Teaching Cyber Resilience for Critical Infrastructure Systems

William Arthur Conklin[1]
waconklin@uh.edu

Anne Kohnke[2]
akohnke@ltu.edu

[1]College of Technology
University of Houston
Houston, TX

[2]College of Management
Lawrence Technological University
Southfield, MI

Abstract - Successful cyberattacks will occur no matter how much money and resources are dedicated to the problem. At the same time, the sectors in the current national infrastructure have not developed an effective standard strategy to protect themselves. The paradigm we present here argues that a cyberresilient strategy is an effective and cost-efficient approach to protecting the critical systems that power our way of life. This paper presents both a staged approach to implementing cyber-resilient systems as well as a general curriculum and pedagogy for disseminating this knowledge.

Keywords

Cybersecurity, Cyberresilient Strategy

1 INTRODUCTION

Cyberspace is full of adversaries ranging from state-sponsored hackers to skilled cybercriminals, to any person with a grudge and a connection to the Internet. Because of the proliferation of such threats, cyberattacks on the numerous elements of the U.S. critical infrastructure are a daily fact of life. For instance, the Industrial Control Systems-Computer Emergency Response Team (ICS-CERT) reports that U.S. industrial control systems were attacked at least 245 times over a 12-month period (OAS, 2015). In other parts of the world, a 2015 attack on Ukraine's power grid left 700,000 people without electricity (Brasso, 2016). The perpetrators of the Ukrainian attack were observed conducting similar attacks against the U.S. energy sector (Brasso, 2016). Although there was not an actual service disruption, many experts believe that those exploits were a probe for future moves on the U.S. infrastructure (Brasso, 2016).

The reason why the protection of our national infrastructure is so critically important is that a major exploit, like a successful cyberattack on the electrical grid, could leave the U.S. cloaked in darkness and unable to communicate without any form of twenty-first century transport. It would likely kill many thousands of citizens, perhaps millions, either through civil unrest, failure of public systems, or mass starvation (Brasso, 2016; Maynor, 2006).

Notwithstanding the disastrous nature of cyberattacks, the industries in our current national infrastructure have not developed coherent plans or effective strategies to protect themselves (Brasso, 2016). This includes the Chemical Sector; Commercial Facilities: Communications; Dams; the Defense Industrial Base; Emergency Services; Energy: Financial Services; Food and Agriculture; Government Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors, Materials, and Waste; Transportation; and Water and Wastewater Systems (PPD-21, 2013, p.2).

At the heart of the problem are the automated supervisory control and data acquisition (SCADA) systems that perform the myriad functions that underwrite

our daily life. In the generic SCADA architecture, data from sensors or manual inputs are sent to programmable logic controllers (PLCs) or remote terminal units (RTUs), which then pass that information through to human operators along a SCADA network. The complex control networks are central to the day-to-day achievement of the purposes of each of these sectors and SCADA operations permit unified control of dispersed devices through standard protocols. SCADA is ubiquitous in the infrastructure in that these types of systems underwrite the remote operation of a wide variety of systems and services.

The rise of microprocessors and programmable logic controllers (PLCs) in the early 1970s allowed organizations to remotely control their automated processes. In the 1990s, the introduction of more sophisticated networking and PC-based interfaces resulted in local area network (LAN) based SCADA systems (Russel, 2017). This continuing dispersal inevitably morphed into wide area network (WAN) connections and the internet. This final step ensured real-time access to the operations of everything from, manufacturing assembly lines, to home heating systems, often through remote devices (IEEE, 2012). This type of access helps organizations and even individuals make data-driven decisions about their individual operations (Boyer, 2010).

SCADA utilizes multiple software processes and hardware elements to monitor operational behavior, gather data, and record the second-by-second actions of every machine and device in a SCADA supervised system (Van Hoa, 2016). Thus, the components of a SCADA system are diverse. In practice, SCADA systems can manage large-scale organizational operations over great distances at multiple sites. The diversity and the wide dispersal of the sensors and controllers that comprise a typical system make SCADA tempting targets for attack.

This is especially true because the PLCs and RTUs in a SCADA system are deployed without any consideration of their resistance to attack. Therefore, there have been long-standing concerns about the overall SCADA powered infrastructure being vulnerable to cyberwarfare and cyberterrorism attacks and is one reason why

the cyber-resilience approach has gotten a lot of recent interest (Eisenhauer, 2006; Nat-Geo, 2017; Symantec, 2014; E-Y, 2014).

The cyber resilience approach is particularly suited to ensuring the continuing survivability of SCADA systems because the focus of a cyber resilient strategy is to maintain core functionality at all costs without consideration of defending less critical, or peripheral elements. The strict emphasis on survivability is the reason why cyber resilience, versus cybersecurity, is the approach of choice for critical systems.

Cybersecurity is based around ensuring all logical points of access to secure space whether electronic, human, or physical and normally requires an extensive resource commitment. Whereas, cyber resilience only ensures those elements that are deemed critical to system survival, this is particularly relevant to SCADA given the encapsulated, specific purpose function of most of the components in something like an electrical power system. In effect, each component's limited, well-defined purpose makes it easier to identify and protect only the critical elements.

Since the requirement to maintain the functioning of a few critical components is less resource intensive than the need to ensure the confidentiality, integrity and availability of all assets within secure space, cyber resilience is much more resource efficient. The narrowing of scope allows protection measures to be concentrated onto a far smaller attack surface, which theoretically ensures more effective protection for the things that simply can't be allowed to fail.

2 THE SEVEN STAGES OF CYBER RESILIENCY

Cyber resilience is founded on classification, prioritization, and comprehensive strategic policy-based deployment of a rigorous set of real-world security controls (Symantec, 2014). Cyber resilience involves the creation of a set of well-defined processes, which react to penetrations of the organizational perimeter (US-CERT, 2016). These standard processes are both electronic and behavioral in focus and they are designed to protect key assets, as well as ensure optimum recovery of the overall system in the event of successful attack (Symantec, 2014). This process is embodied

in seven generic principles shown in Figure 1 (Conklin, Shoemaker, & Kohnke, 2017).

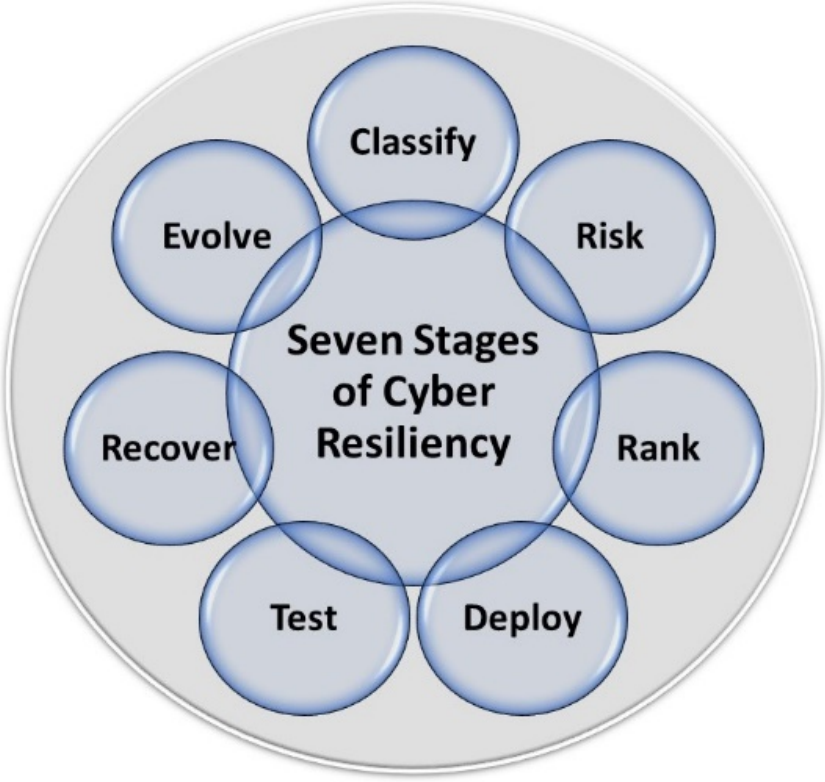

Figure 1, The Seven Stages of Cyber Resiliency

1. *Classify*—If assets are not identified, they cannot be protected therefore, all SCADA system assets must be identified, labeled, and arrayed in a coherent baseline of "things." This baseline describes all potential protection targets and it is maintained under strict configuration management. This is comparable to the "Classification" phase of the NIST Risk Management Framework (NISTb, 2014) and embodies the dictates of FIPS 199 (NISTa, 2004).

2. *Risk*—Resiliency requires appropriate situational awareness. Therefore, a broad-spectrum risk assessment must be performed that characterizes all known threat scenarios as they apply to the identified asset base of the SCADA system. This is a risk assessment process comparable to the "Security Assessment" phase of NIST SP 800-53a (NIST SP 800-53A Rev.4, 2014).

3. *Rank*—Assets in which the SCADA system absolutely can not afford to have compromised are selected, evaluated and a provably effective countermeasure response is deployed for each of the chosen assets. This is primarily an engineering design exercise, driven by knowledge of the components and their inter-relationships which was obtained in the "Classify" phase. Resources are focused on assuring only those components that are designated as critical. The resources that are left over are then allocated to protection and recovery of the rest of the system. This is analogous to the "Select" phase of the NIST Risk Management Framework (NISTb, 2014).

4. *Deploy*—The functionality to ensure resilience must be baked-into the architecture of the SCADA system in such a way that critical functions are assured; presuming a largely successful attack. This is a pure design/control deployment exercise comparable to the "Implement" phase of the NIST Risk Management Framework (NISTb, 2014) but control design and deployment are based on the recommendations for the relevant baselines as specified in NIST 800-53(4), (NIST SP 800-53A Rev.4, 2014).

5. *Test*—the SCADA system's architectural resilience must be assured. This is a planning and oversight function that characterizes the effectiveness of critical control performance against stated mission goals. Methods like penetration testing apply here. This is an assessment process comparable to the "Assess" phase of the NIST Risk Management Framework (NISTb, 2014).

6. *Recover*—Well-defined processes are documented and established to ensure that all of the SCADA systems functions are fully restored within requisite parameters. This is comparable to the "Plan-Purpose-Scope-Relationship" recommendations embodied in NIST SP 800-37 Rev. 1 (NISTc, 2010) and it embodies metrics suitable to evaluate disaster recovery performance (Bradford, 2017).

7. *Evolve*—The organization dynamically adjusts the SCADA system's cyber-resilient architecture based on lessons learned. This is comparable to the implementation of the NIST Cyber Security Framework process (NIST-CSF, 2014).

3 EMBEDDING CYBER RESILIENCE INTO HOW WE EDUCATE

Even though this commonly accepted seven-stage model specifies a viable evolutionary process for developing cyber-resilience in SCADA systems, it still lacks practical application. Therefore, to ensure that cyber-resilience is put into practice, the details about the specific activities and tasks that need to be performed must be widely disseminated in a complete and coherent fashion, which has been the traditional role of professional education and training.

The knowledge, skill, and ability (KSA) requirements for each of the requisite functions in this staged model must be fleshed out to educate practitioners about the steps necessary to create a cyber-resilient process. We have chosen to present the structuring and delivery of a model curriculum for cyber-resilience organized by the seven generic stages of the process.

3.1 Principle 1: Classify

In some respects, cyber resilience is nothing more than a specialized continuity management solution. The aim of cyber-resilience is to maintain critical organizational functions at all costs. In this respect, the decisions that come out of the cyber resilience classification process will determine how the business will invest its precious time and resources. Thus, the identification process is perhaps the most important step in creating a cyber-resilient organization because the outcome of the classification process will drive every subsequent protection action.

The key to cyber resilience is understanding what constitutes core functionality in each system and that is essentially an engineering design issue. All computerized systems are complex and highly interdependent so the essence of success lies in the identification of just those essential functions and relationships necessary to ensure basic system survival. Accordingly, a deliberate and formally documented classification activity is the logical starting point. Cyber resilience assumes that all systems will eventually be compromised. Given this assumption, the cyber resilience function ensures specifically targeted controls. These controls are designed to ensure that only the critical subset of functions essential to the continuing operation of the system are fully protected, even if all other system activities are compromised. This is an organization-wide exercise whose aim is to understand the criticality, sensitivity, and priority of all items in the asset base. It involves all stakeholders because buy-in is an essential condition for embedding changes in the organization.

Along with the mandate to ensure the survival of core functionality, the cyber resilience identification process also defines straightforward and effective paths to restore any of the lower priority functions that might have been lost in the actual compromise. For instance, the PLC is the key element in a sensor array. If it is lost, then all the sensors are lost. Consequently, its survival is critical, whereas loss of a given sensor might be acceptable if it does not monitor some other function that is deemed critical. The identification and dependency process is the logic that a student must understand to perform a capable triage of system components. The

specific practices for doing that are explicitly outlined in the classification process that is described in FIPS 199 (NISTa, 2004).

3.2 Principle 2: Risk

Risk assessment provides timely and accurate understanding of the threat status of all critical system components. This is essentially a risk assessment function. Risk assessments identify and evaluate all potential threats on a given attack surface. The evaluation then drives the engineering decisions about the best way to ensure the requisite continuity. The aim is to fully understand every conceivable threat, incident, natural or manmade events, that warrants a targeted protection mechanism. This includes natural disasters, cyber incidents, acts of terrorism, sabotage, and destructive criminal activity targeting critical components of the enterprise infrastructure (PDD-21, 2014). The outcome of this phase is a detailed map of the threat environment, sufficient to support good engineering decisions with respect to explicit protection approaches.

For instructors who require a structured model of the process, the security control assessment approach outlined in NIST 800-53(4) is an excellent template for understanding the steps involved in structuring and conducting a robust and comprehensive risk assessment process (NIST SP 800-53A Rev.4, 2014). The recommendations are detailed as well as logical and can be easily transferred into a unit on risk assessment for digital threat identification and evaluation. The added advantage of adopting 800-53 as the model is that its recommendations fit very well with all of the other relevant NIST standards in this area.

3.3 Principle 3: Rank

Prioritization is the next logical step in the cyber-resilience process. Once the organization's assets have been identified and baselined and the threat environment characterized, the criticality of all assets in the system is ranked. For SCADA, this is a targeted ranking process that focuses only on that specific system. This is also an engineering design activity however, it should involve all stakeholders because all

engineering activity takes place in a business environment that might be more political than logical.

SCADA functioning might impact any associated person, process, technology, or facility that is involved in the business however, some system assets are more critical to simple survival than others. Therefore, the ranking process must authoritatively identify, document, and ensure only those components whose loss would compromise the system's mission, vision, values and purposes (PDD-21, 2014). Unfortunately, ranking can turn into a political free-for-all where various stakeholders attempt to enforce their own agendas. Obviously, this cannot be allowed to happen if the eventual architectural solution is going to be truly resilient. Therefore, criticality must be understood based on a clear map of system functions and dependencies, which are referenced in an objective and rational way to the mission and goals of the organization.

From a teaching standpoint, a rigorous set of protection requirements are specified for just those assets that directly enable the organizational mission. Rigor is defined as the ability to resist any known or conceivable method of attack (PDD-21, 2014). Protection mechanisms are specified and designed to maintain the uninterrupted functioning of each system asset within the cyber resilience protection scheme. A detailed discussion outlining the requisite KSAs for the selection process is provided in the "Select" section of NIST SP-800-37(1) (NISTc, 2010, p.24).

3.4 Principle 4: Deploy

The deploy stage focuses on the specific controls required to make a critical asset resilient. At the generic level, this is a strategic governance process. Deploy creates and then embeds the substantive controls that have been developed to effectively ensure the mission, goals and objectives of a given infrastructure system. In this phase, the explicit control set for each critical asset is substantively created and deployed.

Additionally, this stage prioritizes those objectives and implements targeted control actions to most effectively achieve priority objectives. It then analyzes and assesses the deployed control set to ensure that the resultant infrastructure satisfies the critical purpose. If documented control objectives are not met, then the Deployment process undertakes the necessary analysis to modify controls, or plug gaps. A detailed discussion outlining the requisite KSAs for the deployment process is provided in the "Implement" section of NIST SP-800-37(1) (NISTc, 2010, p.28).

3.5 Principle 6: Recover

This stage focuses on continuity management. The goal of recovery planning is to ease the impact of disruptive events for all aspects of the system and is accomplished by developing and executing a well-established set of plans to ensure rapid restoration of non-critical services (PDD-21, 2014). To achieve this end, the overall system operating environment is studied to identify all potential failure modes and then a proper strategy is developed to recover from potential breakdowns, or disruptions.

The goal is to create a complete and effective recovery process that will address all plausible types of compromises to the non-critical elements of the system. The plan for incident recovery must be explicit for each asset and lessons learned are compiled to develop improvement strategies. This requires an operational plan capable of identifying, analyzing, responding to, escalating and learning from all adverse incidents. A detailed discussion outlining the requisite KSAs for the deployment process is provided in NIST SP-800-34(1) (NISTd, 2010).

3.6 Principle 7: Evolve

The Evolve stage serves as the formal basis for identifying and deploying process and technological responses and improvements across the organization. Evolution is required to continue to maintain the organization's cyber resilience goals as the threat picture changes. In this stage, measurable improvements that could increase the resilience of critical assets are identified, analyzed, and systematically deployed.

The effects of currently deployed processes and technology improvements are measured and the effectiveness of the selected process improvement is characterized. The five functions that must be executed mirror those of the NIST Cyber Security Framework (NIST-CSF, 2014).

Evolution is driven by the collection and analysis of data from lessons learned about the day-to-day execution of the resilience process. Improvement recommendations are supported by data obtained from the deployment of prior process and technology controls. Nevertheless, because this is essentially a "maintenance," activity this type of analysis involves ongoing testing and risk estimation. Lessons-learned typically involve objectively evaluating the performance of deployed processes against plans, objectives, standards, and procedures; as well as the outcomes of organizational innovation and deployment process. US-CERT provides a template for itemizing the steps of an organizational review and evolution process. The steps and requisite capabilities are outlined in detail and provide excellent material for a systematic evolution process (US-CERT, 2016).

4 CONCLUSION

The increased presence of advanced cyber threats makes it inevitable that all organizations will ultimately be targeted (OAS, 2015). Cyber resilience recognizes that there are too many advanced hacking tools to prevent sophisticated attackers from finding the cracks in even the most robust cyber-security system (Lois, 2015). The concept of cyber-resilience goes far beyond the classic boundaries of better hardware and software access controls (EY, 2014). Instead, organizations establish a "cyber resilience strategy" that gives them the ability to withstand and recover rapidly from disruptive events (EY, 2014).

Practically speaking, the best argument for cyber-resilience is that it concentrates resources where they will make the most difference. This is particularly germane to SCADA in that any attack on an infrastructure element threatens a lot more than simple business processes. Thus, cyber-resilience is a particularly important aspect

of ensuring survival and easing recovery of the critical systems that underwrite our way-of-life. Accordingly, cyber resilience requires the organization to spend whatever it takes to develop a well-defined, explicit set of controls to ensure survival of only those critical elements that cannot be compromised. The controls must assure provable protection of core functionality and the various interdependencies in the enterprise's eco-system (EY, 2014).

It is our belief that little substantive education has taken place when it comes to protecting the critical infrastructure, particularly as it applies to SCADA systems. There is no standard model for good educational practice that provide guidelines or best practices of how to reliably protect critical infrastructure components, given the inevitability of failure in traditional approaches. The ideas presented here are a start toward eventually overcoming this lack of knowledge. It presents a process and a framework for structuring and communicating standard cyber-resilience best practice to the educational community at large.

REFERENCES

[1] Bradford, C. (2017), *Disaster Recovery Metrics: What They Are and How to Use Them*, Recovery Zone, [online] http://www.storagecraft.com/blog/disaster-recovery-metrics-use/ .

[2] Boyer, S. A. (2010). In *SCADA Supervisory Control and Data Acquisition. USA: ISA - International Society of Automation*. ISBN 978-1-936007-09-7.

[3] Brasso, B. (2016). *Cyber Attacks Against Critical Infrastructure Are No Longer Just Theories*, [online], Fire-Eye, [online] https://www.fireeye.com/blog/executive-perspective/2016/04/cyber_attacks_agains.html .

[4] Conklin, W.A., Shoemaker, D. and Kohnke, A. (2017), *Cyber Resilience: Rethinking Cybersecurity Strategy to Build a Cyber Resilient Architecture*, Paper presentation at the 12th International Conference on Cyber Warfare and Security, Dayton, OH

[5] Eisenhauer, J., Donnelly, P., Ellis, M., and O'Brien, M (2006). *Roadmap to Secure Control Systems in the Energy Sector*, Energetics Incorporated, Sponsored by the U.S. Department of Energy and the U.S. Department of Homeland Security.

[6] EY. (2014). *Achieving Resilience in the Cyber Ecosystem*, [online], Ernst and Young, [online] http://www.ey.com/Publication/vwLUAssets/cyber_ecosystem/$FILE/EY-Insights_on_GRC_Cyber_ecosystem.pdf .

[7] IEEE. (2012). *Introduction to Industrial Control Networks*. IEEE Communications Surveys and Tutorials, [online] PDF.

[8] Lois, J. E. (2015). *It Can Happen to You: Know the Anatomy of a Cyber Intrusion*. Navy Cyber Defense Operations Command (NCDOC), Story Number: NNS151019-05, Release Date: 10/19/2015.

[9] Maynor and R. Graham (2006). *SCADA Security and Terrorism: We're Not Crying Wolf*, X-Force, Black Hat, [online] /BH-Fed-06-Maynor-Graham-up-1.pdf

[10] Nat-Geo. (2017). *American Blackout*. National Geographic Channel, [online] http://channel.nationalgeographic.com/american-blackout/

[11] NISTa (2004). FIPS 199 *Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems*. Gaithersburg, MD: National Institute of Standards and Technology.

[12] NISTb (2014). *Risk Management Framework*. Gaithersburg, MD: National Institute of Standards and Technology.

[13] NISTc. (2010). *NIST Special Publication 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems, A Security Life Cycle Approach*. Gaithersburg, MD: National Institute of Standards and Technology

[14] NIST-CSF. (2014), *Cyber Security Framework*, Gaithersburg, MD: National Institute of Standards and Technology.

[15] NISTd. (2010), *NIST Special Publication 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems*. Gaithersburg, MD: National Institute of Standards and Technology.

[16] NIST SP 800-53A Rev.4. (2014) *Assessing Security and Privacy Controls in Federal Information Systems and Organizations Building Effective Assessment Plans*, Gaithersburg, MD: National Institute of Standards and Technology.

[17] OAS. (2015). *Report on Cybersecurity and Critical Infrastructure in the Americas, Organization of American States*, Trend Micro Incorporated, [online] https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/critical-infrastructures-west-hemisphere.pdf .

[18] PPD-21. (2013). *Presidential Policy Directive 21: Critical Infrastructure Security and Resilience* [online], The White House, [online] https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil .

[19] Russel, J. (2015). *A Brief History of SCADA/EMS*. [online] http://scadahistory.com/.

[20] Symantec. (2014) *A Manifesto for Cyber Resilience*, Symantec, [online] https://www.symantec.com/content/en/us/enterprise/other_resources/b-a-manifesto-for-cyber-resilience.pdf .

[21] US-CERT. (2016) *Cyber Resilience Review (CRR)*, Department of Homeland Security, [online] https://www.us-cert.gov/sites/default/files/c3vp/crr-fact-sheet.pdf .

[22] Van Hoa, N., Tran, Q. T., and Besanger, Y. (2016), *SCADA as a service approach for interoperability of micro-grid platforms*. Sustainable Energy, Grids and Network. doi: 10.1016/j.segan.2016.08.001.