CYBER SECURITY AT U.S. NUCLEAR POWER PLANTS

WILLIAM R. GROSS
Senior Project Manager, Engineering
NUCLEAR ENERGY INSTITUTE
wrg@nei.org

Ensuring safety and security is the top priority at nuclear power plants. As the cyber threat advances, and as plants make increasing use of digital technologies, the potential for adverse consequences that could result from a cyber attack increases. Nuclear plants in the United States have significant experience in establishing cyber security programs. The plants have robust physical protection and cyber security programs and are well protected against both physical and cyber attacks. Additionally, the U.S. Nuclear Regulatory Commission has established mandatory and enforceable requirements to defend against cyber attacks.
This article briefly reviews the U.S. plants' cyber security history; provides an overview of the NRC's regulatory requirements for cyber security; describes protective measures the plants have implemented; summarizes observations from independent organizations; explores lessons learned; describes industry priorities over the next few years; and concludes with policy considerations that may inform future regulatory actions.

BACKGROUND

U.S. Plant Cyber Security History - Awareness of the emerging risks associated with increased reliance on digital technologies was highlighted at the plants in the late 1990's in the run-up to 2000. At that time, there was considerable concern over the "Y2K" issue and the potential impacts that could occur. While there was no appreciable impact from the Y2K changeover, the seed was planted for the industry to take a close look at how integration of digital technologies could impact facility risk, particularly with respect to the potential for a cyber attack to adversely impact facility safety, security or reliability.

Industry efforts related to cyber security accelerated after the terrorist attacks of September 11, 2001. In February 2002, the Nuclear Energy Institute (NEI) formed a cyber security task force that remains active today. The task force began to develop guidance that nuclear plants could use to establish and implement comprehensive cyber security programs, building on an approach developed by Pacific Northwest National Laboratory for performing cyber security assessments. The result is NEI 04-04, "Cyber Security Program for Power Reactors." The NRC reviewed the guidance and, in 2005, informed NEI that it provides an acceptable approach for developing a cyber security program. The following year, the industry's chief nuclear officers voted to adopt the NEI 04-04 cyber security program at all U.S. nuclear power plants. Industry-wide implementation was completed in 2008.

NRC'S REQUIREMENTS FOR CYBER SECURITY

The NRC implemented two significant rulemakings to address cyber risks. In 2007, the agency revised its design basis threat requirements to include a cyber attack as an explicit attribute of both the internal and external threats. The NRC also included cyber security program requirements in a 2009 revision to the physical protection rule, 10 CFR 73.54. NEI worked to develop templates for the cyber security plan (NEI 08-09) and associated implementation schedule. Implementation of the cyber security plan was divided into two phases. During the first phase, nuclear power plants implemented those measures that will have the greatest effect on reducing cyber risk. This work

LA CIBERSEGURIDAD EN LAS CENTRALES NUCLEARES ESTADOUNIDENSES

Las centrales nucleares tienen como primera prioridad garantizar la seguridad y la protección física. Conforme vayan avanzando las ciberamenazas, y como las centrales hacen un uso cada vez mayor de las tecnologías digitales, va aumentando la posibilidad de efectos adversos como consecuencia de un ciberataque. Las centrales nucleares de los Estados Unidos tienen una amplia experiencia en el establecimiento de programas de ciberseguridad. Las centrales tienes una protección física y programas de ciberseguridad robustos, y están bien protegidos contra los ataques tanto físicos como cibernéticos. Además, la Comisión Reguladora Nuclear de Estados Unidos ha establecido requisitos obligatorios y ejecutables para defender contra los ataques cibernéticos.
En este artículo se hace un breve repaso de la historia de la ciberseguridad de las centrales estadounidenses; se resumen los requisitos reguladores de la NRC para la ciberseguridad; se describen las medidas de protección que han puesto en marcha las centrales; se resumen las observaciones de las organizaciones independientes; se analizan las lecciones aprendidas; se exponen las prioridades de la industria para los próximos años; y por último se señalan unas consideraciones políticas que pueden sustentar las futuras acciones reguladoras.

was completed by the end of 2012, and the NRC completed its inspections by the end of 2015. During the second phase of implementation, now under way, licensees are performing cyber security assessments on less significant assets and implementing the programmatic elements needed to maintain the cyber security program. This work will be completed by the end of 2017.

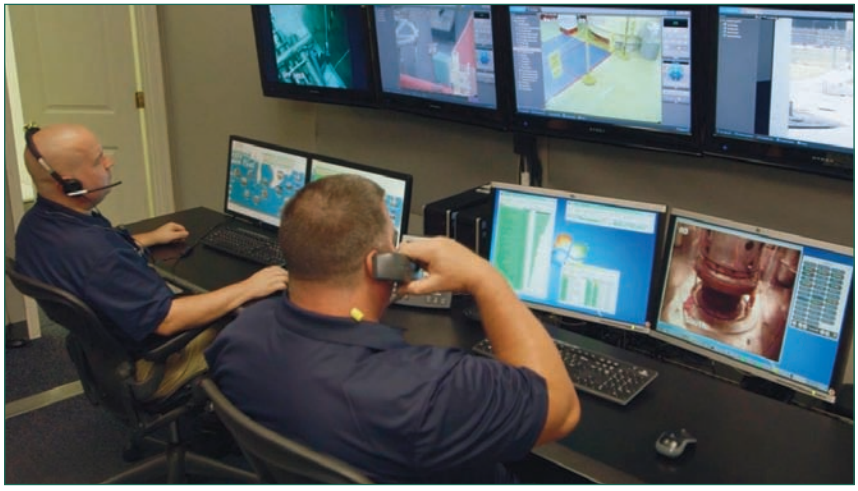
PROTECTIVE MEASURES

Nuclear power plants have several attributes that limit their vulnerability to cyber risk. First, they do not rely on data from outside the plant to maintain safety, security or reliability. Second, nuclear plants have well-defined programs to control how work is performed and maintain strong quality and configuration management programs. Third, their safety culture drives a very high degree of procedural adherence, and great pains are taken to ensure that personnel are trustworthy and reliable.

The first seven milestones implemented by the plants during phase one focused on identifying and eliminating the potential pathways for attack and implementing controls to protect the plant's most critical assets. These key elements include:

1) Establishment of a cyber security assessment team;
2) Identification of critical systems and critical digital assets;
3) Isolation of essential plant digital assets;
4) Mitigation of threats associated with use of portable media and equipment;
5) Enhancement of walk-downs to detect cyber tampering;
6) Protection of essential digital assets associated with key safety equipment; and
7) Institution of ongoing monitoring and assessment of controls that have been implemented.

The Cyber Security Assessment Team (CSAT) is the principal group responsible for establishing the cyber security program at each nuclear power plant. The CSAT includes individuals with extensive knowledge in digital plant systems, nuclear power plant operations, engineering, cyber security, physical security, and nuclear safety experience and technical expertise. They also receive special training to ensure their ability to perform cyber security assessments.



The CSAT identified the Critical Systems (CSs) and the Critical Digital Assets (CDAs) required to be protected against cyber attacks. The scope of 10 CFR 73.54 includes assets associated with safety, security, emergency preparedness and support systems. Structures, systems, and components (SSCs) in the balance of plant that are relied on for electrical generation, and that have a nexus to radiological health and safety are also included.

Plant digital assets were isolated from network-based attacks through the implementation of hardware-based data diodes that protect the most critical systems from remote attacks. Isolating the plant systems from the Internet and from the corporate business network also is critical to guard against external threats.

Comprehensive controls over the use of portable media and portable equipment were implemented. Portable media and equipment are used to perform maintenance on, or to transfer electronic information (e.g., data, software, firmware, virus engine updates and configuration information) to and from plant process equipment. Careful use of portable media and equipment is required to minimize the spread of malicious software to plant process equipment.

Individuals in the plant who perform walk-downs of equipment (e.g., security, operations, engineering) received training on the observation and identification of cyber-related tampering. This helps to guard against observable cyber-related insider actions.

Cyber security controls were identified, documented, and implemented for digital assets that could adversely impact the safety of the plant. The site physical protection program provides high assurance that these elements are protected from physical harm, while the cyber security program enhances defense-in-depth.

Finally, monitoring and assessment activities were established ensure that protective measures remain in place and effective.

MONITORING RESULTS

Two organizations recently completed assessments of cyber security of U.S. nuclear power plants: One focused on plant implementation, the other on the legal and regulatory framework.

A 2015 report by the U.S. Department of Homeland Security's (DHS) Office of Cyber and Infrastructure Analysis concluded that the plants have strong cyber security programs. "Nothing suggests that a cyber attack executed through the Internet could cause a nuclear reactor to malfunction and breach containment. Nuclear power reactors have comprehensive safeguards that protect control-system safety and security and prevent the misuse of portable media (e.g., Universal Serial Bus [USB] devices) and portable equipment (e.g., maintenance laptops) from circumventing these protections," the DHS report stated.

In January 2016, the Nuclear Threat Initiative (NTI) released the third edition of its internationally focused Nuclear Security Index, covering both theft and sabotage of nuclear material. The United States received a maximum score for cyber security.

LESSONS LEARNED

Perhaps the most challenging element of implementing the NRC's cyber security requirements is the scope of systems and equipment that must be

protected. These requirements are an integral part of a facility's strategy to prevent radiological sabotage (i.e., significant core damage and spent fuel sabotage). However, the broad scoping language of the NRC rule has been interpreted as requiring licensees to protect systems and equipment that have no nexus to sabotage that could have a radiological impact. Plants have identified thousands of digital assets for inclusion in the program. Resources expended on non-risk-significant assets diminishes licensees' ability to focus resources on the most important equipment.

To address this concern, the industry developed NEI 13-10, "Cyber Security Control Assessments," Revision 4, which provides a consequence-based approach to the implementation of cyber security controls for CDAs. The NRC has endorsed this guidance. Early reports from plants indicate that licensees are seeing a 75 percent or better reduction in the number of full-scope cyber security assessments that must be performed.

The industry also is addressing lessons learned related to the selection of standards used for the protection of digital assets. The U.S. nuclear industry and the NRC used a National Institute of Standards and Technology standard that provides cyber security controls tailored for classic information processing systems. These standards are not tailored to the types of digital components found in nuclear power plants (e.g., instrumentation and control systems). NEI 13-10 includes guidance for addressing these IT security controls for the types of assets found in the plants. While it is prudent to use widely acceptable standards, it may be best to consider using a standard intended for industrial environments.

CONCLUSIONS

Clarity and consistency are vitally important. The nuclear utilities in the United States are generally highly cohesive in addressing regulatory requirements, and the cyber security requirements are no exception. Each plant utilizes templates for its cyber security plan and implementation schedule, which provide a good basis for consistency. However, NRC inspections have revealed differences in implementation among the utilities, as well as differences between implementation at the plants and NRC expectations.

INDUSTRY PRIORITIES GOING FORWARD

As the industry moves toward full program implementation, NEI is focused on ensuring consistency in implementation across the industry and alignment with NRC expectations. These objectives will be accomplished through workshops, public meetings, benchmarking visits and site audits. New guidance will be developed, as needed, to ensure these objectives are met.

Additionally, NEI will work to ensure that licensees derive maximum value from NEI 13-10. This NRC-endorsed guidance supports consistency in implementing cyber security controls in a manner that aligns with NRC expectations. It also facilitates focusing on high-consequence assets, while reducing unnecessary effort on low-consequence assets.

NEI will continue to engage with the NRC to promote a rulemaking to address the industry's concerns with the broad scoping language. This is a long-term effort that should be pursued for regulatory stability.

Policy Considerations – Having directly engaged with the industry and the NRC for nearly a decade regarding the implementation of cyber security programs, NEI has identified four key points that may be useful in informing future policy:

1) Requirements related to cyber security should clearly state the performance objective. Specifically, they should state that the objective of the cyber security program is to prevent radiological sabotage or theft of nuclear material. This clarity is vital in informing the types of systems and equipment that are protected against attack and in evaluating the adequacy of implemented countermeasures.
2) The scope should be directly related to the performance objective. The cyber security program should protect any digital asset whose compromise by a cyber attack would likely result in radiological sabotage or theft of nuclear material. Security programs, including cyber security, implement defense-in-depth for the protection of vital equipment. Clearly defined scoping language is essential to ensure that the correct assets are at the center of the defense-in-depth protections implemented through the cyber security program.
3) The program should incorporate a risk-informed, graded approach to the identification of assets and the application of cyber security controls. NEI 13-10 provides one methodology to accomplish this; however, other approaches could be considered. For example, risk insights from plant probabilistic risk assessments could be used to identify essential equipment or to inform the implementation of cyber security controls.
4) Policies should be sufficiently flexible to allow utilities to leverage nationally or internationally recognized standards for the protection of their digital assets. This flexibility would allow utilities to use standards appropriate for the types of assets they need to protect. For example, the utility could use one standard for industrial equipment and another standard for general purpose equipment, as appropriate. This flexibility also would allow internationally scoped nuclear utilities to use a consistent set of cyber security standards across their enterprises, minimizing the overhead of maintaining compliance with multiple standards.

The cyber threat will only continue to grow, and to be successful at protecting the plants, dedicated and persistent effort will be needed. The U.S. plants are well positioned to protect the health and safety of the public.■