A PROVEN APPROACH FOR EFFECTIVE COMPUTER SECURITY SELF-ASSESSMENTS AT NUCLEAR FACILITIES

G.P. LANDINE
C.S. GLANTZ
G.A. COLES
Pacific Northwest National Laboratory
Richland, Washington, USA
Email: guy.landine@pnnl.gov

Abstract

A proven method for conducting cybersecurity self-assessments at nuclear power plants is now available for international use. This method was originally developed by Pacific Northwest National Laboratory, under the sponsorship of the U.S. Nuclear Regulatory Commission (NRC), for use at U.S. nuclear power plants. The "Method," described in NUREG/CR-6847 "Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants," was originally a limited release document that was withheld from public disclosure but is now publicly available. The Method provides a systematic, phased, and risk-informed approach to help decision makers and security specialists understand their relative cybersecurity posture. Completed Method assessments may be used to support or validate selection of computer security controls to mitigate cyber threats as well as demonstrate compliance with regulations or statutes enacted by competent authorities. The Method assesses the cybersecurity posture of key systems at a nuclear facility with a focus on protection of design base functions. It considers both physical and digital elements of system vulnerabilities and the resulting potential consequences from exploitation. It is well-suited for addressing blended cyberattacks. A semi-quantitative analytical approach is used in the evaluation of potential vulnerabilities, consequences, and risks and provides a technical basis for the selection of security controls to mitigate cyberattacks. The Method's application at U.S. nuclear power plants has been very encouraging. The only nuclear plant in the United States that did not have adverse findings during its initial NRC computer security inspection prepared for inspection through the diligent application of this self-assessment method and the implementation of recommendations that came out of that self-assessment. Nuclear facilities around the world might find application of the Method extremely helpful for making cost-effective, risk-based decisions regarding computer security and for preparing to pass computer security inspections by their competent authorities.

1. INTRODUCTION

In the past, digital computer systems played a limited role in the operation of nuclear power plants and other nuclear-related facilities. Computers and other digital assets are now playing a growing role in safety, security, emergency response, and balance of plant systems at nuclear power plants. This includes applications in reactor monitoring, system operations, equipment design and testing, recordkeeping, maintenance, planning, and work scheduling. Many plant computer systems are being linked into digital networks that extend across the plant and, in many cases, are connected to large and diverse organization networks.

Concurrent with the expanding use and connectivity of plant-based computer systems, the cyber threat is growing. New domestic and international adversaries are emerging, information on the digital control systems used in nuclear power plants is widely available, and new tools are appearing that can be used by adversaries to exploit vulnerable control systems. As a result of these developments, cybersecurity risks are increasing. There is a growing need to assess and address these risks in a systematic manner.

In recognition of these growing risks, in 2002 the U.S. Nuclear Regulatory Commission (NRC) contracted with Pacific Northwest National Laboratory to assess cybersecurity at a selected set of nuclear power plants and develop the Method to assist all of the U.S. licensees in assessing the risk of their plants' nuclear safety systems, physical security systems, emergency preparedness systems, and associated support systems. NUREG/CR-6847 [1] provides the risk assessment backbone for the industry cyber security program outlined in NEI-0404 [2]. In 2009, this Method,

presented here as Revision 1 of NUREG/CR-6847, was revised to incorporate feedback from industry users and become compatible with the cybersecurity requirements in 10 CFR 73.54 [3], the cybersecurity guidance provided in RG-5.71 [4], and industry guidance for the development of cybersecurity plans [5]. However, NUREG/CR-6847 was kept from public and international release until recently because of its designation as “sensitive nuclear information” under the provisions of 10 CFR 2.390 [6].

Now that the Method is available to the international community, its structured approach can be used by organizations operating nuclear facilities to scrutinize their critical systems, identify their critical digital assets (CDAs), systematically evaluate the vulnerabilities of these assets, assess the consequences to the plant of a successful exploitation of one or more of these assets, estimate cybersecurity risks, identify potential enhancements to cybersecurity strategies and security controls, and select a set of security enhancements that provide high assurance that CDAs are adequately protected from cyberattack.

2. APPROACH

The Method allows organizations to conduct a thorough self-assessment of cybersecurity at their respective facilities. The Method is an acceptable way of evaluating risks and making risk management decisions for critical systems in a manner that is consistent with 10 CFR 73.54 [3] and RG-5.71 [4]. The Method goes into more detail on how to make risk-informed decisions using information obtained during the self-assessment than does the IAEA’s 2016 publication, Conducting Computer Security Assessments at Nuclear Facilities [7]; however, the two approaches are compatible, with the Method fitting neatly into the framework provided by the IAEA’s assessment guidance.

2.1. Self-Assessment Focus

For U.S. nuclear power plants, the focus of the licensees’ cybersecurity assessments are its CDAs, analogous to Sensitive Digital Assets in IAEA parlance. When the Method is applied to evaluate a CDA, it is essential that the assessment include not only that CDA but also other digital assets that are directly or indirectly connected to the CDA. In other words, if a digital asset is in some way communicating or sharing information with a CDA, this digital asset must be assessed by the Method in a manner comparable to that of the CDA to which it is connected (either through direct or indirect connections). If it is not feasible to perform this assessment on a growing web of connections, the CDA must be considered to have connections that are vulnerable to cyberattacks. This must be clearly marked in the assessment records and carried forward into the assessment of cybersecurity risk. It is therefore to the benefit of the plant to characterize all connections and associated digital assets to the fullest extent practicable.

The Method focuses on assessing cybersecurity in a way that addresses the full spectrum of cyber threats up to and including the design basis threat. Threats include those cybersecurity events that originate within the plant, within the parent corporation of the plant, from vendors, and from those who have no previous connection to the plant or industry. The cybersecurity self-assessment begins with the formation of an assessment team and is followed by an eight-stage process, shown in Fig. 1.

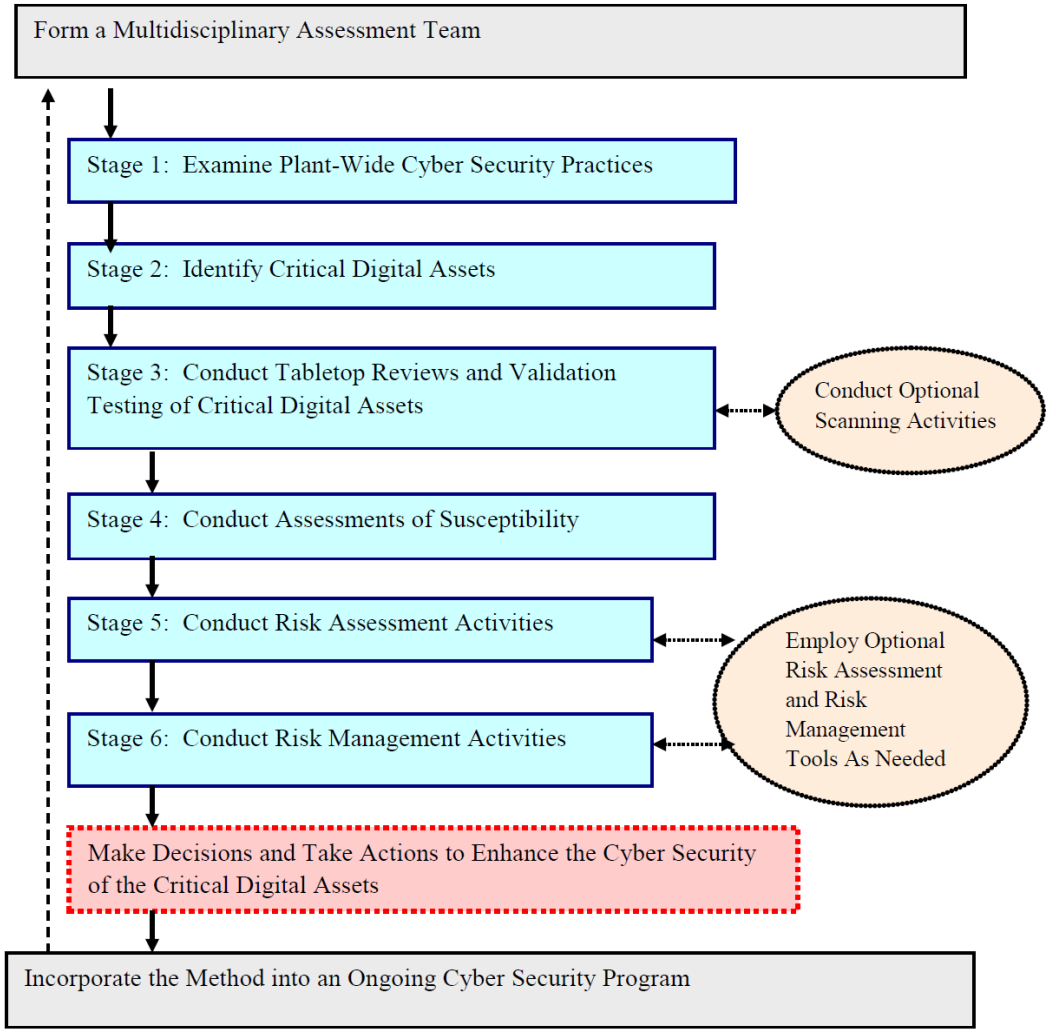

Fig. 1. Simple Flowchart for the Cyber Security Self-Assessment Method

In forming the cybersecurity self-assessment team, staff should be selected to cover a broad range of technical knowledge. The team should have one or more representatives with knowledge of:

- Cybersecurity, including detailed knowledge of threats, attack vectors, vulnerabilities, security strategies, and security controls.
- Information and digital system technology, including software development and application, computer system administration, and computer networking, with an emphasis on the digital systems involved in plant operations and business systems.
- Nuclear power plant operations, engineering, and safety, including knowledge of overall facility operations and plant technical specifications. Staff representing this area must be able to trace the impact of a vulnerability or series of vulnerabilities in a CDA outward through plant subsystems and systems.
- Physical and operational security, including in-depth knowledge of the plant's physical and operational security programs.

Operationally, the cybersecurity self-assessment team would have four to seven members. An example team might consist of:

— Three cyber security specialists with knowledge of plant computer systems, business computer systems, and computer networking.
— One plant systems-engineer with expert knowledge of digital systems including instrumentation and control systems.
— One licensed plant operator with expert knowledge of the operation of all key plant systems.
— One physical security specialist with expert knowledge of the plant's physical security systems and personnel security program.

2.2. Stage 1 – Preliminary gathering and examination of information products

This first stage involves the assessment team's initial work to gather and examine information products related to cybersecurity, including both facility and the broader organization's governing cybersecurity policies, procedures, and other documentation. These information products should document the design and implementation of the facility's cybersecurity program. This documentation should outline roles and responsibilities, the facility and larger organization's cybersecurity defensive strategy, and policies for the selection, placement, and operation of security controls. The team should also gather information on facility resources that can play a role in cybersecurity, including information on the computer networks that operate within the plant such as diagrams for control system networks, business network, and connections with external organizational networks (e.g., company-wide networks that connect the nuclear facility to other facilities such as offsite company business offices or other energy infrastructure assets).

In addition, the team should collect information on the plant's physical security program that play a role in limiting unauthorized access to digital assets, including computer systems and networks. Similarly, information is required on operational security programs such as personnel security training requirements, security screening of employees and contractors, supply chain security requirements, and cybersecurity-related procurement requirements for hardware and software. The information should be collected and reviewed before the team starts interviewing staff and assessing the onsite configuration of digital assets and implementation of security controls. Additional information will be gathered later in the assessment process, but a solid foundation should be examined prior to the subsequent stages in the assessment process.

2.3. Stage 2 – Identify CDAs

This stage involves identifying the CDAs to be assessed, which begins with identification of critical plant systems, digital devices that are functional components of the critical systems, and the grouping of digital devices into CDAs. In many cases, this work has already been done to support the facility's cybersecurity program.

2.4. Stage 3 – Tabletop review and validation activities

This stage covers onsite assessment of the implementation of cybersecurity. It begins with a tabletop review that involves computer network information to identify any discrepancies between policy or network diagrams and actual implementation. It also involves interviews with staff about the actual assignment of roles and responsibilities, implementation of procedures, and other aspects of the cybersecurity program.

A key element of this stage is validation activities. Validation requires physical inspections (walk-downs) and review of electronic settings. The focus of this stage is to assess the location, connectivity, vulnerabilities, and cybersecurity controls associated with each CDA and any directly or indirectly connected digital assets. In the authors extensive experience, it is not uncommon to find the actual deployment and configuration of digital assets to be somewhat different from what are provided in facility documentation. The nature of digital connections and their rapid evolution often results in less rigorous configuration management than traditionally required for non-digital systems. Discrepancies between planned and actual deployment of digital devices, systems, and software is fertile ground for physical and cybersecurity vulnerabilities involving CDAs.

Another potential aspect of this stage of the assessment involves electronic testing. Electronic scanning of CDAs can quickly identify weaknesses in networked systems, providing a list of priority items to consider for patching or securing. Scanning tools should be used only by knowledgeable cybersecurity professionals to avoid causing a failure on the network. Scanning should only be conducted if specific conditions are met, including only conducting scanning when systems are offline (such as during refuelling outages).

2.5. Stage 4 – Assess threats and vectors of attack

Given the information acquired in the previous stages regarding the configuration CDAs and the security controls protecting them, assess security threats to CDAs and potential vectors of attack. This includes evaluating capabilities of potential threat agents, credible methods of attacks, and potential attack vector scenarios. Use attack trees (or a comparable method) to characterize pathways. Information on threat agents should consider individual hackers, organized crime groups, terrorist organizations, nation states, and insiders (including facility staff members, vendors, and contractors). Information on threats may be available from industry, national, and international organizations.

Information on credible methods of attack may be developed by facility personnel or in conjunction with other organizations, such as their parent organization, industry cybersecurity groups, or national or international security agencies. If information is gathered from groups, facility personnel may fine-tune the group's generic characterization to address any potential types of cyberattacks that are specific to their facility.

Threat and system information can be used to develop attack trees. These provide a systematic approach, using graphical and mathematical representations, to assess cybersecurity vulnerabilities and risks for computer systems that may be subjected to a cyberattack. Attack trees represent cyberattacks using a tree structure, with the attack's goal (if malicious) or system failure (if inadvertent) presented at the top of the tree, and different pathways and possibilities for achieving a security failure branching downwards. The attack tree shows the various elements of the defensive strategy, security controls, and attack mitigation methods that would have to be overcome by the attack to reach its goal or achieve a system failure.

2.6. Stage 5 – Conduct assessments of susceptibility

Susceptibility is a simple, relative measure of the cumulative cyber vulnerability of a critical system. While not a replacement for a detailed cybersecurity vulnerability assessment that could be generated through a detailed attack tree analysis, it does provide a quick, initial view of the susceptibility of a CDA to a successful cyber exploitation.

To evaluate susceptibility, the assessment team should use information gathered in preceding stages of the Method to evaluate the physical security, digital exposure, and effectiveness of deployed cybersecurity elements. Specific criteria that are evaluated to determine susceptibility include the physical and digital exposure for each CDA taking into account the connectivity pathways, the type of digital connections (e.g., to modems, local area networks, wireless ports) present along the evaluated pathways, and the effectiveness of digital protections for the CDA along each connectivity pathway. This evaluation examines the degree to which defensive strategies, security controls, and attack mitigation methods have been effectively implemented to protect against the cyber exploitation of the CDA.

2.7. Stage 6 – Assessment of consequences

In this stage the assessment team characterizes the potential consequences that could occur to the plant if one or more CDA was subjected to cyber exploitation. The CDA consequence analysis is used to:

— Identify and describe the ways in which a CDA can interact with critical systems;

— Identify and describe the types of digital compromises (i.e., loss of confidentiality, integrity, or availability of the asset or its data) that could negatively impact a plant system;
— Identify the potential consequences for each type of digital compromise;
— Determine if any of the potential consequences are reduced by existing security controls (including countermeasures, response and recovery programs, or backup systems);
— Assess whether adverse consequences could occur as a result of direct or indirect influence of the compromised CDA;
— Determine the worst-case consequence level for the plant from a cyber exploitation of the CDA.

2.8. Stage 7 – Assessment of risk

In the first part of this stage, a simple, general, qualitative risk estimate is made that defines risk as the combination of the susceptibility of a CDA to a cyberattack and the consequences to the plant from that cyber exploitation. The reason for adopting this qualitative approach is that information might not be readily available to support a full quantitative evaluation of the probability that a cyberattack will be attempted, succeed, and result in an adverse consequence to a plant. As a result, a characterization of overall susceptibility is used as a surrogate for probability in this initial evaluation of the risk of each of the licensee's CDAs.

In the second half of this risk assessment stage, a semi-quantitative or quantitative assessment of risk could be made for selected CDAs. This assessment could be made using attack trees (or a comparable method) for all CDAs for which known vulnerabilities were identified during the tabletop and validation inspection, those CDAs that are in the "high impact" category for potential consequences associated with a successful cyberattack, and those critical digital assets whose general risk levels does not meet or is close to (e.g., within one risk level) of meeting the high assurance standard for the protection of critical systems (as discussed in 10 CFR 73.54 (a) [3])

2.9. Stage 8 – Conduct risk management activities

This stage of the Method is designed to assist the assessment team in identifying approaches for dealing with cyber vulnerabilities and evaluating risk management options (e.g., enhanced security controls) to achieve "high assurance that critical systems are adequately protected from cyberattack" (10 CFR 73.54(a) [3]). The objectives of this stage are to:

— Identify potential new management, operational, and technical security controls that can address uncovered cyber vulnerabilities and enhance cybersecurity.
— Document how existing cyber vulnerabilities and/or consequence levels would be reduced by security control enhancements or additions and identify new vulnerabilities or consequences that the potential security controls might introduce.
— Estimate the costs associated with implementing the security controls.
— Evaluate the cumulative risk reductions that would be achieved through implementation of enhanced or new security controls.
— Identify those individual or sets of security controls that would reduce risk and achieve high assurance that critical systems are adequately protected from cyberattack.
— Use cost information to select security controls that would meet the requirements in a cost-effective manner.
— Prepare a report detailing the risk management process and recommendations.

3. USING THE METHOD

The Method can provide a key component in an ongoing cybersecurity management program. The Method provides a structured approach to assess cybersecurity risks and risk management decisions. Reassessments should be conducted at a frequency that is appropriate for the nuclear facility, with a greater frequency for higher risk facilities.

For many nuclear facilities this could be annually or once-every two years. Once the initial assessment is completed, updating key information, documenting findings, and reassessments should involve significantly less time and resources. In addition to normally scheduled reassessments, a reassessment might be warranted when one of the following conditions arises:

- Significant modifications to or introduction of new critical systems, CDAs, connected digital assets, or connections to a CDA;
- Significant changes in the threat environment (including changes in cyber exploitation technologies and techniques);
- Identification of significant new cyber vulnerabilities;
- Development of new cost-effective protective actions;
- Substantial modifications to cybersecurity requirements, guidance, security controls, and defensive strategies.

4. REAL-WORLD APPLICATION OF THE METHOD

Although approved by the NRC, there has never been a regulatory requirement in the United States for nuclear power plants to apply the Method. In the United States, regulatory inspections have followed a checklist, compliance-based process rather than a performance-based process. Self-assessments conducted prior to NRC inspections at most U.S. nuclear plants have tended to follow a checklist approach to anticipate potential regulatory inspection issues. However, some sites have applied the Method in full to guide their cybersecurity programs and prepare for NRC cybersecurity inspections.

A full application of the Method was made at the San Onofre Nuclear Generating Station prior to their first NRC cybersecurity inspection. Findings from the Method process were documented, and significant issues were addressed prior to the NRC inspection. The result was that the San Onofre plant was the only U.S. nuclear power plant to pass their initial NRC regulatory inspection without a single adverse finding. While the application of the Method was not the only factor contributing to this stellar performance, San Onofre’s commitment to the risk- and performance-based approach embodied in the Method clearly played a role in this excellent outcome. The San Onofre staff, including their cybersecurity team, was able to demonstrate to the NRC that not only were they meeting the prescribed requirements of the applicable regulations, but they were cognizant of and addressing their cybersecurity issues in a well-documented, risk-based manner. In other words, they were not simply doing work to check off regulatory boxes but were making informed cybersecurity decisions based on a careful analysis of threats, vulnerabilities, consequences, and risks.

5. CONCLUSION AND PATH FORWARD

Originally blocked from public disclosure and international access because of NRC security restrictions, it is gratifying that this risk-based, cybersecurity assessment method is now available for public examination and potential use at nuclear facilities around the world. International operators of nuclear facilities can now replicate the successful application in supplementing regulatory checklist assessment methodologies with the more comprehensive risk-based approach outlined in NUREG/CR-6847 [1]. Using this information, nuclear facilities can develop a better appreciation of their cybersecurity threats, vulnerabilities, consequences, and risks that should provide for better risk management decisions based on costs and risk reduction.

REFERENCES

[1] GLANTZ, C., BASS, R., CASH, J., COLES, G., GOWER, D., HEILMAN, J., LAMMERS, M., THOMAS, J, Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants, NUREG/CR-6847, U.S. Nuclear Regulatory Commission, Washington, D.C., 2004.

[2] NUCLEAR ENERGY INSTITUTE, Cyber Security Program for Power Reactors, NEI-0404, Washington, D.C., 2004.
[3] CODE OF FEDERAL REGULATIONS 10 CFR 73.54, Protection of Digital Computer and Communication Systems and Networks, https:/www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html
[4] NUCLEAR REGULATORY COMMISSION, Cyber Security Programs for Nuclear Facilities, RG-5.71, Washington, D.C., 2010.
[5] NUCLEAR ENERGY INSTITUTE, Cyber Security Plan for Nuclear Power Reactors, NEI-0809, Washington, D.C., 2010.
[6] CODE OF FEDERAL REGULATIONS 10 CFR 2.390, Public Inspections, Exemptions, Requests for Withholding, https:/www.nrc.gov/reading-rm/doc-collections/cfr/part002/part002-0390.html
[7] International Atomic Energy Agency, Conducting Computer Security Assessments at Nuclear Facilities, Nuclear Security Series No. 17, Vienna, Austria, 2011.