Addressing Critical Infrastructure Cyber Threats for State and Local Governments

Application of a Threat-Centric Approach through the NIST Cybersecurity Framework

Introduction

"Our country will, at some point, face a major cyber event that will have a serious effect on our lives, our economy and the everyday functioning of our society."

This grave warning came from the former United States Secretary of the Department of Homeland Security Janet Napolitano back in 2013. Fortunately, this has not yet come true. Nevertheless, few will dispute that a large-scale cyber attack on a federal, state, or local government's critical infrastructure would have significant, long-term impacts on society. Never before has there been such an urgent need to act – and not just at the federal level.

Entrusted with the safety and protection of the public from a variety of threats, state and local governments (SLGs) must continuously develop their capabilities and knowledge of today's sophisticated cyber threats. Recent high-profile attacks by malicious state and non-state actors against both commercial and government entities have raised awareness and created a renewed sense of urgency to better understand and protect critical operations. In 2015, the National Association of State Chief Information Officers cited cybersecurity as the number one strategic IT priority for state and local government agencies.[1]

While IT organizations at the SLG levels are renewing focus on securing their networks, safeguarding citizen data and personal information, and building resilience against malicious actors, they face unique challenges due to limited resources, complex regulations, and an increasingly sophisticated threat environment. With so many competing priorities – and a need to make sure everyone from executives to security practitioners are coordinated – SLGs need a framework to tackle challenges and address risk.

Critical infrastructure sectors often face some of the greatest challenges due to the vital services they provide and the impact that could result should they be breached. A cyber attack on a critical infrastructure's networks could cause serious disruptions in the oil and natural gas, electric, water, transportation, telecommunications, and financial sectors. The increased interconnectedness of our networks through the acceleration of the Industrial Internet of Things (IIoT) increases the threat surface and destructive capacity of these attacks. SLGs must be actively engaged with industry to apply an effective risk management approach across all critical infrastructure sectors that promotes resiliency should a breach take place.

This white paper will explore these unique challenges facing SLGs in addressing cyber threats aimed at critical infrastructure and offer guidance on resources available to better prepare organizations. Moreover, it will explore how SLGs can adopt a threat-centric approach to improve critical infrastructure resiliency, reliability, and preparedness by following the National Institute of Standards and Technology (NIST) Cybersecurity Framework. This model reduces complexity and provides visibility, continuous control, and advanced threat protection across the extended network and attack continuum before, during, and after a cyber attack. It also provides SLGs with a tested, risk-based approach to tackle cyber threats.

[1]NASCIO, Federal Advocacy Priorities, January 22 2015, available at: http://www.nascio.org/Newsroom/ArtMID/484/ArticleID/62/NASCIO-Releases-Federal-Advocacy-Priorities-Cybersecurity-tops-list-followed-by-modernizing-regulations-and-collaborating-on-broadband-projects

Case Study:
Oil and Natural Gas

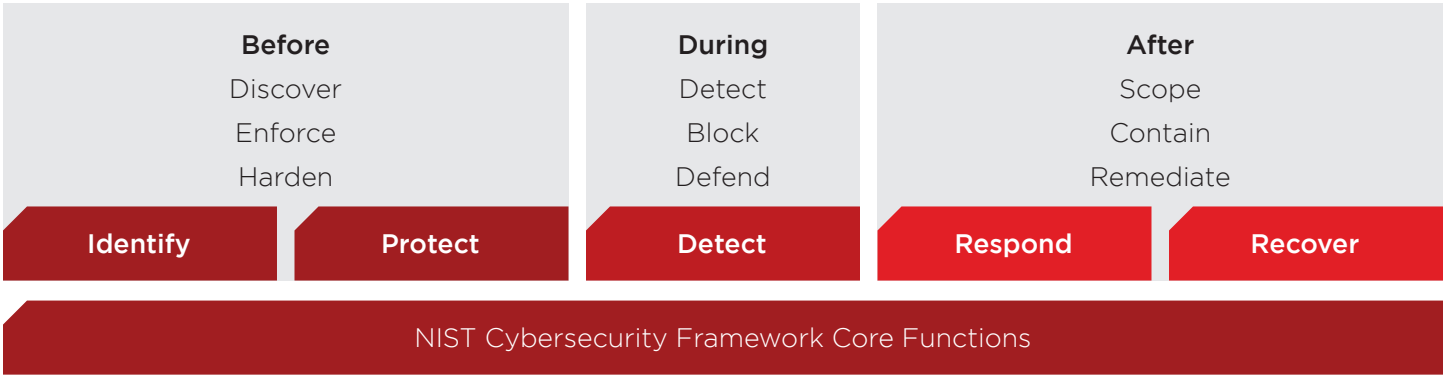
Malicious cyber-attacks stemming from an insider threat is a growing concern given the ensuing damage it can quickly cause. In August 2012, a person with privileged access to Saudi Aramco's (the Saudi state-owned oil company) computers unleashed a computer virus that erased three-quarters of the company's corporate PCs and resulted in an immediate shutdown of the company's internal network. Segregation of the company's internal communications network from the company's oil production operations limited the physical damage that could have ensued.

Key Resources: The NIST Cybersecurity Framework

On February 12, 2013, President Barack Obama issued Executive Order 13636, "Improving Critical Infrastructure Cybersecurity." The order directs the Executive Branch to "enhance the security and resilience of the Nation's critical infrastructure"[2] by developing a voluntary and technology-neutral cybersecurity framework for critical infrastructure sectors, promoting the adoption of robust cybersecurity practices, and enhancing the quality and efficiency of cyber threat information sharing.

Critical infrastructure sectors, as defined by Executive Order 13636, are "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[3] The result of the Executive Order is the *NIST Framework for Improving Critical Infrastructure Cybersecurity*,[4] a set of standards for cybersecurity risk established to protect the complex systems of interconnected components and subcomponents within critical infrastructure sectors. It is a joint effort between industry and government to address the increasing role of cybersecurity in physical security by creating a comprehensive approach – including standards, guidelines, and practices – for protecting critical infrastructure.

Critical infrastructure networks are becoming smarter, more automated, and more connected, which makes them more vulnerable to cyber threats. Since networks were originally designed to provide information for control purposes in an isolated, air-gapped network, prevention of cyber attacks was not considered in the original business and design process. Now recognized as a major flaw and risk factor, this design must be adapted to improve its cybersecurity capabilities. Both public and private sectors have prioritized implementing new standards focused on both cyber and physical risk management.



[2]The White House, Office of the Press Secretary, Executive Order – Improving Critical Infrastructure Cybersecurity, February 12 2013, available at: https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[3]Ibid.

[4]From here on the NIST Framework will often be referred to as the "NIST Cybersecurity Framework", the "NIST Framework" or the "Framework"

Technology alone has never been enough to protect the critical infrastructure sector from the growing number and sophistication of cyber threats, and this is something the NIST Framework recognizes from the start. Half of the Framework's core categories cannot be addressed by technology alone, reflecting the importance of people and process. Rather, the Framework Core reflects the roles of people and processes alongside technology. The Core is organized into five concurrent and continuous cybersecurity "functions." They are (1) Identify, (2) Protect, (3) Detect, (4) Respond, and (5) Recover. These functions define the Framework's risk-based approach that dynamically engages in an ongoing process of identifying, assessing, and responding to risk.

Beyond laying out five core functions, the NIST Cybersecurity Framework also defines roles that people, processes, and technology should assume in an effort to help organizations optimize their cybersecurity activities and creates a common set of language for clearer communications. A common language provides a foundation upon which all members of an organization – whether executives or IT staff – can understand their risk (internal and external) and assess their most critical assets. Because SLGs often have limited resources devoted to protecting their systems, the Framework suggests prioritizing assets to determine their highest priorities, and associated facets, in order to maximize the impact of cybersecurity spending and align cybersecurity with business risk. What is novel about the NIST Framework is that it does not call for nor create new standards. Instead, the Framework assembles all standards, guidelines, and practices that are working effectively in the private sector, and puts forth a comprehensive process for using them in a coherent way to address risk. By complementing existing risk management programs, the Framework addresses the importance of process-related security controls like clearly defined incident detection and response processes. Many organizations have well-defined risk management programs that include business continuity and disaster recovery plans, but fall short when it comes to cybersecurity risk management. The Framework's success is realized by its organizational ability to integrate effective cybersecurity risk management directly into an organization's overall risk management programs.

Technology-based solutions have never been sufficient to combat cyber threats, and their limitations are becoming more visible as the application of IIoT expands. As seen within the critical infrastructure sectors, security is no longer confined to perimeter defense and organizations must protect across the entire attack continuum and continue to adapt their organizations to evolving threats. The NIST Cybersecurity Framework ensures future extensibility and enables technical innovation by focusing on how people, process, and technology work in conjunction.

Addressing cybersecurity is now a board room conversation and priority. Risk management and incident response plans must be communicated to all stakeholders and receive buy-in from the Board of Directors, stakeholders, and C-suite leadership. Moreover, risk mitigation and incident responses plans should be practiced, tested, and adjusted to ensure that best practices and appropriate security controls are being implemented. The Framework will continue to evolve with technological innovation and new business requirements. For agencies and organizations of all sizes, particularly SLGs, it should be seen as a valuable resource as they respond to changing threats and adjust their own approaches to securing both the physical and networked components of their organizations.

Most significant is the universal applicability of the Framework. Apart from the critical infrastructure sector, healthcare providers, higher education institutions, and other entities can benefit from adopting the Framework. It enables all organizations to improve security and resilience in the absence of a perfect plan. The growth in number and sophistication of cyber attacks coupled with the expansion of the IIoT has created an urgent need for risk mitigation, containment, and remediation strategies. The NIST Cybersecurity Framework applies to all organizations across the public and private sectors, regardless of size, degree of risk, or level of attack sophistication.

Case Study: Transportation

Cyber intrusions can yield sizable financial costs. After the May 2015 train crash that paralyzed the Northeast corridor, Amtrak estimated that each day of lost service carried a potential economic loss of $100 million to affected businesses and consumers.[5] America's railroads account for 40% of intercity freight volume with 3 million cars filled with food, 2 million filled with chemicals, and the transportation of 70% of all coal.[6] A cyber attack on a major passenger or freight carrier could inflict comparable damage to regional or even national economies.

Dynamic Challenges for State and Local Government

For SLGs, protecting critical infrastructure networks is a growing concern as control and management systems become increasingly dependent on information technology. The IIoT creates an entirely new economy, but it also introduces new vulnerabilities into the equation due to increased automation and an increase in the number of interconnected devices. Industrial control systems were not originally built with advanced cybersecurity defenses in mind, which makes them more vulnerable to being compromised. In 2007, the Aurora Test demonstrated the ability of a cyber attack to destroy physical components of the electric grid. The experiment used a computer program to rapidly open and close a diesel generator's circuit breakers out of phase from the rest of the grid to cause an explosion. Another example of critical infrastructure at heightened risk for a cyber attack is the railroad system, which places infrared thermometers, ultrasound scanners and sensors, and microphones alongside railroad tracks to scan trains and identify equipment that is degraded or at risk of failing. If a cyber actor gained access to a monitoring system and altered the data, a railroad company could be unaware of an equipment failure and would be unable to prevent the consequences.

SLGs struggle to combat cyber threats in critical infrastructure sectors due to increasingly constrained budgets, a scarcity of qualified security personnel, and the sectors' underlying culture that typically segments operations. Budget challenges will always be an issue for SLGs. Trying to keep up with the ever-changing cyber threat environment with limited resources creates significant challenges for SLG leaders. These financial constraints make it increasingly difficult to hire professionals that understand both digital security and industrial control systems. There is a "human capital vulnerability" that opens the doors to cyber attacks, as 50% of the Framework's risk management approach is people and processes. SLG IT departments continue to focus too many of their resources on prevention and not enough on monitoring and response. Roughly 80% of state IT security budgets currently emphasize prevention measures, with only 15% focusing on monitoring and 5% on response.[7]

Another challenge unique to critical infrastructure sectors is the lack of coordination and communication between operational technology (OT) and information technology (IT) teams. Reliance on technology and the interconnectivity of OT and IT silos have expanded the potential vulnerabilities and increased potential risk to the critical infrastructure sector.[8] The concept of bringing these disciplines together to manage threats facing critical infrastructure sectors provides an instant value proposition for organizations. "Converged Security" would improve communication, security incident response, cybersecurity budgets, and the aggregation of security intelligence. Now more than ever, there is an increasing need for the two traditionally independent silos to converge, despite their history as separate entities with competing priorities.

[5]Crain's New York Business, Amtrak crash could cost economy $100M a day, May 14 2015, available at: http://www.crainsnewyork.com/article/20150514/BLOGS04/150519940/amtrak-crash-could-cost-economy-100m-a-day

[6]CSO, Tunnel vision: Train security as critical as planes and automobiles, September 8 2014, available at: http://www.csoonline.com/article/2603014/critical-infrastructure/tunnel-vision-train-security-as-critical-as-planes-and-automobiles.html

[7]StateScoop, "States need to embrace cybersecurity framework, experts say," August 26 2015, available at: http://statescoop.com/csf-story/

[8]National Institute of Standards and Technology, Framework for Improvising Critical Infrastructure Cybersecurity, February 12 2014, available at: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

The Road Ahead: Industry and Government Working Together

Cyber vulnerabilities make the adoption of a risk management approach an increasingly vital part of protecting critical infrastructure networks. However, organizations and agencies cannot implement it on their own and require coordination and communication across both the public and private sectors. SLGs can best respond to critical infrastructure sector cyber threats by collaborating with the Federal government and the private sector. For example, in an effort to leverage cost effective cybersecurity solutions, it is imperative that SLGs engage in information sharing via public-private partnerships, such as critical infrastructure Information Sharing and Analysis Centers (ISACs) that provide comprehensive sector analysis shared within the sector, with other sectors, and with the Federal government.[9] Public and private sector entities should share knowledge about the changing threat environment, encountered attacks, and incident response to better collectively inform today's approaches to cybersecurity and risk management. SLGs should also leverage the information sharing provided by Fusion Centers, mechanisms created by the Departments of Homeland Security and Justice to receive, analyze, disseminate, and gather threat information.[10] Fusion Centers are uniquely situated to empower SLGs to protect critical infrastructure by leveraging information from decision-making components at all levels of government and industry.

SLGs can also take advantage of cyber initiatives from the National Governors' Association, the National Association of State CIOs (NASCIO), the SLTT Cyber Engagement Program, and the C^3 Voluntary Program in addition to the NIST Cybersecurity Framework. The Critical Infrastructure Cyber Community C^3 ("C Cubed") Voluntary Program is a partnership among the Department of Homeland Security, various sector-specific government agencies, and the critical infrastructure community to help people understand and use the NIST Cybersecurity Framework. This program facilitates outreach efforts like webinars that allow participants to collaborate and ask questions. It also encourages feedback from past participants and shares the feedback with NIST so that future revisions can be improved. SLGs that collaborate through public-private partnerships will have a substantial advantage to counter today's cyber threats to the critical infrastructure sector.

Why a Threat-Centric Approach Works

Never before has it been so vital to take a threat-centric approach that addresses cybersecurity across the entire attack continuum – before, during, and after the attack. Threat-centric security improves visibility, provides context and consistent control, and reduces complexity and fragmentation. Cisco has built its threat-centric security offerings to align with the NIST Cybersecurity Framework's five core functions: Identify, Protect, Detect, Respond, and Recover.

In a threat-centric model, the "Before" phase provides the necessary capabilities to discover, enforce, and harden which are essential steps to achieve the Framework's "Identify" and "Protect" core functions. Critical infrastructure sectors must better understand the cyber threat landscape as a first step in prioritizing their assets and structuring their cybersecurity risk management and incident response plans. This includes identifying the cyber threat actors, understanding their motivations, and comprehending their sophistication and capabilities. Cyber attacks to critical infrastructure networks and systems can intentionally corrupt information, deny access to or delay information, destroy or overwhelm networks, undermine their integrity, and steal sensitive information for financial gain. Not every asset requires the same level of security so organizations have to identify their critical assets, prioritize them based on sustaining operations, and designate them with a risk tolerance. Knowing the risk surface is essential to designing a risk management plan and comprehensive set of security controls that reflect an adaptive threat. While often challenging for critical infrastructure sectors due to legacy industrial control systems, organizations should strive to have security controls integrated into the underlying infrastructure planning and design process.

The "During" phase offers solutions that allow critical infrastructure sectors to detect, block, and defend against sophisticated attacks, thus aligning with the Framework's "Detect" function. Part of an organization's risk management plan involves the development of security controls that continuously monitor for anomalies and other notable events. Organizations know what assets they need to protect, highlighting the significance of detection processes that implement the appropriate security controls in a timely manner. These processes determine what networks or systems are compromised and which ones should be quarantined or taken off-line. The "During" phase of the attack continuum is central for critical infrastructure networks and systems because they are interconnected and an attack on one can have implications for others. For example, if the electric power grid is brought down, many utilities and transportation sectors could not operate without power. Further, the stakes are much higher for critical infrastructure sectors. Extending beyond financial costs and a damaged reputation, the consequences of a cyber attack could potentially impact societal order and the general public's physical well-being.

[9]National Council of ISACs, Information Sharing and Analysis Centers (ISAC), available at: http://www.isaccouncil.org/aboutus.html

[10]U.S. Department of Homeland, National Network of Fusion Centers Fact Sheet, August 21 2015, available at: http://www.dhs.gov/national-network-fusion-centers-fact-sheet

Finally, the "After" phase enables organizations to scope and contain an attack after a breach and to quickly remediate the damage. These critical competencies align with the Framework's "Respond" and "Recover" functions that support swift recovery to normal operations, reducing the impact of an attack. Upon breach detection, critical infrastructure sectors must implement an incident response plan, developed as part of their risk management strategy. It takes a network to fight a network, thus responding to a cyber attack must use a networked approach where all entities across an organization are involved – from IT and executive leadership to legal and physical security. The traditional IT and OT security silos must converge to provide the most effective incident response. As part of their response to a cyber attack, organizations should develop an internal and external communications plan that outlines the cyber event, risk management processes being deployed, initiatives in place to remedy the situation, and next steps for the organization. As soon as the cyber threat is mitigated, recovery planning begins by assessing security (IT and OT), evaluating lessons learned, and improving risk management processes.

Regardless of the industry, size, or resources available, organizations will never be fully protected from today's cybersecurity threats. Therefore, a threat-centric approach to addressing today's risks provides a tangible approach to swiftly and knowledgeably respond across an entire organization with prioritization to the most critical assets should a cyber incident happen. Cisco's alignment with the NIST Cybersecurity Framework is designed to provide intelligent cybersecurity for the real world.

Conclusion

Critical infrastructure is made of complex networks and systems that sustain our society and economy and a disruption to just one system could have grave consequences for other sectors, especially at the state and local government levels. State and non-state actors with malicious intent pose a profound threat to governments, private businesses, and consumers worldwide. The advent of the IIoT and the resulting interconnectedness of our networks accentuate these vulnerabilities. Furthermore, entities and individuals operating in this network rely on connected technologies in virtually every aspect of daily life, increasing the scope and severity of damage when an attack occurs. The consequences of cyber attacks on critical infrastructure sectors can be catastrophic in today's increasingly networked environment.

The Chertoff Group
1399 New York Avenue, NW
Washington, DC 20005
202 552-5280
www.chertoffgroup.com

Cisco Systems, Inc.
Corporate Headquarters
170 West Tasman Drive
San Jose, CA 95134
www.cisco.com