# Webinar: Building Blocks to Support Cybersecurity in the Power Sector

## June 25, 2020

## Presented by the Resilient Energy Platform

*Developed through the USAID-NREL Partnership, the Resilient Energy Platform provides expertly curated resources, training materials, data, tools, and direct technical assistance in planning resilient, sustainable, and secure power systems.*

# Responses to Attendee Questions

A recording of the webinar and the webinar slides are available at https://resilient-energy.org/training-and-resources/webinars.

While we were able to answer some attendee questions during the webinar, we did not have enough time to respond to all the great questions we received. Our presenter, Maurice Martin, Senior Cybersecurity Research Leader at National Renewable Energy Laboratory, kindly provided responses to those questions. We sent these responses directly to the attendees who asked the questions and compiled them in this document.

## Question 1

What is the right data governance strategy to minimize cyber risk?

### *Answer*

*In developing a data protection strategy, the first step is to conduct a data inventory. What data are you storing? How sensitive is that data? What is your high-value data? What are the possible consequences if this data were deleted or if other parties obtained a copy? How is it used? The second step is to understand your data flow. Where does the data move within your organization? If it goes outside of your organization, where does it go? With your inventory and your data flow in place, you can conduct a risk assessment of your data and prioritize security measures. The International Association of Privacy Professionals offers a "Guide to developing a data protection management program" online for free--visit https://iapp.org/resources/article/guide-to-developing-a-data-protection-management-program/ NREL can review utilities' data protection strategy--for details see the contact information on this web site.*

## Question 2

Does cyber insurance exist?

### *Answer*

*Cyber insurance, like other forms of insurance, is a way to transfer risk to another party. You pay a premium to an insurer, and in the event of an incident (cyber attack), the insurer pays some money to you to help mitigate the injury of the attack. However, cyber insurance is challenging because cyber attack is a relatively new phenomenon. Floods have occurred regularly throughout history; our understanding of*

*their likelihood and impact is well developed. Insurers have a relatively small body of data to use when setting the appropriate rates for cyber insurance. Further complications arise on the buyers side--many buyers don't see the need--and the insurers side--they're uncertain how to price and market the insurance. Deloitte has published a good analysis of the challenges to cyber security: https://www2.deloitte.com/us/en/insights/industry/financial-services/cyber-insurance-market-growth.html. Because cyber insurance can sometimes be offered as an add-on to another type of policy, a good starting point is to discuss with your current insurer what (if any) options they offer for cyber. Note that availability of cyber insurance will vary widely between countries and regions.*

## Question 3

How effective is it to assign responsibility for monitoring cyber threat intelligence (CTI)?

### *Answer*

*Monitoring cyber threat intelligence (CTI) is half the story. Someone must also be tasked with responding to CTI that seems relevant to the devices and systems in operation at your facilities. To be effective, the person or persons must have time allocated for both monitoring and response, and others must be prepared to cooperate as needed in the response. If resources (staff time and whatever tools are needed) are allocated and management supports the effort, monitoring (plus response) can be quite effective.*

## Question 4

How can we encourage regulators to be proactive in cyber security if there is a lack of technology on the utility side?

### *Answer*

*Look to the future and encourage the regulator to do likewise. Today, there may not be much automation or cyber-physical technology on your system, but that's likely to change. The economic drivers for digitalization are many. Discuss with your regulator industry trends in digitalization. If you're comfortable doing so, share your own plans for digitalization. Explain that the entire nation has a stake in the secure, reliable operation of the electrical grid, and that managing risk should be a shared responsibility between all parties (including government regulators).*

## Question 5

What technical skills are preferable for a CS specialist looking to work in utility cybersecurity?

### *Answer*

*Among utilities, there is an ongoing debate about whether it's better to train a power engineer in cybersecurity or train a cybersecurity specialist in power systems. Opinions vary, but many lean toward the former. In that case, your power engineer should understand the basics of network defense, network segmentation, the Purdue model, access control (and the principle of least privilege), policy, and the safe way to update software/firmware on an industrial control system.*

## Question 6

As cyber threats continue to evolve, power regulators need to increase their technical capacities. How can power regulators in developing countries enhance their technical capabilities?

### *Answer*

*Education on cybersecurity is available through online learning resources. NREL cannot endorse any particular provider, but an Internet search will reveal a number of options. Power regulators should have basic understanding of technical controls (such as network security) and in-depth understanding of governance, policy, and guidance. An excellent free resource for regulators is available here: https://pubs.naruc.org/pub/9865ECB8-155D-0A36-311A-9FEFE6DBD077*

## Question 7

How does one protect a firewall from hackers?

### *Answer*

*Firewalls are often a first line of defense for network security. However, their software must be up-to-date and they must be carefully configured to reflect the security architecture in use. Understanding the type of data flowing through the firewall, configuration the firewall for that data, and keeping the software patched will ensure you get the best protection from your firewall.*

## Question 8

How can cybersecurity become smart enough to proactively warn utilities about attempted attacks?

### *Answer*

*Cyber threat intelligence (CTI) is a way to anticipate attacks before they happen. By reading alerts based on attacks observed at other organizations, you can anticipate attacks that may be headed your way. Look for a trusted source of CTI that is relevant to your business and the equipment you use.*

## Question 9

Kindly mention few budget-friendly cybersecurity systems in power sector.

### *Answer*

*For perimeter protection for networks, a firewall is a good place to start. Prices vary widely; inexpensive models lack features found on pricier models, but they can still offer basic protection. (Note: NREL cannot endorse any product or company. For guidance or selecting firewalls, discuss with other utilities who are already using them and check online reviews.)*

## Question 10

Does limiting access to a network mean a lower chance of cyberattack, similar to going analog vs digital?

### *Answer*

*Analog systems do not have the same cyber vulnerabilities as digital systems. For this reason, some utilities have chosen to delay digitalization in order to avoid cyber risk. However, the economic drivers for digitalization are many, and are likely to become stronger over time. For instance, meters that can be read remotely save utilities in the U.S. a great deal of money, especially on systems with low line density (that is, a small number of customers per kilometer of distribution line). It's likely you'll move to digital systems eventually, but when and how you make that transition depends on your business and customer service priorities and the maturity of the technology you choose to install.*

## Question 11

How do I know I am using the right building block?

### *Answer*

*Blocking unwanted network traffic is most often done at the network perimeter using a firewall. Best practice in industrial control systems (ICS) networks is to use a firewall that is specifically made for and IC environment, rather than adopting one intended for an IT network (corporate network). To see how well your firewall performs, you can conduct a penetration test in which a third party attempts to breach the firewall and reports on any discovered vulnerabilities. NREL is able to conduct penetration tests--for details see the contact information on this web site.*

***If you are interested in exploring additional training materials, tools, data, case studies and other publications that support decision makers in assessing power sector vulnerabilities, identifying resilience solutions, and making informed decisions to enhance power sector resilience at all scales, please visit the Resilient Energy Platform at www.resilient-energy.org.***