THE OFFICIAL PUBLICATION OF THE UTILITIES TECHNOLOGY COUNCIL

UTC Journal

4th Quarter 2018

Best Practices in SUPPLY CHAIN CYBERSECURITY IN THE POWER SECTOR

DEBBIE VAN OPSTAL
Executive Director,
US Resilience Project.

DHS recently warned utilities that Russian government hackers accessed the U.S. electric grid control systems in 2016 and 2017, breaking into secure systems by first penetrating the networks of their vendors. Cyberattacks through the supply chain clearly represent a new frontier of risk for the power sector. How are utilities coping with these threats?

Interviews with a sample set of 9 utilities from across the country – ranging from very large and sophisticated companies to small coops and municipals -- suggest that, in fact, they're thinking creatively about cybersecurity solutions. Their cutting-edge strategies and best practices warrant sharing more broadly.

What do we mean by Cyber Supply Chain Risk? Until recently, supply chain was simply a procurement function, largely unrelated to risk management. Today, utility managers worry about:

- Purchase of tainted or counterfeit software or firmware
- Risks that data could be stolen or altered or control systems corrupted through breaches in a vendor's IT security or lax employee vetting
- Compromise or theft of data that is being processed or stored by a third party
- Risks that remote access channels could be used to compromise operations

Five Organizing Principles for Supply Chain Cybersecurity Risk Management

The interviews demonstrated that utilities are adopting strategies that increase their ability to withstand cyberattacks -- or diminish their impact.

- **Link Security to Reliability**. The power industry is first-in-class in reliability – and utilities are recognizing that reliability processes can make them more resistant to attack. When engineers design systems to be safe for humans or reliable for grid operations, security goals are achieved along the way. Well-designed systems tend to fail safe, minimizing the impact of the problem if attackers find a vulnerability.
- **Build it in, rather than bolt it on**. Leading firms make security a forethought, rather than an afterthought. Risk management and cybersecurity teams are integrated organizationally into major technology procurement and vendor selection decisions.
- **Know what normal looks like**. Utilities believe that a best practice to minimize the risks of corrupted hardware or software is to define the parameters of what constitutes "normal" – and to have enough visibility into the system to know when the system is not behaving normally.
- **Look for the Value-Add from Cybersecurity**. Cybersecurity teams demonstrate the business value of engaging with them: help with technology selection processes, vendor risk management and ongoing work with vendors on configuration or other issues. They create a demand-pull for these services, which are often outsourced by business units.
- **Develop a risk management methodology**. Not all risks are created equal. Although every technology acquisition deserves some level of scrutiny, utilities that have developed a comprehensive risk management plan can calibrate risk to the right level of controls.

Managing Critical Cyber Supply Chain Risks

There are a number of specific concerns by NERC and FERC: vendor risk management systems, remote access controls and software integrity. The utilities interviewed had best practices and processes in each.

Vendor risk management systems: Vendor risk management in the power sector has gotten much more complicated for at least three reasons:

- globalization of the supplier base with increased risk of untrustworthy suppliers
- greater connectivity (e.g. smart grid, IOT) with greater remote access risk
- Outsourcing of data into the cloud with potential for breaches

Larger utilities, not surprisingly, have already begun instituting more rigorous supplier approval processes. Security requirements are increasingly reflected in their RFPs and vendor contracts, although stronger scrutiny and comprehensive vendor controls remain a goal for many utilities. Cloud vendor security is perhaps the most advanced area of vendor risk management, with utilities implementing the NIST 800-53 framework.

But, rigorous vendor risk management processes are more difficult for small utilities – which don't believe they have the clout to impose requirements on global vendors. Instead smaller utilities are applying different strategies to reduce supplier risks:

- Reduce the number of vendors to a few trusted partners and build strong relationships with them.
- Stay with mainstream players, avoiding flashy new products or start-ups.
- Create a security checklist of basic controls every vendors must comply with .
- Institute an authorization process with background checks and training for contractors and vendors before allowing virtual or physical access.

Remote access risk management: As companies have strengthened their firewalls, the risk that intruders could sneak into the system through the supply chain back door - piggybacking on a vendor's remote connection – has become a more serious concern. Utilities of all sizes are clearly taking this risk seriously. Some of their solutions:

- **Isolate the SCADA system completely**, eliminating remote access by vendors and employees alike. In one case, the company pays SCADA vendors to fly out to the facility to provide in-person services.

Well-designed systems tend to fail safe, minimizing the impact of the problem if attackers find a vulnerability.

- **Maintain identical development and quality assurance systems in-house**. The vendor works through problems on the identical system, not the actual operating system -- and the utility takes charge of transferring any changes to its production system.

For areas other than SCADA, utilities are instituting stricter controls on vendor access. Best practice is to have a thorough understanding of the requirements and what systems the vendor needs to access to perform the work.

Rules of Thumb in Managing Remote Access:

- **Never give a vendor full-time, independent access.** Require a work order or some other form of communication before a vendor can come on-site.
- **Continuous monitoring of vendors while they are the system**. Some companies go even further: the vendor guides the work but a company employee executes it.
- **Maintain network security monitoring.** Automated tools for network monitoring can be expensive, but any enterprise switch or router has the ability to send off netflows. Utilities believe that they need a dedicated person to analyze the data and validate that the system is operating as expected.

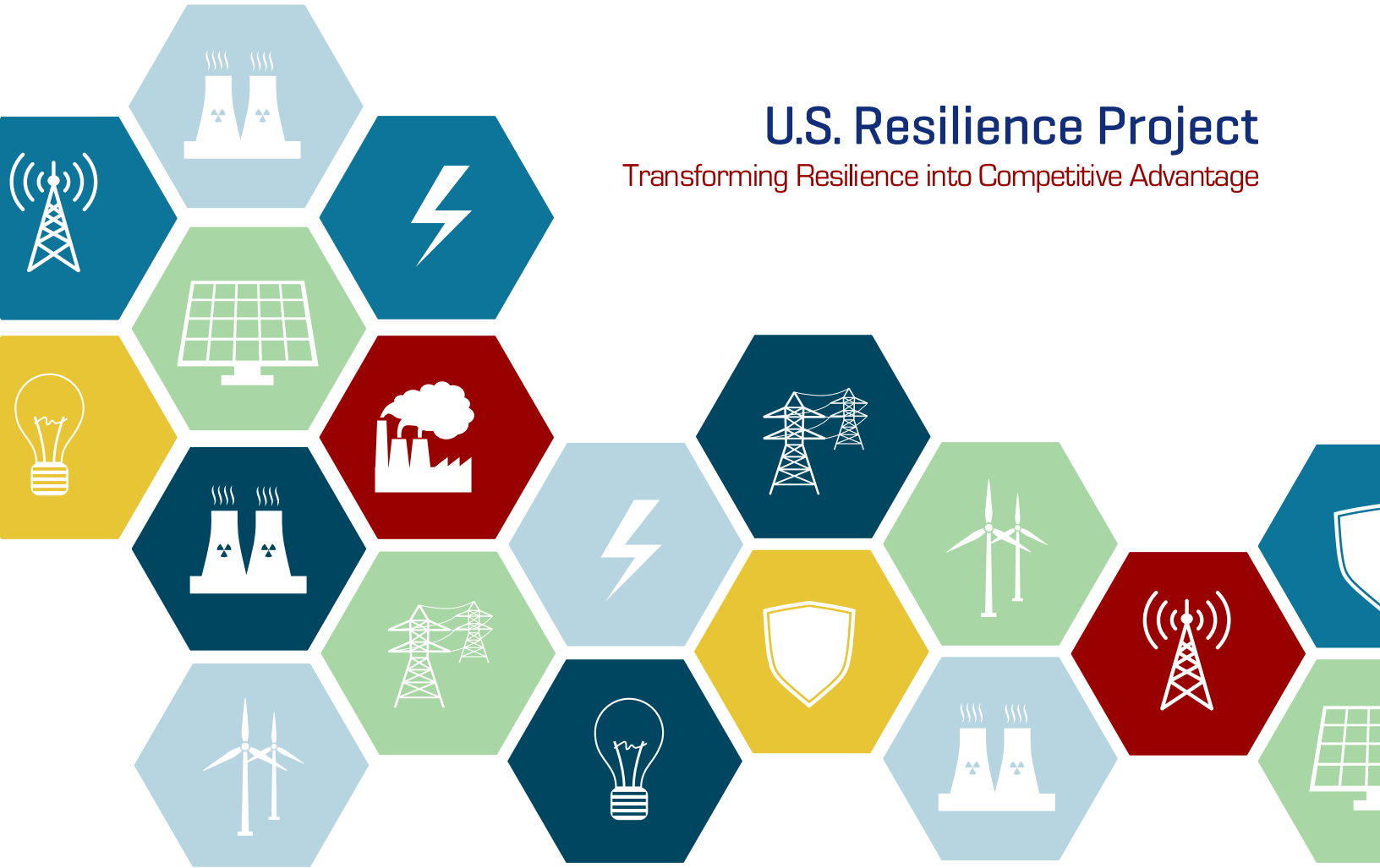
Software Integrity

Software integrity can be jeopardized at the time of purchase and delivery, during patching or vendor maintenance. This is a thorny problem that utilities are still

coming to grips with. Some of their solutions include:

- **Limit purchases to brand names.** Utilities also work with vendors to reduce the attack surface -- hardening settings in the firmware or Bios or disabling features that don't need to be enabled. Some use hardening templates available from NIST.
- **Test before applying.** This can range from testing new software or patches on a server to completely isolated testbeds. In this area, larger firms have a clear advantage with better equipment. But there are things that every utility can do:
    - Explore partnership opportunities with local universities to gain access to test facilities.
    - Take advantage of vendor's laboratory facilities to test.
- **Know what software is in the environment.** A best cybersecurity practice is understanding what software is running, particularly in legacy systems, and be intentional about adding new software. By the same token, it's critical to:
    - Make sure there are processes to maintain software
    - Develop processes to identify any new software that has been brought in that may not be part of the approved system
- **Verify the hashes on downloaded software**, making sure it wasn't tampered with in transit.

Attacks on the cyber assets of America's power sector pose a serious, ongoing threat – and vendors represent a vulnerable attack vector. But, the proactive steps being taken by the utility industry to block or minimize these risks should become part of the national conversation on how to protect what is arguably our nation's most critical infrastructure.



U.S. Resilience Project

Transforming Resilience into Competitive Advantage