Cybersecurity Threats Are Always Evolving, So Should Nuclear Cybersecurity Regulation

June 20, 2019—Since more people—and even nations—face threats in the digital world, cybersecurity is critical. In the energy sector, nuclear plants have years of success and expertise in cybersecurity that allow them to stand among the most secure facilities in the country.

Last week the Fissile Materials Working Group (FMWG)—an organization committed to preventing proliferation—and the Stimson Center released a joint report, urging cyber and nuclear security stakeholders around the globe to “come together to share information, experiences, knowledge and best practices.”

The report’s recommendation makes me think about how I’ve seen the U.S. industry evolve into a cybersecurity leader over my career in this field.

The U.S. nuclear industry began looking at the potential consequences with the increasing adoption of digital technologies just over 20 years ago with the excitement around the turn of the millennium, Y2K. (For a fun read, check out some of the concerns about the world coming to an end.) Nuclear utilities did not sit on the sidelines for Y2K—we got active. We stood up an informal team of industry experts to assess the potential impact and to implement remediation strategies and, as a result, there was no impact to our sector. Tragedy averted.

On Sept. 11, 2001, that whole story changed. The whole world changed. Our attention swung from innocent computer challenges to cybersecurity. While computer security was a rapidly developing field, the concept of industrial cybersecurity was not even in its infancy. There was nothing, nada, zilch.

From 2001 onward, the industry developed and implemented regulations, guidance and protections for the industry as whole. I have not been shy about talking about
what the industry has done to advance their programs to meet evolving threats and requirements from the U.S. Nuclear Regulatory Commission. Nuclear plants are the most well-protected critical infrastructure in the United States.

If I could boil down our 20 years of experience, I would have two key takeaways:

1. Cybersecurity programs must be informed by the threat.

   It is vital to have a solid understanding of the threat we face, including its objectives and capabilities. It underpins our process for identifying the computer systems we will protect, and it informs the protective and detective features we put into place. The inverse is also true: We must be able to look at all elements of the program—the assets we are protecting and the protective measures—and adjust to align with the threat environment.

   In the U.S., we are poised to re-evaluate our programs based on the threat environment. We go above and beyond protecting mission critical assets. But we are also protecting assets that are simply not attractive to the adversary and, in some cases, we are implementing protective measures that are not adding value. We need to focus our programs as soon as we can on significant, likely targets.

2. Nuclear regulatory frameworks must be flexible to meet the cyber threat.

   The NRC has two elements that are vital to ensuring effective nuclear cybersecurity:
   
   - Cyberattacks are integrated into the scope of what the agency evaluates against (also known as the design basis threat), and
   - Regulations have specific performance-based cybersecurity program requirements.

   The NRC and the industry have a shared responsibility to ensure that regulatory guidance and oversight activities do not stifle cyber program innovation. As the FMWG report identifies, “It has been shown that compliance does not necessarily equate to security.”

   We must ensure we don’t end up with static programs that cannot be easily adapted to align with the best available understanding of the threat.

   Our industry cybersecurity task force is focused on continuous improvement. As we move through 2019, they are engaged in evaluating all elements of the cyber program to ensure that we are protecting the right computer systems and the protective measures are efficient and effective.  

---

Baranwal to Lead DOE's Office of Nuclear Energy

June 20, 2019—Today, the U.S. Senate confirmed Rita Baranwal to be assistant secretary of energy at the U.S. Department of Energy's Office of Nuclear Energy. The following statement can be attributed to Maria Korsnick, president and chief executive officer at the Nuclear Energy Institute:

"We congratulate Rita Baranwal on her confirmation to lead the Department of Energy's Office of Nuclear Energy. NEI and the U.S. nuclear industry look forward to working with her in this new role in which she will bring her unique expertise and talents to fulfill Secretary Perry’s outstanding vision for U.S.
nuclear leadership.” <<NEI Media Team, media@nei.org

Milestones

Russia’s VVER-TOI Reactor Certified by European Utilities

The European Utility Requirements organization has formally certified as compliant the Russian-designed VVER-TOI nuclear power reactor design, which was developed from the VVER-1200. Atomenergoproekt, a subsidiary of Russian state nuclear corporation Rosatom, announced the VVER-TOI design in 2010, developed using technical results from the VVER-1200 project.
This design has an upgraded pressure vessel, increased power to 1,300 megawatts, improved core design to increase cooling reliability, further development of passive safety, lower construction and operating costs, and a 40-month construction time. It also will use a low-speed turbine-generator. << Adapted from World Nuclear News

NRC Completes Clinch River Site Safety Review

The U.S. Nuclear Regulatory Commission has published its final safety evaluation report on the Tennessee Valley Authority’s application for an early site permit (ESP) for the potential use of a site at Clinch River for two or more small modular reactors. The regulator concluded there are no safety concerns to prevent issuing such a permit.
An ESP certifies that a site is suitable for the construction of a nuclear power plant from the point of view of site safety, environmental impact and emergency planning, but it does not specify the choice of technology. The permit is valid for 10 to 20 years, renewable for an additional 10 to 20 years. << Adapted from World Nuclear News

Contracts

AECOM and Toshiba Expand Decommissioning Collaboration

U.S.-based AECOM and Toshiba Energy Systems & Solutions Japan agreed to step-up their collaboration providing decommissioning services to nuclear power plants in Japan.
Through an agreement signed by AECOM and Toshiba ESS, the companies will promote “combined and joint services to Japanese utility owners in a prompt manner.”
The two companies have been working together since 2014. Toshiba ESS has played a key role in the constructing and decommissioning of nuclear power plants in Japan. << Adapted from World Nuclear News

North Wind to Prepare San Onofre Used Fuel Transfer Strategy

Southern California Edison has contracted North Wind Inc to develop a strategic plan that will assess the feasibility of relocating used nuclear fuel currently stored at the San Onofre Nuclear Generating Station to a “commercially reasonable, off-site facility.”
North Wind will work with SCE to develop the strategic plan over 20 months.
North Wind will also engage with a broad range of stakeholders to learn their preferences and attitudes about used nuclear fuel and its eventual disposition, SCE said. << Adapted from World Nuclear News