technologies to communicate and sense or interact with their internal states or the external environment.”[16] Nevertheless, many of the components of both the NIST and Linkov frameworks inherently address many of the most pressing security concerns regarding Operational Security. The most critical vulnerabilities with Operational Security tend to revolve around the interactions between systems. Protecting data in transit and coordinating with external entities are both examples of metrics covered by the above frameworks that apply not just to IT, but to OS as well. Security for networked devices stretches for the product’s entire lifecycle, [17] and the physical dispersion of IoT technologies presents extra challenges. [18] Operational technology as defined here, while not new, has only recently become large enough to warrant significant attention. Research on operational security is ongoing, but many of the best practices for IT need only be viewed through a slightly different lens in order to apply to the Internet of Things. Best practices mentioned herein should be thought to implicitly apply to manufacturers of the IoT if they do not refer to the security of the operational technology explicitly.

[14] Geer, D. (2014, July 9). The Internet of Things: Top Five Threats to IoT Devices. Retrieved from http://www.csoonline.com/article/2134265/network-security/the-internet-of-things--top-five-threats-to-iot-devices.html?page=2.

[15] Olstik, J. (2014). The Internet of Things: A CISO and Network Security Perspective. Enterprise Strategy Group. Retrieved from http://www.cisco.com/c/dam/en_us/solutions/industries/docs/energy/network-security-perspective.pdf.

[16] Gartner IT. The Internet of Things (n.d.). Retrieved from http://www.gartner.com/it-glossary/internet-of-things.

[17] Wind River. (2015). Security in the Internet of Things: Lessons from the Past for the Connected Future. Retrieved from http://www.windriver.com/whitepapers/security-in-the-internet-of-things/wr_security-in-the-internet-of-things.pdf.

[18] Ernst and Young. (2015). Cybersecurity and the Internet of Things. Retrieved from http://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/$FILE/EY-cybersecurity-and-the-internet-of-things.pdf.

# 3. Our Framework

In developing the framework we would use to assess cyber resilience, we considered the reality that resilience is a fairly new concept in the cybersecurity policy arena. The NIST framework is widely promoted by the federal and many state governments, as well as several cross-sector governing organizations. However, Linkov et al addressed the concern that many risk-based assessments conflate risk and resilience; these assessments may lack efficacy in promoting resilience. Therefore, we chose to move forward with the framework that most effectively addressed the more nuanced components of cyber resilience. Compared with the NIST framework, the Linkov framework is more comprehensive and straightforward, but Linkov et al did not address the activities associated with threat detection to the same degree as the NIST framework. Therefore, we decided to create a relatively unique and more robust framework by combining Linkov's framework with NIST's to better address the Forum's Core Principles. This framework was created to assess cyber resilience among organizations, industries, and sectors through examinations of incident reports and relevant survey data. Below is our simplified blank framework.

***Table 2 – Framework Structure***

| | ***Plan & Prepare*** | ***Detect*** | ***Absorb*** | ***Recover from*** | ***Adapt to*** |
|---|---|---|---|---|---|
| ***Physical*** | | | | | |
| ***Information*** | | | | | |
| ***Cognitive*** | | | | | |
| ***Social*** | | | | | |

The categories of the matrix are further defined as follows. The columns utilize the NAS Disaster Resilience components of Linkov et al's framework, with the exception of "Detect;" this category was drawn from the NIST framework to address perceived weaknesses:

- **Plan and prepare** is defined as the foundation for keeping services available and assets functioning during a malfunction or attack.
- **Detect** refers to the immediate recognition of an attack or malfunction and triggering the implementation of containment procedures.
- **Absorb** involves continuing to function during attack and repel or isolate the attack.
- **Recover** entails getting back all functions and services to pre-attack levels.
- **Adapt** requires utilizing knowledge and experience gained from the event to become more resilient.

The rows refer exclusively to the Network-Centric Warfare doctrine:[19]

- The **Physical** domain is comprised of physical resources and design and capabilities of those resources.
- The **Information** domain includes information and information development regarding the physical domain.
- The **Cognitive** domain includes the use of physical and information to make decisions.
- The **Social** domain is the organization structure and communication to make cognitive decisions.

Each cell has between two and eight specific component metrics that seek to measure the cyber resilience of the organization. These metrics are a combination of those suggested by Linkov et. al.[20] and NIST[21] with the wording modified for consistency.  As noted above, the metrics are interrelated and influence one another throughout the matrix.

***Table 3 – Framework with Metrics***

| | ***Plan & Prepare*** | ***Detect*** | ***Absorb*** | ***Recover from*** | ***Adapt to*** |
|---|---|---|---|---|---|
| ***Physical*** | (1) Implement controls/sensors for critical assets<br>(2) Implement controls/sensors for critical services<br>(3) Assessment of network structure and interconnection to system components and to the environment<br>(4) Redundancy of critical physical infrastructure<br>(5) Redundancy of data physically or logically | (1) Monitor the physical environment to detect potential cybersecurity events<br>(2) Monitor personnel activity to detect potential cybersecurity events | (1) Signal the compromise of assets or services<br>(2) Use redundant assets to continue service<br>(3) Dedicate cyber resources to defend against attack | (1) Investigate and repair malfunctioning controls or sensors<br>(2) Assess service/asset damage<br>(3) Assess distance to functional recovery<br>(4) Safely dispose of irreparable assets | (1) Review asset and service configuration in response to recent event<br>(2) Phase out obsolete assets and introduce new assets |

[19] Alberts, D. (2002). Information age transformation, getting to a 21st century military. *DOD Command and Control Research Program*. Retrieved from http://www.dtic.mil/get-tr-doc/pdf?AD=ADA457904

[20] See note 10

[21] See note 11

| | | | | | |
|---|---|---|---|---|---|
| | separated from the network<br>(6) Protect data-in-transit | | | | |
| ***Information*** | (1) Inventory physical devices, systems, software platforms, and applications within the organization<br>(2) Map organizational communication and data flows<br>(3) Catalog external information systems<br>(4) Categorize assets and services based on sensitivity or resilience requirements<br>(5) Documentation of certifications, qualifications and pedigree of critical hardware and/or software providers<br>(6) Prepare plans for storage and containment of classified or sensitive information<br>(7) Identify external system dependencies<br>(8) Identify internal system | (1) Detect malicious code<br>(2) Detect unauthorized mobile code<br>(3) Monitor external service provider activity to detect potential cybersecurity events | (1) Observe sensors for critical services and assets<br>(2) Effectively and efficiently transmit relevant data to responsible stakeholders/ decision makers<br>(3) Document, implement, and review audit/log records in accordance with policy | (1) Log events and sensors during event<br>(2) Review and compare systems before and after the event | (1) Document incident's impact and cause<br>(2) Document time between problem and discovery/discovery and recovery<br>(3) Anticipate future system states post-recovery<br>(4) Document point of entry (attack)<br>(5) Categorize incidents consistent with response plans<br>(6) Continuously improve protection processes |

| | | | | | |
|---|---|---|---|---|---|
| | dependencies | | | | |
| ***Cognitive*** | (1) Anticipate and plan for system states and events<br>(2) Understand performance trade-offs of organizational goals<br>(3) Scenario-based cyber wargaming<br>(4) Include cybersecurity in human resources practices<br>(5) Test response and recovery plans | (1) Analyze detected events to understand attack targets and methods<br>(2) Aggregate and correlate event data from multiple sources and sensors<br>(3) Determine impact of events<br>(4) Establish incident alert thresholds | (1) Use a decision making protocol or aid to determine when event can be considered ‘‘contained’’<br>(2) Determine if mission can continue<br>(3) Focus effort on identified critical assets and services<br>(4) Utilize applicable plans for system state when available | (1) Review critical points of physical and information failure in order to make informed decisions<br>(2) Establish decision making protocols or aids to select recovery options | (1) Review management response and decision making processes<br>(2) Determine motive of event (attack)<br>(3) Mitigate newly identified vulnerabilities or document as accepted risks<br>(4) Understand the impact of incidents |
| ***Social*** | (1) Identify and coordinate with external entities that may influence or be influenced by internal cyber-attacks (establish point of contact)<br>(2) Educate/train employees about resilience and organization’s resilience plan<br>(3) Manage identities and credentials for authorized devices and users<br>(4) Manage and protect physical and remote access to assets | (1) Define roles and responsibilities for detection to ensure accountability<br>(2) Communicate event detection information to appropriate parties<br>(3) Continuously improve detection processes | (1) Locate and contact identified experts and resilience responsible personnel<br>(2) Protect communications and control networks<br>(3) Share effectiveness of protection technologies with appropriate parties | (1) Manage public relations and repair reputation after events<br>(2) Communicate recovery activities to internal stakeholders and executive/ management teams<br>(3) Determine liability for the organization | (1) Evaluate employees response to event in order to determine preparedness and communications effectiveness<br>(2) Assign employees to critical areas that were previously overlooked<br>(3) Stay informed about latest threats and state of (the art protection methods/share with organization<br>(4) Voluntarily share information with external stakeholders to achieve broader |

|  |  |  |  |  |  |
|---|---|---|---|---|---|
|  | (5) Prepare/establish resilience communications<br>(6) Establish a cyber-aware culture<br>(7) Understand and manage legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations |  |  |  | cybersecurity situational awareness |

# 4. Assessing Public Sector Cyber Resilience

To demonstrate the utility of our framework we briefly examine public sector cybersecurity policy. In general, the public sector lags behind the private sector in adequately addressing cybersecurity. However, while there are limitations in access to data regarding private sector cybersecurity practices, there has been significant analysis of government practices. Despite the broader focus on cybersecurity rather than cyber resilience, we still feel that addressing public sector initiatives allows us to show how our framework could be used to evaluate institutional cyber-practices.

### 4.1 Cyber Resilience Among the States

According to several of the leading state governing organizations, state governments are not adequately addressing cyber security, and addressing resilience specifically is not yet within the purview of most state policy.[22] However, many states are making strides to better understand cyber threats to both public and private information systems, and thus, becoming more resilient. In this section, we will examine the policies and practices that state governments are employing to address cybersecurity in general.

***State Chief Information Security Officers (CISOs)***

In the past several decades, the CISO has become a ubiquitous and institutionalized position within American state governments. According to a recent survey of all state CISO's, the top five priorities of the position, after advising the state Chief Information Officer (CIO), are cybersecurity policy and planning; intrusion detection and response management; enterprise vulnerability management; training and awareness; and information sharing partnerships (e.g. Multi State Information Sharing and Analysis Center (MS-ISAC)).[23] CISO's also reported in 2014 that the top three barriers to adequately addressing cybersecurity issues were lack of a sufficient budget; ever-changing and ever-more sophisticated threats; and a talent crisis stemming from the public sector's competitive disadvantage of lower salaries than the private sector.[24]

To combat the challenges CISOs are facing, NASCIO makes seven recommendations:[25]

1. Define and establish new executive roles;
2. Communicate risks and impacts to business leaders to garner support and funding;
3. Document and approve cybersecurity strategy;

[22] Spidalieri, F. (2015). State of the States on Cybersecurity. Pell Center for International Relations and Public Policy. Retrieved from http://pellcenter.org/wp-content/uploads/2015/11/Pell-Center-State-of-the-States-Report.pdf

[23] NASCIO. (2015). Moving Forward: Leadership Toolkit for State CISOs. Retrieved from http://www.nascio.org/Portals/0/Publications/Documents/2015/NASCIO_StateCISOToolkit_Final-a.pdf

[24] Deloitte-NASCIO. (2014). State Governments at Risk: Time to Move Forward. Retrieved from http://nascio.org/Portals/0/Publications/Documents/Deloitte-NASCIOCybersecurityStudy_2014.pdf

[25] Ibid.

4. "Define and measure" by establishing metrics and integrating them into the business plan;
5. Periodically assess security by remaining up to date on current threats and ensuring resiliency;
6. Collaborate with Human Resources to attract new talent; and
7. Embrace outsourcing of cybersecurity functions to compensate for being unable to acquire the talent directly.

***States Leading the "Cyber Pack"***

In November 2015, The Pell Center for International Relations and Public Policy at Regina Salve University released a report entitled *The State of the States on Cybersecurity*. This report identified eight states as being at the forefront of cyber preparedness and resilience: California, Maryland, Michigan, New Jersey, New York, Texas, Virginia, and Washington.[26] The report assessed states based on a Cyber Readiness Index comprised of five "key areas":

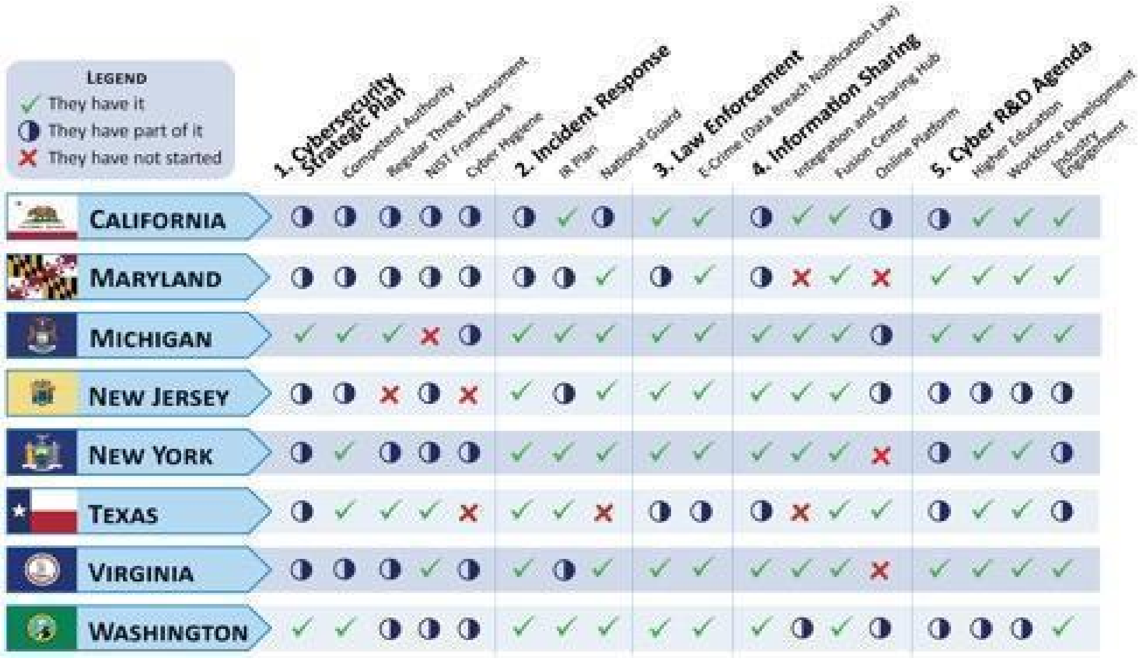
1. State Cybersecurity Strategic Plan: Including a specific plan to address threats and increase resilience, a clear chain of command and designation of responsible authorities, annual threat assessments for state agencies and critical infrastructure networks, and adoption of established policies and standards, such as those developed by NIST;[27]
2. Incident Response: Clear designation of the state government entity responsible for addressing incidents as they occur, published and widely available response plans, especially for incidents involving critical infrastructure networks, clearly defined roles for the Homeland Security Advisors, National Guard and/or Fusion Centers;[28]
3. E-crime and Law Enforcement: Development of laws to protect residents against cyber-crimes, including data breach notification laws, established relationships with law enforcement, and state's ability to combat cyber-crime;[29]
4. Information Sharing: Presence of a state information sharing and analysis center (ISAC), participation in ISACs that have cross-level and cross-sector reach, presence of a state Fusion Center and its capacity to assess data and share its findings in a timely manner, and the presence of a state website allowing greater public access and contribution to information regarding current cyber threats;[30] and
5. Cyber Research and Development, Education, and Capacity Building: state investments in cybersecurity, supporting universities and K-12 institutions in their efforts to research cybersecurity and those that offer curriculums or programs in the field, public-private-

[26] Spidalieri, F. (2015). State of the States on Cybersecurity. Pell Center for International Relations and Public Policy. Retrieved from http://pellcenter.org/wp-content/uploads/2015/11/Pell-Center-State-of-the-States-Report.pdf
[27] Ibid.
[28] Ibid.
[29] Ibid.
[30] Ibid.

academia partnerships promoting preparedness and resilience, and state incentives to promote cybersecurity training and workforce development.[31]

A chart summarizing the findings of the Pell Center is displayed below:

***Table 3 – State of Cyber Resilience among states***



LEGEND

✓ They have it

◑ They have part of it

✗ They have not started

| | 1. Cybersecurity Strategic Plan | Competent Authority | Regular Threat Assessment | NIST Framework | Cyber Hygiene | 2. Incident Response | IR Plan | National Guard | 3. Law Enforcement | E-Crime (Data Breach Notification Law) | 4. Information Sharing | Integration and Sharing Hub | Fusion Center | Online Platform | 5. Cyber R&D Agenda | Higher Education | Workforce Development | Industry Engagement |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| CALIFORNIA | ◑ | ◑ | ◑ | ◑ | ◑ | ◑ | ✓ | ◑ | ✓ | ✓ | ◑ | ✓ | ✓ | ◑ | ◑ | ✓ | ✓ | ✓ |
| MARYLAND | ◑ | ◑ | ◑ | ◑ | ◑ | ◑ | ◑ | ✓ | ◑ | ✓ | ◑ | ✗ | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ |
| MICHIGAN | ✓ | ✓ | ✓ | ✗ | ◑ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ◑ | ✓ | ✓ | ✓ | ✓ |
| NEW JERSEY | ◑ | ◑ | ✗ | ◑ | ✗ | ✓ | ◑ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ◑ | ◑ | ◑ | ◑ | ◑ |
| NEW YORK | ◑ | ✓ | ◑ | ◑ | ◑ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ◑ | ✓ | ✓ | ◑ |
| TEXAS | ◑ | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✗ | ◑ | ◑ | ◑ | ✗ | ✓ | ✓ | ◑ | ✓ | ✓ | ◑ |
| VIRGINIA | ◑ | ◑ | ◑ | ✓ | ◑ | ✓ | ◑ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ |
| WASHINGTON | ✓ | ✓ | ◑ | ◑ | ◑ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ◑ | ✓ | ◑ | ◑ | ◑ | ◑ | ✓ |

*Source: Spidalieri, Francesca. State of the States on Cybersecurity. November 2015. Pell Center for International Relations and Public Policy. Page 8*

As can be seen from the chart above, even those states that are doing the most to address growing cybersecurity concerns are failing to ultimately become cyber resilient.  To give a broad assessment based on our framework, the states largely fail to plan and prepare as evidenced by the overall lack of robust strategic plans. However, they do appear to be improving in detection, response and recovery, especially through the development and implementation of incident response plans. Further, the states are making strides to improve the social domain of cyber resilience as evidenced by those proficiently addressing information sharing and research and development, although work remains to be done.

[31] Ibid.

## 4.2 Cyber Resilience at the Federal Level

### *The National Infrastructure Protection Plan*

The National Infrastructure Protection Plan (NIPP), which was released in 2006 and has since been revised in 2009 and 2013, was designed as an adaptable guide for assessing current risk, policy, and strategic environments. It provides a foundation for joint efforts between the private sector and federal agencies, also referred to as "sector-specific agencies" (SSA), to achieve the vision of a "nation in which physical and cyber critical infrastructure remain secure and resilient, with vulnerabilities reduced, consequences minimized, threats identified and disrupted, and response and recovery hastened."[32] SSA's have their origins in Presidential Policy Directive 21 (PPD-21).[33] PPD-21 identified 16 critical infrastructure sectors, thus designating 16 associated federal SSA's. These are responsible for providing institutional knowledge and specialized expertise to facilitate and support the resilience programs of their respective sectors.

The NIPP establishes a framework for sharing information across and between federal and nonfederal stakeholders within each sector via sector coordinating councils and government coordinating councils. Sector coordinating councils serve as a liaison between sectors and state actors. Government coordinating councils enable interagency, intergovernmental, and cross-jurisdictional coordination within and across sectors. Additionally, the NIPP also created a list of recommendations ("Call to Action steps") to guide the efforts of the SSA's and their sector partners in advancing security and resilience under three broad categories: building on partnership efforts; innovating in risk management; and focusing on outcomes.[34] The ten Call-to-Action-Steps, as listed in the report are:

1. Determine collective actions through joint planning efforts;
2. Empower local and regional partnerships to build capacity nationally;
3. Leverage incentives to advance security and resilience;
4. Enable risk-informed decision making through enhanced situational awareness;
5. Analyze infrastructure dependencies, interdependencies, and associated cascading effects;
6. Identify, assess, and respond to unanticipated infrastructure cascading effects during and following incidents;
7. Strengthen coordinated development and delivery of technical assistance, training and education;
8. Improve critical infrastructure security and resilience by advancing research and development solutions;

[32] U.S. Department of Homeland Security. (2013). NIPP 2013: Partnering for Critical Infrastructure Security and Resilience. Retrieved from https://www.dhs.gov/sites/default/files/publications/NIPP-Fact-Sheet-508.pdf

[33] White House. (2013). Presidential Policy Directive 21 (PPD 21), Critical Infrastructure Security and Resilience.

[34] U.S. Government Accountability Office. (2015). GAO-16-79: Critical Infrastructure Protection: Sector Specific Agencies Need to Better Measure Cybersecurity Progress. Retrieved from http://www.gao.gov/products/GAO-16-79

9. Learn and adapt during and after exercises and incidents;
10. Establish performance metrics for monitoring cybersecurity related activities and incidents.

The following table summarizes the findings from the Government Accountability Office's assessment of each agencies' compliance with the recommendations proposed by the NIPP:[35]

***Table 4 – Evaluation of Sector Specific Agencies***

| **Sector Specific Agency** | *NIPP's Call-to-Action Steps* | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | ***1*** | ***2*** | ***3*** | ***4*** | ***5*** | ***6*** | ***7*** | ***8*** | ***9*** |
| Chemical | ● | ● | ○ | ● | ● | ● | ● | ● | ● |
| Commercial facilities | ● | ● | ○ | ● | ● | ● | ● | ● | ● |
| Communications | ● | ● | ○ | ● | ● | ● | ● | ● | ● |
| Critical Manufacturing | ● | ● | ○ | ● | ● | ● | ● | ○ | ● |
| Dams | ● | ● | ○ | ● | ● | ● | ● | ● | ● |
| Defense industrial base | ● | ● | ○ | ● | ● | ● | ● | ● | ● |
| Emergency Services | ● | ● | ○ | ● | ● | ● | ● | ● | ● |
| Energy | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| Financial services | ● | ● | ○ | ● | ● | ● | ● | ● | ● |
| Food and Agriculture | ● | ● | ○ | ● | ● | ● | ● | ○ | ○ |
| Healthcare and public health | ● | ● | ● | ● | ● | ● | ● | ○ | ● |
| Information Technology | ● | ○ | ○ | ● | ● | ● | ● | ● | ● |
| Nuclear reactors, materials and waste | ● | ● | ○ | ● | ● | ● | ● | ● | ● |
| Transportation Systems | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| Water and wastewater systems | ● | ● | ○ | ● | ● | ● | ● | ● | ● |

● Steps were addressed ○ Steps were **NOT** addressed

This assessment by the GAO comprehensively describes the state of cyber resilience in some of the most important sectors in the U.S. Almost all sectors have made great progress in the last decade by addressing many of the steps created by the NIPP that would help improve the state of cyber resilience throughout the country. One of the concerns, as highlighted in the report, has

[35] Adopted from Table in *GAO-16-79 Report, p. 23*

been the failure of most sectors in identifying incentives that would promote further improvements in their security and make them more resilient when attacked. However, the evaluation does note that efforts are being made in establishing working groups to identify appropriate incentives to encourage cybersecurity improvements. It is also concerning to note that among the 16 different agencies, only three (the Department of Defense, the Department of Energy, and the Department of Health and Human Services) have established performance metrics for monitoring cybersecurity-related activities and incidents.

The recommendations of NIPP 2013 are broad when compared to the comprehensive nature of our framework. However, there are similarities and overall they cover aspects from all twenty cells of our framework. Also, we should note that GAO's assessment of the Sector Specific Agencies highlights the failure of the NIPP in setting up mechanisms for implementing its recommendations.

### 4.3 Cyber Resilience in the International Arena

***European Union***

In 2013, the European Union Agency for Network and Information Security (ENISA) signed the WEF principles on cyber resilience. ENISA has also conducted a number of projects to promote cyber resilience. Three of these projects are:

1. The AMBER Project aimed to coordinate the study of cyber resilience by measuring and benchmarking computer systems and their components. It fostered European research addressing challenges posed by current and forthcoming computer systems and computer-based infrastructure.[36]
2. The ResumeNet Project was designed to build a framework for resilience in future Internet systems. It proposed a straightforward strategy for building resilient networked systems, with a focus on continual improvement processes.[37] The project's authors also proposed a mechanism to support the framework; most components of the mechanism overlap with the metrics in our framework. They also suggest experimentation to assess the efficiency of the framework and mechanisms.
3. The ResiliNets Project was conducted with an eye towards understanding and progressing the state of resilience and survivability in computer networks.[38]

In December 2015, the European Commission passed the EU Data Protection Reform.[39] Additionally, representatives of EU member states reached agreement on the draft Network and

[36] ENISA. (2011). Measurement Frameworks and Metrics for Resilient Networks and Services: Challenges and Recommendations. Retrieved from https://www.enisa.europa.eu/publications/metrics-tech-report/at_download/fullReport.

[37] Ibid.

[38] Ibid.

Information Security (NIS) Directive. The NIS Directive contains some essential regulations that would advance cyber resilience the region. The draft directive lists the different entities and legislative frameworks that each member state have to establish; it requires Cooperation Network and Computer Security Incident Response Teams (CSIRT) be developed to improve cooperation between member states; it imposes new network and information security requirements on operators of essential services; and it encourages the use of EU standards to promote standardization among member states.

### *The Business-Software Alliance's (BSA) National Cybersecurity Dashboard: An International Assessment*

The Business-Software Alliance (BSA), a leading advocate for the software industry, developed a framework for policymakers to evaluate their respective nations' capacity to address cyber threats. The framework contains five components: legal foundations, operational capabilities, public-private partnership, sector-specific cybersecurity plans, and education.

Using this framework, the BSA has published several regional and national cybersecurity "dashboards," providing a straightforward picture of international cybersecurity readiness in different countries. According to their reports, there are considerable discrepancies among regions' and countries' cybersecurity capability under their framework. The ten countries (Australia, China, India, Indonesia, Japan, Malaysia, Singapore, South Korea, Taiwan, and Vietnam) being investigated in Asia-Pacific region are not proactive enough to build up their cybersecurity capacity. They have generally been slow to develop comprehensive national cybersecurity strategies, and to implement the necessary legal frameworks.[40] The region has not been performing well in creating public-private partnerships.[41] In comparison with the Asia-Pacific region, cybersecurity of member states in the European Union demonstrates much more maturity, but there still exist discrepancies in specific components of the framework in EU member states.[42]

In the report, Germany, the United Kingdom and Estonia demonstrate a high capability to deal with cyber threats.[43] They adopted a comprehensive cybersecurity strategy very early and complemented it with a strong cybersecurity legal framework. They also have well-established national-level operational entities to administer cybersecurity affairs. Furthermore, they also have developed formal and informal public-private partnerships. In Estonia, though there is no formalized public-private partnership, public entities informally work closely with relevant

[39] European Commission. (2015). Agreement on Commission's EU Data Protection Reform Will Boost Digital Single Market. Retrieved from http://europa.eu/rapid/press-release_IP-15-6321_en.htm

[40] BSA. (2015). Asia-Pacific Cybersecurity Dashboard: A Path to a Secure Global Cyberspace. Retrieved from http://cybersecurity.bsa.org/2015/apac/assets/PDFs/study_apac_cybersecurity_en.pdf.

[41] Ibid.

[42] Ibid.

[43] Ibid.

private-sector organization. In Germany, there is the Alliance for Cyber Security and the UP KRITIS partnership. In contrast, the assessment of the ten countries being investigated in the Asia-Pacific region indicates that they still have much to do to improve their countries' cyber resilience capacity. Except for the establishment of operational entities, the ten countries being surveyed are not doing as well as their European counterparts. Though BSA's dashboard is used to assess states' cybersecurity rather than cyber resilience, it is still a good indicator demonstrating countries' preparedness for cyber threats, providing us a basic understanding on those countries' readiness for cyber resilience.

The five components of BSA's assessment framework are closely relevant to our framework.[44] Full-fledged legal foundations ensure that the physical and information assets in the cyber world are protected by the legal system. Operational capabilities such as a well-functioned computer emergency readiness team (CERT), through improved coordination and information sharing, can help both public and private entities deal with cyber-attacks more effectively in each phase of an incident. Public-private partnerships, which are essential elements in shaping the social factors of cyber resilience, also facilitate coordination and information sharing from the "plan and prepare" phase to the "adapt to" phase. A sound cybersecurity strategic plan can cover all the elements in our framework and ensure that organizations are prepared in the face of cyber-attacks. By raising awareness for cyber resilience in both the public and private arenas, education can help the whole society and individual entities to be more conscious of cyber resilience issues. Though BSA's assessment framework does not specifically cover all of the elements in our framework, the five components are consistent with our framework.

[44] Ibid.

# 5. Applying the Framework

The framework that we outlined in the first section of this paper has been designed to assess the resilience of cyber systems and would ideally serve as a guide to create secure and resilient systems, as well as improve existing ones for public or private organizations. As in the Linkov framework, each metric can be populated using relevant (metric specific) qualitative and quantitative data, which can then be evaluated by security experts to generate system specific improvements to improve resiliency.

One of the biggest challenges we faced in assembling this report was associated with obtaining real-world historical data regarding the frequency and severity of cyber incidents and the risk associated with them. Organizations with established cyber security infrastructure and protocols do record and document such data, but they are kept confidential, largely due to the proprietary nature of information. The current regulations in the U.S. and most parts of the world require the reporting of only a subset of cyber-attacks,[45] which has resulted in the lack of publicly available data that is required to understand and analyze trends and any other aspects of attacker behavior. Concerns regarding privacy and the potential disclosure of data further discourage information sharing. We found that the most applicable source of publicly available data was PricewaterhouseCoopers' Global State of Information Security Survey (GSISS),[46] which was also highly restricted and could not be used to conduct any sort of comprehensive quantitative analysis which would address issues such as cross-industry comparisons of threat sources, safeguards implementations, and executive-level involvement.

Furthermore, these limitations on data availability could also be due to the nature of cyber incidents; where there are delays between the occurrence, detection and reporting of attacks. We should also note that the vast array of possible weaknesses an attacker could exploit may not be perfectly quantifiable. Software vulnerabilities sometimes remain unidentified for long periods of time and dependencies of organizations on third-party infrastructure limit visibility into the status of various assets.

In an ideal world where access to this information was possible, we would have worked on assessing our framework to create analytical models that could test an organization's existing structures and protocols. We would have then been able to determine the extent to which the framework could be used as an evaluation tool for organizations to become more secure and more resilient.

However, this vast gap between the requirements and actual availability of data resulted in a change in direction of the project. The next section provides an overview of the GSISS, its

[45] World Economic Forum. (2015). Partnering for Cyber Resilience Towards the Quantification of Cyber Threats. Retrieved from http://www3.weforum.org/docs/WEFUSA_QuantificationofCyberThreats_Report2015.pdf
[46] PricewaterhouseCoopers. The Global State of Information Security Survey 2016. Retrieved from http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html

objectives, methodology, and limitations, followed by a Questionnaire designed to address these limitations. We follow this in the next section with a discussion of best practices to address ten of the metrics in our framework.

### 5.1 PricewaterhouseCoopers (PwC) Global State of Information Security Survey

***PwC Survey Information***

The Global State of Information Security Survey (GSISS) has been conducted by PricewaterhouseCoopers (PwC), in partnership with the journals, CIO, and CSO, for 18 years. It is a global survey of more than 10,000 executives including CEOs, CFOs, CIOs, CISOs, CSOs, and IT and security directors from companies in 127 countries. The GSISS seeks to assess how organizations are addressing growing and evolving cybersecurity concerns across industries and sectors. PwC provides a global analysis of the findings, as well as individual analyses for 12 of the industries surveyed.

***Population Methodology***

The questions answered by GSISS respondents provide insight into the challenges faced by firms worldwide and methods of cybersecurity employed to combat those threats. Many of these questions are framed in such a way that they align with our matrix, thus allowing us to populate our matrix with cross-industry data. For example, question 3 of the “Incidents” section of the GSISS asks, “How was your organization impacted by the security incidents?” The answers to this question help us better understand how firms “assess service / asset damage” after an attack, which is a component metric that comprises part of the cell where the “Physical” row meets the “Recover From” column.

In another example, metric 3 where the “Information” row meets the “Detect” column emphasizes the need to monitor external service provider activity to detect cybersecurity events; GSISS question 1 under the “safeguards” section offers some insight, as the third answer to this question details what percentage of respondents keep security standards and baselines for third parties. These are two examples. A complete list of matchings between our metrics and the GSISS questions are attached to this report as Appendix I. Further explanation of Appendix I can be found below.

***Limitations***

While the GSISS provides data that aligns with our matrix, the data it provides is neither a complete nor perfect fit. Of the matrix’s 20 cells, in only five are all component metrics covered by the GSISS data; four cells are not covered at all. Nevertheless, the survey offers an opportunity to assess 31 of the 76 component metrics. Further, restricted public access to the data collected from the survey limited our ability to conduct analyses of the GSISS findings and prohibited us from conducting any independent quantitative analysis such as cross-industry comparisons of threat sources, safeguards implementations, and executive-level involvement.

### *Our Additional Questions*

While the GSISS offers a substantial first look at cyber resilience through a global lens, it does not address many of the metrics in the "Physical" and "Information" rows and the "Absorb" and "Adapt" to columns of our matrix. With four cells in our matrix that are completely missed by the GSISS (Physical/Plan and Prepare, Absorb, Adapt to; and Cognitive/Absorb), we developed additional questions that seek to fill in the gaps. The supplementary questionnaire can be found in Appendix I along with the complete list of matchings between survey questions and our framework.

In the Appendix you will see the matrix, coded to represent the metrics addressed by the GSISS and those that are omitted. Those that have been matched to a GSISS question are coded in green, while those metrics that cannot be measured by a corresponding question in the GSISS, and thus could be measured by the Bloustein Supplementary Questionnaire are coded in red. After each metric is a notation indicating which survey the metric can be measured by and the specific corresponding question and response category.

## 5.2 Best Practices

The cyber resilience framework created in this project has been designed to assess the level of cyber resiliency among organizations, industries, and sectors through examination of data on cyber infrastructure and incident reports of past attacks. Such an assessment was beyond the scope of this project due to the aforementioned limitations of data availability. This led to a decision reached jointly with the Forum to focus on selecting individual components of the framework, metrics that would be the fundamental components for any organization aiming to be cyber resilient, and develop best practices for them.

Following discussions with the World Economic Forum, our team selected ten metrics from the framework that we deemed would be integral to organizations in every industry:

1. Understand and manage legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations;
2. Establish a cyber-aware culture;
3. Educate/train employees about resilience and organization's resilience plan;
4. Documentation of certifications, qualifications and pedigree of critical hardware and/or software providers;
5. Identify and coordinate with external entities that may influence or be influenced by internal cyber-attacks;

6. Include cybersecurity in human resources practices;
7. Test response and recovery plans;
8. Scenario-based cyber wargaming;
9. Assessment of network structure and interconnection to system components and to the environment; and
10. Monitor personnel activity to detect potential cybersecurity events.

The purpose of this Best Practices discussion is to create a set of guidelines for each of these components that can be used by organizations to set up protocols or evaluate existing structures. The assessment includes developing a definition of the metric based on research of governing organizations and industry leaders. The best practices offer examples of exemplary policies already put in place by organizations, as well as specific recommendations for policies to best address the metrics. The objective of these guidelines is not to dictate rules, but rather to shed light on various aspects of the metric, so that organizations can make decisions to improve security and resiliency.

**1. Understand and manage legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations (Matrix Location: Social/Plan & Prepare #7)**

NIST defines a methodology for developing this metric under the guidelines of Executive Order 13636.[47] Privacy and civil liberties obligations are most likely to arise when organizations come into contact with personal information in the course of their cybersecurity activities, though there are also implications when the personal information is utilized outside of cybersecurity activities. This applies to the Internet of Things as well; for example, utility providers are adopting “smart meters” at a growing rate. A drop in power consumption could indicate that the home is temporarily vacant, as the owners are perhaps on vacation.[48] This data, if acquired by criminals, could be used to target houses for burglary, leaving the utility liable if the breach was due to that firm’s negligence.[49]

NIST acknowledges that organizations have a direct responsibility to protect individuals’ information and to measure how well organizations address the privacy and civil liberty concerns, NIST developed five broad categories containing several potential actions and processes:[50]

[47] National Institute of Standards and Technology. (2014). Framework for Improving Critical Infrastructure Cybersecurity. Retrieved from http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

[48] Wind River. (2015). Security in the Internet of Things: Lessons from the Past for the Connected Future. Page 4. Retrieved from http://www.windriver.com/whitepapers/security-in-the-internet-of-things/wr_security-in-the-internet-of-things.pdf.

[49] Ibid.

[50] Ibid.

1. Governance of cybersecurity risk;
2. Approaches to identifying and authorizing individuals to access organizational assets and systems;
3. Awareness and training measures;
4. Anomalous activity detection and system and assets monitoring; and
5. Response activities, including information sharing or other mitigation efforts.

The Department of Homeland Security (DHS) has published a set of institutionalized policies to protect privacy and comply with privacy laws that are an example of best practices for other organizations to follow.[51] Since 2008, DHS has had a formalized set of policies called the Fair Information Practice Principles (FIPPs), which consist of the following eight principles:

1. Transparency;
2. Individual participation;
3. Purpose specification;
4. Data minimization;
5. Use limitation;
6. Data quality and integrity;
7. Security; and
8. Accountability and auditing.

Together, the NIST recommendations and DHS policies indicate best practices for remaining proficient in understanding and implementing privacy protection requirements. These entail having clearly delineated policies regarding limiting access to data, data storage and usage, and a plan to systematically review all policies and procedures within the organization, as well as regulations and laws implemented outside the organization.

**2. Establish a cyber-aware culture (Matrix Location: Social/Plan & Prepare #6)**

Ensuring cyber resiliency has come to entail more than simply addressing the needs of the IT department. Many organizations are beginning to understand that in order to truly become cyber resilient, they must foster a culture of cyber awareness. This requires not only the recognition that promoting resilience requires more than the IT department, but also ensuring that cyber security practices are integrated into business operations.[52]

In their recommendations for cultivating an organizational cyber-aware culture, the journal CSO stresses that the "weakest link of the cybersecurity chain" is individuals. Thus, the awareness

[51] U.S. Department of Homeland Security. Cybersecurity & Privacy. Retrieved from https://www.dhs.gov/sites/default/files/publications/privacy_cyber_0.pdf

[52] Contos, B. (2015, August 27). Cyber Security Culture Is A Collective Effort. Retrieved from http://www.csoonline.com/article/2977014/security-awareness/cyber-security-culture-is-a-collective-effort.html

must permeate throughout the organization to all employees, including both workers and executives. Establishing a cyber-aware culture then also encompasses several other metrics included in this list of best practices, including numbers 3. Educating and training employees about resilience and the organization's resilience plan, and 6. Including cybersecurity in human resources practices.

In March 2016, Eze Castle Integration published a whitepaper that outlines four best practices to "Creating a Culture of Security".[53] They are as follows:

1. Create a computer incident response team (CIRT). The CIRT operates not only in conjunction with the IT department, but also helps develop and deploy resilience practices including creating training programs, responding to incidents, and promoting effective information sharing with stakeholders and industry groups.
2. Define your terms. Create and disseminate a formal security plan that clarifies definitions and organizational policies.
3. Deliver comprehensive training. Again, this importance of strengthening the knowledge and practices of employees was stressed by CSO. Eze Castle Integration also suggests reaching out to vendors that offer specialized and customizable trainings.
4. Remember the internal culture reaches out externally. This entails recognizing that in the hyperconnected economy that organizations now operate in, business practices and cyber resilience are impacted by outside actors, such as third-party vendors and the regulatory climate (see metrics 1 and 5). However, it is also recognizing that employee actions can jeopardize security even if they are not directly related to business practices, e.g. breached or corrupted personal email accounts may cause organization vulnerabilities.

We feel that together, these four practices are a clear example of the sound policies that organizations can implement to achieve establishment of a cyber-aware culture.

### 3. Educate/train employees about resilience and organization's resilience plan (Matrix Location: Social/Plan & Prepare #2)

The range of possible threats to any entity is often too wide for any firm to possibly address them all; therefore, threats must be prioritized, and these priorities should drive the content of training programs. According to the Financial Industry Regulatory Authority (FINRA), firms have begun to further delineate between topics suitable for general staff and those targeted to specific audiences. Common topics in general training include recognizing risks, handling confidential

[53] How to Create A Cyber Security Culture + Employee Security Awareness.  Retrieved from http://www.hedgeco.net/blogs/2016/03/11/cybersecurity-plans/

information, password protection, escalation policies, physical security, and mobile security. The topics covered by targeted training are usually more technical in nature, often requiring professional IT training; these topics include privilege management, application lifecycle, application security, and software vulnerability.

FINRA also observed that training typically happens annually and that delivering training during the new employee hiring process is a popular method. However, this is not necessarily the most effective practice. Firms increasingly need to rely on *ad hoc* training in the face of more rapidly evolving threats; delivery of *ad hoc* training after cybersecurity events helps staff become more proficient in and aware of cybersecurity techniques. FINRA's 2015 report provides an example of such training:[54]

> "In this instance, a hacker was able to gain access to a client's personal email. The hacker then portrayed himself as the client of the firm and sent written instructions to wire transfer funds to an offshore bank account. Since the amount of the transfer was not unusual and the client frequently wired transferred funds, neither the registered representative nor branch office staff called the client to confirm the transaction. Only after the funds were sent, did the firm discover that the source of the transfer instructions was fraudulent. After completing the investigation, which revealed the lapse in firm procedures, the firm implemented new required verification of client instructions and rolled out a specific training requirement for all registered representatives and support staff. The firm provided the training materials and required branch management to host a meeting for all employees within their respective offices to ensure everyone was aware of the new requirements to verbally confirm all transfer instructions received."[55]

The lesson here is that the timing of a training program is just as important a factor in cyber resilience as is the content of that training program. The example provided by FINRA clearly indicates a best practice in selecting the timing of training. The training can be supplemented with alternative forms of delivery: interactive training modules with audiences help to increase retention and training delivered by outside vendors helps organizations keep pace with emerging threats.

### 4. Documentation of certifications, qualifications and pedigree of critical hardware and/or software providers (Matrix Location: Information/Plan & Prepare #5)

Many firms rely heavily on third-party vendors to provide cybersecurity services. Qualifications and certifications can demonstrate the ability of those vendors to adequately secure their clients information technology systems; organizations must be able to understand the importance of vendor qualifications to ensure that any potential contractors are vetted properly.

[54] The Financial Industry Regulatory Authority.  (2015). Report on CyberSecurity Practices. Retrieved from https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf.

[55] Ibid.

To accomplish this, best practices should include performing pre-contractual due diligence on all prospective vendors. This should be followed with ongoing awareness of a vendor's credentials throughout the life of the contract.

FINRA suggests establishing contractual terms appropriate to the sensitivity of information and systems for which the vendor will maintain access. These terms should govern the ongoing relationship between the two parties, and should consider the vendor's obligations post-contract.[56] An example is provided below:

> "The Legal team, working with all due diligence teams, is the custodian of contract language requirements and has standardized contract wording based on the type of engagement. All contracts include standardized language for 28 identified areas, including controls, the right to audit, confidentiality and security, regulatory compliance, insurance coverage, business continuity planning, subcontracting, encrypting, incident reporting, storage of data and an exit strategy. The contract will also identify service level agreements for monitoring of required controls during the duration of the engagement. If standardized contract language is not used, an exception process is followed to have the language approved by the appropriate risk teams, business units and Enterprise Risk Management."[57]

This example indicates a best practice in formulating contractual terms to protect the cybersecurity service buyer's benefits. In addition to the steps above, it is vital to consider the vendor's systems and processes in the firm's overall risk assessment process. Organizations should factor a vendor's performance into future risks assessments to determine whether or not to continue services.

**5. Identify and coordinate with external entities that may influence or be influenced by internal cyber-attacks (establish point of contact) (Matrix Location: Social/Plan & Prepare #1)**

Cyber resilience is not limited to technical domains, but rather requires the attention of a wide variety of fields and skill sets. As the business world becomes more technologically interconnected, cyber resilience cannot be viewed in a vacuum by any organization. There are many benefits to building partnerships between stakeholders and this metric can be viewed through two lenses. The first lens examines the relationship between firms and public sector actors, such as the Federal Bureau of Investigation (FBI). The second, a more "literal" reading of the metric, considers communication between any two firms whose IT infrastructure are integrated, often through financial transactions. Both of these perspectives are also relevant to

[56] Ibid.
[57] Ibid.

the Internet of Things as well. The automation of electrical networks carries national security implications, and smart homes often rely on technology produced by different manufacturers. Those devices are only as strong as their weakest link, from a security perspective.

As disconnects between the capabilities and motivations of two different parties can lead to confusion, and arguably exacerbate problems[58], many state actors are establishing more formal and informal partnerships. For example, Germany has established the Alliance for Cyber Security, and the UP KRITIS partnership to boost collaboration and coordination between public and private sectors. In the United States, the most recent cybersecurity bill (the Cybersecurity Information Sharing Act, or CISA) is almost entirely focused on improving data sharing and communication between the American security services and private firms. Given that many critical infrastructure which we rely on every day are managed by private entities, it is critical to build effective partnership between public and private sectors.

Public sector allies are just one external entity, however; increasingly, IT systems are becoming interconnected. One report by the SANS Institute defined external entity as "any company that provides goods or services to a Company, and requires a financial transaction as a result of these goods or services. These include hardware, software, and consulting vendors."[59] This definition is close to being outmoded; as more firms use external vendor software, such as payroll systems, the threat of a computer virus outbreak spreading across systems has increased. In the event of an attack, computer security incident response teams (CSIRTs) are often responsible for coordinating the response.[60] Communication before attacks between two (or more) firms' CSIRTs prior to attacks can help ensure that each organization remains up to date, and isn't becoming a weak link in an interconnected system. In the event of an attack, those CSIRTs can then coordinate to ensure that security events are contained, and do not spread.

Organizations should decide what type of CSIRT fits best within their organization, as we believe that CSIRts are the best unit for coordinating communications with external entities. To help determine the type of CSIRT, Carnegie Mellon's Software Engineering Institute publishes a handbook for creating CSIRTs, as well as formalizing their roles and protocols.[61] We also advise organizations to supplement the Carnegie Mellon document with NIST's guidelines for incident

[58] FitzGerald, B. & Sander, A. (2015). Opinion: Cybersecurity Collaboration Needs A Toolkit. So We Built A Prototype. Retrieved from http://www.csmonitor.com/World/Passcode/Passcode-Voices/2015/1204/Opinion-Cybersecurity-collaboration-needs-a-toolkit.-So-we-built-a-prototype.

[59] Pielocik, M. (2004). Social Engineering: The Friendly Hacker. Page 12. SANS Institute. Retrieved from https://www.giac.org/paper/gsec/3792/social-engineering-the-friendly-hacker/106104

[60] Proffitt, T. (2007). Creating and Managing an Incident Response Team for a Large Company. Page 15. SANS Institute. Retrieved from https://www.sans.org/reading-room/whitepapers/incident/creating-managing-incident-response-team-large-company-1821

[61] Brown, M. J., Stikvoort, D., Kossakowski, K., Killcrece, G., Ruefle, R. & Zajicek, M.. (2003). Handbook for Computer Security Incident Response Teams (CSIRTs). Retrieved from http://repository.cmu.edu/cgi/viewcontent.cgi?article=1570&context=sei

handling, which detail recommended steps for establishing relationships and communicating with external parties during attacks.[62]

### 6. Include cybersecurity in human resources practices (Matrix Location: Cognitive/Plan & Prepare #4)

When considering cybersecurity and resilience as it relates to Human Resources, there are two key considerations: the first involves protecting the sensitive data of employees themselves, and the second involves protecting the firm and its customers from insider threats. This metric focuses on the latter. Since the breach of the Office of Personnel Management and the Sony hacks, more attention is being paid to the sensitivity of employee records.[63]

The SANS Institute issues annual Security Awareness Reports; the 2016 report is titled "Securing the Human",[64] and is based off of survey responses that can help to inform cybersecurity policy. Specifically, the survey indicates that efforts to promote awareness via employee training, often administered by human resources departments, often run into common challenges.

Among those challenges is basic funding. Firms tend to underinvest in awareness training, with most firms surveyed dedicating less than $10,000 to security awareness. Only 5% of the survey's respondents work on their security awareness programs full time. There is a human element that cannot be overlooked with regards to cybersecurity, something as simple as a strong user password could be the difference in preventing an attack. All too often, firms neglect to invest adequately in training on even these simple measures. That said, while ensuring that well-intentioned employees are aware of their responsibilities in contributing to a secure environment, firms must also address the issues of insider threats.

NIST provides several best practices with regards to guarding against insider threats. One in particular stands out: in publication 800-53, Revision 4, titled "Security and Privacy Controls for Federal Information Systems and Organizations," NIST suggests assigning levels of risk to employees:[65]

> "Indications of increased risk from individuals can be obtained from a variety of sources including, for example, human resource records... The monitoring of individuals is closely coordinated with management, legal, security, and human

[62] Cichonski, P., Millar, T., Grance, T. & Scarfone, K. (2004). Computer Security Incident Handling Guide. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

[63] Helms, M. M. Best Practices for Protecting Employee Data in the Age of Cybersecurity Issues. Retrieved from http://hrprofessionalsmagazine.com/best-practices-for-protecting-employee-data-in-the-age-of-cybersecurity-issues/

[64] SANS Institute. (2015). SANS Securing The Human 2015 Security Awareness Report. Retrieved from https://securingthehuman.sans.org/media/resources/STH-SecurityAwarenessReport-2015.pdf

[65] NIST. (2013). F223

> resources officials within organizations conducting such monitoring and complies with federal legislation… policies, directives, regulations, and standards."

The PwC data suggests that insider threats, often in the form of disgruntled employees, remain one of the most common sources of cyber-attacks. Researchers believe it is likely that a former employee of Sony was responsible the 2014 hack, the most high-profile attack of that year.[66] By investing in employee training, and evaluating risk from new hires, firms can adequately incorporate cybersecurity into Human Resources practices.

**7. Test response and recovery plans (Matrix Location: Cognitive/Plan & Prepare #5)**

With regards to response and recovery, the SANS Institute's InfoSec library provides an excellent guide to testing response and recovery plans. "Disaster Recovery Plan Testing: Plan the Cycle, Cycle the Plan," authored by Guy Krocker in 2002, still contains excellent guidance for ensuring the core concern of resiliency: that a business can "bounce back" after attacks.[67] Krocker's work focuses on Disaster Recovery Plans (DRP's). It emphasizes the importance of prioritizing.[68]

> "Each business-critical process defined in the DRP should be completely reassessed for currency and prioritized based on the Business Impact Analysis (BIA) and the Residual Risk (RR) determined via Risk Analysis of threats, vulnerabilities and safeguards. Performing mandatory recovery testing on processes with a high RR and catastrophic BIA is a no-brainer and easily defensible to management. It is the less obvious values that will require management decisions as to what levels they deem acceptable. The recovery practitioner can simplify the process by implementing a ranking system in which the management can make decisions based on empirical data as opposed to subjective evaluations." (Krocker 2002, 4)

Once this has been performed, responsible parties have to select a testing methodology. There is no one methodology that will fit every DRP, and responsible parties must weigh methodologies for their ability to test the DRP to the fullest extent possible, remain cost-effective, cause minimal impact in the form of service disruptions/outages, and produce results which provide quality input for improving the DRP in the future. Krocker's proposed paradigm utilizes a series

[66] Faughnder, R. & Hamedy, S. (2014). Sony insider -- not North Korea -- likely involved in hack, experts say. Retrieved from http://www.latimes.com/entertainment/envelope/cotown/la-et-ct-sony-hack-inside-job-not-north-korea-20141231-story.html

[67] Krocker, G. W. (2002). Disaster Recovery Plan Testing: Cycle the Plan, Plan the Cycle. SANS Institute InfoSec Reading Room. Retrieved from https://www.sans.org/reading-room/whitepapers/recovery/disaster-recovery-plan-testing-cycle-plan-plan-cycle-56.

[68] Ibid. Page 4.

of multiple methodologies that iteratively increase in complexity and length; the iterative nature ensures a process of continuous improvement.[69]

***Image 1 – DRP Cycle Testing Scenario***

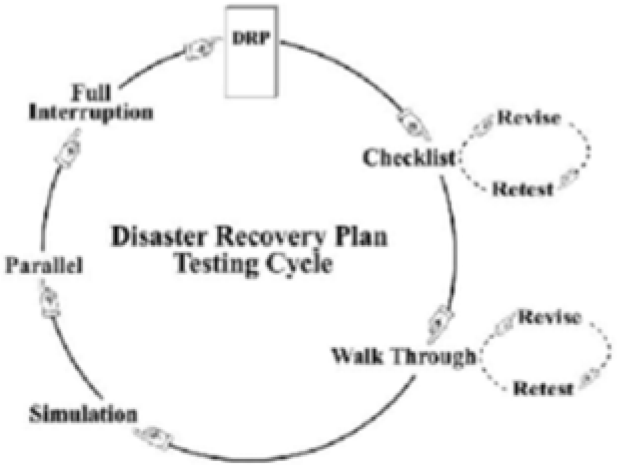


Illustration of DRP Cycle Testing Scenario, SANS Institute, 2002

In addition to the steps listed on the DRP Cycle Testing Illustration (and detailed in Krocker's paper), the organization must ensure that the test team contains members from a broad cross-section of the organization's departments, audit the cycle, and "close the loop," ensuring that the issues identified in previous phases have been addressed.

### 8. Scenario-based cyber wargaming (Matrix Location: 8. Cognitive/Plan & Prepare #3)

Cyber-incidents are unpredictable in both nature and scale. Even if a firm has the most sophisticated cyber security infrastructure there are no guarantees of complete security. Infrastructure and protocols play an important role as they are capable of addressing the weaknesses in an organization's ability to detect and respond to attacks; but they are insufficient when judging its ability to manage a cyber crisis and take the timely decisions to enact cyber defense or system continuity plans.[70] The challenge posed by this constant unpredictability gave rise to a more advanced preparation concept, cyber war-gaming.

As defined by the Wall Street Journal, a war-game is a simulation of a prolonged attack, that aims to provide lessons before a real event and enables learning during an attack.[71] In short, it can develop the organization's ability to interpret and apply experience into real-time learning. Cyber war games involve learning across multiple levels of decision-makers, and can be

[69] Ibid.

[70] Banks, S. B, & Stytz, M. R. (2014). Cyber Warfare Simulation to Prepare to Control Cyber Space, *National Cybersecurity Institute Journal*, 1 (2),

[71] Deloitte. (2014, September). An Introduction to Cyber War Games. *The Wall Street Journal*. Retrieved from http://deloitte.wsj.com/cio/2014/09/22/an-introduction-to-cyber-war-games/

structured specifically to bring together the CISO, security teams, incident response, as well as the risk, and crisis-management teams.[72]

To most organizations, a real-world attack simulation is as much a 'game changer' as actually being targeted. In both cases, the organizations expect to learn hard lessons but the war game process ensures that the organization is ready to absorb the lessons and identify the benefits without the consequence of facing the damages of an actual breach. [73]

Cyber war games are new and are slowly being adopted because there are currently only a handful of bodies that are capable of conducting such exercises.[74] The Department of Homeland Security (DHS) carries out “the most extensive government sponsored cyber security exercise of its kind,”[75] a biennial exercise series called Cyber Storm. The latest exercise, Cyber Storm IV,[76] involved 1,250 participants that came from both public and private sector agencies from eleven countries.[77]

Deloitte LLP,[78] Intel Corporation,[79] and Cisco Systems[80] are some of the private sector firms that have developed comprehensive cyber war-game workshops that they use internally as well as provide as third-party vendors. Below is a comprehensive best practices guide to design and run a cyber war-game;[81] one that combines the core elements of multiple existing simulation programs mentioned above.

As highlighted by cyber security expert Dan Solomon, a simulation exercise incorporates a “fundamental surprise”, one that the organization has not anticipated, along with a number of

[72] Ibid.
[73] Ibid.
[74] McKinsey & Company. Playing War Games to Prepare for a Cyberattack. Retrieved from http://www.mckinsey.com/business-functions/business-technology/our-insights/playing-war-games-to-prepare-for-a-cyberattack
[75] U.S. Department of Homeland Security. Cyber Storm: Securing Cyber Space. Retrieved from https://www.dhs.gov/cyber-storm
[76] Ibid.
[77] Ibid.
[78] Deloitte. Prepare for the Unexpected Cyber Threat War-Gaming Can Help Decrease The Business Impact of Cyber Incidents. Retrieved from http://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-aers-cyber-war-gaming-sales-sheet-07272014.pdf
[79] Casey, T. & Willis, B. (2008). Wargames: Serious Play that Tests Enterprise Secuirty Assumptions. Retrieved from https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Intel%20-%20Wargames-%20Serious%20Play%20that%20Tests%20Enterprise%20Security%20Assumptions.pdf
[80] CISCO. Cisco Security Cyber War Games. Retrieved from https://www.cisco.com/c/dam/en/us/products/collateral/security/spa-overview.pdf
[81] This best practices section has been compiled using the article by Dan Solomon, though it can also be viewed as an integrated summary of the fundamental characteristics of Deloitte LLP’s, Intel Corporation’s and Cisco Systems’ simulation designs. All of the aforementioned organizations’ designs are very similar when broken down to their basic principles. The Wall Street Journal article also specifically highlights these basic principles specifically in relation to Deloitte LLP’s simulation protocols.

"situational surprises", ones that are known to organizations, but occur with minimum warning.[82] The article also notes that most of the pre-exercise planning should focus on developing appropriate knowledge and intelligence, so that the exercise can be carried out in a manner that is controlled and continuously evolving, while also systematically testing the capabilities of the response teams and coordination between teams within an organization.[83] The simulation can commence with a technical event to kick off the assessment of initial implications; the initial objective is to test detection by the systems and the response teams.[84]

This should be followed by the examination of decision making protocols, specifically assessing decision makers by analyzing their reasoning and responses.[85] This stage would also examine the team's communication effectiveness, to assess the individuals involved and their roles in the response process of taking alerts/indications, followed by the transformation of that information into knowledge throughout this first technical phase.[86] At this point the event may be taken in a new direction, or a major new technical event may be introduced to trigger a new cycle of detection and decision-making. The evaluation of the first phase of the simulation may focus more on how the new event affects the decisions previously taken, the need for additional resources, and whether a new risk assessment should take place. Whereas for the second phase, i.e. the escalation of the attack, the evaluation can examine who is assessing the risk throughout the event, who is involved in the process, what indicators are in place, and how they conduct a timely assessment of the possible implications from the new event.[87] This ensures a balance between security and implementation of appropriate response, while also recommending a list of immediate tactical priorities that need to be re-assessed, to strengthen the organization's protocols and personnel.[88]

The most important phase of these simulations are the end-of-exercise workshops,[89] as they not only help participants understand existing information gaps that can then be used to improve security measures. They also serve as a forum for the participants to provide their feedback, which can be then used to improve the simulation exercises, as well as discuss security priorities of organizations, from board-level down through the management levels and security teams.

As one can directly imply from the above guide, running a simulation is not a straightforward task and requires specialized skills and a vast array of resources. Hence, cyber wargaming is expensive. Large organizations can afford to run in-house programs based on existing guides and

[82] Solomon, D. (2014). The role of cyber war games in developing advanced cyber defence. Retrieved from http://www.scmagazineuk.com/the-role-of-cyber-war-games-in-developing-advanced-cyber-defence/article/354670/
[83] Ibid.
[84] Ibid.
[85] Ibid.
[86] Ibid.
[87] Ibid.
[88] Ibid.
[89] Ibid.

some extra personnel, while smaller organizations can participate in exercises run by third-party organizations, such as cyber security firms or larger organizations within their industry.

### 9. Assessment of network structure and interconnection to system components and to the environment (Matrix Location: Physical/Plan & Prepare #3)

In an increasingly connected world, it is essential that the resources of an organization be accessible from anywhere at any time. Greater access implies more targets, and subsequently a larger potential for attacks, which makes network security an important metric in any cyber resilience framework. "To keep up with this deluge of modern threats, automated and semi-automated solutions are necessary."[90] However, designing such systems requires a distributed architecture that should support development and testing. Several system architectural forms are focused on providing a platform that facilitates risk-assessment of the individual components.

The objectives of a network assessment should be to identify the risks to the network, network resources, and data.[91] Paquet notes that "the intent of the assessment should be to identify portions of a network, assign a threat rating to each portion, and apply an appropriate level of security."[92] This is essential, as it helps provide a workable balance between the security of, and access to, networks.

Typically, each network resource should be categorized into one of the three risk-levels, as defined by Cisco Systems.[93] Low-risk systems are those which would have minimal legal or financial implications, are not connected to other systems in a way that would permit access, and can easily be restored. Attacks on medium-risk systems could cause moderate disruptions to the firm's business, or pose legal and financial ramifications; medium-risk systems also could allow access to other systems if security is breached. High-risk systems are those that, if penetrated, could cause extreme impacts to business, potentially threaten the health and safety of persons, require significant effort to restore, and possibly expose the firm to significant legal or financial consequences. This risk assessment strategy applies to IoT devices, though the practical application of the strategy focuses on assessing the individual vulnerabilities of each device deployed and isolating data as much as possible.[94]

[90] Rush, G. D. (2015). Cyber Security Research Frameworks for Coevolutionary Networks Defense. Retrieved from http://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-15-29293
[91] Paquet, C. (2013). Network Security Concepts and Policies. Retrieved from http://www.ciscopress.com/articles/article.asp?p=1998559
[92] Ibid.
[93] CISCO. (2015). Network Security Policy: Best Practices White Paper. Retrieved from http://www.cisco.com/c/en/us/support/docs/availability/high-availability/13601-secpol.html
[94] AT&T. (2016). The CEO's Guide to Security the Internet of Things. Page 15. Retrieved from https://www.corp.att.com/cybersecurity/docs/exploringiotsecurity.pdf

Cisco Press has published several papers on the topic of network assessment.[95] These resources, in conjunction with Cisco Systems' white paper "Network Security Policy: Best Practices," serve as the best practice for this metric, and should be used as a guide for setting organizational policy.

### 10. Monitor personnel activity to detect potential cybersecurity events (Physical/Detect #2)

A variety of tools already exist to monitor the physical environment.[96] Security protocols for physical office locations are already well established; employee access cards and visual surveillance help ensure that employees remain in authorized areas. This section will deal more extensively with the electronic artifacts of employee behavior, as atypical system use may offer signals that someone could be using a stolen login.

Previous security paradigms emphasized signature-based detection methods, such as antivirus software and network intrusion detection, but these methods have declined in efficacy.[97] Instead, Shackleford suggests analytics focused on context-based behavioral modeling. "By collecting lots of data, as well as putting data into context of their organization's policies, processes and people, security professionals can more quickly identify activities that could be deemed suspicious".[98]

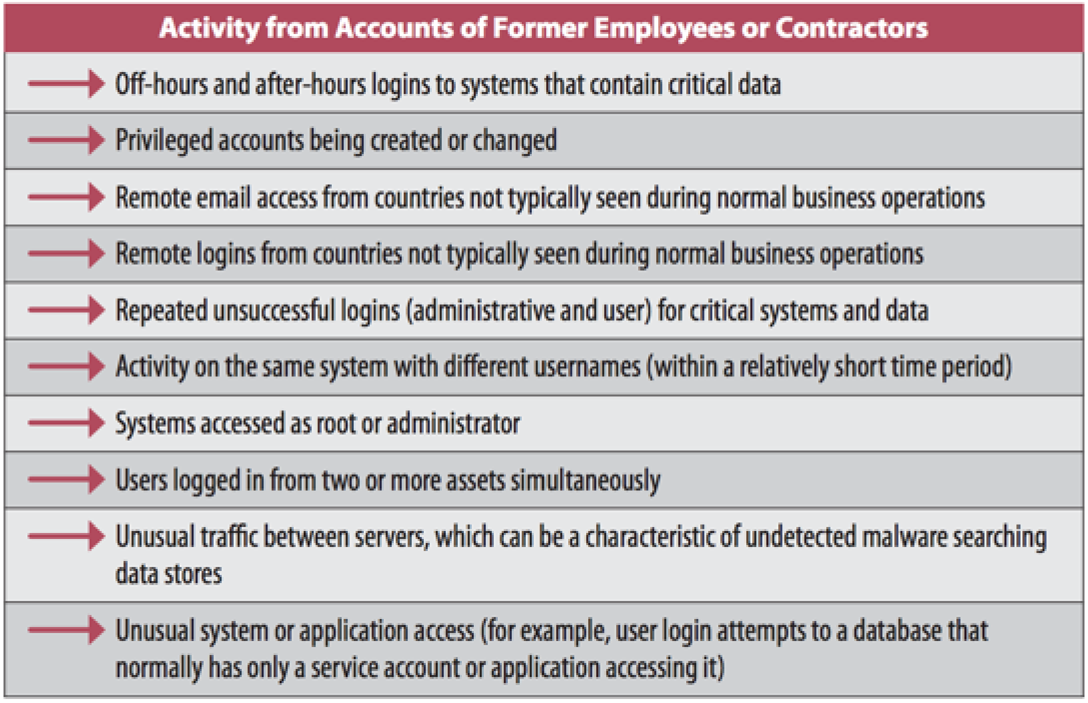
[95] Paquet, C. (2013). Network Security Concepts and Policies. CISCO. Retrieved from http://www.ciscopress.com/articles/article.asp?p=1998559&seqNum=2

[96] Shackleford, D. (2016, February). Active Breach Detection: The Next-Generation Security Technology? SANS Institute. Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/active-breach-detection-next-generation-security-technology-36812.

[97] SANS Institute. Eliminating Blind Spots: A New Paradigm of Monitoring Response. Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/eliminating-blind-spots-paradigm-monitoring-response-36712

[98] Ibid. Page 4.

***Table 6 – Monitoring Personal activity***



| Activity from Accounts of Former Employees or Contractors |
|---|
| Off-hours and after-hours logins to systems that contain critical data |
| Privileged accounts being created or changed |
| Remote email access from countries not typically seen during normal business operations |
| Remote logins from countries not typically seen during normal business operations |
| Repeated unsuccessful logins (administrative and user) for critical systems and data |
| Activity on the same system with different usernames (within a relatively short time period) |
| Systems accessed as root or administrator |
| Users logged in from two or more assets simultaneously |
| Unusual traffic between servers, which can be a characteristic of undetected malware searching data stores |
| Unusual system or application access (for example, user login attempts to a database that normally has only a service account or application accessing it) |

*Source: Shackleford 2016, 6*

NIST's "Security and Privacy Controls for Federal Information Systems and Organizations" recommends similar measures.[99] User activity on networks should be monitored, with an eye towards building profiles of expected user behavior. Organizationally-defined atypical usage should be reported to the appropriate party for analysis. User privileges and access to systems should be routinely checked and updated, validating the need for such privileges.

[99] Joint Task Force Transformation Initiative. (2013). Security and Privacy Controls for Federal Information Systems and Organizations. National Institute of Standards and Technology. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

# 6. Conclusion

Data from recent reports suggests that cyber-crime is on the rise, with one survey positing a 19% increase between 2014 and 2015 in costs attributable to cyber-attacks on American firms.[100] The same study also made several key observations highlighting the scale of the problem. Three stand out: that all industries are targets for cybercrime, though to varying degrees; that detection is the most expensive internal activity, closely followed by recovery; and that cyber-attacks are costlier if not contained quickly. Both public and private sector entities rely on electronic systems more than ever before, and with that increased reliance comes greater vulnerability. In the civilian world, firms can only play defense and threats evolve rapidly. Cyber resilience is important, and growing more important each year.

As this report has attempted to demonstrate, guidance and best practices do exist. The SANS Institute in particular stands out as an accessible repository of timely, valuable research into the changing landscape of cyber-crime. Additionally, there exists a growing body of resources for cybersecurity professionals; NIST has published several whitepapers that are less accessible to laymen, but of high value in developing cyber resilience policy within an organization.

The matrix we presented in this report should help organizations better understand the metrics that need to be established to judge their progress in becoming cyber resilient. The GSISS combined with our supplementary questionnaire should help point the way toward assessing industry and sector-wide progress toward cyber resilience. Finally, the best practices that we have identified should give organizations a place to look to find models of cyber resilience for several of the most important metrics.

Unfortunately, as new technologies continue to change the way firms do business, new vulnerabilities emerge. The development of the Internet of Things increases the degree to which systems are interconnected; a security flaw in a smart thermostat could potentially expose an entire network to attacks. Guidance for these threats is still evolving, and will likely continue to change rapidly for the foreseeable future. Where gaps exist in our current matrix, further research is needed. Additionally, while publicly accessible data exists showing percentages of respondents (aggregated by industry and region), the underlying data itself is necessary for more nuanced analyses. Presently, the firms that collect data on threats are loathe to share data that would be useful in answering these questions.

Every year, security firms and academics create new resources that can help firms better address cyber resilience. Perhaps once the domain of only the largest, most web-centric firms, this topic is now a critical component of any large organization. In today's world, firms cannot ignore cyber resilience; much like accounting or human resources, it is a necessary component of

[100] Ponemon Institute. (2015). 2015 Cost of Cyber Crime Study: Global. Page 3. Retrieved from http://www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report/ See page 3.

running a successful organization. But as this paper has hopefully demonstrated, a proactive approach to countering evolving threats is possible for any organization.

# Appendix I

**Framework integrated with GSISS and Bloustein supplementary question matches:**

Notes:

- ‘No GSISS Match [Bloustein Question Label]’: No matches to GSISS, metric covered by Bloustein Supplementary Questionnaire
- ‘Matched to [GSISS Question Label]’: This metric can be matched to at least one specific response category within the GSISS.
- Complete GSISS questions, response option, and respective data for matched questions listed following the matrix.[101]
- Bloustein Supplementary Questionnaire follows the GSISS data.

| | *Plan & Prepare* | *Detect* | *Absorb* | *Recover from* | *Adapt to* |
|---|---|---|---|---|---|
| ***Physical*** | (1) Implement controls/sensors for critical assets [Bloustein Q2A1]<br>(2) Implement controls/sensors for critical services [Bloustein Q2A2]<br>(3) Assessment of network structure and interconnection to system components and to the environment [Bloustein Q2A3]<br>(4) Redundancy of critical physical infrastructure [Bloustein Q2A4] | (1) Monitor the physical environment to detect potential cybersecurity events [GSISS IQ1A1-A5]<br>(2) Monitor personnel activity to detect potential cybersecurity events [GSISS RQ1A4, A7] | (1) Signal the compromise of assets or services [Bloustein Q5A4]<br>(2) Use redundant assets to continue service [Bloustein Q5A5]<br>(3) Dedicate cyber resources to defend against attack [Bloustein Q5A8] | (1) Investigate and repair malfunctioning controls or sensors [Bloustein Q8A1]<br>(2) Assess service/asset damage [GSISS IQ3A1-A9; IQ4A1-A7]<br>(3) Assess distance to functional recovery [Bloustein Q8A2]<br>(4) Safely dispose of irreparable assets [Bloustein Q8A3] | (1) Review asset and service configuration in response to recent event [Bloustein Q8A4]<br>(2) Phase out obsolete assets and introduce new assets [Bloustein Q8A6] |

[101] Questions, Responses and Numeric Data are directly taken from PricewaterhouseCooper’s The Global State of Information Security Survey 2016 Data Explorer. Retrieved from http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/data-explorer.html

| | | | | | |
|---|---|---|---|---|---|
| | (5) Redundancy of data physically or logically separated from the network [Bloustein Q2A5]<br>(6) Protect data-in-transit [Bloustein Q2A6] | | | | |
| ***Information*** | (1) Inventory physical devices, systems, software platforms, and applications within the organization [Bloustein Q3A1]<br>(2) Map organizational communication and data flows [Bloustein Q3A2]<br>(3) Catalog external information systems [Bloustein Q3A3]<br>(4) Categorize assets and services based on sensitivity or resilience requirements [Bloustein Q6A1]<br>(5) Documentation of certifications, qualifications | (1) Detect malicious code [Bloustein Q5A2]<br>(2) Detect unauthorized mobile code [Bloustein Q5A3]<br>(3) Monitor external service provider activity to detect potential cybersecurity events [GSISS IQ1A3-A5; SQ1A3] | (1) Observe sensors for critical services and assets [GSISS RQ1A2, A7]<br>(2) Effectively and efficiently transmit relevant data to responsible stakeholders/ decision makers [GSISS SQ3A2, A3]<br>(3) Document, implement, and review audit/log records in accordance with policy [Bloustein Q5A13] | (1) Log events and sensors during event [GSISS RQ1A2]<br>(2) Review and compare systems before and after the event [GSISS IQ1A1-A9] | (1) Document incident's impact and cause [GSISS IQ2A1-A14; IQ3A1-A7]<br>(2) Document time between problem and discovery/discovery and recovery [Bloustein Q8A7]<br>(3) Anticipate future system states post-recovery [Bloustein Q8A8]<br>(4) Document point of entry (attack) [Bloustein Q8A9]<br>(5) Categorize incidents consistent with response plans [Bloustein Q6A3]<br>(6) Continuously improve protection processes [Bloustein Q6A4] |

|  |  |  |  |  |  |
|---|---|---|---|---|---|
|  | and pedigree of critical hardware and/or software providers [GSISS SQ1A3]<br>(6) Prepare plans for storage and containment of classified or sensitive information [Bloustein Q6A2]<br>(7) Identify external system dependencies [Bloustein Q3A4]<br>(8) Identify internal system dependencies [Bloustein Q3A5] |  |  |  |  |
| ***Cognitive*** | (1) Anticipate and plan for system states and events [GSISS SQ1A1; LQ3A1, A2]<br>(2) Understand performance trade-offs of organizational goals [GSISS LQ2A4]<br>(3) Scenario-based cyber wargaming [GSISS SQ2A1]<br>(4) Include cybersecurity in human resources practices [GSISS SQ2A2; LQ1A7] | (1) Analyze detected events to understand attack targets and methods [GSISS IQ2A1-A14; SQ1A5, A6]<br>(2) Aggregate and correlate event data from multiple sources and sensors [Bloustein Q5A9]<br>(3) Determine impact of events [GSISS IQ3A1-A9; IQ4A1-A7] | (1) Use a decision making protocol or aid to determine when event can be considered ‘‘contained’’ [Bloustein Q5A14]<br>(2) Determine if mission can continue [Bloustein Q5A7]<br>(3) Focus effort on identified critical assets and services [Bloustein Q5A10]<br>(4) Utilize | (1) Review critical points of physical and information failure in order to make informed decisions [Bloustein Q8A5]<br>(2) Establish decision making protocols or aids to select recovery options [GSISS SQ1A1] | (1) Review management response and decision making processes [Bloustein Q4A3]<br>(2) Determine motive of event (attack) [Bloustein Q8A10]<br>(3) Mitigate newly identified vulnerabilities or document as accepted risks [Bloustein Q6A5]<br>(4) Understand the impact of incidents [GSISS IQ3A1-A9; IQ4A1-A7] |

| | | | | | |
|---|---|---|---|---|---|
| | (5) Test response and recovery plans [GSISS LQ3A7] | (4) Establish incident alert thresholds [Bloustein Q5A1] | applicable plans for system state when available [Bloustein Q5A12] | | |
| ***Social*** | (1) Identify and coordinate with external entities that may influence or be influenced by internal cyber-attacks (establish point of contact) [GSISS RQ1A7; RQ4A5; RQ6A6]<br>(2) Educate/train employees about resilience and organization's resilience plan [GSISS LQ1A8; SQ1A2]<br>(3) Manage identities and credentials for authorized devices and users [GSISS RQ1A1, A5]<br>(4) Manage and protect physical and remote access to assets [Bloustein Q2A7]<br>(5) Prepare/establish resilience communications [Bloustein Q2A8]<br>(6) Establish a cyber-aware | (1) Define roles and responsibilities for detection to ensure accountability [Bloustein Q4A1]<br>(2) Communicate event detection information to appropriate parties [Bloustein Q5A6]<br>(3) Continuously improve detection processes [GSISS RQ2A5-A7] | (1) Locate and contact identified experts and resilience responsible personnel [Bloustein Q4A2]<br>(2) Protect communications and control networks [Bloustein Q5A11]<br>(3) Share effectiveness of protection technologies with appropriate parties [GSISS SQ3A2] | (1) Manage public relations and repair reputation after events [GSISS RQ4A5; RQ6A6]<br>(2) Communicate recovery activities to internal stakeholders and executive / management teams [GSISS LQ1A3-A5; RQ4A4]<br>(3) Determine liability for the organization [GSISS LQ2A2-A4] | (1) Evaluate employees response to event in order to determine preparedness and communications effectiveness [Bloustein Q4A4]<br>(2) Assign employees to critical areas that were previously overlooked [Bloustein Q4A5]<br>(3) Stay informed about latest threats and state of (the art protection methods/share with organization [GSISS RQ1A6; RQ2A1-A4]<br>(4) Voluntarily share information with external stakeholders to achieve broader cybersecurity situational awareness [GSISS SQ3A1; RQ1A6; RQ2A1-A4] |

| | | | | | |
|---|---|---|---|---|---|
| | culture [GSISS RQ6A2]<br>(7) Understand and manage legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations [GSISS RQ2A8; RQ5A5; RQ6A7] | | | | |

## Index for Matched Question Labels:

Notes:

- PwC divides its questions into four broad categories: Incidents, Safeguards, Leadership, and Results
- Label interpretation Example: “ICQ1A1-5” indicates “Incidents Question 1, Answers 1 to 5”
- Percentages in parentheses indicate the **% of respondents that chose the given option, from all industries in all regions**.

| *Incidents Q1* | *What is the number of security incidents detected in the past 12 months?* |
|---|---|
| IQ1A1 | 0 or none **(13.46%)** |
| IQ1A2 | 1-9 **(32.18%)** |
| IQ1A3 | 10-49 **(15.66%)** |
| IQ1A4 | 50 or more **(31.59%)** |
| IQ1A5 | Do not know **(7.1%)** |
| Incidents Q2 | *What was the estimated likely source of security incidents?* |
| IQ2A1 | Current employees **(33.56%)** |
| IQ2A2 | Former employees **(28.6%)** |
| IQ2A3 | Current service providers/consultants/contractors **(21.93%)** |
| IQ2A4 | Former service providers/consultants/contractors **(19.04%)** |
| IQ2A5 | Suppliers/business partners **(15.87%)** |
| IQ2A6 | Customers **(14.12%)** |
| IQ2A7 | Hackers **(22.59%)** |
| IQ2A8 | Organized crime **(17.86%)** |
| IQ2A9 | Activists/hacktivists **(16.7%)** |
| IQ2A10 | Competitors **(21.02%)** |
| IQ2A11 | Foreign entities and organizations **(13.07%)** |
| IQ2A12 | Foreign nation-states **(8.13%)** |
| IQ2A13 | Domestic intelligence service **(6.28%)** |

| | |
|---|---|
| IQ2A14 | Do not know **(8.69%)** |
| *Incidents Q3* | *How was your organization impacted by the security incidents?* |
| IQ3A1 | Customer records compromised **(38.27%)** |
| IQ3A2 | Employee records compromised **(33.25%)** |
| IQ3A3 | Loss or damage of internal records **(25.93%)** |
| IQ3A4 | Theft of “soft” intellectual property (e.g., processes, institutional knowledge, etc.) **(24.52%)** |
| IQ3A5 | Theft of “hard” intellectual property (e.g., strategic business plans, deal documents, sensitive financial documents, etc.) **(23.06%)** |
| IQ3A6 | Brand / reputation compromised **(21.74%)** |
| IQ3A7 | Loss of customers **(16.82%)** |
| IQ3A8 | Legal exposure/ lawsuit **(9.61%)** |
| IQ3A9 | Do now know **(11.19%)** |
| *Incidents Q4* | *Estimated total financial losses as a result of all security incidents (US dollars)* |
| IQ4A1 | $49,999 or less **(30.53%)** |
| IQ4A2 | $50,000 to $99,999 **(16.51%)** |
| IQ4A3 | $100,000 to $499,999 **(16.23%)** |
| IQ4A4 | $500,000 to $999,999 **(16.18%)** |
| IQ4A5 | $1 million to $9.9 million **(6.99%)** |
| IQ4A6 | $10 million or more **(10.25%)** |
| IQ4A7 | Do not know **(3.31%)** |
| *Safeguards Q1* | *Which security safeguards has your organization implemented?* |
| SQ1A1 | Have an overall security strategy **(57.67%)** |
| SQ1A2 | Have an employee security awareness and training program **(53.02%)** |
| SQ1A3 | Have security standards/baselines for third parties **(52.11%)** |
| SQ1A5 | Conduct threat assessments **(49.2%)** |

| | |
|---|---|
| SQ1A6 | Actively monitor/analyze security intelligence **(48.05%)** |
| *Safeguards Q2* | *What strategic initiatives has your organization's adopted to improve its security program?* |
| SQ2A1 | Risk-based security framework **(91.54%)** |
| *Safeguards Q3* | *What people-related processes has your company adopted to improve security?* |
| SQ3A1 | Formally collaborate with others in the industry **(64.72%)** |
| SQ3A2 | Have a senior executive who proactively communicates the importance of information security to the entire organization **(73.12%)** |
| SQ3A3 | Board actively participates in overall cybersecurity strategy **(45.09%)** |
| *Leadership Q1* | *Which of the following describes the role of your organization's CISO, CSO, or other senior information security executive?* |
| LQ1A3 | Collaborates with internal stakeholders to better understand business issues and needs **(36.22%)** |
| LQ1A4 | Communicates information security risks and strategies directly to executive leaders **(42.91%)** |
| LQ1A5 | Delivers regular (at least four times a year) information security risk updates to the Board of Directors **(34.77%)** |
| LQ1A7 | Has the authority necessary to adequately lead the information security program **(27.97%)** |
| LQ1A8 | Advocates for employee security training and awareness programs **(23.69%)** |
| *Leadership Q2* | *Which of the following statements describes the role of your organization's CEO in cybersecurity practices?* |
| LQ2A2 | Understands that cybersecurity is a top business risk **(42.83%)** |
| LQ2A3 | Supports sufficient funding and resources for the cybersecurity program **(38.45%)** |
| LQ2A4 | Understands the costs and benefits of the cybersecurity program **(38.52%)** |
| *Leadership Q3* | *In which of the following areas does your organization's Board of Directors actively participate?* |
| LQ3A1 | Overall security strategy **(45.09%)** |

| | |
|---|---|
| LQ3A3 | Security policies **(40.85%)** |
| LQ3A7 | Review of security and privacy testing **(19.48%)** |
| *Results Q1* | *Which of the following components of cloud-based security has your organization adopted?* |
| RQ1A1 | Advanced authentication (multifactor, biometrics, smartphone tokens) **(54.57%)** |
| RQ1A2 | Real-time monitoring and analytics **(55.87%)** |
| RQ1A4 | Threat intelligence **(45.56%)** |
| RQ1A5 | Identity and access management **(47.96%)** |
| RQ1A6 | Collaboration and information sharing **(34.52%)** |
| RQ1A7 | Detection and response capabilities **(32.99%)** |
| *Results Q2* | *What impact has collaboration with others had on your organization's security program?* |
| RQ2A1 | Share with and receive more actionable information from industry peers **(56.15%)** |
| RQ2A2 | Share with and receive more actionable information from Information Sharing and Analysis Centers (ISAC') **(45.78%)** |
| RQ2A3 | Share with and receive more actionable information from government entities **(39.87%)** |
| RQ2A4 | Share with and receive more actionable information from local and national law enforcement agencies **(37.38%)** |
| RQ2A5 | Improved threat intelligence and awareness **(41.9%)** |
| RQ2A6 | Receive more timely threat intelligence alerts **(34.52%)** |
| RQ2A7 | Detect more security incidents **(27.74%)** |
| RQ2A8 | Improved regulatory compliance **(21.43%)** |
| *Results Q4* | *What impact has the adoption of a risk-based framework had on your organization?* |
| RQ4A4 | Stakeholders better understand information security gaps and how to improve them **(37.09%)** |

| | |
|---|---|
| RQ4A5 | Improved internal and external collaboration and communications **(31.8%)** |
| *Results Q5* | *What impact has the use of advanced authentication technologies had on your organization?* |
| RQ5A5 | Improved Regulatory compliance **(37.65%)** |
| *Results Q6* | *In what areas have Board participation helped improve your organization's information security program?* |
| RQ6A2 | Encouraged an organizational culture of information security **(37.92%)** |
| RQ6A6 | Internal and external collaboration and communications **(27.17%)** |
| RQ6A7 | Regulatory compliance and risk disclosure **(25.92%)** |

## Bloustein Supplementary Questionnaire

Notes:

- This questionnaire was created specifically to fill in the gaps left by the GSISS. However, it is designed so that it could easily be integrated into the GSISS or it could be administered separately or on its own.
- Above many of the questions are a highlighted sentence that explains the skip logic. This means that these questions will only appear if the respondent has selected an related response earlier in the survey. For example, the skip logic for Question 2 is “Answer If Which security safeguards has your organization implemented? Have an overall security strategy Is Selected.” This means that the respondent will only be asked to answer Question 2 if they selected that their organization has an overall security strategy when answering Question 1.

Q1 Which security safeguards has your organization implemented? (Please check all that apply)

❑ Have an overall security strategy (1)
❑ Have an employee security awareness and training program (2)
❑ Have security standards/baselines for third parties (3)
❑ Have a CISO in charge of security (4)
❑ Conduct threat assessments (5)
❑ Actively monitor/analyze security intelligence (6)

Answer If Q1 Which security safeguards has your organization implemented? Have an overall security strategy Is Selected

Q2 Does your security strategy include any of the following preparations? (Please check all that apply)

❑ Implement controls/sensors for critical assets (1)
❑ Implement controls/sensors for critical services (2)
❑ Assess network structure and interconnection to system components and the environment (3)
❑ Create redundancy of critical physical infrastructure (4)
❑ Create redundancy of data, separated from the physical network (5)
❑ Protect data-in-transit (6)
❑ Manage and protect physical and remote access to assets (7)
❑ Formalized incident response plan or policies (8)

Answer If Q1 Which security safeguards has your organization implemented? Conduct threat assessments Is Selected

Q3 Do your threat assessments include any of the following data? (Please check all that apply)

❑ Inventory physical devices, systems, software platforms, and applications within the organization (1)
❑ Map organizational communication and data flows (2)
❑ Catalog external information systems (3)
❑ Identify external system dependencies (4)
❑ Identify internal system dependencies (5)

Q4 Has your organization implemented any of the following employee practices? (Please check all that apply)

- ❑ Defined roles and responsibilities for detection to ensure accountability (1)
- ❑ Prepare/establish resilience communications (2)
- ❑ Post-incident review of management response and decision-making processes (3)
- ❑ Evaluate employees' responses to incidents in order to determine preparedness and communications effectiveness (4)
- ❑ Assign employees to critical areas that have been previously overlooked (5)

Answer If Q2 Does your security strategy include any of the following preparations? Formalized incident response plan or policies Is Selected

Q5 Does your organization's incident response policies include any of the following? (Please check all that apply)

- ❑ Established incident alert thresholds (1)
- ❑ Detect unauthorized code (2)
- ❑ Detect malicious code (3)
- ❑ Signal compromise of assets or services (4)
- ❑ Use redundant assets to continue service (5)
- ❑ Communicate event detection information to appropriate parties (6)
- ❑ Determine if mission can continue (7)
- ❑ Dedicate cyber resources to defend against attack (8)
- ❑ Aggregate and correlate event data from multiple sources and sensors (9)
- ❑ Focused effort on identified critical assets and services (10)
- ❑ Protect communications and control networks (11)
- ❑ Utilize applicable plans for system state when available (12)
- ❑ Document, implement, and review audit/log records in accordance with policy (13)
- ❑ Utilized decision making protocol or aid to determine when an event can be considered "contained" (14)

Answer If Q1 Which security safeguards has your organization implemented? Have an overall security strategy Is Selected

Q6 Does your security strategy include any of the following processes? (Please check all that apply)

- ❑ Categorize assets and services based on sensitivity or resilience requirements (1)
- ❑ Prepare plans for storage and containment of classified or sensitive information (2)
- ❑ Categorization of incidents consistent with response plans (3)
- ❑ Continuously improve protection processes (4)
- ❑ Mitigate newly identified vulnerabilities or document as accepted risks (5)

Answer If Q2 Does your security strategy include any of the following preparations? Formalized incident response plan or policies Is Selected

Q7 Does your organization's incident response plan include post-incident policies?

- ○ Yes (1)
- ○ No (2)
- ○ Don't know (3)

Answer If Q7 Does your organization's incident response plan include post-incident policies? Yes Is Selected

Q8 Does your organization's post-incident response policies include any of the following? (Please check all that apply)

- ❏ Investigate and repair malfunctioning controls or sensors (1)
- ❏ Assess distance to functional recovery (2)
- ❏ Safely dispose of irreparable assets (3)
- ❏ Review asset and service configuration in response to the event (4)
- ❏ Review critical points of physical and information failure in order to make informed decisions (5)
- ❏ Phase out obsolete assets and introduce new assets (6)
- ❏ Document time between problem and discovery/discovery and recovery (7)
- ❏ Anticipate future system states post-recovery (8)
- ❏ Document point of entry (9)
- ❏ Determine motive of event (10)