Mounting an Active Cyber Defense in the Nuclear World[1]

Introduction

Recent high-profile cyberattacks have begun to shed light on the risks inherent in our hyper- connected world. Despite these warning shots, the world remains collectively exposed. The pace of digitization and the rise of complex, hyper-connected systems increase the likelihood of more damaging cyberattacks in the future. This presents the question: how can the benefits of digital technology be unlocked in a responsible way?

Today's cyber threats are increasingly dangerous, and include sophisticated, target-focused attacks.[2] These attacks often rely upon enduring vulnerabilities such as human behavior and practices. They can also utilize custom exploits and access gained through supply chain vulnerabilities, and have proven effective in compromising conventional cybersecurity defenses. Well-resourced, persistent adversaries can defeat[3] even the most technologically advanced security solutions, meaning that responses must extend beyond technology and tools.[4]

At a nuclear facility[5], such an attack could compromise sensitive information or manipulate security, safety, or automation systems, with potentially catastrophic consequences.

Disturbingly, cyberattacks against critical infrastructure now occur with such frequency that the discovery of remote-control malware in an infrastructure control network no longer rings alarm bells unless it is specifically targeted to that facility.[6] This cultural shift to grudging acceptance of inadequate security measures is dangerous as it is often difficult (if not impossible) to determine the intent behind and full consequences (intended and unintended) of an attack.

Background and the Current Approach

To respond to these challenges a new strategy is needed, one that will minimize the consequences of a cyber intrusion and take advantage of tailored cyber defense practices. In the age of targeted cyberattacks it is no longer sufficient to simply build walls. The "fortress mentality" that has underpinned much of information security is no longer enough. Prevention alone is ultimately doomed

---

[1] This paper was prepared by Michael Assante and edited by NTI staff.

[2] The ability to exploit weaknesses in the complex system-of-systems that comprise modern organizations has invented underground markets, empowered activists, and transformed intelligence gathering and war fighting. The adversarial "cyber" threat actors that engage in targeted attacks continue to expand at an alarming rate, defeating security prevention and detection technology/controls, challenging conventional analysis, and invalidating existing reliability and safety design methods. Examples include campaigns and malware such as Snake, Ice Fog, Black Energy, Duqu, MiniDuke, Stuxnet, Regin, Night Dragon, etc.

[3] "What concerns me most about external cyber threats is that our current response model doesn't fit the existing world. We are responding to an asymmetric threat with a symmetric response, and we are behind. Alan Webber, IDC research director, 2016.

[4] http://www.csoonline.com/article/2980937/vulnerabilities/researcher-discloses-zero-day-vulnerability-in- fireeye.html

[5] Nuclear facilities include: nuclear reactors, enrichment and reprocessing plants and storage and research facilities. The potential implications of a successful cyberattack at such facilities varies.

[6] Reuters online, Christoph Steitz and Eric Auchard, German nuclear plant infected with computer viruses, operator says, April 27, 2016 http://www.reuters.com/article/us-nuclearpower-cyber-germany-idUSKCN0XN2OS

to fail; while walls should be built, alone these are insufficient.[7]

Given the potentially catastrophic consequences, the nuclear industry cannot afford to rely solely upon cyber walls in the age of cyber cannons. A successful, destructive cyberattack could profoundly shake collective confidence in the safety of nuclear energy. At the same time, the deployment of digital technologies in nuclear complexes around the world will not slow down, but can and should be informed by new thinking on cyber-physical defense strategies.

In the United States, for example, the Nuclear Regulatory Commission (NRC)[8] adopted guidance for a set of industry-developed guidelines in the 2005. The NRC issued a security rule in 2009 that required licensees submit a cybersecurity plan for every nuclear power plant to the NRC that described how the plant would implement their cybersecurity program and the necessary plant-by-plant schedule for implementation. Phase I is complete with implemented controls for most significant digital assets. Phase II is scheduled to be completed in the 2016-2017 timeframe, with licensees completing a full implementation of their reviewed cybersecurity program. The NRC recognizes that network segmentation-based prevention is not sufficient and has directed licensees to address additional avenues for cyberattacks. Unfortunately, this progress is being outpaced by demonstrated cyberattacks that have successfully defeated accepted industry practices inside of industries like financial services, which are considered far more mature and more invested in security technology. Some of the challenges to better cybersecurity for the nuclear industry include:

- Globally uneven and inconsistent regulatory approaches;
- Insufficient cyber training for facility engineers and operations staff;
- Overreliance on segmentation and one-way data flows as the basis of 'protection';
- Few security tools optimized for plant operational technology (OT) environments;
- Little detection capability beyond administrative networks;
- Very few practitioners experienced in industrial automation and safety systems; and
- Generally static environments that require a great deal of planning to address security vulnerabilities.

Referring to the diagram below, much of the current approach at nuclear facilities (and infrastructure generally) relies on secure architectures and simple passive defenses. The primary strategy is to prevent the dangers that come from infections of critical digital systems by isolating them from the Internet. A few countries have taken initial steps to develop both information protection programs and prevention-focused cybersecurity requirements[9]. These early efforts were showcased at the first dedicated "International Conference on Computer Security[10] in the Nuclear World," held by the International Atomic Energy Agency (IAEA) In June of 2015. Globally, the state of security ranges from

[7] Ars Technica, German nuclear plant's fuel rod system swarming with old malware, April 27, 2016

[8] 10CFR73.54 provides NRC the authority to regulate cybersecurity, the requirements include the need for a cybersecurity program that would be a component of the operating licenses. These requirements provided assurance that digital computer and communication systems and networks associated with safety and important to safety functions, security functions, emergency preparedness functions (including off-site communications), and support systems (SSEP) would be adequately protected up to and including the design basis threat (DBT).

[9] Several countries sent delegates to the IAEA's International Conference on Computer Security, providing presentations on regulatory frameworks and cybersecurity programs to include Canada, German, and the Republic of Korea to name a few.

[10] The very use of the term Computer Security seems to highlight how far behind the nuclear complex falls behind the conventional thought curve, let alone new thinking about cyber defense

few requirements and capabilities beyond business or administrative networks to an overreliance upon segmentation schemes and the identification of Critical Digital Assets to be prioritized for protection.

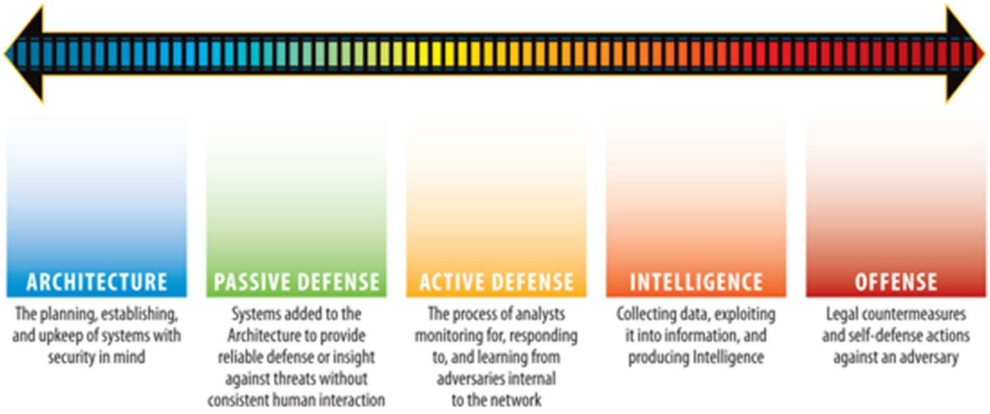

Figure 1: The Sliding Scale of Cybersecurity as conceptualized by Robert M. Lee of the SANS Institute[11]

This paper advocates moving to a new approach, which would also include active defense. Certain elements of the current approach, such as using continuous diagnostics monitoring[12] (CDM) to manage infrastructure, people, and processes and find and fix vulnerabilities, will play an important role in supporting an active defense strategy, but nuclear facilities must move beyond these tactics to embrace a more active strategy to counter persistent and well-resourced adversaries.

Establishing an Active Cyber Defense

Building walls to hide behind is an ineffective strategy in our modern world. Rather, we must pursue a strategy that allows defenders to better understand adversaries and anticipate their strategies and tactics for the purposes of finding and disrupting them—i.e. an active cyber defense.

An active defense--the process of analysts monitoring for, responding to, learning from, and applying their knowledge of threats internal to the network in order to detect, block, and eject adversaries.

An active defense strategy will make use of tools at the Architecture and Passive Defense stages of the Sliding Scale of Cybersecurity (Figure 1). CDM, for example, as well as actions taken to design security into networks as they are built, would fall under the Architecture heading. Security products and technologies added on to the system and network architecture that provides added visibility into the networked environment would fall under the Passive Defense heading. These tools would reduce the noise on the network by countering known malware and generating alerts, logs, or other visibility data into abnormalities that might indicate a focused and persistent adversary. In addition, see the NTI paper *on Reducing the Cyber Threat to Digital Systems: Minimizing Complexity,* for more information, as greater amounts of complexity increases the difficulty to define and identify deviations from normal expected behavior.

[11] https://www.sans.org/reading-room/whitepapers/analyst/sliding-scale-cyber-security-36240

[12] Richard Bejtlich, Chief Security Strategist of FireEye has been a vocal critic of CDM as a method to identify and respond to threats; he has made multiple congressional testimonies and blog entries regarding the topic. Some of this thoughts can be found here: http://taosecurity.blogspot.com/search/label/cdm

Together, a proper investment in Architecture and Passive Defense creates a defensible environment. However, this environment is not successfully defended until an active element, humans focused on countering threats, is introduced. Highly-trained and empowered security personnel anticipating, detecting, and neutralizing highly-trained adversaries within a defensible environment constitutes a defense strategy that does not lag behind the threats.[13]

Elements of an Active Cyber Defense

Establishing a cyber defense begins with understanding what must be protected. This is different than being required to stop any cybersecurity compromise or intrusion. A true cyber defense begins with the assumption that cyber prevention efforts will fail. Defense is about detecting a failure, quickly collapsing an attacker's free-time, anticipating their next moves, and disrupting their plans by removing options and eradicating capability and presence. The goals of cyber defenders are established by risk and engineering evaluations to determine which systems and data are critical to the mission of the facility. The focus should be on the critical functions that must be maintained or protected.

Cyber defense requires a working understanding of the digital and physical systems that can be compromised and leveraged to mount a deeper attack. This demands an accurate and current understanding of what systems exist and how they interact. Cyber defenders must identify surfaces that can be attacked and the pathways that attackers might use to reach them. This understanding is not easily achieved, and often requires more work than anticipated; in order to maintain this understanding, a separate team should verify the initial understanding and the data should be updated through a strong change control process. Most systems are complex enough that a tool, such as an asset tracking system, is necessary to house and manage the relevant information. This data cannot simply catalogue how a system is designed to work and communicate, but must be extended to capture all of the possibilities of how a system can be interacted with or communicate.

An organization must possess an appropriate number of well-trained and skilled staff serving in dedicated defense roles[14] to ensure success. This foundational element can be challenging, as people with demonstrated technical skills, creativity, and flexibility are difficult to find and retain.[15] While their numbers matter in terms of the ability to investigate and adequately respond to multiple indicators of compromise and suspicious behaviors while evolving their defensive capabilities to deal with the next intrusion attempt or to detect ongoing intrusions, the right skill mix is far more important than a large bench of defenders. In critical infrastructure, this skill mix involves a longer list of roles than conventional security. These include[16]:

- Threat intelligence analyst;
- Intrusion analyst;
- Incident responder;
- Forensic analyst;

[13] The key difference between an active and passive defense is the activity of the human operator. Passive defenses are tools and practices placed on top of the network architecture to provide a layer of security against adversaries whereas an active defense can only be performed by humans taking a proactive approach to security, often by leveraging the architecture and passive defenses.

[14] Although staff should be dedicated in their role, specific roles do not necessarily need to be onsite at the facility and can be leveraged across a complex.

[15] http://www.chicagotribune.com/business/ct-us-universities-cybersecurity-training-20160411-story.html

[16] ibid

- Malware reverse engineer; and
- Technical or team director.

Please see Appendix A for full descriptions of these roles.

Cyber defenders must assemble the proper tools and implement them to sufficiently cover both the most likely paths an attacker would take and the prioritized pathways[17] based on the identification of critical systems. Traditional approaches, such as monitoring segmentation or enforcement zones, while valuable processes, often fail as attackers figure out how to circumvent those gates. To make this more difficult for attackers, cyber defenders must implement broad monitoring and detection capabilities inside of networks and systems that are likely to be compromised, can be used as initial foothold or transit for attackers, house information or credentials that could assist attackers, or are considered critical and high-priority for protection.

Detection is only possible if one possesses a capable suite of sensors and can deploy those sensors to achieve the proper amount of coverage *as* industrial environments would benefit from custom sensors and novel techniques for detecting suspicious commands). Because advanced threat actors use Tactics, Techniques, and Procedures (TTPs) and train to avoid currently-available signature-based cyber detection solutions, cyber defenders need deep capabilities to detect and analyze communications and system behaviors.

Cyber defense must be able to contain and eradicate attackers. A cyber defense is not complete without the necessary capabilities to reduce and eliminate attacker options, communications, and tools. Where physical attacks are concerned, metrics (such as response time) exist to evaluate authorities' capabilities and calculate an "adequate" response or protection scheme. There is no such structure in place when it comes to the digital aspects of cyberattacks. The execution of the actual response should be well coordinated so that defenders can act swiftly and comprehensively within the attackers' Observe, Orient, Decide, Act (OODA) decision cycle. Defender actions can alert attackers, so preparing to act in a quick manner should place pressure on attackers as defenders begin to reduce the amount of options available. One of the more successful strategies is to remove interactive remote access while containing compromised systems and eradicating attacker presence.

The clear recognition of the risks associated with intelligent and co-adaptive cyber adversaries highlights the importance of a defense-based protection strategy. The preparation required to properly overlay a cyber defense for a defensible environment will provide benefits in both efficiency and system reliability.

Transitioning to an Active Cyber Defense

Transitioning to an active cyber defense begins by preparing a defensible environment and builds through fielding capable cyber defenders to achieve a more resilient, safe, and reliable infrastructure. The elements of a cyber defense includes good IT practices, verified architectures, properly instrumented and monitored systems, and well-equipped technical specialists.

Change at the facility level is unlikely to occur without changes at the regulator level. Regulators must

[17] Conducting a cyber-driven engineering evaluation of the critical functions and systems that can cause the greatest damage identifies prioritized paths.

recognize that the current approach is unlikely to succeed in the face of a determined adversary—as a key first step, regulators should ensure the facility operator will hire a defense team director and require the facility business and operational units to support him or her in the preparation, implementation, and training phases is the first step to building a program. A proposed outline for starting such a program is as follows:

- Preparation for a cyber defense;
- Team building, skills, and tools;
- First stage of a cyber defense;
- Planning to improve and mature a defense;
- Investments required; and
- Navigating challenges.

Organizations with an existing information security program could begin to develop an initial cyber defense capability by selecting IT and security staff to begin preparing plans and serving as incident responders, threat intelligence analysts, and intrusion analysts. This ad-hoc group could help newly hired team members with the proper competency mix to onboard, orient, and hit the ground running. This staff could also be sent to training to acquire the necessary hands-on skills to serve permanently in these roles.

Preparing to develop a cyber defense would require the technology management organization to identify computing assets and networking infrastructure, characterize and baseline network traffic, and track data flows. The simple process of capturing and analyzing traffic from facility control system networks would improve network performance as misconfigurations and problems are identified and addressed. The next step would be to conduct an engineering assessment to identify systems that are critical to achieving specific facility functions for both safety and operations. This evaluation should include how a particular piece of software, device, or network can be used maliciously, through existing functionality or modification, to disrupt processes, compromise safety, and/or damage equipment under control. The evaluation will result in a list of critical systems that can be used to identify potential attack surfaces and pathways.

The process of combining technology management specialists with facility engineering staff should expand the shared view of cyber risk. The cyber defense team should work with facility operations staff, in a joint effort to develop abilities to monitor and detect compromises and suspicious behavior. Risk scenarios will help by illuminating opportunities to engineer away potential consequences or to identify critical segments and systems to be monitored.

The transition to an active cyber defense at nuclear facilities will not be easy. In contrast to the current approach, it will require well-planned investments, additional hiring, and the use of more powerful security tools wielded by technically skilled and adaptive cyber defenders. Some individual facilities will find it very difficult to hire and retain highly technical staff; these entities would need to leverage national or industry shared-resources to develop their initial program. Centralizing deeper technical skills to include malware reverse engineering and intrusion analysis may offer a more effective strategy for a nuclear complex, but every facility should have dedicated staff with skills in both detection and incident response. Facility technology management practices need to be reviewed to address security concerns and enable a more dynamic change control process to manage attack surfaces and investigate suspicious activity. One of the most challenging requirements will be to develop a facility- specific approach to conducting cyber defense operations while in an operating state. This will demand the

successful integration of engineering and operations staff into the planning and decision-making process for the facilities cyber defense.

The ultimate goal is to develop and implement a capability that goes beyond simple prevention and provides an ability to detect and disrupt cyber intrusions and attackers. This positions the facility to better protect nuclear-significant systems and data. An integrated cyber defense strategy includes corresponding actions by facility operations to monitor critical system integrity, maintain safe operating conditions, and understand how adversaries operate inside of compromised systems. The greater situational awareness during cyber events can help to satisfy regulatory reporting requirements and provide a measure of confidence by being able to describe what systems are impacted and how that activity can be contained.

Conclusion

Advanced cyber actors are undeterred by static cybersecurity programs. The only way to manage the risk from an intelligent and co-adaptive threat is to build a cyber defense rooted in good security architectures and passive defenses, but having an effective active component. Nuclear infrastructures around the world have experienced non-catastrophic cyber incidents. Current defenses have proven adequate when facing less-structured, less capable cyber actors and standard Internet-facing cyberattacks, but are untested with more advanced cyber actors. The static defenses are required, but are insufficient to protect nuclear systems from more powerful cyber actors and future cyber threats.

A cyber defense that assumes static prevention will fail is necessary to respond to sophisticated cyber attackers. The stakes in nuclear infrastructure, as in military and government networks, are too high— meaning that they, too, must field cyber defense teams. It is paramount to develop a nuclear cyber defense strategy that is comprehensive, active, and clear-eyed about current threats. There are very real benefits that extend far beyond an enhanced cybersecurity posture and ability to defend systems. There are challenges in terms of available manpower, but increasing technical cyber skills is a necessity— not a luxury— in today's digitally empowered world.

Appendix A: Active Cyber Defense Personnel Summary

Threat Intelligence Analyst. A Threat Intelligence Analyst is responsible for establishing intelligence requirements, formulating a collection plan, collecting, analyzing, and disseminating information about the organization's threat landscape to the appropriate teams. It is also paramount that Threat Intelligence Analysts understand the difference between generating and consuming intelligence. Threat analyst working through the appropriate legal and security frameworks can disclose, share, and collaborate to analyze incidents with the broader community as a part of an active defense strategy.

Intrusion Analyst. Intrusion Analysts are those individuals who hunt throughout their organization to detect and initiate analysis on threats inside the organization's environment. These personnel take full advantage of the data available including network and system logs, network topologies and data flows, and alerts generated from the security architecture to find the threat, remediate it if it is incidental or minor, or make recommendations to initiate incident response procedures in the event of a more serious compromise. Senior intrusion analysts can also help make recommendations to the architects of the network to better shape the network into a more defensible system.

Incident Responder. Incident Responders are the front line defenders when a breach occurs. Not all compromises on a network require incident response. However, in the event that decision makers initiate incident response procedures these personnel ensure understanding of the scope of the problem. In practice, Incident Responders are guided by the other security personnel in the organization to infected systems and by their own analysis of the threat's indicators. Primary goals for incident responders include scoping the threat, collecting forensic evidence with volatile evidence prioritized, and working with architecture teams and system engineers to contain and remediate the threat once it is understood. More senior incident responders help posture the organization ahead of an incident to better prepare the planning, procedures, and response efforts. A significant majority of work done for any incident is done during the planning stages.

Forensic Analyst. Forensic Analysts interrogate collected forensic evidence to identify the impact of a compromise. Understanding the impact should include answering questions such as the what, where, when, and how of the compromise. These analysts prioritize uncovering the truth of the investigation, which ultimately leads to better understanding the threat itself. Traditionally, forensic analysis has been a back shop function of security, which took place over the course of months instead of directly complimenting the current security efforts. Forensic Analysts that are taking part in an active defense role should work to get the most viable data out of the evidence as quickly as possible for the purpose of injecting it into the security process.

Malware Reverse Engineer. Threats are not always malware based, but an overwhelming majority of threats faced today are enabled by malware or focused on its use. Malware Reverse Engineers should be able to analyze the malware in a timely way to support the hunt for it and its variants throughout the organization as well as understand its capabilities. Understanding malware capabilities can help prioritize defense and incident response efforts especially when multiple threats are being faced simultaneously. These analysts should be keenly aware of the organization's priorities and valuable assets to help guide informed decisions and remediation efforts against threats targeting these priorities or assets.

Technical/Team Director. Those individuals filling the Technical Director role for an organization's active defense efforts should be fully aware of their organization's operating environment to include the

people, processes, and technology present. This includes an understanding of the current security architecture of the organization as well as the efforts and tools leveraged by the active defenders. This position is responsible for collecting, coordinating, and communicating with government authorities and internally to respond to and capture the lessons learned from interactions with the adversary. The purpose of this effort should be to help the organization and its architecture evolve over time into a more secure state.