Cyber Resilience and Response

2018 Public-Private Analytic Exchange Program

In today's cyber threat environment, organizations are complementing their cybersecurity posture with cyber resilience to maintain operations in the face of adversarial activity.

Although the cyber response actions incorporated into cyber resilience models are better understood, the Cyber Resilience and Response (CRR) team discovered that little is known across the public and private sectors about the specific techniques and design principles associated with implementing cyber resilience.

To raise awareness and educate multiple audiences, the CRR team developed this report on cyber resilience techniques and design principles, focused specifically on the capability to withstand adversarial activity. The report centers around the recently released "cyber resiliency" definition from the National Institute of Standards and Technology (NIST), and uses published reports, team interviews, and survey responses to support its key takeaways.

Cyber Resilience and Response Team Members:

Name	Organization
Peter M. (Champion)	Federal Bureau of Investigation
Rachel Bruenjes	U.S. Department of Homeland Security
Michael Cohen	The MITRE Corporation
Jade Freeman	U.S. Department of Homeland Security
Ryne Graf	Midwest Operating Engineers
Moh Kilani	Truman National Security Project
Caroline O'Leary	Brookfield Property Partners
Christopher Pashley	U.S. Customs and Border Protection
John Ryan	Augusta University
Genevieve Shannon	McDonald's Corporation
Grayson Walters	SAIC
Thomas Wills	American Express

Table of Contents

Abstract	**1**
Team Members	**2**
Contents	**3**
Key Takeaways	**4**
Scope	**4**
Definition of Cyber Resilience	**5**
Evolving Concepts of Cyber Resilience	**5**
Why Cyber Resilience?	**6**
The Value Proposition for Cyber Resilience	**7**
NIST's Cyber Resiliency Publication	**8**
NIST's Cyber Resiliency Techniques and Design Principles	**9**
Growing Cyber-Physical Threats against Critical Systems	**12**
Findings From Research and Case Studies	**15**
Gaps and Challenges in Current Cyber Resilience Practices	**22**
Cyber-Physical Critical Sector Partnership	**28**
Policy Recommendations	**34**
Appendix A	**37**

Key Takeaways

Understanding the ideal state of cyber resilience is imperative, but it will remain a lofty goal in the face of Advanced Persistent Threat (APT)[1] if we cannot move past these age-old realities:

- Technology refresh cycles are too long.
- Critical infrastructure is locked in to a limited number of vendors.
- Proprietary code "outlives" its developer.
- Vendors aren't always designing with security in mind.

Scope

The Cyber Resilience and Response (CRR) team has prepared this paper in association with the Department of Homeland Security (DHS) Analyst Exchange Program (AEP). The team has spent six months gathering relevant background and data from publications, open-source writing, interviews, and panel discussions. The team additionally conducted in-person interviews with cybersecurity experts from a variety of industries in Seattle, Washington. These industries included, but were not limited to, aviation, computer software, energy, and state/local government entities. Several representatives from companies were also engaged during the team's weekly meetings to provide an overview of their cyber operations, as well as an insight into their industry's cyber resiliency-related concerns.

The team additionally developed and conducted a survey for relevant companies to better understand their concerns and outlook for the future, and opportunities that could be created between the public and private sectors. This survey allowed the team to gather feedback from those companies that could not meet in-person, or who may not have spoken candidly in-person.

[1] Per NIST SP 800-39: *An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception).*

Definition of Cyber Resilience

Over time, the term *resilience* has been defined and interpreted in numerous ways, depending on the context in which it is used. The National Academy of Sciences (NAS) provided a definition of resilience based on the extant literature and consistent with the international disaster policy community, U.S. governmental agency definitions, and National Research Council (NRC) as "the ability to prepare and plan for, absorb, recover from, and more successfully adapt to adverse events." [2] In *Presidential Decision Directive 21: Critical Infrastructure Security and Resilience (PDD-21),* resilience was defined as the "ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions.

These extant definitions are linked to the key features, *adapting, preparing, withstanding, and recovering*. These features are described as the following:

> ***Adapt***: Change in management approach or adjusting response strategies in advance to disruptive events and future threats, enabled by learning from previous disruptions.
>
> ***Prepare***: Predict, anticipate and plan for potential threats or stressors and identify and monitor critical functions of the systems at risks.
>
> ***Withstand***: Maintain business operations without performance degradation or loss of functionalities under the hazardous conditions.
>
> ***Recover***: Rebound or restore from an adverse event to full business operations, performance, and functionalities.

In this paper, the CRR team defines resilience in cyberspace as:

> Resilience in cyberspace: The ability to *adapt* to changing conditions and *prepare* for, *withstand*, and rapidly *recover* from disruption.[3]

Evolving Concepts of Cyber Resilience

The concept of cyber resilience first rose to prominence on the national level in 2012, after the

[2] National Research Council. 2012. Disaster Resilience: A National Imperative. Washington, DC: The National Academies Press. https://doi.org/10.17226/13457.
[3] Adopted from March 2018 Draft version of NIST Publication NIST SP 800-160, Volume 2

issuance of *Presidential Decision Directive 21 (PDD-21).* Although PDD-21 launched the topic into highly visible discussions, several organizations had been working on cyber resilience previously. In October 2011, the Carnegie Mellon Computer Emergency Response Team (CERT) published its CERT Resilience Management Model (CERT-RMM) v1.1. Furthermore, in 2010, The MITRE Corporation published its Cyber Resilience Engineering Framework (CREF). Since that time, additional public and private organizations have been working to evolve the concept of cyber resilience. It should be noted that the focus of our research is on the concept of *withstand* of cyber resilience.

Why Cyber Resilience?

Cyber resilience is important for mission-essential systems that support our national security, homeland security, essential government services, and the critical infrastructure that supports the nation's economy. Cyber resiliency is that attribute of a system that assures it continues to perform its mission-essential functions even when under cyber-attack. For services that are mission-essential, or that require high or uninterrupted availability, cyber resiliency should be built into the design of systems that provide or support those services.

Cyber resiliency is particularly important for a subset of critical infrastructures known as *lifeline sectors* or *strategic infrastructures*. A 2015 NIAC Report "identified [….] five sectors or sub-sectors to be core members of the [Strategic Infrastructure Executive] Council because of their centrality to the resilience of most of the other sectors and their national security implications when disrupted:"[4]

- Electricity
- Water
- Transportation
- Communications
- Financial Services

Although ideally, each strategic sector or sub-sector would be resilient, not every IT and OT system within them will be because it would be cost-prohibitive. The mission-essential systems within those sectors or sub-sectors, however, should be prioritized when developing cyber resilience, as these systems would be favored targets in a coordinated cyber-attack on the United States.[5]

[4] NIAC, *Executive Collaboration for the Nation's Strategic Infrastructure Final Report and Recommendations*. March 20, 2015.
[5] DHS/I&A. (U) Russian Targeted Cyber Operations Against US Critical Infrastructure. 14 May 2018.

In NIST's 2018 publication subtitled, *Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems*, the importance of cyber resilience is described as follows:

> For the nation to survive and flourish in the 21st century where hostile actors in cyberspace are assumed and IT will continue to dominate every aspect of our lives, we must develop trustworthy, secure IT components, services, and systems that are cyber resilient.[6]

Cyber resilient systems are those systems that need security measures or safeguards to be "built-in" as a foundational part of the system architecture and design. Moreover, these systems display a high level of resiliency; the systems can withstand a cyber-attack, and can continue to operate even in a degraded or debilitated state, further carrying out mission-essential functions.

The Value Proposition for Cyber Resilience

Cyber resiliency has value at both the enterprise and at the societal level. How to quantify its value in economic terms at both levels is described below.

Cyber Resiliency Value at the Enterprise Level

Deploying and maintaining cyber resiliency as described, for example, in NIST's SP 800-160 Vol.2, costs more than deploying and maintaining traditional cybersecurity measures. That is due to the inherent complexity and dynamic nature of cyber resiliency techniques (Appendix D of the NIST publication). Despite the increased deployment and maintenance costs, the CRR Team believes that on a lifecycle-cost basis, cyber resiliency costs the enterprise less than traditional cybersecurity measures. The primary reason for this belief is the ability of cyber resiliency to withstand cyber-attacks and thereby avoid enterprise downtime and lost revenues.

A sophisticated cyber-attack intending to shut down a critical infrastructure enterprise could shut-down the enterprise for several weeks, rather than just several days, as is typically the case with less-sophisticated cyber-attacks.[7] Calculating the cost of lost revenue and possible customer abandonment from a several week outage, compared to the cost of implementing cyber resiliency design principles and techniques, is what determines whether cyber resiliency is cost effective for the enterprise. Taking a lifecycle approach, one would assume that a critical infrastructure enterprise would be hit with a sophisticated cyber-attack at least once every 5 years and would be down for several weeks. If the loss from shutdown exceeds the cost of the preventive cyber resiliency measures, then cyber resiliency is a good investment. In other words, if the cost of

[6] *Cyber Resiliency Considerations for the Engineering of Trustworthy Secure System, NIST SP 800-160, Vol.2, March 2018*
[7] Council on Economic Advisors, *The Cost of Malicious Cyber Activity to the U.S. Economy.* 2018. P. 13.

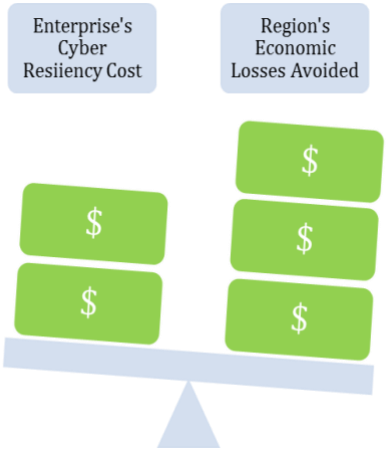
implementing cyber resiliency measures is less than the losses avoided by investing in the resilience measures, the enterprise business case can be made.

Cyber Resiliency Value at the Societal Level

Even if a cyber resilience-specific investment does not yield a net economic benefit at the enterprise level, it may still yield an economic benefit at the societal level. Critical Infrastructure firms who know that a shutdown of their enterprise would have ripple effects throughout the region in which they are located should be able to make that case to their local and State Government, as well as to the Federal Government. Critical Infrastructure sectors that have been identified as strategic infrastructures by NIAC have a high likelihood to yield net economic benefits at the regional level, since all other firms depend upon them.

When an enterprise in any of these strategic infrastructures finds that it cannot make the business case for cyber resiliency for itself yet recognizes how dependent other enterprises are upon them, they are able to make the business case at the regional societal level.

The CRR Team has found that one of the best tools to help make that case is generically referred to as Computable General Equilibrium (CGE) modeling.[8] A CGE model will not only compute the direct economic impact on the sector under which the firm falls, but will also compute the regional economic impact on all firms in the region that depend on them. The model output is a loss of regional GDP and Consumer Surplus. That loss can be compared with the cost of implementing cyber resiliency at the firm to determine if there is a net economic benefit to the region (*See Figure* 1). If there is, the firm should provide its CGE analysis to the local, State, and Federal Government to demonstrate that, on a regional basis, cyber resiliency is a worthwhile investment and that those governments should cost-share with them. For the Federal Government, the appropriate departments to appeal to would be DHS, which is the lead for PPD-21 implementation, and the firm's Sector Specific Agency (e.g., DOE for the Electric Sub Sector).



The Regional Societal Economic Business Case

NIST's Cyber Resiliency Publication

[8] Glyn Wittwer (Editor). *Multi-regional Dynamic General Equilibrium Modeling of the U.S. Economy: USAGE-TERM Development and Applications*. 1st ed. 2017 Edition

A key point that differentiates cyber resiliency from cyber security is that cyber resiliency continues to function even after the adversary has penetrated the security perimeter of a network and has compromised cyber assets. Even at the later stages of the cyber kill chain, cyber resiliency can help to prevent the adversary gathering intelligence on, exfiltrating data from, or taking control of mission-essential systems. The many functions that cyber resiliency can serve post-compromise ("right of boom") are described in NIST SP 800-160, Vol. 2.[9]

NIST's publication can be viewed as a handbook for achieving cyber resiliency outcomes based on a system engineering perspective on system life cycle processes. It allows the experience and expertise of the organization to determine what is correct for its purpose. Organizations can select, adapt, and use some (or all) of the cyber resiliency constructs (i.e., goals, objectives, techniques, approaches, and design principles). Organizations can apply those constructs to the technical, operational, and threat environments for which systems need to be engineered. The cyber resiliency constructs can be used for new systems, system upgrades, or repurposed systems. These constructs can be employed at any stage of the system life-cycle. Organizations can take advantage of any system or software development methodology including, for example, waterfall, spiral, or agile. The tailorable nature of the engineering efforts and the life-cycle processes ensure that the systems resulting from the application of the cyber resiliency design principles are sufficient to protect stakeholders from suffering the unacceptable losses of their key assets and the associated economic and national security consequences.

NIST's Cyber Resiliency Techniques & Design Principles

The many things that can be done at the system-design stage as well as at the operation and maintenance stages are described in the NIST publication's sections 2.2.3 CYBER RESILIENCY TECHNIQUES AND APPROACHES and 2.2.4 CYBER RESILIENCY DESIGN PRINCIPLES. Those overviews sections are supported by detailed descriptions of the techniques and design principles in APPENDIX D CYBER RESILIENCY TECHNIQUES, APPENDIX F DESIGN PRINCIPLES, and APPENDIX G CONTROLS SUPPORTING CYBER RESILIENCY.

Applying these resiliency techniques and design principles to critical infrastructures is particularly important not only to prevent the disruption of vital lifeline services, but also to

[9] Other organizations besides NIST have also published Cyber Resiliency guidance. For example, Microsoft announced a new initiative codenamed "Trusted Cyber Physical Systems (TCPS)" that aims to protect critical infrastructure through resilient design and hardware isolation. See: https://blogs.windows.com/business/2018/04/24/trusted-cyber-physical-systems-looks-to-protect-your-critical-infrastructure-from-modern-threats-in-the-world-of-iot/

prevent long-term damage to the physical infrastructure itself. For example, within the Electric Power Subsector, there are long lead-time replacement physical assets, such as extra high voltage transformers and large-scale high-power turbo-generators. These assets would take months, if not years, to replace if they were significantly damaged or destroyed. Therefore, making the cyber-controlled safety and protection systems associated with those long lead-time physical assets more cyber resilient is essential to prevent long term disruption of electric power services.

Per NIST's new design principles, engineering cyber-resilient systems involves the following characteristics that should be considered when designing new systems or enhancing existing ones.

1. *Focus on the mission and business objectives*: This involves maximizing the ability of organizations to complete critical mission or business functions despite an adversary being present on their systems and threatening their operation. As organizations make their systems and components more resilient, they should recognize this is being done to support mission and business assurance. In some cases, system components that are less critical to mission or business effectiveness may be sacrificed to contain a cyber-attack and to maximize mission assurance.[10]

2. *Focus on the effects of the APT defined as a set of stealthy and continuous computer hacking processes, often orchestrated by a well-resourced criminal enterprise or nation state actor that targets a specific entity*: The resources available to an APT, its stealthy nature, its targets of interest, and its ability to adapt in the face of defender actions make it a dangerous threat. Additionally, the APT may mask their behavior to appear as the result of human error, structural failure, or natural disaster. By focusing on APT activities and their potential effects, systems engineers can design systems that anticipate, withstand, recover from and adapt to a broad and diverse set of adverse conditions and stresses.

3. *Assume that the adversary will compromise or breach the system or organization*: This belief is fundamental to the design of cyber resilience, the justification being that a sophisticated adversary cannot always be kept out of a system or quickly detected/removed from it. This assumption acknowledges that modern systems are large and complex entities that will always have weaknesses and flaws that attackers will be able to target and exploit.

[10] Ross, R., Graubart, R., Bodeau, D., & McQuaid, R. (2018, March). *Engineering of Trustworthy Secure Systems.* Retrieved from nist.gov: https://csrc.nist.gov/publications/detail/sp/800-160/vol-2/draft

4. *Assume that the adversary will maintain a prolonged presence in the system or organization:* The adversary may present a persistent and long-term issue, and the stealthy nature of the threat makes it difficult for the organization to be sure that the threat has been completely eradicated. This notion additionally recognizes the ability of the APT to adapt to mitigation, rendering tactics that were previously effective against the threat now ineffective. Of additional consideration is the fact that despite an organization's successful eradication of a threat actor's presence, it may return and regain a presence. In some situations, the best outcome an organization may be able to achieve is containing the adversary's presence or slowing its lateral movement long enough for the organization to achieve its primary mission objectives before losing the critical systems capabilities.

Table 1 describes cyber resiliency objectives that can be used to enable stakeholders to assert their resiliency priorities based on the mission or business functions they are obligated to protect. (See Appendix A).

A cyber resiliency technique is a set of technologies and processes intended to achieve one or more of the objectives set forth during the prioritization process. These techniques are defined as both the capabilities it provides as well as the intended consequences of using the technologies or process that it includes. The cyber resiliency techniques should be applied selectively to the architecture design based on the business mission or functions and their supporting system resources. Trade-offs will need to be made as these techniques have natural synergies as well as conflicts when used together. These techniques are expected to change over time as threats evolve and advancements are made in the research of security and evolution of their best practices. Table 2 describes cyber resilience techniques that can be used during the selection process to pick which techniques fit the business functions and their underlying system resources. (See Appendix A).

In our interviews, the organizations from the critical infrastructure and aviation sectors found the techniques of redundancy and segmentation to be beneficial to their design. For redundancy, one organization was looking at building a fully redundant power generation facility to keep them running if both their primary and secondary power providers had a major outage. The use of segmentation was cited as an important technique to limit the risk posed by legacy applications and systems that couldn't be upgraded to supported version of software.

Strategic cyber resiliency design principles guide and inform engineering and risk analyses throughout the system lifecycle. These core principals highlight different structural design principals, cyber resiliency techniques, and approaches that organizations can take to apply the techniques. Table 3 describes five strategic cyber resiliency design principals, and identifies

related design principals from other disciplines. (See Appendix A). These principals should be driven by an organization's risk management strategy, and in particular the process of risk-framing. This process involves considerations and assumptions about threats the organization should prepare for, constraints on risk management decision making, and organizational priorities and their associated trade-offs.

In our interviews with organizations, the need to focus on common critical assets to prioritize the limited resources they had available for security design and enhancement came up repeatedly. Additionally, organizations found benefit in moving to cloud-hosted solutions to implement the principle of agility and adaptability in their architectures. The cloud-hosting model removes the complexity of maintaining physical hardware, as well as opens the door to new strategies of hosting systems in different regions and dynamically adjusting resources to meet increased demand.

Structural cyber resiliency design principles guide and inform design and implementation decisions throughout the system life cycle. Many of these structural design principles are consistent with or leverage security and or resilience engineering principles from other disciplines. In Table 4, the first four design principals are related to protection strategies and design principles that can be applied in mutually supportive ways. The next three design principles are related to design principles for resilient engineering and survivability. Three more design principles follow that are driven by the concern for the operational environment changing on an ongoing basis and are focused on the idea of evolution. The final four structural design principles are driven by the need to manage the effects of malicious cyber activities, even when those activities are not detected. The provided descriptions of how these structural design principles are applied can be used to help stakeholders understand how their concerns are being addressed. (See Appendix A).

Growing Cyber-Physical Threats Against Critical Systems

Electrical Grids Exploitation

The type and scope of attacks targeting the electrical grid have grown in recent years with nation-state adversaries leveraging destructive attacks to cause power outages and damage critical systems that operate the electrical grid. A recent example is the attack on the Ukraine power grid that took place on December 23, 2015 when a phishing email installed malware on the command systems of the *Prykarpattyaoblenergo* power control center in the western Ivano-Frankivsk region of Ukraine. This malware was used to take control of circuit breakers at 30 substations across the region and to switch the substations offline, effectively causing a power blackout that effected more than 230,000 residents. The attackers took this a step further by disabling the backup power supplies to two of the three distribution centers to prolong the outage

and to prevent the operators from effectively responding. An investigation performed by Dragos Security and other investigators asserts that the attackers planned their assault over several months, performing reconnaissance to study the network and to steal operator credentials, finally launching a synchronized assault in a highly-coordinated manner to take down the target systems simultaneously. According to Robert M. Lee a co-founder of Dragos Security, "It was brilliant. In terms of sophistication, most people always focus on the malware that's used in an attack. To me what makes sophistication is logistics and planning, and operations, and what's going on during the length of it. And this was highly sophisticated."[11]

While the outage only lasted 1-6 hours, the control centers were still not fully operational two months later. This was partially due to the effort taken by the adversaries to damage control systems by overwriting the firmware on devices at 16 of the substations, leaving them unresponsive to any remote commands from the operators. While power has been restored, the workers have to control the circuit breakers manually. Many of the U.S.' control systems don't have manual backups like the physical breakers they had in Ukraine. This means that, should an attacker sabotage the automated control systems in the U.S., it would be much more difficult for workers to restore power. Per Lee, "Operation-specific malicious firmware updates in an industrial control setting has never been done before. From an attack perspective, it was just so awesome. I mean, well done by them. Once you rewrite the firmware, there's no going back from that to aid recovery. You must be at that site and manually switch operations. Blowing these gateways with firmware modifications means they can't recover until they get new devices and integrate them." The same serial-to-Ethernet converters that were overwritten by attackers are also used in the U.S. power distribution grid. Additionally, phishing emails with the same malware named BlackEnergy3 have been detected as attempting to infect other power systems in Europe and the U.S., demonstrating that the attackers aren't limited to targeting Ukraine.

Customers that were attempting to call the Ukraine power companies were also hindered by an ingenious use of telephone denial-of-service attack during which thousands of bogus calls appearing to come from Moscow area codes were used to overwhelm and confuse the customer service call centers. Per Lee, "What sophisticated actors do is they put concerted effort into even unlikely scenarios to make sure they're covering all aspects of what could go wrong." The final phase of the attacker's sabotage included running a malware called KillDisk to erase the files and software from the operator's workstations to render them useless. That malware was set with a specific timer to automatically start erasing 90 minutes into the attack, meaning the attackers had to carefully plan the different phases of the operation to align with their malware triggers.

The attack in 2015 was followed up by a second attack in December of 2016 using a more

[11] Zetter, K. (2016, March 3rd). *Inside the Cunning, Unpredented Hack of Ukraine's Power Grid*. Retrieved from Wired.com: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

evolved version of malware named "Crash Override," known to be only the second ever case of purpose-built malicious code designed to disrupt physical systems after Stuxnet. The new malware can automate mass power outages and includes plug-in components to allow attackers to adapt it to different electric utility company's systems. The ability of this feature would allow for widespread outages to last much longer than the second blackout in Kiev. Per Lee, "This is extremely alarming for the fact that nothing about it is unique to Ukraine. They've built a platform to be able to do future attacks."[12] Instead of gaining access to the Ukraine power utilities networks and manually switching off power substations like they did in 2015, this time the malware was used to fully automate the attack, and could "speak" directly to the grid equipment, sending commands in the obscure protocols those control systems use to switch power on and off. This is scalable attack software that can run without any feedback from the attackers, meaning it can target more secure networks that are disconnected from the internet. Once a system is infected, the malware automatically maps out control systems and locates critical targeted equipment.

Additionally, it records network logs and send that information back to the attackers to let them learn how the power control systems function over time. The malware's swappable component design means it could be easily adapted to power protocols used in the U.S or elsewhere, downloading new modules when the malware can connect to the internet. The malware also has built in the ability to destroy all files on a system it infects, effectively covering its tracks and destroying any evidence of its presence.

A more disturbing capability of the malware is an exploit it can use against digital relay equipment that gauges the charge of grid components and protects them by opening circuit breakers if it detects dangerous power levels. By using the exploit, the malware could disable the safety system requiring a manual reboot to restore it. If the attackers used this capability in combination with overloading the electrical charge on grid components, they could cause physical damage or destroy them completely. According to Mike Assante, a power grid security expert and instructor at the SANS institute, "This is definitely a big deal, if it's possible to disable the digital relay, you risk thermal overload of the lines. That can cause lines to sag or melt and can damage transformers or equipment that's in line and energized." Taking this a step further, if attackers target multiple elements of the grid en-masse, they could cause what's known as a *cascading outage* where a power overload in one region spills over to the neighboring region and so-on, causing large-scale outages.

In talking with representatives from Dragos security, it was apparent that attacks against critical physical systems in the power industry and beyond are increasing in sophistication and

[12] Greenberg, A. (2017, June 12th). *'Crash Override': The Malware That Took Down A Power Grid*. Retrieved from wired.com: https://www.wired.com/story/crash-override-malware/

frequency. Critical infrastructure in Ukraine has been repeatedly targeted over the past three years with some utilities switching to manual operation as a defense against cyber-attacks that can use their control networks against them. As most power providers and distributors use outsourced integrators to maintain their networking systems, an attack that causes physical damage could result in weeks of outages while the integrators scramble to replace the physical systems. Additionally, these attacks have spread from the power sector to additionally targeting the oil and natural gas sector in countries like Saudi Arabia. Similar behavior of the malware has been seen targeting and disabling critical safety systems to open the door to potential attacks that could result in physical damage or destruction. Where oil refineries are concerned, if taken to an extreme, the attacks could cause an explosion with loss of life. This scenario could even happen unintentionally, as the attackers are trying

Disruptive Technology and ICS/SCADA Systems

The role of disruptive technology, like blockchain, was debatable to some of the utilities. The Pacific Northwest National Laboratory (PNNL) had more commentary in that realm, given its expertise in blockchain and electrical grids. As an example, the role of blockchain in Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems has yet to be widely discussed, while PNNL sees this as a relevant topic.

ICS and SCADA proprietary software are updated very infrequently, if at all, and should be viewed carefully in the face of APT. Cyber-attacks on ICS and SCADA systems have increased with every passing year, in some cases doubling per year. George Razvan Eugen, ("Ghostshell") the hacker who penetrated the FBI, NASA, the Pentagon, and the Russian government says, "Like the internet, SCADA was never created with security in mind. SCADA servers in Brazil and just about everywhere else are exposed to the most basic attacks. Connecting to a programmable logic controller takes one simple step: use the client interface to breach the targeted protocol."[13]

Snohomish PUD, Deloitte, PNNL and others pointed out that there is no silver bullet, and over-hyped (but potentially useful) technology like blockchain can lull stakeholders into a false sense of security. Cyber-resilience is an ongoing challenge, changing weekly, and requires a commensurate ability to track, adapt, withstand and respond. Ultimately, resilience is not simply an issue of systems, but also policy and workforce expertise.

Findings from Research and Case Studies

[13] A. Segal , "Brazil's Critical Infrastructure Faces a Growing Risk of Cyberattacks," *Council on Foreign Relations*. [Online]. Available: https://www.cfr.org/blog/brazils-critical-infrastructure-faces-growing-risk-cyberattacks. [Accessed: 17-Jun-2018].

Understanding the ideal state of resilience is imperative, but enhancing resilience policy will remain a lofty goal in the face of an APT if we can't move past these age-old realities. In this section, we examine common cyber risks and consequences identified from the CRR team's research and case studies.

Technology refresh cycles are too long

Several participants that the team interviewed stated that the security and resiliency issues can be significant, especially in legacy systems, if technology is not refreshed at reasonable time intervals. The concept, "Technology refresh," refers to the timely replacement of equipment/IT elements to ensure continued reliability of said equipment and/or improved function and speed.[14]

Within the system development life cycle, this issue touches on phases four and five, Operations Maintenance and Disposal, respectively.[15] Part of the "Operations Maintenance" phase of the cycle includes items like replacing old hardware and providing regular updates to existing systems.

For example, if a company does an audit and discovers they've been running on a much older version of an operating system (OS) for years, an update is likely in order. In that same vein, a refresh could mean retiring certain technology altogether, which refers to the "Disposal" phase of the development cycle. For instance, a simpler disposal could be a company discarding a department's old desktop computers to adopt laptops of a different brand. Something complex could be a business removing a large part of its existing IT infrastructure to redesign it with more security in mind.

While the general information and communications technology (ICT) industry recommends implementing a full technology refresh over about a 5-year-cycle (more frequent depending on sector), many businesses use much longer cycles than this. The longer the length of time between cycles, the more likely you may run into the issues of certain infrastructure programs falling out of their period of vendor support, the *local hero phenomenon* (the only people who can keep legacy systems working become irreplaceable), and other obsolescent system limits that could leave one more likely to fare poorly in withstanding an attack.[16]

---

[14] Solution One. (2016, July 15th). *What Is A Technology Refresh Cycle And Why You Need One.* Retrieved from SolutionOneNow.com: https://www.solutononenow.com/productivity/what-is-a-technology-refresh-cycle-and-why-you-need-one/

[15] Bernstein, R. (2017, March 17th). *5 System Development Life Cycle Phases.* Retrieved from Concordia.edu: https://online.concordia.edu/computer-science/system-development-life-cycle-phases/

[16] Clarke Willmott. (2015, December 17th). *Technology Refresh: Nightmare, Opportunity or Both?*Retrieved from Clarkewillmott.com: https://www.clarkewillmott.com/news/technology-refresh-nightmare-opportunity-or-both/

So how could a timely, properly implemented, technology refresh plan impacts a business's ability to be resilient in withstanding an attack? Say a small company wants to improve their resilience without paying large amounts of money for third-party knowledge. The right parties could make a refresh plan to transition critical company information into a cloud-based backup and recovery system.[17] This way, when disaster strikes, the business needn't worry about being able to access the vital data necessary to sustaining day to day business operations. An alteration like this could make a world of difference for an organization in crisis, but the organization has to make the purposeful effort to review current IT stock and actually make those plans and changes at the right time.

Technology refresh should be implemented not just when a business's existing infrastructure gets older, but any time a business undergoes a merge, includes a new sector/major service or when the demands of its existing environment change. If an organization has outsourced something or has managed service to handling its ICT, experts say it should be sure to develop agreements with those services that include an obligation for technology refresh within a certain time regularity.[18]

Ideally, for tech refresh cycles to be optimal in cyber resilience, a company must start planning for it when (or before) the technology is acquired in the first place. As a business's older systems inch closer to becoming obsolete, employees will likely start to see an increase in failure rates and a subsequent longer downtime, regardless.[19]

Critical infrastructure is locked in to a limited number of vendors

According to Joe Weiss, a managing partner at Applied Control Systems, "The diversity of power companies is essentially a mirage, since there are only eight to ten vendors worldwide that manufacture the kind of generators used in ICSs."[20]Additionally, ICS components are commonly shared across a range of critical infrastructure systems that can result in vulnerabilities in these components affecting multiple sectors and industries. An example of this was the Stuxnet worm that exploited a vulnerability in a vendors SCADA software with the intended target being uranium enrichment facilities in Iran. The malware had the unintended effect of spreading to other industries including oil and natural gas, with Stuxnet infecting the same vendors software

[17] Salesforce, UK. (2015, November 17th). Why Move To The Cloud? 10 Benefits Of Cloud-Computing. Retrieved from Salesfore.com/uk: https://www.salesforce.com/uk/blog/2015/11/why-move-to-the-cloud-10-benefits-of-cloud-computing.html
[18] PwC. (2015, June). *Outsourcing: How cyber resilient are you?* Retrieved from Pwc.com: https://www.pwc.com/us/en/financial-services/regulatory-services/publications/assets/cyber-security-tprm.pdf
[19] Lee, M. (2012, November 9th). *Stuxnet infected Chevron, achieved its objectives.* Retrieved from zdnet.com: https://www.zdnet.com/article/stuxnet-infected-chevron-achieved-its-objectives/
[20] Reed, B. (2017, February 7). *5 Benefits of Establishing a Technology Refresh Cycle.* Retrieved from Alphanumeric.com: http://info.alphanumeric.com/blog/benefits-establishing-technology-refresh-cycle

at an oil and gas corporation.[21] In total Stuxnet infected over 100,000 systems spread across 155 countries according to the antivirus company Symantec.[22]

Another risk posed by the limited number of available vendors is the threat of supply chain attacks. According to researchers at CrowdStrike on June 27, 2017 the destructive malware known as NotPetya was deployed using a legitimate software package employed by organizations operating in Ukraine. The attack used an update mechanism built into the software to provide updates and distribute them to the vendor's customers. This same mechanism had been used a month earlier to deploy other ransomware attacks. Supply chain attacks exploit a trust relationship between software or hardware vendors and their customers. These attacks can be widespread targeting the entire trusted vendor's customer base and are growing in frequency as well as sophistication.[20]

In a separate incident, CrowdStrike tracked a nation-state threat actor known as Energetic Bear that targeted the supply chain of critical infrastructure to bundle their "Havex" malware into software installers provided by several energy sector vendors to their customers. This resulted in the attackers gaining remote access to sensitive systems at the power companies.[20]

In our interview with representatives from the airline industry, challenges emerged regarding upgrading critical airport systems, such as baggage claims that need to be operational 24/7. Additionally, they explained that vendors supporting shared systems were less inclined to perform upgrades because of the complexity and number of parties that would need to be involved in testing and approving of the upgrade.

In poor weather conditions, like fog, the system is essential in aiding safe landings. According to Alexandre Fiacre, the secretary general of France's UNSA-IESSA air traffic controller union, "The tools used by Aeroports de Paris controllers run on four different operating systems that are all between 10 and 20 years old."[23] These systems are poorly maintained as over time it becomes increasingly difficult to find staff who have the expertise to work with the outdated software. According to Facre, "We are starting to lose the expertise to deal with that type of operating system, in Paris, we have only three specialists who can deal with DECOR related issues, and this problem is getting worse with one of them retiring next year; we haven't found anyone to replace him."

---

[21] Armerding, T. (2017, March 22). *Critical Infrastructure: Off the web, out of danger?* Retrieved from CSO Online: https://www.csoonline.com/article/3183528/critical-infrastructure/critical-infrastructure-off-the-web-out-of-danger.html

[22] Falliere, N., O Murchu, L., & Chien, E. (2011, February 11th). *symantec.com.* Retrieved from W32.Stuxnet Dossier: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[23] Bright, P. (2015, November 11th). *Failed Windows 3.1 system blamed for shutting down paris airport.* Retrieved from ars Technica: https://arstechnica.com/information-technology/2015/11/failed-windows-3-1-system-blamed-for-taking-out-paris-airport/

Organizations should review the commercial and open source products they are using and be aware of and prepare for potential attacks using legitimate vendor's software as the infection vector. Anomaly-based detection and visibility into the software running on critical systems is essential for detecting and stopping these types of attacks.

Proprietary code "outlives" its developer

In our talks with representatives from the airlines industry, legacy software and systems were a primary concern, with significant planning and resources being spent on replacing legacy systems with modern alternatives that can be patched and better secured. For the legacy systems that can't be replaced, there was a concerted effort to segment these systems from the rest of the network and to put in place additional monitoring to detect and limit cyber-attacks against these outdated systems. Shared systems like those at airports that have shared gates used by multiple airlines were another concern, as these systems are provided as-is by the airport, and in many cases, are running outdated operating systems like Windows XP.

Airlines have little control over the configuration or maintenance of these shared systems that they must rely on for check-in and ticketing customers at the gate. These systems are also in public areas, where interviewed airline officials admit any person with the proper attire could access the computers and plug in a USB drive or otherwise tamper with the system. These systems are connected back to the airlines' networks for tracking check-ins, and could act as an avenue for an attacker to access these networks. Many airports are slow to replace these systems, as doing so requires coordination and approval by multiple parties and vendors.

A well-known case of proprietary code outliving its developer occurred at a Parisian airport where, on November 7th, 2015, a failure of a system running the legacy Windows 3.1 operating system released circa 1992 caused a temporary shutdown of the airport. The system was running a program known as DECOR to communicate Runway Visual Range (RVR) information to pilots.

In another case, a U.S. airline encountered a computer glitch on October 11th, 2015 that prevented passengers from checking in for their flights, causing widespread delays around the nation. This outage was believed to have been caused by a failure of a legacy technology system, which resulted in staff having to write down tickets and boarding passes by hand as a temporary workaround. According to Daniel Baker, CEO of FlightAware, "The airlines are operating with legacy systems that were designed when the airlines were a lot smaller than they are now. If you look at the fleet size in 1980s compared to today, the growth has been extraordinary. They're trying to scale these platforms for the much larger airline they've become and it's hard to keep

up with passengers' expectations."[24]

Many airlines link their transactional systems to travel agencies and other booking providers through use of a Global Distribution System that can also be used as their reservation system. These systems run software that in many cases were created in the 1960s and haven't been changed or updated much since. Many of the systems are based on legacy programming languages like COBOL, which 70% of universities are no longer including in their programming curriculum, and where the average age of a COBOL programmer is 55 years old.[25] According to Dave Vecchio, research vice president of application development at Gartner Inc., "In 2004, the last time Gartner tried to count Cobol programmers, the consultancy estimated that there were about 2 million of them worldwide and that the number was declining at 5% annually."

Airlines rely on the legacy Global Distribution System's for nearly every function of flight, including reservations, check-ins, cargo accounting as well as filing flight plans, calculating fuel needs, and providing pilots with preflight paperwork. This creates a recipe for disaster when an error in these systems can ground all flights. Airlines have been implementing additional systems that have to interface with the legacy systems, such as internet booking, flight status displays, and ticket kiosks that can cause more points of issue when a failure does occur. Airlines and critical infrastructure can perform disaster recovery drills to test failover and worst-case scenarios, as well as engineer stability and recovery into these critical systems.[26]

Vendors aren't always designing with security in mind

Organizations face an increasing risk from vendors that don't design their software, hardware, or services with security best practices in mind. A primary example of this is the use of default passwords by vendors selling all types of software and hardware. This poses a risk when the software or hardware is brought online for use in a production environment without having the default password changed. Attackers make use of this knowledge to scan for and log in to systems and services using lists of known default passwords.

An example of this was in 2010 when the Stuxnet malware exploited a hard-coded default password (CVE-2010-2772) in a vendor's SCADA system that allowed for local users to access a back-end database and alter configuration settings within it.[27] This default password had been

[24] Zaslow, A. (2015, October 12th). *Outdated Technology Likely Culprit in Southwest Airlines Outage.* Retrieved from nbcnews.com: https://www.nbcnews.com/business/travel/outdated-technology-likely-culprit-southwest-airlines-outage-n443176
[25] Trikha, R. (2015, July 6th). *The Inevitable Return of COBOL.* Retrieved from hackerrank.com: https://blog.hackerrank.com/the-inevitable-return-of-cobol/
[26] Leffler, G. (2017, January 27th). *Legacy code can cost you billions. Just ask an airline.* Retrieved from linkedin.com: https://www.linkedin.com/pulse/legacy-code-can-cost-you-billions-just-ask-airline-greg-leffler
[27] Veluz, D. (2010, October 1st). *STUXNET Malware Targets SCADA Systems.* Retrieved from trendmicro.com: https://www.trendmicro.com/vinfo/in/threat-encyclopedia/web-attack/54/stuxnet-malware-targets-scada-systems

known about and posted online for several years prior to the Stuxnet attack. According to Steve Bellovin, a computer scientist from Columbia University, "Default passwords are and have been a major vulnerability for many years. It's irresponsible to put them in, in the first place, let alone in a system that doesn't work if you change it. If that's the way the (omitted) system works, they were negligent."[28]

Hard coded passwords are not just a problem for this specific vendor but have been known to be used across the ICS industry. According to Joe Weiss, "Well over 50 percent of the control system suppliers hard-code passwords into their software or firmware. These systems were designed so they could be used efficiently and safely. Security was simply not one of the design issues."

Another type of vendor security design issue is the supply chain attack. This type of attack targets less-secure elements of a vendor's distribution network, and can involve tampering with a vendor's software product to install a rootkit or other malware backdoors. A recent case of this was an attack by a threat actor known as DragonFly, that targeted critical infrastructure vendors supplying industrial routers and remote access appliances. The attackers compromised several vendor's websites and content management systems to replace legitimate software installers with malicious files that would capture the login credentials of the customers. According to Dale Peterson, with DigitalBond, "Industrial control system vendors are often soft targets for cyber criminals and state sponsored actors: with weak security around corporate web sites and a lack of security features such as signed firmware updates that would make it more difficult for an attacker to compromise a software package."[29]

The organizations from the interviews found it challenging to get their vendors to make basic security updates, such as upgrading from Windows server 2003 to a more modern operating system. These problems are compounded by the sheer number of applications and third-party developed software used to operate a complex business like an airline.

Intra-State Relations, Systems Assessment, and Unknowns

According some of the interviewed stakeholders, it is unknown whether a cyber-physical attack could render their grid(s) inoperable, or if it could return to manual operations in an emergency. Academics expressed doubt that a return to manual operations was possible. However, some utilities disagreed stating that a return to manual operations is possible. Representatives from Dragos Security doubted cyber-attacks aimed at physical components like substations would

[28] Zetter, K. (2010, July 19th). *SCADA system's hard-coded password circulated online for years.* Retrieved from wired.com: https://www.wired.com/2010/07/siemens-scada/
[29] Paul. (2014, July 4th). *Industrial Control Vendors Identified in Dragonfly Attack.* Retrieved from securityledger.com: https://securityledger.com/2014/07/industrial-control-vendors-identified-in-dragonfly-attack/

succeed. Representatives from the MITRE saw that as a distinct possibility, in agreement with Idaho National Laboratory (INL), which succeeded in damaging a diesel generator through its transmission system in 2007.[30]

Gaps and Challenges in Current Cyber Resilience Practice

Lack of Cyber-Electrical SMEs; usage of general measures.

Cyber resilience is important not only for IT cyber systems, but also for Operational Technology (OT) Cyber systems. Within OT systems, ICS are an important subset, as they control the processes that ultimately produce the tangible goods in our economy.

To address the issue of securing ICS, DHS formed the Industrial Control Systems Joint Working Group (ICSJWG). The group was formed to enable industry and government to work together to achieve a common objective for securing ICSs across all critical infrastructure sectors that employ ICSs. In their 2011 report, *Cross-Sector Roadmap for Cybersecurity of Control Systems*, the ICSJWG articulated its vision for securing ICS:

"Within 10 years, control systems throughout the CIKR sectors and Federal Partners will be able to operate securely, robustly, and *resiliently*, and be protected at a level commensurate with risk. Control systems throughout the CIKR sectors and Federal Partners will be able to operate with no loss of critical function in vital applications *during* and *after* a cyber event without impacting the overall mission of the facility."

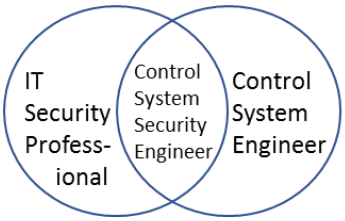
To achieve and sustain this vision for secure and resilient ICS, there is an urgent need to educate and train a new breed of professional who could be called Hybrid Cyber-Electrical SMEs. The need for Hybrid Cyber-Electrical SMEs was identified by Dragos on a team phone interview on April 4, 2018. Dragos has extensive experience in securing ICS for critical infrastructure owners/operators. The need for such hybrid or interdisciplinary personnel is also suggested by NIST in its GUIDE TO INDUSTRIAL CONTROL SYSTEMS (ICS) SECURITY (Special Publication 800-82 Revision 2) where it states,

"While the control engineers will play a large role in securing the ICS, they will not be able to do so without collaboration and support from both the IT department and management. IT often has

[30] "Cyber Threat and Vulnerability Analysis of the U.S ...," 01-Aug-2016. [Online]. Available: https://www.energy.gov/sites/prod/files/2017/01/f34/CyberThreatandVulnerabilityAnalysisoftheU.S.ElectricSector.pdf. [Accessed: 17-Jun-2018].

years of security experience, much of which is applicable to ICS. As the cultures of control engineering and IT are often significantly different, their integration will be essential for the development of a collaborative security design and operation."

The problem arises because the education and training of control system engineers and IT security professionals is vastly different. One may view the creation of Hybrid Cyber-Electrical SMEs in terms of creating an intersection of two the sets of disciplines:



Hence, in view of the increasingly sophisticated and growing threats to critical infrastructure ICS, there is a need for colleges and universities to develop and offer hybrid degrees, or at least an allowable combination of major and minors. Similarly, employers need to support the periodic training of such personnel so that they can stay abreast of ICS cyber security threats and the best security practices, including cyber-physical resilience, to thwart them

Sub-National Partnership in Collaboration with Federal Government and Private Sector is Key for Resilience

The creation of resilient systems needs partnerships, and the inclusion of all stakeholders is critical. This is especially true for cyber-physical assets, like utilities and electrical grids. Although the Federal government supplies the mandate for national security, most cyber-physical critical sectors are under the auspices of state or local government.[31] In the era of cyber-warfare, this necessitates a greater than ever partnership for national security.

Sub-national collaboration has been globally proven to be an effective method in creating

[31] D. Dittrich, "DIMS Operational Concept Description v 2.9.1¶," *DIMS Operational Concept Description v 2.9.1 - DIMS Operational Concept Description 2.9.1 documentation*. [Online]. Available: http://dims-ocd.readthedocs.io/en/latest/index.html. [Accessed: 17-Jun-2018].

partnerships for large-scale problems.[32][33] There are numerous examples of sub-national partnerships, including the C40, the WHO Healthy Cities, 100 Resilient Cities, the Public Regional Information Security Event Management (PRISEM) program and its successor, PISCES.[34] The PRISEM program is highly lauded example of subnational partnership. The PRISEM program, while largely designed for information sharing, exemplifies the speed and efficiency of such partnerships for utilities.

PRISEM/PISCES

The DHS-funded PRISEM, which began in 2008, was a regional cyber-security information sharing program for local government in Washington State. PRISEM was billed as "a community service, which aggregates and processes cyber-security logs and event data across a number of local jurisdictions and maritime ports, provides correlated alerts, and extends cyber situational awareness across the greater Puget Sound region."[35]

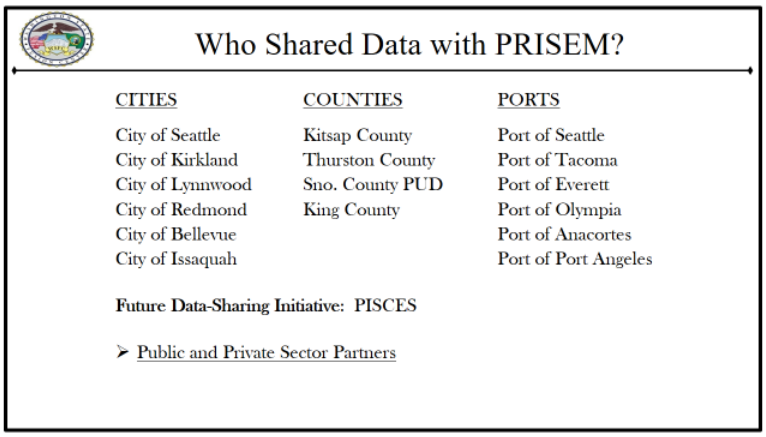
Many Washington-based interviewees vocally hailed PRISEM as an excellent, low-cost program, and lamented its shutdown. According to Port of Seattle representatives, warnings from PRISEM were often weeks ahead of MS-ISAC or E-ISAC. According to the Office of the Chief Information Officer of Washington State, PRISEM served "seven cities and counties, six maritime ports, a hospital, and two energy utilities, with expansion underway. Integrated with analysts at the Washington State Fusion Center, it is the only such system in the United States."[36] Representatives of the Washington State Fusion Center and the University of Washington stated it cost roughly $550,000 annually for nine years.[37]

The Rapid Technology Adaptation Program: Cyber-Security 1- Botnet Detection and Mitigation Phase 2 (RTAP) in the DHS Science & Technology Directorate provided PRISEM's funding until 2013. RTAP intended to deploy research-grade technology for botnet detection, enhance information security, and increase participant compliance.[38]

---

[32] 2012 in review: cities commit to (and are achieving) ghg reductions," c40 Blog, December 31, 2015, http://www.c40.org/blog_posts/2012-in-review-cities-commit-to-and-areachieving-ghg-reductions.
[33] P. M. Haas, "Introduction: epistemic communities and international policy coordination," *International Organization*, vol. 46, no. 01, p. 1, 1992.
[34] Acuto, M.; Morissette, M.; Tsouros, A. City Diplomacy: Towards More Strategic Networking? Learning with WHO Healthy Cities. Glob. Policy 2017, 8, 14–22.
[35] Snohomish PUD and PNNL. "PRISEM Briefing." 2013 https://www.snopud.com/Site/Content/Documents/cyber/PrisemBriefing_032613.pdf
[36] "PRISEM," *OCIO*. [Online]. Available: https://ocio.wa.gov/news/prisem. [Accessed: 17-Jun-2018].
[37] Interview: Dave Dittrich, Director of Research, PRISEM
[38] D. Dittrich, "DIMS Operational Concept Description v 2.9.1¶," *DIMS Operational Concept Description v 2.9.1 - DIMS Operational Concept Description 2.9.1 documentation*. [Online]. Available: http://dims-ocd.readthedocs.io/en/latest/index.html. [Accessed: 17-Jun-2018].

It included the University of Washington, the Washington State Fusion Center, Snohomish PUD, multiple cities like Seattle, Redmond and Bellevue, multiple counties, as well as a number of ports. At the time, it was the only known example of sub-national public-private partnership for a cyber-physical critical sector.[39]



PRISEM introduced the concept of managed IT security services into the local government sphere. Beyond simple information, it developed an action-oriented partnership, leveraging expertise for organizations with limited resources. The program aimed to provide a reporting method for events and trends, as well. Some of the R&D included:

- Cross-organizational correlation
- Automated escalation to US-CERT and NCIC
- Collective Intelligence Framework (CIF) integration
- Self-directed access control

PRISEM correlated event data from Netflow botnet detection with a commercial Security Information Event Management system (SIEM) to detect computers with high probability of infection. Through the CIF system, PRISEM allowed for Indicators of Compromise to provide historical attack context, and create real-time watch lists, while the regional map allowed for geographic and visual situational awareness.

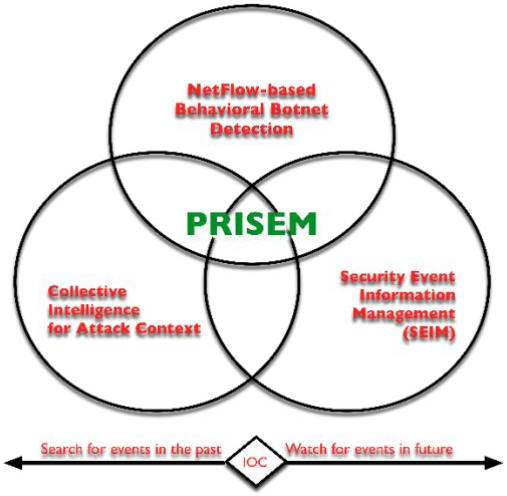
PRISEM intended to fill in the gaps of other sharing methods that do not scale or aggregate and provide little situational awareness. PRISEM was the first sub-national partnership to have a Cooperative Research and Development Agreement (CRADA) with US-CERT for declassified Indicators of Compromise, which would be sent via MITRE's Structured Threat Information eXpression format (STIX). The partnership aimed to link IOCs with Tools, Tactics and Procedures (TTPs) with Courses of Action for actionable threat intelligence. PRISEM representatives view most sharing methods as reactive, adding that intelligence classification

[39] D. Dittrich, "DIMS Operational Concept Description v 2.9.1," *DIMS Operational Concept Description v 2.9.1 - DIMS Operational Concept Description 2.9.1 documentation*. [Online]. Available: http://dims-ocd.readthedocs.io/en/latest/index.html. [Accessed: 17-Jun-2018].

sometimes hinders the free-flow of information to engaged stakeholders, echoing the comments of Idaho National Laboratory.[40]

The founders of PRISEM, including the director of research, emphasized that "local government is the first responder."[41] PRISEM researchers note that a comprehensive system without local governments is not comprehensive. They add that nearly all critical infrastructure is in SLTT jurisdictions, where information security is a secondary concern, despite the reliance of all response services on information technology. SLTTs often have antiquated technology, lacking both financial resources and the technical capacity of the Federal government. Succinctly said, the difference in technical capacity between a local utility, or city government, and the NSA or DHS is quite vast.

PRISEM researchers identified a few limitations in their method. Firstly, a secure and real-time communication method for participants was absent, due to the commercial SIEM user interface. Secondly SIEM's commercial nature did not allow for integration of developed tools or algorithms. Thirdly, users must be trained on manual data entry for CIF via an API or browser plug-in, as the vendor portal does not do this directly. Finally, IOC data was shared arbitrarily, in thousands-long lines of columnar data, and difficult to manipulate. Traffic Light Protocol tagging was likewise arbitrary.

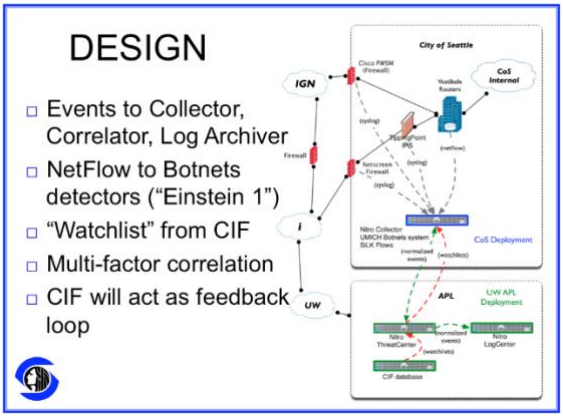


Despite these limitations, participants held PRISEM in high esteem. PRISEM's successor, the PISCES program, expands on its parent's success by exploring workforce development and research. The lack of state funding has driven PISCES to be led by the private sector.[42]

[40] Cyber Threat and Vulnerability Analysis of the U.S ...," 01-Aug-2016. [Online]. Available: https://www.energy.gov/sites/prod/files/2017/01/f34/CyberThreatandVulnerabilityAnalysisoftheU.S.ElectricSector.pdf. [Accessed: 17-Jun-2018]

[41] D. Dittrich, "DIMS Operational Concept Description v 2.9.1¶," *DIMS Operational Concept Description v 2.9.1 - DIMS Operational Concept Description 2.9.1 documentation*. [Online]. Available: http://dims-ocd.readthedocs.io/en/latest/index.html. [Accessed: 17-Jun-2018].

[42] C. Wood, B. Freed, and R. Duffy, "Collaboration to protect critical government infrastructure reboots, eyes national expansion," *StateScoop*. [Online]. Available: https://statescoop.com/collaboration-to-protect-critical-government-infrastructure-reboots-eyes-national-expansion. [Accessed: 17-Jun-2018].



Specifically, PISCES is supported by Frazier Healthcare Partners, a Seattle-based private equity firm. Additionally, PISCES has a technology transfer agreement with DHS Science & Technology Directorate for evolving and developing tools. Led by Michael Hamilton, of Critical Informatics, who led PRISEM, PISCES targets "down-market local governments…for water purification, waste-treatment, communication for law enforcement, emergency management, traffic management." Hamilton says PISCES is "completely operational" in a partnership with Western Washington University (WWU). They are combining the event monitoring technology of Critical Informatics with WWU's cyber-security training, allowing for analysts to learn via experience and "live fire."

Sub-National Collaboration is Faster and More Efficient

> *"By concentrating the brainpower of humanity in relatively small geographic areas, cities have promoted the kinds of interactions that nurture creativity and technological advances. They have been the drivers of progress throughout history, and now—as the knowledge economy takes full flight—they are poised to play a leading role in addressing the challenges of the twenty-first century."*
> — Michael Bloomberg, Former Mayor of New York and President of the Board of the C40

Sub-national policy functions efficiently for several key reasons. The most important is the relative agility of local and state government in comparison to the larger bureaucracies at the Federal level. The ability to implement policy is more streamlined, particularly at the level of city, and utility. The physical nearness of local stakeholders to critical infrastructure and to each other is an additional factor. Similarly, the ability to share threat information—simple communication—is faster at the sub-national level because of personal relationships. These two factors lessen the lag time between policy creation, implementation, and review, while allowing from-the-ground-up policy to authentically reflect local needs. Sub-national entities have fewer resources than their federal counter-parts, however.

Direct stakeholder engagement further allows sub-national policy to be effective. It creates networks for stakeholders from all sectors to directly engage on a persistent, formal basis with decision-makers. This enlarges and empowers a topic-based community or sector, like the energy sector, to influence policy by setting the agenda based on their collective assessments.

Sub-national partnerships legitimize and amplify stakeholder influence. 63% of sub-national networks include partnership and buy-in from organizations like UNICEF, Google, SAP, Cisco, Bloomberg Philanthropies, Booz Allen Hamilton, the Rockefeller Foundation, or the World Bank.[43] When sub-national partnerships include such technical and financial giants, it not only empowers the topical community, it turns the member cities into regional policy centers with lobbying clout that attract investment. In the case of cyber-physical assets resilience, research investment grounded in the needs of the utilities is paramount.

On a practical level, this type of multi-lateral partnership leads to knowledge sharing, best practices, joint experimentation and development, as well as strategic management of resources. Sub-national partnerships and networking expose member governments and organizations to the shared technical capacity of the pooled network, filling in technical, strategic, or financial gaps.

Sub-National Partnerships Show a More Granular View

National partnership with local governance creates a more granular and accurate assessment of security and resilience challenges. The Federal government, along with the private sector, has a greater capacity to assess such changes and inform local governments, in a top-down fashion. Federal agencies can help assess local utilities and inform them of resiliency pain points in the context of APTs. But the opposite is also true; bottom-up information can give greater context to larger security assessments.

The Ukrainian utilities provided an in-depth view into the Russian attack to the E-ISAC, for example. Another example is the joint cyber-audit between Snohomish PUD and the Washington State National Guard. According to Snohomish PUD, the Guard penetrated the PUD's defenses, and compromised their SCADA systems within three days, with a standard spear phishing attack, identifying multiple weaknesses. In this manner, threat and resiliency assessment can also flow upwards.

Cyber-Physical Critical Sector Partnership

In the case of critical sector cyber-physical resilience—as distinguished from security or information sharing—there are appears to be a need for a public-private partnership, starting at the local level. Collaboration through the vertical of government, and the private sector could enable greater resiliency for utilities, by designing and implementing cyber-resilience principles.

In this case, there could be an increased partnership between the intelligence community, cities, states, utilities, cyber-security companies and private foundations. This type of partnership would bring together technical, sector-specific expertise with policy acumen, and potentially funding to

[43] Acuto, M.; Morissette, M.; Tsouros, A. City Diplomacy: Towards More Strategic Networking? Learning with WHO Healthy Cities. Glob. Policy 2017, 8, 14–22.

implement resilient design principles.

Given the rapid nature of the advanced persistent threat against the energy sector, resiliency policy must respond commensurately faster—several steps ahead—with the appropriate stakeholders.

The Potential Aims of a Cyber-Physical Critical Sector Partnership

A multi-sector, locally-driven partnership could assess the resiliency of cyber-physical infrastructure, starting with a systems assessment, while exploring disruptive technology, hybrid workforce development, increased Federal and private partnership, and increased digital hygiene. These are not intended to be prescriptive nor exhaustive in scope.

Intra-State Relations, Systems Assessment, and Unknowns

According some of the interviewed stakeholders, it is unknown whether a cyber-physical attack could render their grid(s) inoperable, or if it could return to manual operations in an emergency. Academics expressed doubt that a return to manual operations was possible. However, some utilities disagreed stating that a return to manual operations is possible. Representatives from Dragos doubted cyber-attacks aimed at physical components like substations would succeed. Representatives from Mitre saw that as a distinct possibility, in agreement with Idaho National Laboratory, which succeeded in damaging a diesel generator through its transmission system in 2007.[44]

Increased Federal Partnership with SLTT

An increased relationship between cities, states, the Federal government, and utilities could lead to increased bi-directional information and technology-sharing.

Information-sharing is a necessity, yet there are two major challenges: privacy and declassification. For utilities, sharing of customer data can be a liability, and civil suits against utilities are not inexpensive. Questions that arose from certain stakeholders: How do they share more effectively? What do they share? What are the implications? How do we change their state's public disclosure laws? How can this interact with PCII?

The Protected Critical Infrastructure Information program (PCII) aims to secure sharing of given information from utilities to the Federal government for vulnerability assessment. PCII prevents

[44] "Cyber Threat and Vulnerability Analysis of the U.S ...," 01-Aug-2016. [Online]. Available: https://www.energy.gov/sites/prod/files/2017/01/f34/CyberThreatandVulnerabilityAnalysisoftheU.S.ElectricSector.pdf. [Accessed: 17-Jun-2018].

shared data from usage in civil suits, litigation and FOIA requests; but PCII is only available to trained government employees.

Likewise, the sometimes-slow Federal declassification of threat information hampers the knowledge of utilities. Without security clearances, utility employees are limited in their access, particularly during an emergency. The DHS Cyber Information Sharing and Collaboration Program (CISCP) requires not only security clearances but also a Cooperative Research and Development Agreement (CRADA). The inability for the utilities, cities and states to have a more freely-flowing dialogue about cyber-threats delays the ability to adopt a robust security and resilience posture. Perhaps an increased presence of cleared Federal personnel, from the cyber-intelligence community, embedded within regional subnational partnerships can be a stepping stone to greater communication.

A stronger link between cities, utilities and the Federal government would not only benefit communication, but also technology development and transfer. The Federal government has a greater capacity for research and development than local governments or utilities. In particular the Department of Energy's National Labs, the DHS Science and Technology Directorate or the NSA's Office of Research and Technology Applications Technology Transfer Program could help cities and utilities develop customized Tools, Tactics and Procedures as needed. While this is not a new concept and already occurs, amplification and formalization of these types of relationships within a regional sub-national network has been shown to increase the capacity of cities and utilities to develop best practices, identify vulnerabilities and create solutions.

Increased Private Sector Partnership

As with any increased Federal partnership, increased partnerships between utilities and the private sector foster development of technology, best practices and inform strategy. As operational and informational technology increasingly converge, and as devices becomes increasingly connected to other devices, as in the Internet of Things, a greater landscape for attack vectors appears. Cyber-security was not a design element in legacy operational technology, creating an additional onus on utilities and their partners to develop Tools, Tactics and Procedures.

As an example, Sacramento Municipal Utility District (SMUD) partnered with Applied Communication Services to research and develop new technology. Through this partnership SMUD and ACS developed an "Intrusion Detection System" for the wireless smart meters, in 2013. It has significantly amplified their cyber-security posture, and "created new security capabilities." Similarly, the utilities of New York have partnered with Booz Allen Hamilton, Siemens, and Power Analytics for secure micro-grids. The three companies will contribute cyber-physical security, technical architecture, and micro-grid technology, respectively.

Cyber-securing the supply chain through the vendors is also a new realm of possibility. Given that 3rd party vendors often do not secure their devices, and update them very infrequently, if at all, some utilities are being pro-active. They are taking the extra step to validate the reliability of vendors and verifying the absence of security vulnerabilities. SMUD has assigned an officer to specifically deal with vendors and assess security of purchased products. Sub-national partnerships not only allow for assessment, and validation of the security of purchased equipment, they allow for feedback and input from the cities and utilities to the vendors, helping to usher in a new era of standards.

Personal Trust Between Local and State Actors

It is not a new thought that fostering more public-private partnership regarding many national security issues is a good idea. The benefits of such a relationship, especially concerning cyber resilience, could create both a safer, more stable cyber and physical environment for businesses, governing bodies on all levels, and citizens alike.[45] Alternatively, at times state and non-state or local actors may have different interests and varied levels of influence in their industries or geographic areas, effectively complicating such cooperation. While this, along with a handful of other obstacles seems to make these kinds of partnerships tricky to navigate, one sticking point that was continuously brought up during research was the issue of "lack of trust" between these parties. During a panel discussion that the team conducted in Seattle, an exchange between state and local representatives fantastically illustrated this complex dynamic.

A professional from a local utility provider explained that in the past, the National Guard had performed a vulnerability assessment or "cyber audit" for the company so that they could get a clearer picture of what they were doing right and what could be improved upon in terms of security and resilience. The woman went on to explain how helpful it was that the Guard was able to provide such assistance in a way that was discrete and would not compromise the business's privacy regarding the public and the government. The utility provider had found a partnership it could trust. Interestingly, a representative from the National Guard added that both they and the company had to fight very hard to keep the final assessment results from being published due to state public disclosure or "Sunshine" laws.[46] Technically meant to inspire an entity's accountability and transparency with the public, several professionals stated that the laws actually need updating to better account for entity privacy, especially when concerned with businesses that fall under the umbrella of critical infrastructure. Some panel participants suggested applying reformations to said public disclosure laws to account for these factors.

---

[45] Rocca, R. (2017, July). *The rising advantage of public-private partnerships*. Retrieved from McKinsey.com: https://www.mckinsey.com/industries/capital-projects-and-infrastructure/our-insights/the-rising-advantage-of-public-private-partnerships

[46] Washington State, Office of the Attorney General. (2018, June 4th). *Open Government*. Retrieved from atg.wa.gov: http://www.atg.wa.gov/opengovernment.aspx

Additionally, there was a particularly fascinating back and forth between the energy utility provider, National Guard representative, and a state official when a district Senator suggested that vulnerability audits like the one described be mandated, at the least, for all critical infrastructure entities. He was met with a strong reaction from both parties. Representatives from the utility provider and the National Guard explained that they felt that the very reason why their partnership worked as well as it did was because it was not mandated, not forced upon them by any regulating body. The cooperation was simple and effective; it was, in a way, a B2B service based on trust without any third parties or mediators.

In reflection of this discussion, the next question that one may logically ask is, "how we might encourage partnerships like these without necessarily requiring it by law?" Perhaps more conversations should be had between the appropriate people about reforming certain public disclosure laws. Additionally, finding ways to educate entities about the services they could potentially provide one another, especially in critical infrastructure, may be a sensible next step. Instead of attempting to make these partnerships happen out of force, why not find a way to promote this type of cooperation on both sides using real-world successes like that of the utility company and the National Guard partnership as prime examples?

Efforts like these could be a great way to instill better cyber resilience practices and trust across all sectors without applying heavy regulation or passing restrictive mandates.

Workforce Development

A hybrid cyber-physical workforce developmental plan is undoubtedly necessary. There must be a cadre of experts that can speak to the needs of cyber issues in the context of electrical grid issues, while doing so in seamless fashion. This workforce hybridization is true for the other critical sectors, as well, such as water and transportation.

Generally, there is a dearth of cyber-expertise in utilities; representatives of Dragos and PNNL remarked that in utilities, city and state government, cyber-security measures are general and not sector-specific. A regional avenue for workforce development could include local trade schools, universities, and apprenticeships, combining academic knowledge, with real-time experience, for sector-specific workforce hybridization. As an example, in a study by the Ponemon Institute, 55% of companies indicated they had one person assigned to SCADA cyber-security while 25% had no personnel.[47] ICS/SCADA is a niche field, far smaller than the larger whole of information security.

In short, the workforce, as well as the policy makers, must become far more cyber-savvy. Information technology and operational technology are converging rapidly, creating new

[47] [47] "Critical Infrastructure: Security Preparedness and Maturity," Ponemon Institute: Unisys, July 2014.

problem sets, challenges and opportunities.[48] Cyber policy is transforming into policy writ-large, in the same way that the *"digital economy"* is actually just *"the economy."*

Increased Digital Hygiene

According to one study, usage of personal devices caused 32% of security incidents in critical infrastructure.[49] Increasing education for utility employees and impressing upon the whole of the organization the importance of digital hygiene is critically important. The New York Power Authority educates employees on specific risks, threats and pre-emptive strategy, like avoiding peripheral devices like USB sticks.[50] The Stuxnet cyber-attack against that crippled the Iranian nuclear program at Natanz made its entrance through a thumb drive.

While the attacks against critical infrastructure can be complex, as they enter the system these attacks often begin with spear phishing and social engineering attacks. This was true in the Russian cyber-attack against Ukraine, and it was true in the joint cyber-audit of Snohomish PUD and the Washington State National Guard.

National Government's Greater Technical Capacity and Available Resources

The National Government has a few departments and agencies who are focusing on cyber resilience today. Their focus includes adopting cyber resilience within their own enterprises as well as providing resources to aid the adoption of cyber resilience by others. Among those Federal departments and agencies are:

- DHS
- DoD/COCOMs/Military Services
- DOE
- DOT
- The IC
- NIST
- NSF

[48] "Cyber Threat and Vulnerability Analysis of the U.S ...," 01-Aug-2016. [Online]. Available: https://www.energy.gov/sites/prod/files/2017/01/f34/CyberThreatandVulnerabilityAnalysisoftheU.S.ElectricSector.pdf. [Accessed: 17-Jun-2018].
[49] "Critical Infrastructure: Security Preparedness and Maturity," Ponemon Institute: Unisys, July 2014,
[50] [50] "Cyber Threat and Vulnerability Analysis of the U.S ...," 01-Aug-2016. [Online]. Available: https://www.energy.gov/sites/prod/files/2017/01/f34/CyberThreatandVulnerabilityAnalysisoftheU.S.ElectricSector.pdf. [Accessed: 17-Jun-2018].

DHS has already established public-private partnerships with all 16 critical infrastructure sectors through establishment of Government Coordinating Councils (GCCs) and Sector Coordinating Councils (SCCs) for each sector. DHS is fostering Cyber Resilience through such programs as:

- Stakeholder Engagement and Cyber Infrastructure Resilience (SECIR) division services https://www.dhs.gov/stakeholder-engagement-and-cyber-infrastructure-resilience

- Critical Infrastructure Cyber Community Voluntary Program (C3VP) https://www.dhs.gov/stakeholder-engagement-and-cyber-infrastructure-resilience

- Cybersecurity Advisors https://www.dhs.gov/stakeholder-engagement-and-cyber-infrastructure-resilience

- Cyber Resilience Review (CRR) https://www.dhs.gov/sites/default/files/publications/CRR%20Fact%20Sheet.pdf

Policy Recommendations

Leverage Existing Partnerships such as ISACs

Organizations can leverage existing private public partnerships such as Information Sharing & Analysis Centers, Sector Coordinating Councils and the National Cyber Forensics & Training Alliance to enhance their cyber readiness and test their cyber communication and response plans.

The concept of Information Sharing & Analysis Centers (ISACs) was introduced in 1998 pursuant to Presidential Decision Directive-63 (PDD-63). The federal government asked each critical infrastructure sector to establish sector-specific organizations to share information about threats and vulnerabilities. 1 Now there are over a dozen ISACs in a variety of different sectors including Communication, Defense, Electricity, Financial Services, Information Technology and Multi-State. Some of the information sharing capabilities include:

- Secure web portals with anonymous incident reporting
- 24 x 7 watch desk for cyber and physical threat reporting
- Member surveys and industry best practices
- Committees and working groups on special topics
- All hazards sector playbooks and tabletop exercise programs

Most ISACs have a Sector Coordinating Council (SCC) that provides strategic leadership at the executive level and collaborates with government partners on policy issues concerning cyber readiness. For example, the Department of Treasury is the Sector Specific Agency for the

Financial Sector Coordinating Council (FSSCC). The FSSCC and Treasury have developed a strong public-private partnership with the shared goal of maintaining a robust and resilient financial services sector.

The National Cyber & Forensics Training Alliance (NCFTA) founded in 2002 is a non-profit corporation focused on identifying, mitigating, and neutralizing cybercrime. In contrast to ISACs, which have a sector=specific mission, the NCFTA takes a cross-sector approach to cybercrime investigations. SMEs from the public, private and academic sectors share information onsite to identify and mitigate cyber threats. Industry partners collaborate with each other in order to better protect their corporate networks and reduce fraud to their customer base. NCFTA hosts a number of different working groups, including one dedicated to Critical Infrastructure Supply Chain issues:

1. https://www.nationalisacs.org/about-isacs
2. https://www.fsscc.org/About-FSSCC
3. https://www.ncfta.net/

Increase Information Sharing and Public-Private Partnership Through the Local, State, and Federal Levels

Critical cyber-physical infrastructure would benefit greatly from regional, SLTT public-private programs, like PRISEM. Regional programs allow stakeholders to leverage proximity, personal relationships and varying levels of resources, be they technical or material. This would amplify cyber-situational awareness, resilience and threat mitigation across a variety of sectors.

These regional programs could enhance the information sharing and coordination between various levels of government. One possibility is increasing the ability for critical infrastructure stakeholders to have sensitive, bi-directional communication with Federal agencies for the purposes of assessment and threat mitigation. In conjunction, regional and SLTT cyber-resilience partnerships would potentially benefit from an increased presence of Federal partners. Conceivably, these Federal partners could be stewards and interlocutors for the programs.

Finally, an increased Federal partnership with regional, SLTT programs could lead to increased decision-maker awareness, technology transfer and funding for critical infrastructure in potentially at-risk regions.

Increase decision-maker awareness and understanding of Cyber Resiliency and its necessity for supporting U.S. national security and the economy of the 21st century

The United States is among the most vulnerable nations in the world to Cyber-attacks given its high degree of dependence on digital information and communications technology (ICT). The

United States also has very sophisticated Cyber adversaries like China and Russia as well as lesser, but growing in sophistication, adversaries like North Korea and Iran. A coordinated Cyber-attack by one of the more sophisticated adversaries could potentially bring the U.S. to its knees economically with a consequent weakening of national security.

To ensure our Cyber-dependent critical infrastructure systems and Government enterprises can withstand a sophisticated coordinated cyber-attack, those systems and enterprises must be made cyber resilient. The first step on the path to cyber resilience begins with an awareness and understanding of cyber resilience and what it can do to withstand such attacks. Unfortunately, as found during the team's trip to Seattle, the level of awareness and understanding among decision-makers in both the private and public sector is very low today.

The CRR Team recommends several initiatives aimed at increasing awareness:

1. That NIST be funded to conduct regional workshops across the nation on its publication, NIST SP 800-160 Vol.2.
2. That DHS make competitive awards to several commercial Cyber security training vendors to offer courses in cyber resiliency.
3. That OMB make cyber resiliency training mandatory for CIOs and CSOs across the U.S. Government.
4. That this report be widely disseminated to critical infrastructure owners/operators, Federal, State, and local agencies.

Appendix A

Table 1. *Cyber Resiliency Objectives*

Objective	Description	Examples Methods to Achieve
Prevent or Avoid	Preclude the successful execution of an attack or the realization of adverse conditions.	• Apply basic cyber hygiene and risk-tailored controls. • Limit exposure to threat events. • Decrease the adversary's perceived benefits. • Modify configurations based on threat intelligence.
Prepare	Maintain a set of realistic courses of action that address predicted or anticipated adversity.	• Create and maintain cyber courses of action. • Maintain the resources needed to execute cyber courses of action. Resources include not only cyber resources, but also personnel (with the proper training) and procedures. • Validate the realism of cyber courses of action. • Use validation methods that include testing or exercises.
Continue	Maximize the duration and viability of essential mission or business functions during adversity.	• Minimize degradation of service delivery. • Minimize interruptions in service delivery. • Ensure that ongoing functioning is correct.
Constrain	Limit damage from adversity.	• Identify potential damage. • Isolate resources to limit future or further damage. • Move resources to limit future or further damage. • Change or remove resources and how they are used to limit future or further damage.

Reconstitute	Restore as much mission or business functionality as possible after adversity.	• Identify untrustworthy resources and damage. • Restore functionality. • Heighten protections during reconstitution. • Determine the trustworthiness of restored or reconstructed resources.
Understand	Maintain useful representations of mission and business dependencies and the status of resources with respect to possible adversity.	• Understand adversaries. • Understand dependencies on and among systems containing cyber resources. • Understand the status of resources with respect to threat events. • Understand the effectiveness of cybersecurity and controls supporting cyber resiliency.
Transform	Modify mission or business functions and supporting processes to handle adversity and address environmental changes more effectively.	• Redefine mission / business process threads for agility. • Redefine mission / business functions to mitigate risks.
Re-Architect	Modify architectures to handle adversity and address environmental changes more effectively.	• Restructure systems or subsystems to reduce risks. • Modify systems or subsystems to reduce risks.

Table 2: *Cyber Resilience Techniques*

Technique	Purpose
Adaptive Response Implement agile cyber courses of action to manage risks.	Optimize the ability to respond in a timely and appropriate manner to adverse conditions, stresses, or attacks, or to indicators of these, thus maximizing the ability to maintain mission or business operations, limit consequences, and avoid destabilization.
Analytic Monitoring Monitor and analyze a wide range of properties and behaviors on an ongoing basis and in a coordinated way.	Maximize the ability to detect potential adverse conditions, reveal the extent of adverse conditions, stresses, or attacks, and identify potential or actual damage. Provide data needed for situational awareness.

Coordinated Protection Ensure that protection mechanisms operate in a coordinated and effective manner.	Require an adversary to overcome multiple safeguards (i.e., implement a strategy of defense-in-depth). Increase the difficulty for an adversary to successfully attack critical resources, increasing the cost to the adversary, and raising the likelihood of adversary detection. Ensure that the use of any given protection mechanism does not create adverse, unintended consequences by interfering with other protection mechanisms. Validate the realism of cyber courses of action.
Deception Mislead, confuse, hide critical assets from, or expose covertly tainted assets to, the adversary.	Mislead or confuse the adversary, or hide critical assets from the adversary, making the adversary uncertain how to proceed, delaying the effect of the attack, increasing the risk of being discovered, causing the adversary to misdirect or waste its resources, and exposing the adversary tradecraft prematurely.
Diversity Use heterogeneity to minimize common mode failures, particularly attacks exploiting common vulnerabilities.	Limit the possibility of loss of critical functions due to failure of replicated common components. Cause an adversary to expend more effort by developing malware or other TTPs appropriate for multiple targets; increase the probability that the adversary will waste or expose TTPs by applying them to targets for which they are inappropriate; and maximize the probability that some of the defending organization's systems will survive the adversary's attack.
Dynamic Positioning Distribute and dynamically relocate functionality or system resources.	Increase the ability to rapidly recover from non-adversarial events (e.g., fires, floods). Impede an adversary's ability to locate, eliminate, or corrupt mission or business assets, and cause the adversary to spend more time and effort to find the organization's critical assets, thereby increasing the probability of the adversary revealing its actions and tradecraft prematurely.
Dynamic Representation Construct and maintain current representations of the posture of missions or business functions considering cyber events and cyber courses of action.	Support situational awareness. Enhance understanding of dependencies among cyber and non-cyber resources. Reveal patterns or trends in adversary behavior.
Non-Persistence	Reduce exposure to corruption, modification, or compromise. Provide a means of curtailing an

Generate and retain resources as needed or for a limited time.	adversary's intrusion and advance and potentially removing malware or damaged resources from the system.
Privilege Restriction Restrict privileges based on attributes of users and system elements as well as on environmental factors.	Limit the impact and probability that unintended actions by authorized individuals will compromise information or services. Impede an adversary by requiring them to invest more time and effort in obtaining credentials. Curtail the adversary's ability to take full advantage of credentials that they have obtained.
Realignment Align system resources with core aspects of organizational missions or business functions.	Minimize the connections between mission-critical and noncritical services, thus reducing the likelihood that a failure of noncritical services will impact mission-critical services. Reduce the attack surface of the defending organization by minimizing the probability that non-mission or business functions could be used as an attack vector.
Redundancy Provide multiple protected instances of critical resources.	Reduce the consequences of loss of information or services. Facilitate recovery from the effects of an adverse cyber event. Limit the time during which critical services are denied or limited.
Segmentation Define and separate system elements based on criticality and trustworthiness.	Contain adversary activities and non-adversarial stresses (e.g., fires, floods) to the enclave or segment in which they have established a presence. Limit the set of possible targets to which malware can easily be propagated.
Substantiated Integrity Ascertain whether critical system elements have been corrupted.	Facilitate determination of correct results in case of conflicts between diverse services or inputs. Detect attempts by an adversary to deliver compromised data, software, or hardware, as well as successful modification or fabrication.
Unpredictability Make changes randomly or unpredictably.	Increase an adversary's uncertainty regarding the system protections which they may encounter, thus making it more difficult for them to ascertain the appropriate course of action.

Table 3: *Strategic Design Principles*

Strategic Design Principles	Key Ideas	Related Design Principles From Other Disciplines

Focus on common critical assets.	Limited organizational and programmatic resources need to be applied where they can provide the greatest benefit. This results in a strategy of focusing first on assets which are both critical and common, then on those which are either critical or common.	**Security:** Inverse Modification Threshold. **Resilience Engineering:** Physical Redundancy, Layered Defense, Loose Coupling. **Survivability:** Failure Mode Reduction, Fail-Safe, Evolution.
Support agility and architect for adaptability.	Not only does the threat landscape change as adversaries evolve, so do technologies and the ways in which individuals and organizations use them. Both agility and adaptability are integral to the risk management strategy, in response to the risk framing assumption that unforeseen changes will occur in the threat, technical, and operational environment through a system's life cycle.	**Security:** Secure Evolvability, Minimized Sharing, Reduced Complexity. **Resilience Engineering:** Reorganization, Human Backup, Inter-Node Interaction. **Survivability:** Mobility, Evolution.
Reduce attack surfaces.	A large attack surface is difficult to defend, requiring ongoing effort to monitor, analyze, and respond to anomalies. Reducing attack surfaces reduces ongoing protection scope costs and makes the adversary concentrate efforts on a small set of locations, resources, or environments that can be more effectively monitored and defended.	**Security:** Least Common Mechanism, Minimized Sharing, Reduced Complexity, Minimized Security Elements, Least Privilege, Predicate Permission. **Resilience Engineering:** Complexity Avoidance, Drift Correction. **Survivability:** Prevention, Failure Mode Reduction.
Assume compromised resources.	Systems and system components, ranging from chips to software modules to running services, can be compromised for extended periods without detection. In fact, some compromises may never be detected. Systems must remain	**Security:** Trusted Components, Self-Reliant Trustworthiness, Trusted Communications Channels. *Incompatible with Security:* Hierarchical Protection.

	capable of meeting performance and quality requirements nonetheless.	**Resilience Engineering:** Human Backup, Localized Capacity, Loose Coupling.
Expect adversaries to adapt.	Advanced cyber adversaries invest time, effort, and intelligence-gathering to improve existing and develop new TTPs. Adversaries adapt in response to opportunities offered by new technologies or uses of technology, as well as to the knowledge they gain about defender TTPs.	**Security:** Trusted Communications Channels. **Resilience Engineering:** Reorganization, Drift Correction. **Survivability:** Evolution.

Table 4: *Structural Design Principles*

Structural Design Principles	Key Ideas	Related Design Principles From Other Disciplines
Limit the need for trust.	Limiting the number of system elements that need to be trusted reduces the level of effort needed for assurance, as well as for ongoing protection and monitoring.	**Security:** Least Common Mechanism, Trusted Components, Inverse Modification Threshold, Minimized Security Elements, Least Privilege, Predicate Permission, Self-Reliant Trustworthiness, Trusted Communications Channels. **Resilience Engineering:** Localized Capacity, Loose Coupling. **Survivability:** Prevention.
Control visibility and use.	Controlling what can be discovered, observed, and used increases the effort needed by an adversary seeking to expand its foothold in or increase its impacts on systems containing cyber resources.	**Security:** Clear Abstraction, Least Common Mechanism, Least Privilege, Predicate Permission. **Resilience Engineering:** Localized Capacity, Loose Coupling. **Survivability:** Concealment, Hardness.

Contain and exclude behaviors.	Limiting what can be done and where actions can be taken reduces the possibility or extent of the spread of compromises or disruptions across components or services.	**Security:** Trusted Components, Least Privilege, Predicate Permission. **Resilience Engineering:** Localized Capacity, Loose Coupling. **Survivability:** Preemption, Hardness, Distribution.
Layer defenses and partition resources.	The combination of defense-in-depth and partitioning increases the effort required by an adversary to overcome multiple defenses.	**Security:** Modularity and Layering, Partially Ordered Dependencies, Minimized Sharing, Self-Reliant Trustworthiness, Secure Distributed Composition. **Resilience Engineering:** Layered Defense. **Survivability:** Hardness, Fail-Safe
Plan and manage diversity.	Diversity is a well-established resilience technique, removing single points of attack or failure. However, architectures and designs should take cost and manageability into consideration to avoid introducing new risks.	**Resilience Engineering:** Absorption, Repairability. **Survivability:** Heterogeneity.
Maintain redundancy.	Redundancy is key to many resilience strategies, but can degrade over time as configurations are updated or connectivity changes.	**Resilience Engineering:** Absorption, Physical Redundancy, Functional Redundancy. **Survivability:** Redundancy, Margin.
Make resources location-versatile.	A resource bound to a single location (e.g., a service running only on a single hardware component, a database located in a single datacenter) can become a single point of failure and thus a high-value target.	**Resilience Engineering:** Localized Capacity, Repairability. **Survivability:** Mobility, Avoidance, Distribution.
Leverage health and status data.	Health and status data can be useful in supporting situational awareness, indicating potentially suspicious behaviors, and	**Resilience Engineering:** Drift Correction, Inter-Node Interaction.

	predicting the need for adaptation to changing operational demands.	
Maintain situational awareness.	Situational awareness, including awareness of possible performance trends and the emergence of anomalies, informs decisions about cyber courses of action to ensure mission completion.	**Resilience Engineering:** Drift Correction, Inter-Node Interaction.
Manage resources and risk adaptively.	Risk-adaptive management supports agility, providing supplemental risk mitigation throughout critical operations, despite disruptions or outages of components.	**Security:** Trusted Components, Hierarchical Trust, Inverse Modification Threshold, Secure Distributed Composition, Trusted Communications Channels; Secure Defaults, Secure Failure and Recovery. **Resilience Engineering:** Reorganization, Repairability, Inter-Node Interaction. **Survivability:** Avoidance.
Maximize transience.	Use of transient system elements minimizes the duration of exposure to adversary activities, while periodically refreshing to a known (secure) state can expunge malware or corrupted data.	**Resilience Engineering:** Localized Capacity, Loose Coupling. **Survivability:** Avoidance.
Determine ongoing trustworthiness.	Periodic or ongoing verification and/or validation of the integrity or correctness of data or software can increase the effort needed by an adversary seeking to modify or fabricate data or functionality. Similarly, periodic or ongoing analysis of the behavior of individual users, system components, and services can increase suspicion, triggering responses such as closer monitoring, more	**Security:** Self-Reliant Trustworthiness, Continuous Protection, Secure Metadata Management, Self-Analysis, Accountability and Traceability. **Resilience Engineering:** Neutral State. **Survivability:** Fail-Safe.

	restrictive privileges, or quarantine.	
Change or disrupt the attack surface.	Disruption of the attack surface can cause the adversary to waste resources, make incorrect assumptions about the system or the defender, or prematurely launch attacks or disclose information.	**Resilience Engineering:** Drift Correction **Survivability:** Mobility, Deterrence, Preemption, Avoidance.
Make the effects of deception and unpredictability user-transparent.	Deception and unpredictability can be highly effective techniques against an adversary, leading the adversary to reveal its presence or TTPs, or to waste effort. However, when improperly applied, these techniques can also confuse users.	**Security:** Efficiently Mediated Access, Performance Security, Human Factored Security, Acceptable Security. **Survivability:** Concealment.

Disclaimer Statement:
"This document is provided for educational and informational purposes only. The views and opinions expressed in this document do not necessarily state or reflect those of the U.S. Government or the Public-Private Analytic Exchange Program participants, and they may not be used for advertising or product endorsement purposes. All judgments and assessments are solely based on unclassified sources and are the product of joint public and USG efforts."