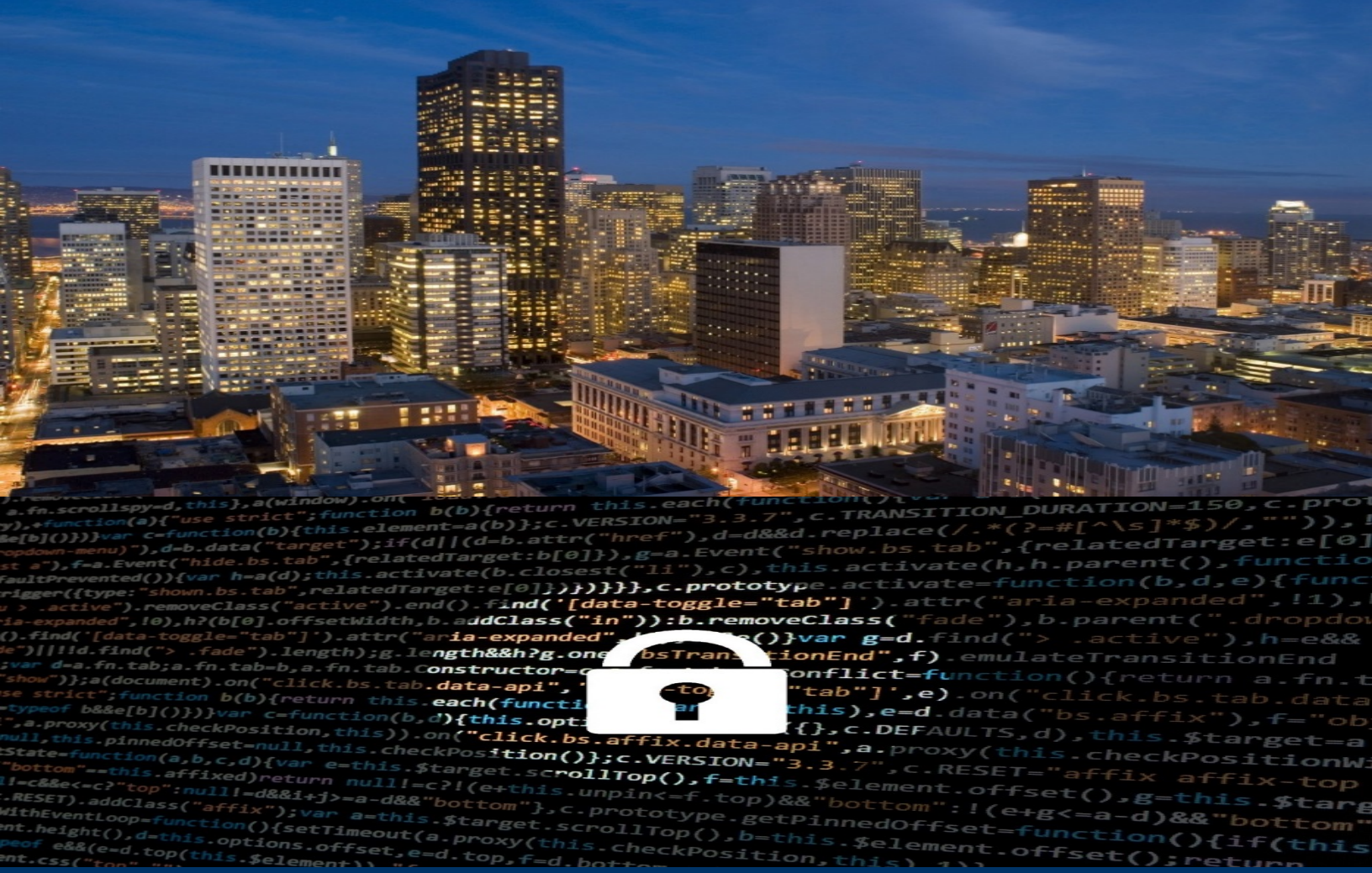


Cyber Resilience White Paper

An Information Technology Sector Perspective

March 2017

Homeland Security

IT SCC

IT GCC

Purpose and Scope

Even though current cyber solutions focus on defense in depth, these solutions do not fully protect organizations against cyber threats. Cyberattacks are increasingly common and system breaches continue to happen, costing organizations time and money due to disruption or data loss. In order to limit the degree of disruption caused by cyberattacks, many organizations are looking beyond the capabilities of cybersecurity tools and adopting holistic, risk-based approaches to understand how to respond and recover from disruptions by maintaining operational effectiveness for as long as possible. To make the enterprise more resilient against cyberattacks, organizations are also identifying internal and external system interdependencies. While awareness of the need for better cyber resilience continues to grow across industries and critical infrastructure, policies and best practices remain inconsistent and require a dedicated approach that addresses the needs of both industry and Federal organizations.

Information Technology (IT) Sector partners, represented by industry via the IT Sector Coordinating Council (SCC) and by government via the IT Sector Government Coordinating Council (GCC), established the IT Sector Resiliency Working Group (RWG) to study industry and government approaches to cyber resilience. The RWG, which consists of industry and government security experts, agreed to study cyber resilience by focusing on three key objectives:

- Establish a Common Definition of Cyber Resilience in the IT Sector: Develop a common definition of cyber resilience among industry and Federal representatives in the IT Sector, which can be applied to the needs of organizations in both the public and private sectors.
- Baseline Current Perspectives on Cyber Resilience: Develop a mutual understanding of public and private sector approaches to cyber resilience, and highlight the unique characteristics of industry and Federal efforts to improve cyber resilience.
- Identify Common Needs to Build a Cyber Resilient Community: Based on the commonalities between industry and Federal organizations, identify areas where IT Sector stakeholders can coordinate resilience activities.

This white paper represents the IT Sector RWG's perspectives and presents the group's initial analysis and discussion regarding the three objectives. Additionally, the RWG recommends that future IT Sector initiatives include those related to cyber resiliency, such as ways to standardize terminology, determine relevant metrics, and balance operational security with strategies to implement better cyber resilience.

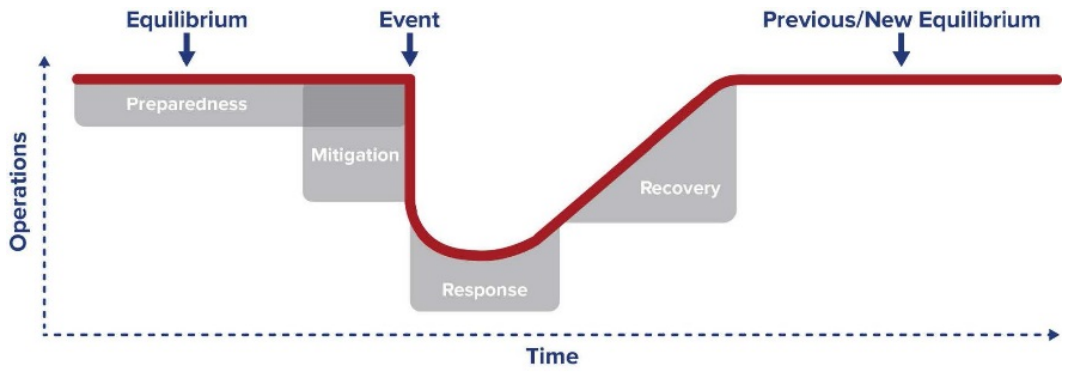
Establish a Common Definition of Cyber Resilience in the IT Sector

A common definition of cyber resilience that organizations can apply to business requirements, capability needs, and implementation strategies is instrumental in advancing cyber resilience in the IT Sector. To that end, the RWG reviewed several definitions of "cyber resilience" to identify one that would be most suited to accommodate the differences between public and private sector stakeholders. To establish that common baseline, the RWG agreed on the following definition of cyber resilience, as stated in the Ponemon Sullivan Privacy Report:

> *In the context of this research, we define cyber resilience as the capacity of an enterprise to maintain its core purpose and integrity in the face of cyberattacks. A cyber resilient enterprise is one that can prevent, detect, contain and recover from a plethora of serious threats against data, applications and IT infrastructure. A cyber resilient enterprise successfully aligns continuity management and disaster recovery with security operations in a holistic fashion.*[1]

In general, a primary goal of cyber resilience is to minimize the disruptive effects of cyber threats to business or mission operations. This goal includes the ability to withstand cyberattacks and the ability to prevent degradation to mission or business effectiveness. Figure 1 conceptually illustrates the objective of cyber resilience, which is to decrease the amount of time between an event and recovery, and limit the operational impact of the event.

Figure 1: Disruption Model for Resilience [2]



While the traditional cybersecurity model encompassing Confidentiality, Integrity, and Availability (CIA) is how many security decisions are made, the goals of cyber resilience focus on Anticipate, Withstand, Recover, and Evolve activities in addition to the CIA model.[3] Examining cybersecurity tools and goals through this lens is important to ensure cyber resilient solutions are developed and deployed to meet specific organizational needs. The goals of cyber resilience are to prevent attacks, detect vulnerabilities, contain consequences, and rapidly recover. A goal of cyber resiliency is to help organizations recover from attacks and mitigate vulnerabilities that make their systems susceptible to some form of cyber exploitation. The tools used to prevent attacks should be coupled with procedures to increase the likelihood that specific technical solutions are able to withstand cyberattacks. Organizations should

---

[1] Ponemon, Larry. "Learning to Thrive Against Threats."*Ponemonsullivanreport.com*. Ponemon Sullivan, 17 Sept. 2015. Web. 20 Nov. 2016. <http://www.ponemonsullivanreport.com/2015/09/17/learning-to-thrive-against-threats/>.
[2] Department of Homeland Security. *Infrastructure Resilience*. Digital image. *Regional Resiliency Assessment Program*. National Protection and Programs Directorate, n.d. Web. 12 Jan. 2017.
[3] Bodeau, Deborah, and Richard Graubart. "Cyber Resilience Metrics." (2016): n. pag. *Mitre Technical Papers.* The Mitre Corporation, May 2016. Web. 30 Jan. 2017.

implement these plans and procedures using the right combination of tools and methods to quickly recover essential operational functionality. They should continually evaluate whether they need to invest in new solutions based on lessons learned to ensure the organization is evolving effectively. The disruption model introduces an approach to evaluate cybersecurity tools by providing a framework for organizations to assess their ability to anticipate, withstand, recover, and evolve.

Baseline Current Perspectives on Cyber Resilience

Beyond establishing a common definition of cyber resilience, determining the specific aspects and considerations that matter to industry and Federal partners is paramount to establishing a common ground for both to work together. As stated in Presidential Policy Directive 21 (PPD-21), strengthening the security and resilience of critical infrastructure against both physical and cyber threats is a national priority. Because a majority of infrastructure assets used to support critical components are owned or operated by the private sector, improving cyber resilience across both industry and Federal systems requires a trusted relationship. Consistent with building trusted relationships, Presidential Policy Directive 41 (PPD-41) states that federal cyber response activities will be guided by several principles including, enabling restoration and recovery, shared responsibility, and respecting affected entities. PPD-41 applies to response activities during cyber incidents including cyber assets, and reflects the intersection point where government often assists critical infrastructure asset owners in the private sector. The importance of making cyber resilient systems to support critical infrastructure is further highlighted by Executive Order (EO) 13636, which recognizes that repeated cyber intrusions against critical infrastructure require new ways to ensure these systems focus not only on security but also on resilience.

Industry Perspective on Cyber Resilience

A resilient system generally holds the same meaning in any field. This concept suggests the anticipation of threats and an evolving response to them; a robust suppleness in the face of attack rather than static fragility. All systems fail to some degree; however, resilient systems endure despite setbacks. Resilience encompasses how the inevitable penetration of defensive perimeters is managed.[4] Although it is a shared national responsibility, many organizations differ in what they believe resilience must achieve – in the assets that must be protected, and how to measure the success of that protection.

Operational continuity is not necessarily the most important business driver in the private sector. For many companies, intellectual property theft is more concerning than business interruption. In fact, systems may never be targeted for disruption, except by nuisance hackers. Some sophisticated attackers do not want to shut things down. Rather, they want to access company assets, including proprietary information, through a working network. For such companies, the largest threat is a foreign nation or criminally-motivated espionage, and the threat is not hypothetical. Hard numbers are impossible to know, but estimates of annual U.S. losses to cyber espionage range from $250 billion[5] to $300 billion[6], with

---

[4] PPD-21 says "Critical infrastructure must be secure and able to withstand and rapidly recover from all hazards." United States. Executive Office of the President. *Presidential Policy Directive No. 21*. Washington, D.C.: Feb. 12, 2013. https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil. Accessed April 8, 2016.

[5] Rogin, Josh. "NSA Chief: Cybercrime constitutes the "greatest transfer of wealth in history." *The Cable*. Foreign Policy Magazine, July 9, 2012. http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/. Accessed April 8, 2016.

[6] The Commission on the Theft of American Intellectual Property. *The Report of the Commission on the Theft of American Intellectual Property*. Washington, D.C.: May 20, 2013.

some estimates reaching as high as one trillion dollars each year.[7] Traditional cybersecurity solutions and strategies focus on minimizing an organization's attack surface and implementing as many deterrents as possible against intrusions or other types of cyberattacks. Unfortunately, these approaches are unable to stay current with the evolving cyber threat landscape, and industry has been forced to create additional strategies that assure business processes are able to continue in the face of a compromised system. These strategies can manifest in several different ways, including techniques such as misinformation and honeypots, which can cause attackers to make incorrect assumptions and waste malware payloads against non-critical systems. Failures by industry companies to incorporate cyber resilient strategies have led to a number of high visibility data breaches across multiple critical infrastructure sectors.

When the imperative is data protection, the set of metrics for measuring a resilient system is quite different. Without trying to be comprehensive, they include situational awareness: the dwell time of adversaries on a breached network, agility in integrating new threat data, and updating defenses. Even in critical infrastructure sectors operated by the private sector where operational continuity is a chief goal, reliability is one metric among many. Cost-effectiveness, for example, looms over any major investment decision, including cyber resilience.[8] Sometimes the cost of remediating or removing footholds into systems is higher than the value of the compromised system. Additionally, these types of remediation activities could cause disruptions to other business systems or impair existing law enforcement activities in the event of criminal investigations. All of these factors need to be evaluated in order for the proper metrics to be extrapolated in useful ways. Not included in the list of primary data protection metrics are time to full system restoration, recovery point objective, or recovery time objective. In some cases, speed can exacerbate the problem rather than solve it. Purging the attacker often requires determining the extent of the penetration, which takes time to observe. Acting too quickly can eradicate signs of compromise risks, leaving undetected pathways back into the system.

Many organizations that make up critical infrastructure are unaware of their newfound status. The Internet is still a relatively new technology and discovery of its full effects is not yet complete. The highly publicized breaches of large retailers reinforce the realization of the interconnected nature of organizations across critical infrastructure sectors. Traditional risk management of domestic operations does not take into account the possibility of a foreign attack bent on sabotage of critical infrastructure. Until recent years, the Atlantic and Pacific oceans combined with U.S. military power might have made such an attack inconceivable. Understanding how an organization and its supply chain partners are part of a larger ecosystem that all organizations rely upon to operate business functions is a new concept for many companies that are becoming more aware of how third-party systems depend on cyber infrastructure. This awareness increases understanding around the vulnerabilities to cyber risks and how those risks could impact supply chain operations.

Concerning data protection and operational continuity, closing the gap from a national security perspective is often treated as a question of greater awareness. Educating senior executives in government and industry about cyber risk is an ongoing process that is of the utmost importance. Education, however, cannot eradicate cost-effectiveness as a consideration to the extent the government may deem necessary

---

[7] United States. The White House. *Cyberspace Policy Review*. By White House. N.p.: n.p., 2009. Print.

[8] As an illustration of how cost can affect resilience, consider the approach of Dominion Virginia Power to its current project of burying electricity delivery cables. Putting underground the entire customer delivery system would be a huge increase in resilience. But that's not what the utility is doing. Instead, the company is taking a risk management approach by replacing main feeder lines and the most outage-prone tap lines with underground cables. Dominion argues that this is the only viable way forward. "No interruptions, no matter what" would cost Virginia ratepayers an untenable amount of $3,000 annually per customer, totaling $83.3 billion in 2005 dollars for the entire project.

for the protection of critical infrastructure. This education can demonstrate how resilient strategies can lead to cost avoidance and aid in an organization's business activities (e.g., mergers, divestitures, acquisitions, etc.). Currently, guidance around cyber resilience is developed for two key audiences, executive decision makers[9] and technical solutions architects[10]. Both audiences focus on different aspects of cyber resilience but need to be in sync when making decisions based on available metrics.

National security is, by definition, a main concern of the Federal Government. Absent a total nationalization of the economy, achieving operational continuity for national security purposes is a task the U.S. Government must achieve through collaboration with the private sector. Where the government's goals for resilience overlap with private sector operations is a space for mechanisms such as incentives and information sharing, particularly where there is a divide between industry's economic goals and the government's national security interests.

Federal Perspectives on Cyber Resilience

The U.S. Government officially recognized resilience as a goal in its 2010 National Security Strategy, which stated that resilience represents the ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruptive events. Acknowledging resilience in national strategy demonstrates the Federal Government's commitment to improving overall cyber resilience, but each Federal agency is often responsible for developing its own policies, processes, and technologies to accomplish its mission. With varying degrees of awareness of cyber resilience and the potential negative impacts of cyber threats among departments and agencies, DHS, as the IT Sector-Specific Agency (SSA), plans to meet across the critical infrastructure community to collect and distribute methods for improving cyber resilience. DHS recognized resilience in the 2014 Quadrennial Homeland Security Review (QHSR), which established a series of goals and objectives in the areas of critical infrastructure, cyberspace, global movement, and supply chain systems. One of the five QHSR missions is devoted to ensuring resilience through hazard mitigation, enhanced preparedness, emergency response, and rapid recovery.

DHS defines resiliency as the ability to adapt to changing conditions, and withstand and rapidly recover from disruption.[11] Resilience is a shared responsibility, whether it is resilience towards acts of terrorism, natural disasters, or cyberattacks. In accordance with the National Infrastructure Protection Plan, the Federal Government, especially DHS, is actively involved with resilience planning and recovery efforts across critical infrastructure sectors and acknowledges that priorities vary across agencies and mission spaces. While the goal of cybersecurity has been to identify and prevent cyberattacks against an organization, more sophisticated attacks or previously unseen 'zero-day' attacks consistently outpace cybersecurity solutions. Across the government, different techniques have been used to lower the risk of attacks, such as the Trusted Internet Connections (TIC) initiative which limits the attack surface of publicly-exposed cyber infrastructure and focuses on bolstering defenses at a smaller number of key ingress-egress points between government networks and the public Internet. However, because some attacks continue to be successful, the government has been working with Internet service providers and IT

---

[9] The Mitre Corporation. "Guidance for Executives." *Industry Perspective on Cyber Resiliency*. The Mitre Corporation, 2015. Web. 30 Jan. 2017. <http://www2.mitre.org/public/industry-perspective/guidance-executives.html>.
[10] The Mitre Corporation. "Guidance for Architects." *Industry Perspective on Cyber Resiliency*. The Mitre Corporation, 2015. Web. 30 Jan. 2017. < http://www2.mitre.org/public/industry-perspective/guidance-architects.htm >.
[11] DHS. "Resilience." *Resilience | Homeland Security*. Department of Homeland Security, 10 Sept. 2015. Web. 30 Jan. 2017. <https://www.dhs.gov/topic/resilience>.

vendors to build redundant systems and networks capable of operating in the face of persistent attacks. Despite improvements, additional cyber resilience methods and capabilities are needed to ensure the government is able to maintain mission integrity and provide necessary services to the public.

The public expectation of the government to ensure availability of public infrastructure and government services remains one of the most significant perspectives from Federal stakeholders. While private sector companies may choose to disconnect networks and systems that are being attacked, often times, government systems and networks must remain accessible to ensure public confidence, availability of critical services, and continuity of operations. This is not to say that the private sector's services are less important than those of the government; it is to say that the private sector and the government have different considerations regarding the consequences of a cyberattack. Industry's chief concern is often based on competitive advantage or financial considerations, while Federal Government concerns must take into account networks and data supporting sensitive or critical missions and operations. PPD-41 mentioned above was designed specifically to clarify the Federal Government's lines of efforts in responding to cybersecurity incidents while recognizing that the "private sector and government agencies have a shared vital interest in protecting the Nation from malicious cyber activity and managing cyber incidents and their consequences."

Recently, some of the most significant and highly publicized types of cyberattacks affecting the Federal Government have been system breaches which led to the theft of sensitive data, such as the one that stole background investigation data from the Office of Personnel Management for millions of staff with security clearances.[12] The Federal Government is concerned with the unique detection challenges posed by both active cyberattacks (e.g., Denial of Service) and data breaches. A cyberattack aimed at disrupting or denying access to online services is very obvious, while a data breach can go undetected for a considerable amount of time. Following any breach, dwell time is a key metric organizations use to determine the potential damage caused by lost or compromised data. Although detection time has improved, the median time from compromise to discovery in 2015 was still 146 days.[13] This length of time undermines the ability of an organization to understand when their mission has been potentially compromised, which is an important aspect the Federal Government requires to achieve an acceptable level of cyber resilience.

Within DHS, the Office of Cybersecurity & Communications (CS&C) regards cyber resilience of particular importance. CS&C's National Cybersecurity and Communications Integration Center (NCCIC) operates at the intersection of the government, private sector, and international network defense communities. The NCCIC, as one example of where private and public sector partners intersect, works with government and industry stakeholders to better understand the drivers for cyber resilience and identifies opportunities to share relevant information. As part of this mission, efforts like Automated Information Sharing (AIS) allow public and private sector stakeholders to share indicators of compromise (IOCs) in near-real time. The NCCIC also provides incident response capabilities and can deploy malware "hunt" teams to assist agencies and organizations in reducing the dwell time of malicious software. Additionally, CS&C also manages the Enhanced Cybersecurity Services (ECS) program. Through this voluntary public-private partnership, DHS is able to share timely, actionable, cyber threat information to help public and private entities protect their computer systems and networks against

[12] Office of Personnel Management. Cybersecurity Resource Center *Cybersecurity Incidents* Web. 7 Feb. 2017 <https://www.opm.gov/cybersecurity/cybersecurity-incidents/>

[13] Mandiant. "Mandiant Trends: 2016." *M-Trends*. FireEye, 2016. Web. 30 Jan. 2017. <https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/Infographic-mtrends2016.pdf>.

unauthorized access, exploitation, and data exfiltration. CS&C contributes to Federal resilience through the National Cybersecurity Protection Systems (NCPS), which provides intrusion detection, advanced analytics, information sharing, and intrusion prevention capabilities. This range of capabilities is further enhanced by CS&C's Continuous Diagnostics and Mitigation (CDM) program, which is intended to provide Federal departments and agencies with the ability to continually identify real-time cyberattacks and intrusions. The CDM acquisition vehicles are available to State, Local, Tribal, and Territorial (SLTT) government entities, as well. These types of sharing efforts are intended to improve the cyber resilience of all participating stakeholders, but are only part of the solution.

Identifying Commonalities and Differences between Federal and Industry Perspectives

Commonalities

Tools and Infrastructure: Systems, network infrastructure, network engineering, and off-the-shelf commercial products provide a predictable range of capabilities used to protect cyber assets regardless of their deployment in the private or public sector. The Federal Government often relies on private sector companies to deliver services to the public. The government frequently purchases tools and infrastructure used to run its systems and networks directly from private sector vendors; therefore, there is an inherent value in sharing best practices, known vulnerabilities, and effective architectures among all stakeholders. Because everyone is using the similar tools and infrastructures, mitigation strategies against cyber threats are, by extension, similar. Staff expertise in operations, protection, and reconstitution is based on similar industry standards and certifications. Even though Federal and industry stakeholders have different fault tolerances, they value the same knowledge, expertise, and skillsets.

Desire to Improve Resilience through Partnerships and Information Sharing: Improved data protection and the ability to keep critical systems operational in the face of an attack is a common goal for both the government and the private sector. Although the drivers of that common goal differ between the government and industry, securing critical infrastructure will require cooperation among IT sector stakeholders. The private sector recognizes the extensive efforts and partnerships undertaken by the Federal Government, and recognizes that DHS works with the owners and operators across 16 critical infrastructure sectors and SLTT governments to secure critical infrastructure and maintain national essential functions. At the same time, the private sector owns and operates a significant majority of critical infrastructure and while CS&C can encourage adoption of security frameworks and resilience strategies, it cannot mandate their adoption.[14] Sharing key metrics and data points is in the best interest of all stakeholders as long as it can be done in a secure and relevant way, and the better everyone understands the factors that go into decision making, the better the quality of information that is shared.

Executive-level Training and Staff Awareness: Leaders at the top of Federal Agencies, as well as private sector companies, have been forced to consider the negative impacts caused by cyberattacks, but still lack the full set of information and understanding to make the types of organizational changes needed to effectively combat attacks. Leaders responsible for protecting mission and/or business interests need to be better informed of the latest threats and mitigation strategies. Additionally, training is not only important for leaders but for all of those tasked with risk management roles at the organization. This

[14] The Office of the Director of National Intelligence puts the ownership figure at 85 percent. United States. Office of the Director of National Intelligence, Information Sharing Environment. *Critical Infrastructure and Key* Resources. Washington, D.C. https://www.ise.gov/mission-partners/critical-infrastructure-and-key-resources. Accessed April 8, 2016.

comprehensive approach to training all staff is critical for turning information sharing into action that prevents disruption.

Difference

Acceptable Risk and Economics: Although the Federal Government and private sector both desire resilient cyber infrastructure, their drivers differ. A primary consideration for the government is continuity of operations and maintaining national essential functions. Generally, the government's risk tolerance is very low for those areas deemed mission-critical, and those areas are funded accordingly. Industry, on the other hand, must pit operational continuity against cost effectiveness and return on investment metrics. The private sector's risk tolerance is rooted in economic considerations and may be higher if the individual organization determines that the mitigation cost outweighs the potential risk of damage done by a cyberattack. Acknowledging these differences is no disservice to either the public or private sectors. By definition, the Federal Government must consider non-economic values, such as national and homeland security. The most recent National Infrastructure Protection Plan even states that, "Government may have a lower tolerance for security risk than a commercial entity."[15]

Adaptability to Changing Conditions: The Federal Government typically requires long-term planning when investing in IT infrastructure. Often, when decisions for investment are made, by the time they are implemented there are several additional security considerations that did not exist at the time the decision was made. Therefore, the government is frequently slower to adapt to new types of attacks. The private sector is typically able to respond more quickly to cyber threats and can implement new tools or network infrastructure more nimbly. However, a majority of organizations do not have the necessary platform to consistently share new solutions and mitigation strategies across critical infrastructure or within the supply chain ecosystem. These differences make up the primary reason why an improved partnership around cyber resilience would benefit everyone; industry is able to keep up with best practices while the Federal Government is better suited for disseminating that information across the critical infrastructure sectors.

[15] United States. Department of Homeland Security. *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience.* Washington: 2013. https://www.dhs.gov/national-infrastructure-protection-plan. Accessed April 1, 2016.

Conclusion and Recommendations

Based on the RWG's initial exploration of the topic, cyber resilience will continue to be an important part of ensuring continuity of operations for the both the Federal Government and industry. This baseline view of cyber resilience could serve as the basis for additional discussion and information sharing on the policies, processes, and technologies that should be developed across the cybersecurity industry to address cyber resilience best practices. Using the disruption model of resilience, the government and industry can examine cyber resilience information to determine how it makes the time delta from attack to recovery as short as possible. Although many of the government's most critical functions and missions are supported by redundant systems, networks, and infrastructure, many functions are supported by infrastructure that the government does not own or operate. In cases where the private sector owns and operates the infrastructure, the priority may be on limiting exfiltration of intellectual property and proprietary information. When a private sector entity is the target of an attack, the primary goal may not be time to recovery, but minimizing theft of proprietary information.

The private sector's acceptance, transfer, or avoidance of risk based on profit differs from the government's risk approach, which is based on mission continuity and maintaining national essential functions. With these observations, the IT Sector RWG makes the following two recommendations.

Recommendation One: The government should develop mechanisms to incentivize information sharing and support resilience in the private sector, particularly where there is a divide between industry's economic goals and government's national security interests. To encourage resilience in the private sector, the government should develop economic incentives for mission-critical private sector organizations that adopt resilience best practices.

Recommendation Two: The IT Sector should develop a set of common metrics that can be used to better measure the effectiveness of cyber resilience strategies. Additionally, explore the appropriate set of specific terms and metrics that will allow vendors to understand requirements and generate more resilient products and services, including identifying efforts in the Federal Government (e.g., NIST) to generate standards for cyber resilience. This working group could also add value by capturing stakeholder needs and providing feedback to standards organizations and solutions vendors.

---

[i] Cover image sourced from http://stockmedia.cc.

[ii] The Department of Homeland Security does not endorse any commercial product, service, or enterprise.