PNNL-XXXXX

Toward a Resilient Cybersecure Hydropower Fleet: Cybersecurity Landscape and Roadmap 2021

Prepared for: Water Power Technologies Office

September 2021

Marie Whyatt
Darlene Thorsen
Mark Watson
Kenneth Ham, Ph.D.
Perry Pederson
A. David McKinnon, Ph.D.
Kyle DeSomber

U.S. DEPARTMENT OF ENERGY

Prepared for the the Department of Energy
under Contract DE-AC05-76RL01830

LIMITED DISTRIBUTION NOTICE

This document copy, since it is transmitted in advance of patent clearance, is made available in confidence solely for use in performance of work under contracts with the U.S. Department of Energy. This document is not to be published nor its contents otherwise disseminated or used for purposes other than specified above before patent approval for such release or use has been secured, upon request, from Intellectual Property Services, Pacific Northwest National Laboratory, Richland, Washington 99352.

Toward a Resilient Cybersecure Hydropower Fleet: Cybersecurity Landscape and Roadmap 2021

Prepared for: Water Power Technologies Office

September 2021

Marie Whyatt
Darlene Thorsen
Mark Watson
Kenneth Ham, Ph.D.
Perry Pederson
A. David McKinnon, Ph.D.
Kyle DeSomber

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99354

Preface

With this roadmap, Pacific Northwest National Laboratory (PNNL) hopes to assist the U.S. Department of Energy’s (DOE’s) Water Power Technologies Office (WPTO) in improving the cybersecurity of hydropower plants across the nation. This effort draws upon collected data from the dams sector, from industrial control system cybersecurity threat reports, from similar work focused on neighboring sectors, and from frank discussions with owners, operators, and vendors. While remaining tightly focused on the needs of hydropower projects, during this landscape study and development of the resulting roadmap, the research team sought to remain informed by the larger energy sector’s vision and direction so that the topics and milestones may fit within a larger vision common to the whole.

Summary

This research team feels it is important to remember that the hydropower sector has a track record of excellent reliability, historically reflecting an effective protective approach practiced in balancing preventive measures with rapid response and recovery in a competitive business environment. Unfortunately, what was successful a decade ago buys no quarter with cyber attackers and in today’s increasingly hostile cyber realm will not carry the sector into the future.

The sector knows it is neither practical nor feasible to protect all assets from damage, whether caused intentionally, accidentally, or by nature. While many would agree with the assertion that you can’t protect all your assets all the time, the corollary is a world apart; if one substitutes “assets” with “safety and security of people” a higher level of diligence is demanded. There is a correlation between the security of the critical control systems at the dam and the safety of people living downstream. Hydropower owners, operators, and stakeholders have continuously sought new approaches and technologies to protect their surrounding communities while reliably delivering power for decades. Their dauntless efforts should be recognized and must be better supported.

Acknowledgments

The Pacific Northwest National Laboratory (PNNL) project team gratefully acknowledges the guidance and assistance provided by the Water Power Technologies Office, and Susan Ennor for her content development guidance, technical writing, and editing. We are also thankful for critical input that provided essential formal information and anecdotal knowledge. We appreciate the opportunity to have researched the subject areas addressed in this report.

The accuracy of the information and the views presented in this report are the responsibility of the authors and do not necessarily represent the opinion of the DOE or other individuals or licensees.

Acronyms and Abbreviations

BEG	bulk electrical grid
BES	bulk electric system
BGP	Border Gateway Protocol
CAC	Common Access Card
CEDS	Cybersecurity for Energy Delivery Systems
CESER	Cybersecurity, Energy Security, and Emergency Response
CIP	critical infrastructure protection
CISA	Cybersecurity & Infrastructure Security Agency
CRISP^{TM}	Cybersecurity Risk Information Sharing Program
CSF	Cyber Security Framework
CSIAC	Cyber Security & Information Systems Information Analysis Center
CTF	Capture The Flag (a kind of computer security competition)
CUI	controlled unclassified information
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DDOS	distributed denial-of-service
DHS	U.S. Department of Homeland Security
DMZ	Demilitarized Zone
DoDIN	U.S. Department of Defense Information Network
DOE	U.S. Department of Energy
E-ISAC	Electricity Information Sharing and Analysis Center
EO	Executive Order
FBI	Federal Bureau of Investigation
IC3	Internet Crime Complaint Center
ICS	industrial control system
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IoT	Internet of Things
IT	informational technology
MFA	multi-factor authentication
MS-ISAC	Multi-State Information Sharing & Analysis Center
NATO	North Atlantic Treaty Organization
NCCoE	National Cybersecurity Center of Excellence
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Security
NIST NCCoE	NIST National Cybersecurity Center of Excellence

NVD	National Vulnerability Database
OE	(DOE) Office of Electricity Delivery and Energy Reliability
OPSEC	operational security
OSI	Open Systems Interconnection
OSINT	open-source intelligence
OT	operational technology
PII	personally identified information
PNNL	Pacific Northwest National Laboratory
RaaS	Ransomware as a Service
R&D	research and development
SCADA	Supervisory control and data acquisition
STEM	science, technology, engineering, and math
TRL	Technology Readiness Level
TVA	Tennessee Valley Authority
USACE	U.S. Army Corps of Engineers
VA	vulnerability assessment
VERIS	Vocabulary for Event Recording and Incident Sharing
VPN	Virtual private network
WaterISAC	Water Information Sharing & Analysis Center
WPTO	Water Power Technologies Office

Glossary

Term	Definition
Azure	Microsoft® Azure is a cloud service offered by Microsoft containing virtualized computing resources provided by Microsoft and hundreds of third parties that can be incorporated into normal operations by both information technology (IT) and operational technology (OT) systems.
Border Gateway Protocol (BGP) Hijacking	BGP hijacking is a cyberattack in which Internet traffic is maliciously rerouted by falsely announcing ownership of groups of IP addresses.
Cybersecurity	In this context, cybersecurity is the protection of interconnected electric power systems from digital attacks.
IT/OT perimeter	The IT/OT perimeter is the network segmentation, sometimes called the DMZ (demilitarized zone), between the IT (e.g. enterprise) network and the OT (industrial) network.
Phishing	Phishing is the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.
Vishing	Vishing is the fraudulent practice of making phone calls or leaving voice messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as bank details and credit card numbers.

Contents

Figures

Tables

1.0 Introduction

The U.S. Department of Energy's (DOE's) Water Power Technologies Office (WPTO), through their Hydropower[1] Program, invests in solutions that improve the contributions of hydropower and pumped storage to the electrical grid. Hydropower owners and operators, and their vendors and partners, rely on WPTO to provide them with early-stage research and innovative technologies, validate new technical solutions, coordinate technology testing, and share information that supports the Office's objectives. Cybersecurity is recognized as an integral part of these efforts to advance the ability of hydropower to deliver flexibility and value to the electric grid. WPTO tasked Pacific Northwest National Laboratory (PNNL) with summarizing the current cybersecurity landscape of the U.S. hydropower fleet in order to identify where research and development (R&D) could address cybersecurity gaps that negatively affect the fleet's obligations to irrigation, the environment, recreation, flood control, and power generation as well as hydropower operators' reputation and financial stability.

This cybersecurity landscape and roadmap supports WPTO in addressing gaps in hydropower cybersecurity by identifying a set of needed capabilities and potential R&D opportunities in a loose implementation timeline from which WPTO can select those most aligned with their objectives. To define these opportunities PNNL scrutinized trending cybersecurity threats and attempted to project future cyber threats, reviewed current and evolving mitigation technologies, attempted to discern mitigation technologies commonly used by hydropower facilities, and identified gaps in cybersecurity tools and technologies caused by either lack of existing tools and technologies or barriers to their adoption. With this knowledge in hand, a roadmap of options was built to fill the identified gaps with investment choices having highest likelihood of adoption and impact. The roadmap choices are binned into near-, mid-, and long-term investment time frames. The result is a set of capabilities anxious for WPTO assistance.

1.1 Purpose

The objectives of this hydropower cybersecurity landscape study and investment roadmap are:

- Define a strategy that moves the needle in the U.S. hydropower fleet's overall cybersecurity such that as WPTO deploys solutions to assist the sector, hydro facilities become less vulnerable, more resilient, and positioned to weather known cybersecurity threats and those not yet imagined.
- Produce a plan of potential R&D investments to improve the cybersecurity and thereby the reliability of hydropower control systems over the next 10 years.
- Guide efforts by WPTO as it plans, develops, and disseminates cybersecurity solutions.

This roadmap complements existing government and industry efforts to improve the security of power plant control systems by identifying needs closely aligned with WPTO objectives that are not the focus of other R&D efforts within DOE or other federally funded programs. Solutions that can be quickly adopted to enable early impacts in securing hydro sector organizations are prioritized. We recognize that this evaluation could be enhanced by a larger collaboration of hydropower experts and further evaluation by experts across industrial control and water technologies.

[1] For simplicity, the term "hydropower" will be used in this document to collectively represent the diverse array of technologies for generating electricity from water not associated with tides or oceans.

1.2 Scope

This cybersecurity landscape and roadmap addresses the cybersecurity protection of both legacy and modernized control systems throughout the U.S. hydropower fleet, and the collection of cyber products used to protect those systems. With plants and equipment that range from large dams to small conduits, hydropower includes a diverse set of operating technologies relative to other generation sectors. The solutions for securing such a diverse landscape are likely to be dependent on the age of the equipment more so than the range of turbine sizes and the variety of turbine types. This evaluation includes new and existing cybersecurity solutions for both operational technology (OT) and information technology (IT) able to be integrated into hydropower sites' industrial control systems (ICS). OT refers to technologies and devices residing in a hydropower plant's industrial network which control and monitor field devices. IT refers to computers, devices, and technologies in a corporate network supporting business functions. Focus is on technologies likely to be successful, including well established or newer technologies and future ones not yet developed or adapted for hydropower environments.

1.3 National Context

WPTO's objectives for cybersecurity arise from its mission of maximizing the benefits of hydropower to the nation. Other DOE offices are tasked with achieving cybersecurity to protect the public from the consequences of a disruption of the bulk electric system (BES) or the water supply system. This cybersecurity landscape and roadmap for hydropower is informed by broader energy sector efforts including the DOE Cybersecurity, Energy Security, and Emergency Response (CESER) office's *CESER Blueprint January 2021*[1] and by its predecessor, the DOE *Multiyear Plan for Energy Sector Cybersecurity 2018,*[2] as well as previous DOE cybersecurity strategy efforts. This context helps WPTO focus on mitigating the cybersecurity challenges facing the achievement of their mission, while benefiting from collaborative efforts toward a common objective of security across the energy sector.

The CESER Blueprint includes five goals reflecting industry and government partners' mission imperatives from across the energy sector. They are:

1. Advance cyber discovery, vulnerability assessment, and rapid risk mitigation.
2. Pursue game-changing R&D and technology transition.
3. Build capacity in the energy sector to understand risks, assess priorities, and identify cost-effective security and resilience improvements.
4. Enhance sector-wide situational awareness to inform decision-making in the energy sector.
5. Coordinate effective and efficient emergency response and recovery efforts.

Hydropower benefits from these sector-wide efforts to secure the energy system, and WPTO's cybersecurity R&D efforts can focus on protection for the value that hydropower provides.

[1] https://www.energy.gov/sites/prod/files/2021/01/f82/CESER%20Blueprint%202021.pdf

[2] https://www.energy.gov/sites/prod/files/2018/05/f51/DOE%20Multiyear%20Plan%20for%20Energy%20Sector%20Cybersecurity%20_0.pdf

1.4 Report Content and Organization

Publicly available data from U.S. government sources specific to hydropower and in sufficient quantity and type to provide meaningful results proved difficult to find. Since a coherent landscape could not be expressed solely based on U.S. government sources, data from reputable U.S. companies which collect cybersecurity data as part of their operations and shares it with the wider community was sometimes used and is duly noted. Knowledge gained from both U.S. government and reputable U.S. companies was reality-checked via meetings and discussions with hydropower operators. All data and graphics sources are thoroughly cited both via footnotes and in the Bibliography.

The ensuing sections of this report are organized as follows:

The Landscape: Hydropower Cybersecurity – This section overviews the hydropower cybersecurity landscape observable today. It first overviews the makeup of the U.S. hydropower fleet's widely-varying equipment ages and types, the many missions hydropower facilities may be required to support, and challenges hydropower operators face. Next is a brief discussion of how current energy demand and new energy generation technologies has forced modernization in the aging U.S. hydropower fleet and resulting cybersecurity challenges. Then cyber threats able to affect hydropower facilities are listed and described, including currently known threats and future threats trends analysis indicate may arise. Finally, technologies and resources meant to assist hydropower operators are touched on.

The Roadmap: A Strategy for Securing Hydropower – The roadmap identifies four overarching cybersecurity goals, describes them, and explains why they are put forth as most pressing. Next is a short discussion explaining alignment with DOE and other agencies' R&D strategies and goals as published in their multi-year plans. Lastly, the 10-year R&D roadmap is given together with a strategy for implementing each goal which contain near-, mid-, and long-term milestones.

2.0 The Landscape: Hydropower Cybersecurity

Hydropower was an early contributor to the electrification of North America, and it still plays a unique role in maintaining the reliability of the electrical grid. More than 2,000 hydropower plants in the United States span the scale from mighty rivers to small canals and conduits, and generate more than half of the renewable energy. High-level efforts to protect the cybersecurity of the energy sector focus first on protecting the public by maintaining the reliability of the electric grid and avoiding physical consequences from improper operation. Plants considered to be “critical infrastructure” because of their role in maintaining grid reliability must comply with a comprehensive set of regulations and requirements.

With cyberattacks on the rise across all sectors of business and industry, even hydropower plants that seem unlikely targets must take active measures to avoid becoming the subject of tomorrow’s headlines. Hydropower plants that have limited impact on the power grid are not compelled to comply with the same requirements as plants designated as critical infrastructure, yet those smaller plants also have an interest in avoiding consequences to their customers, facilities, operations, and business. Minimizing the number and impact of disruptive cyber incidents for all hydropower producers supports WPTO’s objectives by ensuring resources are not directed away from innovation, modernization, and maintenance activities that keep generators available to run and costs in check.

2.1 Facilitating Hydropower Operation

Hydropower differs from other energy generation sectors in that it must manage its “fuel”—water—as a multi-use resource. The priority of electricity generation may at times fall below that of flood risk management, navigation, fish and wildlife conservation, irrigation, recreation, water quality, or municipal and industrial water supply. Numerous constraints and conditions bound the available scope and flexibility of power generation from hydropower facilities, and those constraints potentially change on the scale of hours to minutes.

Despite many possible constraints, hydropower distinguishes itself from most other sources of renewable energy generation by its dispatchability—the ability to provide energy when required. Energy dispatch is important to maintaining the balance of energy supply and demand. Balancing the electric power system requires more than following energy load, it also requires regulating the voltage and frequency, controlling reactive power, and providing reserves. Providing these called-upon services requires the plant to be responsive to signals from grid operators, some of which update on the order of seconds.

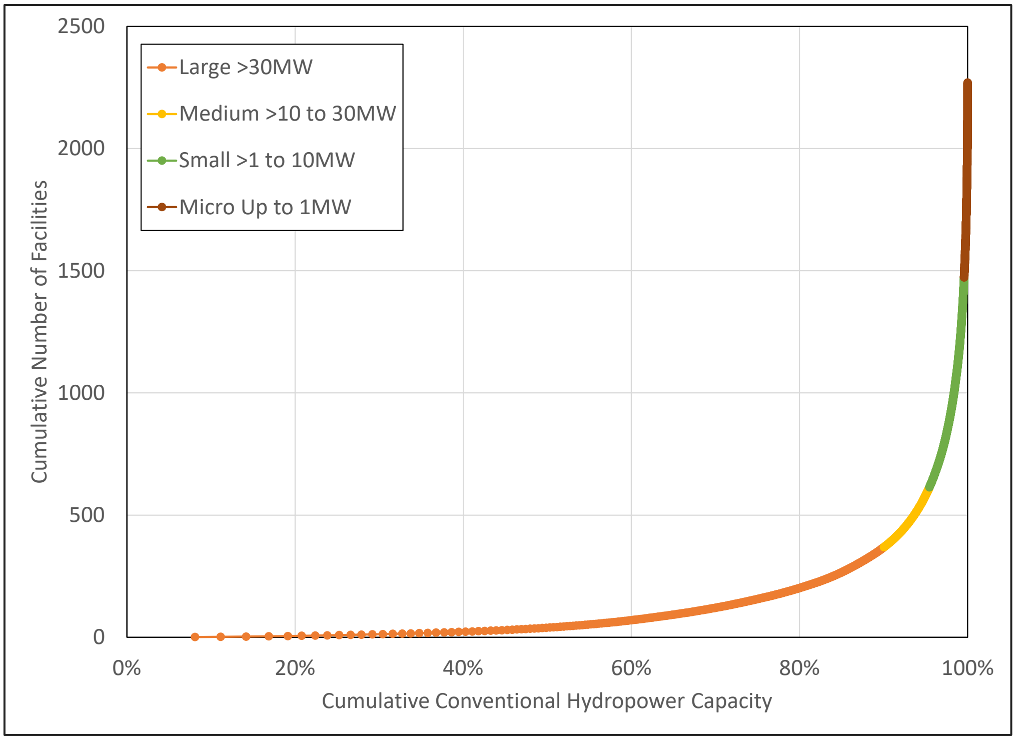


Figure 2.1. Hydropower Capacity as a Function of Plant Size [1]
data source: https://hydrosource.ornl.gov/dataset/existing-hydropower-assets-eha-2020, accessed 10/8/2020

Because hydropower systems are part of natural and manmade water systems, facilities can vary widely, with few plants bearing much resemblance to each other. Figure 2.1 illustrates how fewer than 400 facilities provide 90 percent of the U.S. conventional hydropower capacity. Approximately 1,900 remaining facilities provide the remaining 10 percent. The value that these smaller plants provide grows with their ability to respond to grid signals and address challenges such as transmission congestion and avoidance of carbon emissions by displacing more carbon-intensive generation sources. To be responsive, plants must be connected, and those connections must be secure.

When we examine the makeup of the hydropower fleet, we find that larger-capacity plants make up most of those owned and operated by the U.S. Army Corps of Engineers (USACE), the Bureau of Land Reclamation (Reclamation), and the Tennessee Valley Authority (TVA) (Figure 2.2). These organizations manage numerous plants with enough generation capacity to produce the resources needed to run an effective cybersecurity program. The remaining owner types are quite diverse, but they include smaller organizations that own fewer, smaller plants and may usually have fewer resources to devote to cybersecurity. Those owners would benefit from shared efforts to address cybersecurity risks. WPTO R&D that increases the effectiveness of cybersecurity efforts can reduce costs fleet-wide, helping to keep the cost of hydropower low. Avoiding unnecessary outages and disruptions will also help maintain a reliable, flexible energy supply.

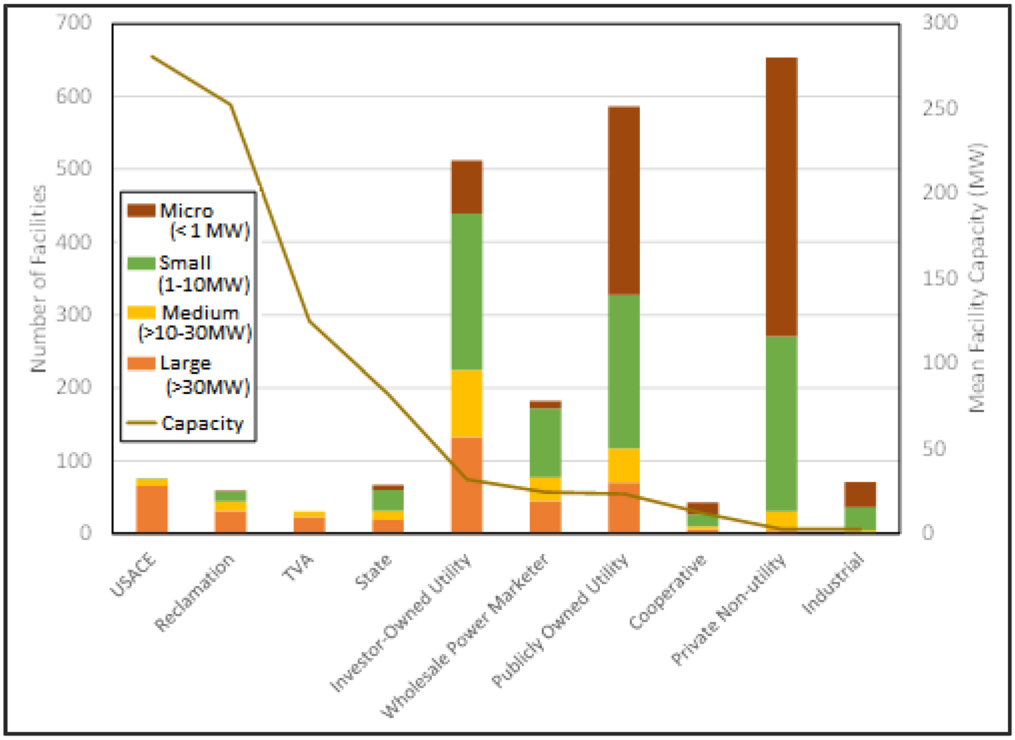


Figure 2.2. Distribution of Hydropower Plant Size by Owner Type [1]
data source: https://hydrosource.ornl.gov/dataset/existing-hydropower-assets-eha-2020, accessed 10/8/2020

2.2 Evolution of Hydropower Systems

Over the long life of a typical hydropower plant, the electrical grid is likely to transform how it operates more than once, requiring plant operations and dynamics that the engineers may not have envisioned. Currently, operators are responding to a growing need for more rapid dispatch of power to balance the supply and demand for electricity in a system that features increasing penetration of variable renewables.[1] Rapid dispatch taxes both the physical equipment and the legacy control systems. Upgrading older analog control systems with the latest digital technology can vastly improve a facility's ability to react to rapid changes in demand, especially if rotating machinery is also refurbished to enhance the flexibility of operation.

Digitalization provides many benefits for operating and managing facilities, but with those benefits comes the possibility that a system can be compromised through the network. The control system of a plant that began life with few digital components can be completely transformed into a connected digital system. Dam operators must incorporate new protections into their security plans and raise staff awareness of new procedures and requirements. Large hydropower plants can more easily muster the funds to upgrade control systems and train staff to address cybersecurity. Smaller plants anticipating a control system upgrade may be more hesitant to take on an uncertain cybersecurity burden. Improved tools, approaches, and guidance can help those plants modernize and deliver more value by reducing uncertainty and keeping the costs of securing systems reasonable.

[1] U.S. Hydropower Market Report. January 2021

Ham et al. (2021) identified nine common types of cyber-physical configurations across a broad sample of hydropower plants. Those configurations reflected the ages, purposes, control schemes, levels of remote operation, and degrees of plant modernization. The network diagram for one of the nine types identified in that study is shown in Figure 2.3. This example diagram shows a close connection between the control of water (Penstock/Gates) and both control systems, that is the network connections carrying data signals and control signals.

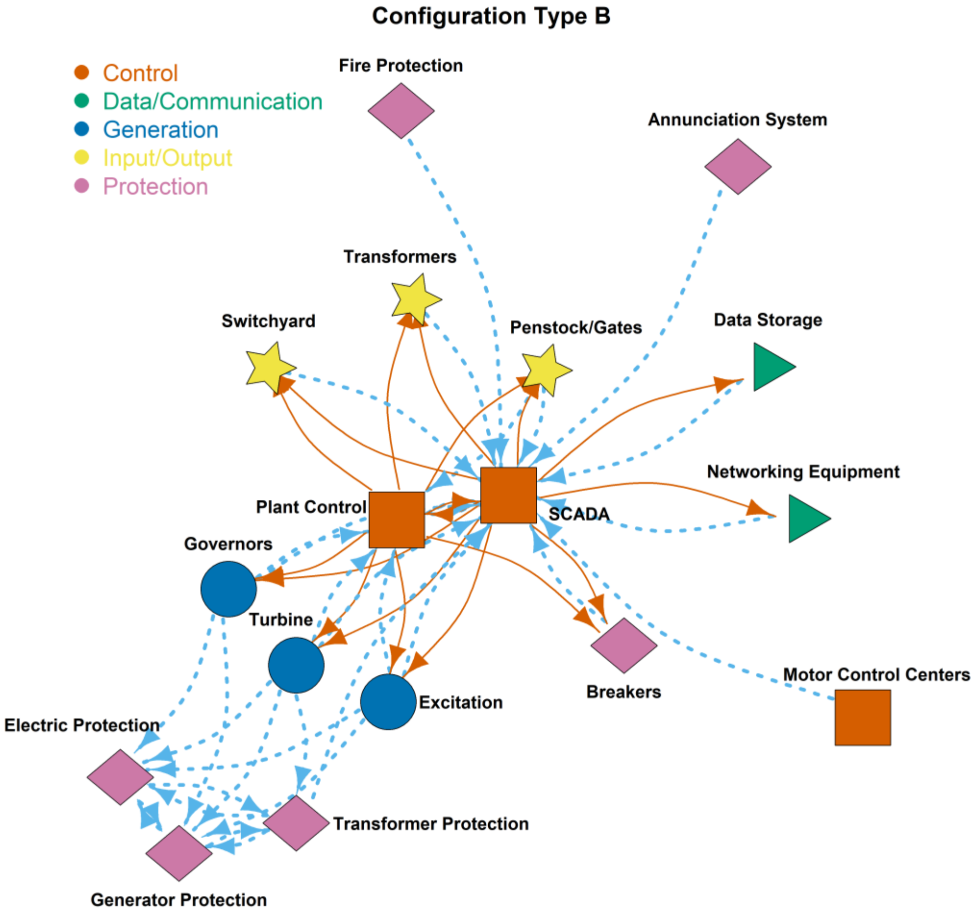


Figure 2.3. Example Hydropower Cyber-Physical Configuration
Type B from Ham et al. 2021[2].
Solid arrows are control connections and dashed arrows are data connections.

Given the integrated control of water resources, hydropower plants present visible targets for nefarious actors. The tools used by those actors continue to grow in sophistication, and vulnerabilities are increasingly shared on the Internet. Given the growing frequency of cyberattacks across all sectors of business and industry, efforts to mitigate the impact of an attack are a necessary part of doing business. As hydropower plants modernize and digitalize control systems to develop new operational capabilities, new vulnerabilities arise. Operators need sophisticated tools that identify known vulnerabilities and how to address them, while providing a way to be alerted to new vulnerabilities as they are discovered.

2.3 General Cyber Incident Trends

Data from the Vocabulary for Event Recording and Incident Sharing[1] (VERIS) community database is plotted in Figure 2.4. The data represents the risk of sensitive information threats. It reveals an increasing number of higher-impact U.S. data breach incidents from 2013 through 2019 which scored ‘painful’ or higher. Incidents rated at the ‘insignificant’ or ‘distracting’ impact levels remain a concern because they may represent initial reconnaissance or practice in advance of a more impactful incident.

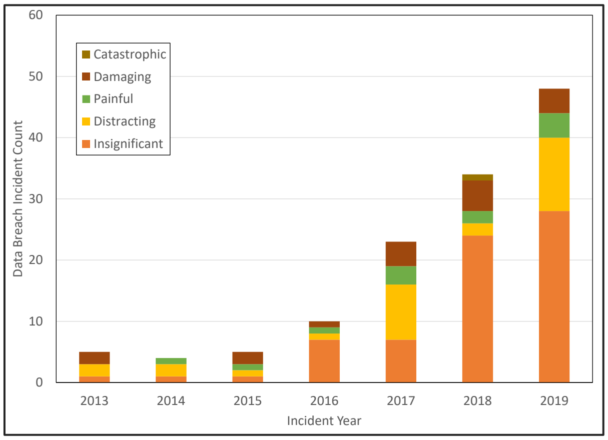


Figure 2.4. Prevalence of Data Breach Impact Levels by Year[3]

Figure 2.5 illustrates how cybersecurity incidents caused by different types of malware change yearly. As a given type of malware is identified and understood, mitigations are constructed and put in place to foil them. An example is cyber incidents attributed to RAM scrapers (dark green line in Figure 2.5). RAM scrapers are a type of malware designed to steal credentials and other sensitive data from computer random-access memory (RAM). In 2015 RAM scrapers were the top-trending malware which resulted in a cybersecurity breach. In cybersecurity parlance, a breach occurs when actual harm is done, such as theft of sensitive information. By 2020 they had become the lowest-trending malware type, most likely due to installed mitigations.

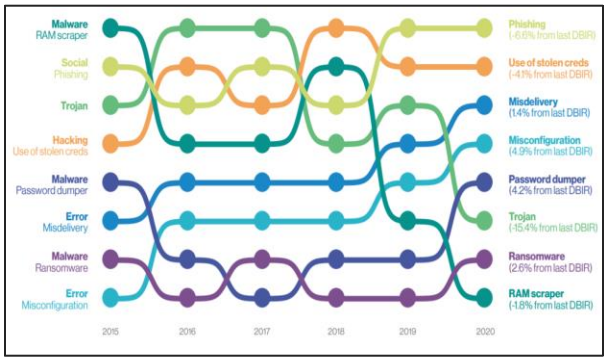


Figure 2.5. Trends in Overall Cybersecurity Breaches Over Previous 6 Years[2], Verizon, *Verizon Data Breach Investigations Report*, 14 Sept 2020[4]

[1] http://veriscommunity.net/vcdb.html
[2] https://www.verizon.com/business/resources/reports/dbir/

Figure 2.6 shows the top 15 overall cybersecurity threat trends seen in Europe for the past six years. It is included because it illustrates how some cyber threats persist at nearly constant levels (e.g., DDoS), others change dramatically (e.g., ransomware), some fall away entirely (e.g., unidentified light green ribbon disappearing in 2017), and new threats emerge (e.g., cryptojacking).

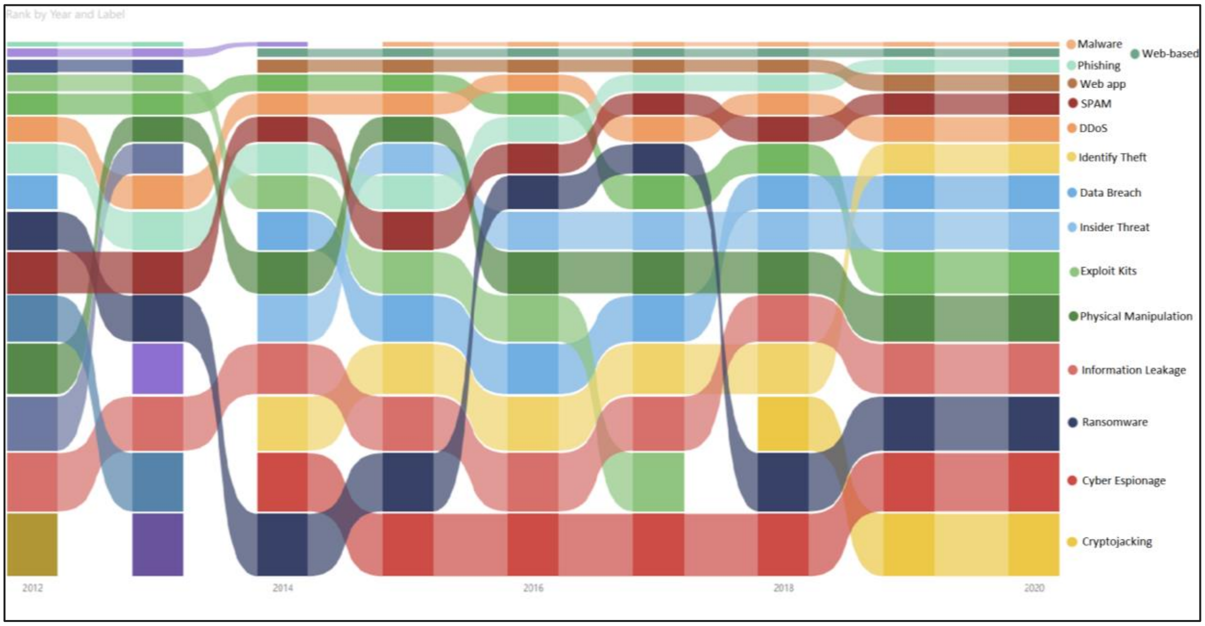


Figure 2.6. Top 15 Overall Cybersecurity Threats Over Previous 6 Years[1], ENISA, 14 Sept 2021[5]

2.4 Industrial Control Systems Cyber Incident Trends

Cybersecurity incidents may occur in IT or OT systems but can negatively affect OT systems regardless of where they originate. According to the 2017 DOE Quadrennial Energy Review[2], cyberattacks targeting OT systems are growing in sophistication and are expected to increasingly resemble conventional attacks that are designed to disrupt physical systems. The timeline in Figure 2.7 shows a worldwide increase in cyber-attacks affecting OT systems in the past two decades. Figure 2.7 focuses on those affecting dams specifically, but includes others as well. To produce the timeline documents and datasets from a wide variety of sources were referenced and used and are listed in the Bibliography section [7].

[1] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends

[2] Quadrennial Energy Review--Second Installment (Full Report).pdf

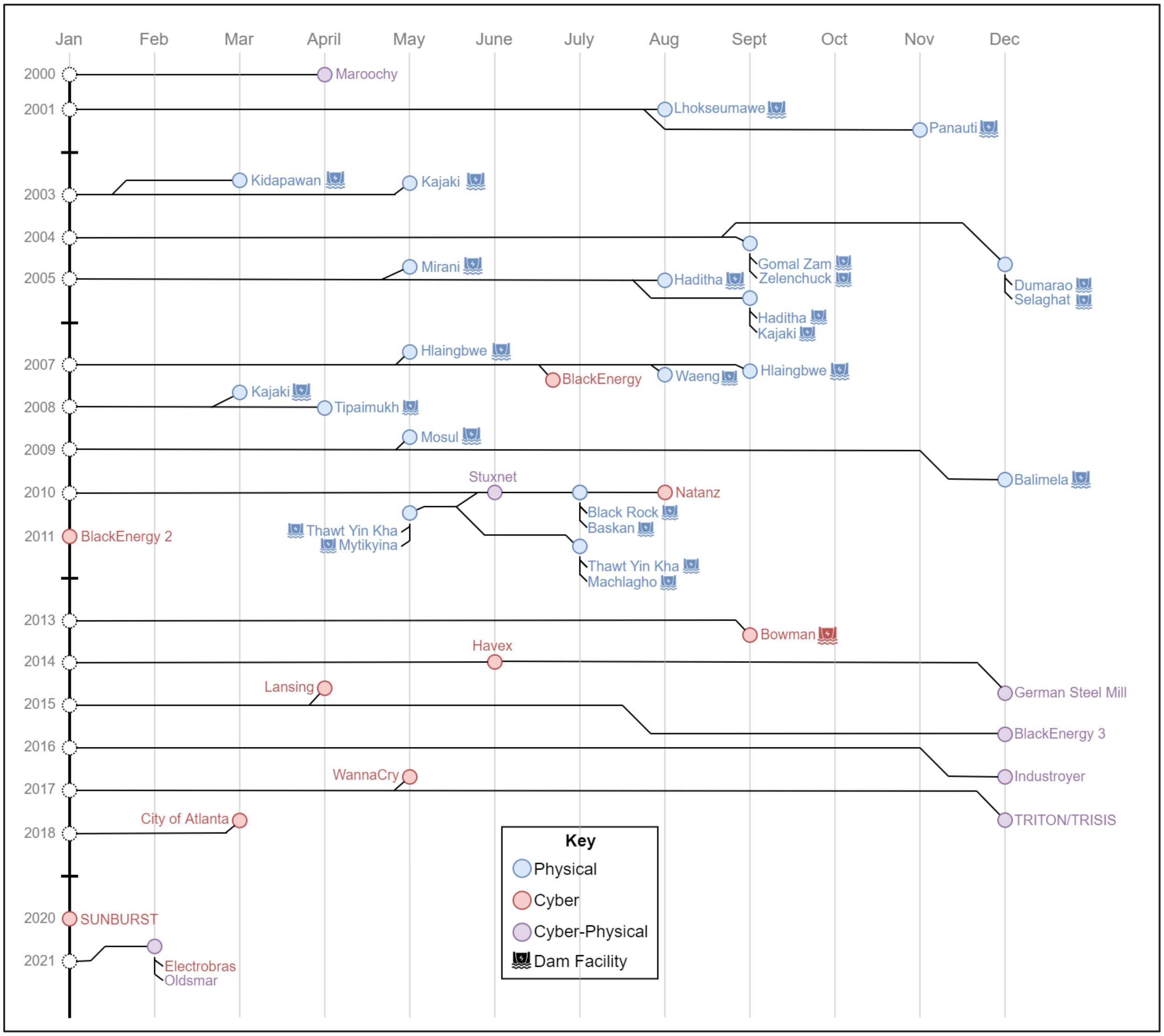


Figure 2.7. Timeline of Threats to Industrial Facilities[7]

The timeline shows 42 cyber attacks over the past 20 years which targeted hydropower facilities worldwide. It includes cyber (e.g., IT), physical, and cyber-physical (e.g., OT) events and shows a clear trend of cyber attacks increasingly affecting OT systems. The attacks included ranged in sophistication from merely gaining an initial access to causing significant harm.

The growth trend the timeline depicts suggests threats against hydropower are changing from targeting only IT systems to also targeting OT systems. At the same time as the U.S. enters this increasingly OT-focused threat environment, the aging U.S. hydropower infrastructure is being asked to add Internet connections into their control system networks in order to be remotely dispatchable and so able to balance fluctuating energy loads, regulate frequency and voltage, control reactive power, and provide spinning reserves.

Figure 2.8 shows a historical summary of more than 30 years of real-world malicious activity affecting ICS. The figure was developed from data in the *Journal of Critical Infrastructure Protection* in the brief *Looking back to look forward: Lessons learnt from cyber-attacks on Industrial Control Systems*[1]. The dataset includes attack type, initial access location, and type of impact and revealed cyber-attacks reached control equipment and field devices, L1 (Level 1) and L0 (Level 0) respectively in the Purdue Model (Figure 2.9) described next. The nearer to Level 0 an attack can reach the more dangerous it is likely to be as it allows hackers to directly operate field devices.

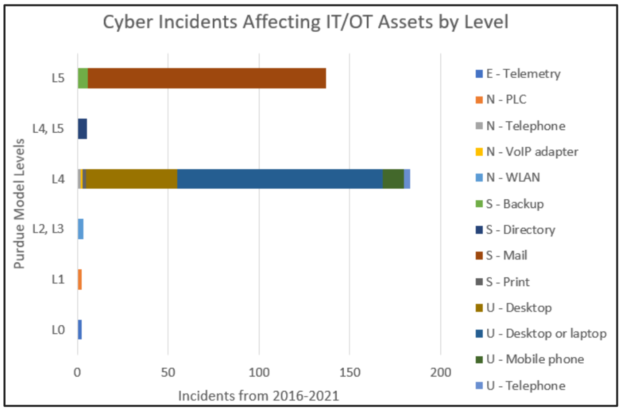


Figure 2.8. Cyber Incidents Affecting IT/OT Assets by Level in the Purdue Model[6]

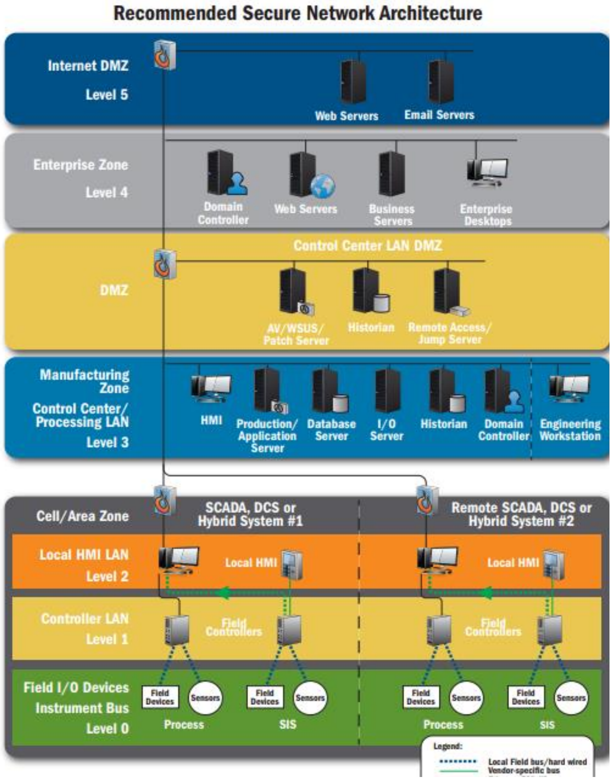


Figure 2.9 Purdue Model (Image Credit: DHS)

The Purdue Model in Figure 2.9 is the best known common model of IT and OT networks and is used by ICS operators and ICS-focused cybersecurity professionals to distinguish computer network security zones. The topmost zones, Levels 4-5, comprise IT network business computing equipment. The lower zones, Levels 0-3, comprise OT network field devices and control systems. The Purdue model can be used to map cyber-attacks to ICS levels. Cyber-attacks have historically occurred in Levels 4-5 but as the shown in Figure 2.7 and Figure 2.8, occurrances are increasingly affecting lower levels. It is reasonable to surmise that a cyber-attack lower in the Purdue model may have a more serious impact, since hackers could possibly gain control of field devices thus causing loss of view and/or control. With increased Internet connectivity combined with increasing attacker sophistication we can expect a similar increase in cybersecurity incidents targeting hydropower.

[1] https://www.sciencedirect.com/science/article/pii/S1874548221000524

Being always reachable to an expanding number of autonomous data-driven systems reverses the former cybersecurity guidance to remain air gapped from other networks, but especially the Internet. The previous strong advocation for strictly separate OT networks is because, historically, connectivity results in greater vulnerability to malicious attacks across critical infrastructure and energy-related assets. However, standalone OT networks seem no longer possible if hydropower facilities are to support a markedly more dynamic electric grid. This means cybersecurity protecting hydropower facilities' control system networks must be enhanced and supported in order to avoid loss of view, loss of control, or even grid outages.

The topmost cybersecurity threats to industrial control systems are summarized here. Data for each of the cybersecurity threats called out below which is specific to hydropower was not available. However, it is reasonable to assume threats to overall OT infrastructure applies, and is therefore acceptable.

- **Exploiting default and hardcoded logon credentials –** Not changing default passwords or using devices which have hardcoded credentials embedded in their software or firmware is a serious security problem, is poor cybersecurity hygiene, and is listed in the Cybersecurity & Infrastructure Security Agency's (CISA's) list of *Bad Practices*[1]:

  > "Use of known/fixed/default passwords and credentials in service of Critical Infrastructure and National Critical Functions is dangerous and significantly elevates risk to national security, national economic security, and national public health and safety. This dangerous practice is especially egregious in technologies accessible from the Internet."

- **Exploiting single-factor authentication and stolen, shared, and guessed logon credentials –** Single-factor authentication is no longer considered sufficiently secure. ICS logons should use multi-factor authentication (MFA), such as a security token (e.g., common access card [CAC], YubiKey®) or a one-time code (e.g., smartphone MFA app, text). CISA has added single-factor authentication to its list of *Bad Practices*:

  > "The use of single-factor authentication for remote or administrative access to systems supporting the operation of Critical Infrastructure and National Critical Functions (NCF) is dangerous and significantly elevates risk to national security, national economic security, and national public health and safety. This dangerous practice is especially egregious in technologies accessible from the Internet."

- **Watering hole attacks –** Watering hole attacks are named for the concept of a predator lying in wait at a place prey often visit. Watering hole attacks can be used for reconnaissance or to plant malware which may act immediately or remain dormant until triggered. Such attacks follow four main steps:

  1. A cybercriminal stalks an individual or group, learning which websites they visit most.
  2. The cybercriminal probes the websites for vulnerabilities allowing exploit code injection.
  3. If a vulnerable website is found, the cybercriminal crafts exploit code able to infect visitors' computers.
  4. Once infected, the cybercriminal can access victims' internal systems and networks.

[1] https://www.cisa.gov/BadPractices

For example, the Oldsmar water treatment plant was a victim of a watering hole attack, which was independent of the well-publicized unauthorized sodium hydroxide (lye) release in February 2021 caused by a different hacker. The compromise resulting from the watering hole attack was discovered while investigating the sodium hydroxide attack. If not for the sodium hydroxide attack, the watering hole attack may never have been detected.

- **Social engineering** – Social engineering attacks via phone, phishing, or vishing have burgeoned and are the primary way hackers gain initial footholds. Since they can happen to anyone at any time all staff must be given training and ongoing awareness about how to detect and respond to social engineering attempts. This enables staff to become the 'human firewall' protecting computing assets. This is supported by an Infosec Institute study[1] conducted in spring 2021. According to Keatron Evans, a Principal Security Researcher at Infosec in an interview[2] with Security Boulevard about the study:

  > What we've found in most cases is that organizations are very reactive to social engineering attacks, but most cultural changes that come as a result of the attacks are short-lived.
  >
  > For example, we have clear data that shows that within 45 days after a successful phishing campaign, users are very aware and do a good job of screening emails, phone calls, and adhering to other anti-social engineering recommendations. … However, when we check again after 60 days or so, we find that these same users have largely reverted back to their old habits.

The most cybersecure corporate cultures tend to exist in cybersecurity, IT, and legal organizations, and in large companies of over 50,000 employees. The least cybersecure tend to be in agricultural and goods distribution. Hydropower facilities are more likely to fall into the latter group, because they have a production structure and do not have a large staff.

- **Ransomware** – Ransomware is currently the most frequent reason hackers target networks. Its goal is to extort money from the owners of the victim network systems. It has been meteorically successful, giving rise to RaaS (Ransomware as a Service). CISA views ransomware as a major threat to ICS and is taking steps to counter the threat, including publishing *Rising Ransomware Threat to Operational Technology Assets,*[3,4] a fact sheet to help OT organizations build resilience, and *Ransomware Guide*,[5,6] which comprises *Part 1: Ransomware Prevention Best Practices*, a checklist of steps to take to secure assets, and *Part 2: Ransomware Response Checklist*, containing steps to follow if a ransomware incident occurs. Important facts to know about ransomware are:

  - **Collateral damage** – When a malware attack compromises an IT network, the OT systems can be unintentionally affected as a side effect. This was demonstrated by

[1] https://www.infosecinstitute.com/wp-content/uploads/2021/06/IQ-Report-Cybersecurity-Culture-Quantified.pdf *(website registration required)*

[2] https://securityboulevard.com/2021/07/reaction-to-social-engineering-indicative-of-cybersecurity-culture/

[3] https://www.cisa.gov/publication/ransomware-threat-to-ot

[4] https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Rising_Ransomware_Threat_to_OT_Assets_508C.pdf

[5] https://www.cisa.gov/publication/ransomware-guide

[6] https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf

the 2021 attack on the Colonial Pipeline by DarkSide ransomware.[1] In that instance, the company powered down servers for 7 days to halt the spread of infection, resulting in delivery delays that caused gasoline and jet fuel shortages and increased prices because of panic buying.

- ○ **Big game hunting** – According to the Federal Bureau of Investigation (FBI), since 2018 ransomware has shifted from reliance on randomly infecting organizations to "big game hunting," targeting organizations viewed as willing and able to pay. According to FBI's public service announcement[2]:

  > Since early 2018, the incidence of broad, indiscriminant [sic] ransomware campaigns has sharply declined, but the losses from ransomware attacks have increased significantly, according to complaints received by IC3 and FBI case information.

- ○ **ICS targeting** – Ransomware has begun specifically targeting ICS, an example being EKANS malware,[3] which upon initial infection specifically searches for and terminates running ICS programs before encrypting files. A joint white paper[4] published by Dragos and IBM X-Force in December 2020 reported ransomware attacks that target companies that have ICS are trending upward:

  > Between January 2018 and October 2020, the number of tracked ransomware incidents impacting industrial companies increased over 500%. In addition, analysis of the frequency of ransomware attacks on industrial organizations per month indicates that attacks have been trending slightly upward over time—with an all-time high in May 2020.

- ○ **State-level Threat actors as partners** – There are fears ransomware crews may have begun acting on behalf of state-sponsored threat actors. Assuming such partnerships exist, cybercriminals may conduct a ransomware operation as usual, but in addition to ransomware may install other malware such as backdoors and rootkits, which presumably the state-level threat actor may use at a later time to quietly gain access.

- **Supply chain attacks** – Supply chain attacks are an emerging threat. Having a software bill of materials (SBOM) is now seen as playing an important role in defending OT against supply chain attacks because SBOMs allow vendors and customers to know exactly what software and libraries are included in devices used in their networks. Executive Order (EO) 10460 mandated SBOMs for U.S. government information systems. However, SBOMs are not yet widely available from OT device vendors. For U.S. government information systems, the U.S. Department of Commerce has published SBOM information and minimum elements SBOMs must include[5,6] which may serve as a starting point for OT vendors.

[1] https://www.fbi.gov/news/pressrel/press-releases/fbi-statement-on-compromise-of-colonial-pipeline-networks

[2] https://www.ic3.gov/Media/Y2019/PSA191002

[3] https://www.fortinet.com/blog/threat-research/ekans-ransomware-targeting-ot-ics-systems

[4] https://www.dragos.com/resource/ransomware-in-ics-environments/

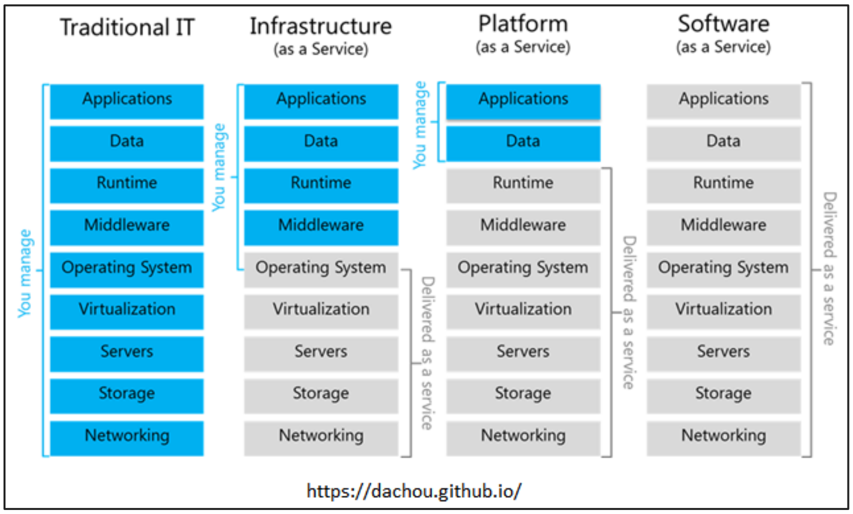
[5] https://www.ntia.gov/SBOM

[6] https://www.ntia.doc.gov/report/2021/minimum-elements-software-bill-materials-sbom

Perhaps the most successful and widely known supply chain attack to date is the SolarWinds attack in which source code for the SolarWinds Orion system management software was hacked by cybercriminals. The compromise became known in November 2020 for which CISA published alert AA20-352A[1]. The GAO has maintained an updated timeline of events[2]. The GAO also published results of a study it had been conducting[3]; the report is sensitive, but an overview is publicly available.

- **Cloud –** Cloud services are new, and in this rapidly evolving environment cloud security is easily misunderstood and misconfigured. Security researchers have identified vulnerabilities the underlying platforms such as in Microsoft® Azure AD Connect[4] and Microsoft® Azure AD Seamless Single Sign-On[5]. The cloud's large Internet Protocol (IP) address space heightens distributed denial-of-service (DDOS) potential because portions of IP address space cannot be blocked by firewall rules without also blocking required services. Also, attackers can more easily be anonymous, operate under a false-flag, and hijack network traffic.[6]

  Major ICS device vendors such as Rockwell Automation, Schneider Electric, Siemens,[7] and WAGO[8] are entering the cloud market and have rolled out programmable logic controller (PLC)-to-cloud product lines. It is likely only a matter of time before vulnerabilities are found and exploited. The graphic in Figure 2.10 shows the different cloud service levels and illustrates the increasing amount of control surrendered to a cloud provider in exchange for freedom from having to manage computing assets.



https://dachou.github.io/

Figure 2.10 Cloud Service Models (IaaS, PaaS, SaaS) Diagram, 15 Sept 2021, https://dachou.github.io/

[1] https://us-cert.cisa.gov/ncas/alerts/aa20-352a
[2] https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic
[3] https://www.gao.gov/products/gao-21-171?utm_source=blog&utm_medium=social&utm_campaign=watchblog
[4] https://blog.xpnsec.com/azuread-connect-for-redteam/
[5] https://www.dsinternals.com/en/impersonating-office-365-users-mimikatz/
[6] https://www.cloudflare.com/learning/security/glossary/bgp-hijacking/
[7] https://new.siemens.com/global/en/products/automation/industrial-communication/cloudconnect.html
[8] https://www.wago.com/us/pfc100

2.5 Information Protection Categories

Information is an asset. For hydropower plants information ranges from sensor readings capturing water level to highly sensitive critical energy/electric infrastructure information (CEII)[1]. Protecting that information from unapproved access and unauthorized alteration, and ensuring critical mission processes maintain uninterrupted access affect the safe and reliable delivery of hydropower.

Protections for hydropower plant information vary. Facilities may be required to follow federal government or State, Local, Tribal, and Territorial (SLTT) government rules; and rules for controlled unclassified information (CUI), consumer privacy, and financial information.[2] In some cases, organizations can look to government or industry regulation to determine which data require security. For sensitive government information, statutory or regulatory restrictions address CUI, official use only information, export-controlled information, and critical energy infrastructure information. In addition, there is also sensitive information that a plant or its owner might create, collect, or exchange. This information might be more difficult to define and can include personally identified information (PII) or sensitive business or process information that if lost, accessed without authorization, or altered inappropriately, might cause financial loss, reputation damage, decreased consumer confidence, or brand erosion. Lastly, site-sensitive information affecting the bulk electric system (BES) can include critical energy infrastructure information about the plant itself, its mission, its design, or how it generates energy. There is also the potential that information, initially of no concern individually, might be able to be combined with other publicly available information to infer a critical infrastructure security concern and pose a risk to the organization or our nation.

Safeguarding this expansive list of sensitive information from corruption or unauthorized access, requires protections across IT and OT systems, by all users of those systems, and can span internal and external access controls of all the systems controlling or managing the plant's operations.[3,4] In addition, information that is made available to a plant to protect itself might require protections beyond the unclassified level, such as when classified information has been shared with a hydropower plant member. In such cases, the authorized person(s) are responsible for:

> Protecting it from persons without authorized access to that information, to include securing it in approved equipment or facilities whenever it is not under the direct control of an authorized person; (b) Meeting safeguarding requirements prescribed by the agency head; and (c) Ensuring that classified information is not communicated over unsecured voice or data circuits, in public conveyances or places, or in any other manner that permits interception by unauthorized persons.(32 C.F.R. §2001.41 (2016)).[5]

As systems evolve and become more interconnected, more protections will be required to protect organizational, governmental, or critical infrastructure information. Protections of sensitive information in the hydropower plant OT and connected IT environment require technical protection of the locations where information is stored, of information in transit across

[1] https://www.ferc.gov/ceii
[2] https://www.archives.gov/cui/registry/category-detail/critical-energy-infrastructure-information
[3] https://www.cisa.gov/sites/default/files/publications/ci-threat-information-sharing-framework-508.pdf
[4] https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-74-Sep20.pdf
[5] https://www.everycrsreport.com/reports/RS21900.html#fn69

systems that share information, and of information shared with personnel who have access to systems with sensitive information. Current technology can provide baseline and evolving security needs for information and applications, but protecting the human who has access to the system from inappropriately sharing that information requires ongoing improvements in technology, in training to keep that information safe, and in personal security controls.

To ensure that the hydropower sector addresses this risk we believe that WPTO can fund improvements in deployed cybersecurity technologies, training, and operational security (OPSEC) controls. We suggest WPTO include in future funding capabilities improvements in controlling the human who has access to sensitive information from inappropriately downloading or sharing information. This can include controls that limit inadvertent or intentional altering of information they do not have permission to change, and training of staff to be aware of adversarial attempts who use open-source intelligence (OSINT) techniques in planning a cyberattack.

2.6 Cyber Assistance

This section discusses a few of the many available resources that can help organizations understand and prepare for cyber threats, and respond to and recover from a cyber incident after one has happened.

2.6.1.1 Bi-directional Cyber Risk Information Sharing

The Cybersecurity Risk Information Sharing Program (CRISP^{TM}) is a direct data sharing and analysis program that is intended to provide the energy sector's critical infrastructure owners and operators with threat intelligence. CRISP is maintained by the E-ISAC. CRISP is a public-private partnership that works by providing owners and operators with a capability to voluntarily share cyber-threat data in near real time. CRISP analysts review the data using U.S. unclassified and classified intelligence information together with technologies and techniques originally developed to defend DOE's networks. The original program was developed for member organizations' IT networks. It identifies malicious traffic within members' IT systems and members then receive machine-to-machine threat alerts, cybersecurity situational awareness information, and mitigation measures.

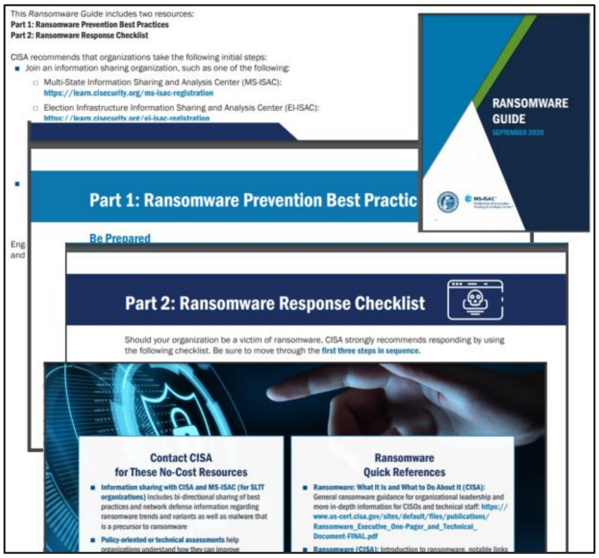
DOE CESER's Cybersecurity for Energy Delivery Systems (CEDS) R&D project seeks to expand energy sector participation in CRISP to the energy sector's OT networks. CEDS implements this via the Cyber Analytics Tools and Techniques Program (CATT™). CEDS is described in DOE's Office of Electricity Delivery and Energy Reliability (OE) *Multiyear Plan for Energy Sector Cybersecurity March 2018.*[1] The multiyear plan seeks to expand CRISP analysis capabilities and share threat indicators in OT systems by piloting real-time OT data sharing and analysis with four utilities in OE's Cybersecurity for the OT Environment (CYOTE™) project.

Assisting the hydropower community to become members of the CRISP public-private partnership could result in big gains for hydropower projects' OT cybersecurity. Security clearances are required, WPTO could help operators gain clearances, removing this barrier.

[1] https://www.energy.gov/sites/prod/files/2018/05/f51/DOE%20Multiyear%20Plan%20for%20Energy%20Sector%20Cybersecurity%20_0.pdf

2.6.1.2 Cyber Assistance: CISA Resources to Fight and Recover from Ransomware Attacks

CISA's mission is to "Lead the national effort to understand and *manage cyber and physical risk to our critical infrastructure."* In January 2021, CISA kicked off a 6-month Campaign to Reduce the Risk of Ransomware. The kick-off followed CISA's release of its *Ransomware Guide*[1] in September 2020, and that was produced in collaboration with the Multi-State Information Sharing & Analysis Center (MS-ISAC). The guide is a succinct 16-page resource that has two parts: *Part 1: Ransomware Prevention Best Practices* and *Part 2: Ransomware Response Checklist* (Figure 2.11).



This *Ransomware Guide* includes two resources:
Part 1: Ransomware Prevention Best Practices
Part 2: Ransomware Response Checklist

CISA recommends that organizations take the following initial steps:

- Join an information sharing organization, such as one of the following:
  - □ Multi-State Information Sharing and Analysis Center (MS-ISAC): https://learn.cisecurity.org/ms-isac-registration
  - □ Election Infrastructure Information Sharing and Analysis Center (EI-ISAC): https://learn.cisecurity.org/ei-isac-registration

Eng
and

Part 1: Ransomware Prevention Best Practic

Be Prepared

Part 2: Ransomware Response Checklist

Should your organization be a victim of ransomware, CISA strongly recommends responding by using the following checklist. Be sure to move through the **first three steps in sequence.**

Contact CISA for These No-Cost Resources

- **Information sharing with CISA and MS-ISAC (for SLTT organizations)** includes bi-directional sharing of best practices and network defense information regarding ransomware trends and variants as well as malware that is a precursor to ransomware
- **Policy-oriented or technical assessments** help organizations understand how they can improve

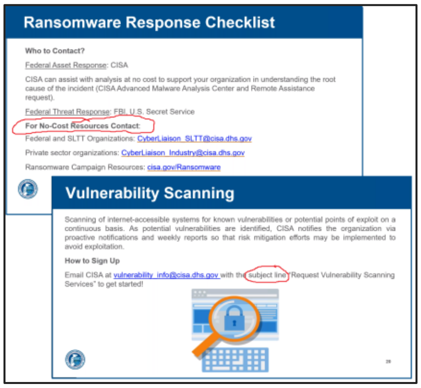
Ransomware Quick References

- **Ransomware: What It Is and What to Do About It (CISA):** General ransomware guidance for organizational leadership and more in-depth information for CISOs and technical staff: https://www.us-cert.cisa.gov/sites/default/files/publications/Ransomware_Executive_One-Pager_and_Technical_Document-FINAL.pdf
- **Ransomware (CISA):** Introduction to ransomware, notable links

Figure 2.11. CISA and MS-ISAC Released a Ransomware Guide that Succinctly Encapsulates Steps for Ransomware Prevention and Response

In June 2021, CISA released a 3-page *Rising Ransomware Threat to Operational Technology Assets* fact sheet (Figure 2.12)—a no-fluff Prepare, Mitigate, and Respond threat guide aimed at OT.

CISA is also rolling out new web-enabled tools including vulnerability-scanning services.



Ransomware Response Checklist

Who to Contact?

Federal Asset Response: CISA

CISA can assist with analysis at no cost to support your organization in understanding the root cause of the incident (CISA Advanced Malware Analysis Center and Remote Assistance request).

Federal Threat Response: FBI, U.S. Secret Service

For No-Cost Resources Contact:

Federal and SLTT Organizations: CyberLiaison_SLTT@cisa.dhs.gov

Private sector organizations: CyberLiaison_Industry@cisa.dhs.gov

Ransomware Campaign Resources: cisa.gov/Ransomware

Vulnerability Scanning

Scanning of internet-accessible systems for known vulnerabilities or potential points of exploit on a continuous basis. As potential vulnerabilities are identified, CISA notifies the organization via proactive notifications and weekly reports so that risk mitigation efforts may be implemented to avoid exploitation.

How to Sign Up

Email CISA at vulnerability_info@cisa.dhs.gov with the subject line "Request Vulnerability Scanning Services" to get started!

Figure 2.12. CISA Offers Services Like Vulnerability Scanning Which Informs Alerts Proactively Mitigating Vulnerabilities

[1] http://www.infosecinstitute.com/wp-content/uploads/2021/05/IQ-Whitepaper-CISA-MS-ISAC-Ransomware-Guide.pdf

The hydropower community may potentially gain much from using these resources. Many are free. A practical and low-cost approach would be to first educate the hydropower community about CISA's new tools, then demonstrate how a hydropower project might use them. Because it is not known exactly how helpful CISA's tools actually are for the hydropower sector, it would be prudent to organize a functional test of the tools at a hydropower site to see and share results and lessons learned. Having such knowledge in hand would encourage hydropower projects to adopt those found to be useful at their own sites. And it would be a low-cost and low-risk confidence-building exercise. These guides and more are available on CISA's website.[1]

2.6.1.3 Cyber Assistance: Ransomware Recovery Services

Working to avoid successful ransomware infections is important. But what needs to be done after an incident has occurred? For IT network environments there is no shortage of commercial companies willing to sell products for purchase. For OT environments there are essentially no products, commercial or otherwise. The best guidance is to work with vendors and law enforcement, as appropriate.

It may be time for a ransomware recovery service for OT environments not tied to a specific vendor and available to any affected facility. Ransomware recovery assistance for OT could be provided as a self-service model. One example is the No More Ransom Project,[2] a Europol public/private partnership portal of which cybersecurity experts from the SANS Institute speak highly.[3] It may serve as an example that could be modeled in the U.S. for OT, starting with smaller hydropower.

2.6.1.4 Cyber Assistance: Threat Advisories and OT Systems

Extensive information about cyberattacks exists from trusted governmental, institutional, and commercial sources. These sources lend authority on cyberattacks and why we must rely on commercial sector information to paint a picture of cyberattacks. Adding to this is the new legislation currently in Congress to require "bipartisan legislation that would require critical infrastructure owners, cybersecurity incident response firms and federal contractors to report cyber intrusions."[4]

However, cyber-threat advisories affecting ICS devices tend to be of limited actionable use to plant operators because they are patterned for IT environments. Advice is of limited help when it only gives the usual generic guidance to apply patches, deploy firewalls, and use only trusted networks. Threat advisories normally include a severity score—a Common Vulnerability Scoring System (CVSS[5]) number between 0 and 19 in the case of the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD). Severity scores can be misleading because they almost without exception ignore the distance an affected product is from the IT/OT perimeter and thus the likelihood of it being attacked and compromised. The IT/OT perimeter is the network segmentation, sometimes called the DMZ (demilitarized zone), between the IT (e.g., enterprise) network and the OT (e.g., industrial) network. Similarly, an advisory that fails to detail impacts a vulnerability has within an industrial environment is of

[1] https://www.cisa.gov/ransomware
[2] www.nomoreransom.org
[3] https://www.sans.org/newsletters/newsbites/xxiii-58/
[4] https://www.cyberscoop.com/warner-24-hours-incident-reporting-notification/
[5] https://nvd.nist.gov/vuln-metrics/cvss

limited use by ICS staff to gauge its effect and severity in their particular ICS. Its helpfulness for deciding if immediate action is imperative or if mitigation can wait is diminished. Each of these is discussed below in greater detail.

Advisories with generic mitigation advice may make sense for IT environments but in many cases are not meaningful to OT operators when they cannot modify systems due to scheduled patch cycles or cannot accept the downtime needed to make and test system changes. Mitigation advice affecting OT systems and devices must include alternate, immediately actionable mitigation guidance that operators can reasonably apply as a temporary measure until equipment can be taken offline for a scheduled maintenance cycle. Alternate mitigation guidance should include specific information such as the affected port number or service to restrict or monitor in the case of network vulnerability, and the specific system hardening steps in the case of local exploitation such as a privilege escalation.

Advisories citing a high severity, but ignoring the likelihood of exposure, fail to allow an OT operator to determine the risk to their specific industrial systems. To be usable, advisories must include information about where an affected product is commonly positioned, such as in which layer of a reference architecture it resides. The Purdue model (Figure 2.9) is well understood in the hydropower community and is a reasonable choice. This knowledge tells the OT operations staff whether any given OT device is directly accessible from the IT/OT perimeter (the DMZ in Figure 2.9) and thus of immediate concern, or whether the device is sectioned off in a subnet away from access points and thus can be mitigated during a scheduled maintenance outage.

Similar to misleading severity scores, advisories that ignore industrial impacts fail to help an OT operator determine whether the vulnerability is of immediate concern or can be addressed later as part of a normal maintenance cycle.

Security advisories about network protocols tend to focus on IT, not OT, protocols. This is because security testing tools were originally made for IT environments and have been slow to change. Because IT networks largely work in the Network Layer (Layer 3 of the Open Systems Interconnection [OSI] Model) security testing tools for IT focus on Layer 3. However, OT devices often operate in the Data Link Layer (Layer 2 of the OSI Model). The active security testing commonly done in IT networks normally is not done in OT networks, because most active security tools do not have the ability to target the Data Link Layer and because sending a malformed packet to a device can knock it offline or destroy it. Security tool vendors have realized this and are striving to fill the gap.

3.0 The Roadmap: A Strategy for Securing Hydropower

WPTO's hydropower program seeks to enable research, development, and testing of new technologies to advance next-generation conventional hydropower and pumped storage systems for a flexible, reliable grid. The role of WPTO is also informed by the Hydropower Vision[1], which is to "Responsibly operate, optimize, and develop hydropower in a manner that maximizes opportunities for low-cost, low-carbon renewable energy production, economic stimulation, and environmental stewardship to provide long-term benefits for the nation." These principles guide WPTO's efforts to secure hydropower facilities to maintain a flexible and reliable supply of clean renewable energy, and to maintain or enhance the value of the benefits of those facilities to society and the environment. These ideas are incorporated in the vision for hydropower cybersecurity efforts at WPTO.

VISION
for Hydropower
Cybersecurity

Within 10 years the U.S. hydropower fleet shall be a conspicuously modernized, well-maintained, and cybersecure source of value for the nation.

3.1 Hydropower Security Goals

Many organizations contribute to improving cybersecurity across the energy sector, especially for facilities considered part of the nation's critical infrastructure. The hydropower sector benefits from those efforts in many ways, but it can be challenging for smaller operators to keep up to date on the latest protections. In addition to protecting critical infrastructure, WPTO has an opportunity to bolster hydropower generators' abilities to avoid costly disruptions, thereby helping to keep electricity costs reasonable, maximizing flexibility, and support the transition to low-carbon energy. The strategic goals are listed below and are examined more fully in the following sections:

- Foster actionable information sharing.
- Develop cybersecurity guidance tailored to common plant types.
- Grow training and workforce development.
- Develop and demonstrate technologies.

3.1.1 Foster Actionable Information Sharing

Organizations need actionable cyber-threat intelligence to maneuver to their most cybersecure posture. Our understanding of whether smaller hydropower facilities feel well-supported in this area is murky because of the lack of available data specifically addressing this question. However, it is likely that smaller hydropower is in the same situation as water and wastewater facilities. A survey[2] conducted earlier this year by the Water Sector Coordinating Council to better understand that sector's cybersecurity challenges and needs identified areas in which utilities asked for federal help. The need for applicable and actionable cybersecurity threat information was listed third among the top four needs.

Supporting this is feedback received from one-on-one interactions with staff at smaller hydropower facilities. The top complaints heard were as follows:

[1] https://www.energy.gov/eere/water/articles/hydropower-vision-new-chapter-america-s-1st-renewable-electricity-source

[2] https://www.waterisac.org/2021survey

1. There is a lack of efficient means to connect public threat advisories to a facility's operational devices; a failure of threat advisories to be automatically ingestible by facilities' asset management software, which could then alert facility operators.

2. There is a lack of a single asset management software solution that does everything facilities need; facilities report having more than one but even then must maintain spreadsheets, requiring considerable staff time to use and keep updated.

3. Publicly available threat advisories give poor indications of whether a threat is serious enough to require facilities to schedule emergency downtime to take equipment out of service for emergency patching.

4. Advisories lack mitigation advice for ICS environments; simply advising to "patch now" is easily implemented by IT network administrators, but fails to take into account the facilities' requirement to first test changes for operational consequences and human safety and then schedule downtime. Interim mitigation alternatives should be included in threat advisories for equipment expected to reside in ICS environments.

Additional details are provided in Section 2.6.1.4, Cyber Assistance: Threat Advisories and OT Systems.

Staff from different facilities strive to keep each other informed of cyber threats they've encountered and mitigation strategies they've enacted in response. We see this accomplished largely via in-person and virtual lunch-and-learn events and during industry conferences. Information sharing in this manner is haphazard because it depends upon chance meetings between whomever happens to attend.

WPTO could help facilitate getting actionable threat intelligence and mitigations to smaller hydropower by nudging existing resources to provide additional guidance that helps operators understand the applicability and severity of threats to hydropower facilities. This could include the following:

- Helping existing threat intelligence become more ICS-friendly by including ICS-specific severity scores and workaround mitigation steps pending facilities' maintenance outage for patching.
- Monitoring classified threat intelligence and preparing curated summaries of declassified versions deemed important and requiring a response by smaller hydropower facilities.
- Billeting a group of hydropower industry professionals with security clearances, thereby enabling hydropower staff themselves to take on the intelligence tasks above for their own industry.
- Determining how best to support peer-to-peer information sharing, then facilitating developing them.

Such efforts by WPTO could help deliver cyber-threat information that conveys the applicability and urgency of cyber threats to hydropower OT systems, and that includes detailed and realistically actionable mitigations implementable in OT systems. Those efforts could accelerate the development of trusted conduits for plant operators to share their knowledge and experiences peer-to-peer and facility-to-sector.

3.1.2 Develop Guidance Tailored to Common Plant Types

As part of this effort, project researchers held listening sessions in the form of lunch-and-learn meetings sponsored by industry, attended and presented at hydropower conferences to engage with hydropower staff at all levels, and became involved with hydropower and bulk electrical grid (BEG) cybersecurity planning via the *Joint IEEE PES-NERC Technical Report on Integration of Cyber and Physical Security into Bulk Power System Planning, Operations, Design, and Restoration Activities* and the *IEEE PES Task Force on Water-Power Systems.*[1] The group and one-on-one discussions with hydropower staff indicated there is a strong desire to be cybersecure, coupled with great uncertainty surrounding how to properly go about it and how to know when the goal has been met. Clearly, this indicates a need for guidance that is tailored to facility types and budgets.

WPTO could fund curation or development of a set of guidance documents and resources aimed at a representative collection of facility types, possibly based on the recently developed hydropower cyber-physical typology mentioned in Section 2.2 Evolution of Hydropower Systems of which one type is illustrated in Figure 2.3. A hydropower operator could spend an afternoon using WPTO resources to identify their facility type, then based on that type to see a list of usual associated cybersecurity needs, obtain an action list, learn how to obtain needed materials and assistance, and determine a plan of action and timeline. In a single sitting they would acquire a clear list of what needs to be done, the level of effort involved, resources to secure, associated costs, and which staff to involve.

The value would be in creating resource collections together with a means for operators to quickly identify which collection fits their facility type. Helping operators avoid wasted time and effort searching for suitable guidance aligns with WPTO's goal to discern what can be done in the short term and for little cost to change the asymmetric advantage that cyber attackers enjoy.

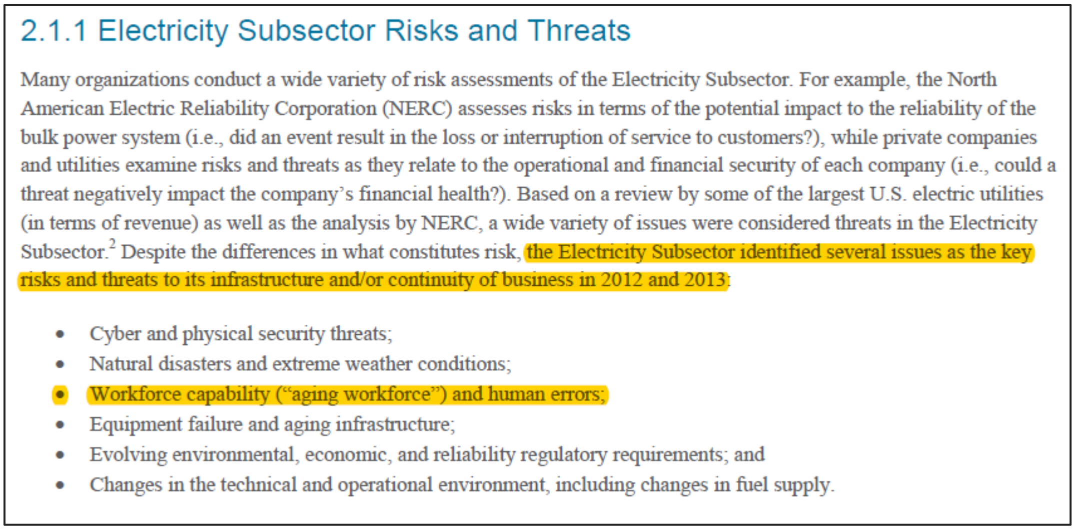
3.1.3 Grow Workforce Development and Cybersecurity Training

3.1.3.1 Workforce Development

According to the DHS *Energy-Specific Plan 2015*[2] there is a substantial need for workforce development and training throughout the electricity subsector (Figure 3.1). The workforce is aging, and retiring professionals must be replaced. Technology is modernizing, so professionals from new fields including cybersecurity must be encouraged toward hydropower careers. A well-functioning, sustainable pipeline of professionals must be in place beginning at least at the collegiate level. Early-age awareness in K-12 of hydropower's societal benefits could further ease the effort. Hydropower will require a specialized approach to encompass the wide variety of equipment ages and types found across the fleet and to help nontraditional young professionals see themselves in hydropower careers. Not addressing this need is seen as a threat to the electricity subsector in the DHS *Energy-Specific Plan 2015*.

[1] https://cmte.ieee.org/pes-wp/

[2] https://www.hsdl.org/?abstract&did=796517



2.1.1 Electricity Subsector Risks and Threats

Many organizations conduct a wide variety of risk assessments of the Electricity Subsector. For example, the North American Electric Reliability Corporation (NERC) assesses risks in terms of the potential impact to the reliability of the bulk power system (i.e., did an event result in the loss or interruption of service to customers?), while private companies and utilities examine risks and threats as they relate to the operational and financial security of each company (i.e., could a threat negatively impact the company's financial health?). Based on a review by some of the largest U.S. electric utilities (in terms of revenue) as well as the analysis by NERC, a wide variety of issues were considered threats in the Electricity Subsector.[2] Despite the differences in what constitutes risk, the Electricity Subsector identified several issues as the key risks and threats to its infrastructure and/or continuity of business in 2012 and 2013:

- Cyber and physical security threats;
- Natural disasters and extreme weather conditions;
- Workforce capability ("aging workforce") and human errors;
- Equipment failure and aging infrastructure;
- Evolving environmental, economic, and reliability regulatory requirements; and
- Changes in the technical and operational environment, including changes in fuel supply.

Figure 3.1. Excerpt from DHS Energy-Specific Plan 2015

Between 5,000 and 97,000 new hires will be needed by 2030, depending upon whether the hydropower industry remains exactly as it is or experiences aggressive growth. According to the DHS *Energy-Specific Plan 2015*:

> Attrition will require the industry to replace at least 10,000 FTEs—33% of the current workforce—by 2030. While this is not a large number in absolute terms, interviews indicated that the people retiring in the next 15 years hold a great deal of critical industry knowledge.

Two DOE OE Efficiency and Renewable Energy (EERE) WPTO reports detail projected workforce development needs through 2050. The 2019 report *Workforce Development for U.S. Hydropower: Key Trends and Findings*[1] revealed that of the 66,500 on-site staff employed in hydropower in 2018, 5,000 are expected to retire or otherwise leave the industry by 2030. New staff will have to be attracted and retained to replace those leaving engineering, skilled trades, managerial, and administrative positions. Industry expansion will drive that number to between 60,000 and 97,000 when taking projected growth in hydropower projects into account, including development of more nonpowered dams, new small hydro facilities, and pumped storage hydropower.

The *Workforce Development for Hydropower*[2] report of 2017 exhaustively breaks down projected workforce development and hiring needs based on 2016 data. This knowledge can be used to plan and develop where and how to introduce cybersecurity awareness into university, community college, and trade school curricula.

3.1.3.2 Cybersecurity Training

The DHS *Energy-Specific Plan 2015* also calls out human error specifically as a threat to the electricity subsector. And indeed, today's most prevalent threat is the unwitting insider, the staff member who in good faith clicks a link in a phishing email specially crafted to trick them. This is explained in Section 2.4 in the discussion of social engineering and effective training

[1] https://www.osti.gov/biblio/1545009-workforce-development-hydropower-key-trends-findings
[2] https://www.osti.gov/biblio/1515066-workforce-development-hydropower

Cybersecurity awareness training and education programs exists for ICS, and reputable companies and government agencies that provide such training abound. However, none of these offerings can be expected to be tailored to smaller hydropower facilities. The best use of funding in this situation may not necessarily be to produce training specifically for smaller hydropower projects. It may be to recommend collections of training programs that already exist and are both effective for smaller hydropower projects and friendly to their budgets.

WPTO could help create a more cybersecurity conscious hydropower culture in a low-cost manner, especially if doing so is planned with attention to where new hiring is expected to take place over the next 10 years. Cybersecurity awareness could be added to new-hire onboarding practices and refreshed periodically with affordable reinforcement exercises and campaigns. This strategy has been found to be effective in decreasing cybersecurity incidents.

For WPTO, one strategy might be to group smaller hydropower projects based on observed and reported needs, inventory existing cybersecurity awareness training programs and choose a candidate subset for trials, administer the candidate curricula to volunteer staff at a collection of hydropower facilities, and then test near-term and long-term efficacy. A training program's effectiveness could be measured by employing a regimen used in scientifically rigorous sociology experiments together with industry-standard cybersecurity compliance testing techniques, such as the phishing measurement software used by professional penetration testers. Further, authors of training materials could be informed about what parts of their training programs were found to be effective and could be given suggestions and encouragement about where to make improvements.

3.1.4 Develop and Demonstrate Technologies

Producing technologies calibrated to lift smaller hydropower owners and operators to a heightened state of cybersecurity is seen as a vital goal and a highly important investment of WPTO's resources. WPTO has successfully shepherded development of advanced hydropower technologies and can do the same with cybersecurity software systems and hardware devices.

Budgets are uncertain, thus near-term development projects can most reliably be planned, executed, completed, and transferred. Mid-term projects may also be feasible but likely will have greater uncertainty for completion. Projects nearer the high end of the technology readiness level (TRL) range offer greater certainty for completion if they are meant to be transferred into the hands of a target audience soon.

Listening sessions with industry revealed some technologies participants view as important to improve. Session participants not involved in day-to-day operations who are able to take a longer view mused about technologies to invent. Asset management software is an example of a technology needing both improvement and innovation. The hydropower industry is vocal about the amount of time currently needed to keep asset management software updated and described its shortcomings; some users have used software from multiple vendors only to find they must still fill capability gaps using basic spreadsheet software. A more visionary approach would be to add capability to assist with determining when vulnerability advisories are applicable to an asset, how likely the described threat is to occur, and whether the threat is sufficiently serious to warrant an emergency outage to apply a fix. Having that ability would aid asset owners' decision-making processes and potentially improve a facility's cybersecurity readiness.

In some cases, WPTO may identify a cybersecurity technology vital to hydropower that has been developed in another sector. Operational tests of existing technologies similar to what other U.S. federal agencies are doing could accelerate adoption in the hydropower sector. A current example is the NIST National Cybersecurity Center of Excellence (NCCoE) project,[1,2] which aims to demonstrate a variety of zero-trust implementations in response to Executive Order (EO) 14028. The EO directs federal agencies to implement zero-trust as a cybersecurity measure in federal information systems. The NIST NCCoE project is a collaboration between the NCCoE and 18 private companies, each having a zero-trust solution. Each collaborating company works with NCCoE to demonstrate approaches to implementing zero-trust architectures that comply with *NIST SP 800-207 Zero Trust Architecture.*[3]

Along the same vein, a WPTO Tech Demo might involve choosing a set of existing technologies advertised as offering features smaller hydropower facilities say they want, trying them out either in a test bed or at a volunteer hydropower facility, and sharing observations and lessons learned via written reports and conference presentations.

Regarding test beds, as of August 2021 the WPTO released a Request for Information (RFI) about testing capabilities and facilities to validate hydropower technology innovations[4]. Because responses are due at a future date after publication of this report, the RFI results can only be guessed at. The authors of this report have high hopes innovative new technologies and existing repurposed ones will soon be available to hydropower, including those enhancing cybersecurity.

3.2 Energy Sector Perspective

The WPTO's hydropower program focuses on a specific portion of the energy sector, while other agencies focus on other portions (fossil, nuclear, wind, solar, etc.). The CESER mission includes enhancing the security of U.S. critical energy infrastructure. As previously mentioned, the *CESER Blueprint January 2021* put forth five goals that are timely and relevant to the energy sector:

1. Advance cyber discovery, vulnerability assessment, and rapid risk mitigation.
2. Pursue game-changing R&D and technology transition.
3. Build capacity in the energy sector to understand risks, assess priorities, and identify cost-effective security and resilience improvements.
4. Enhance sector-wide situational awareness to inform decision-making in the energy sector.
5. Coordinate effective and efficient emergency response and recovery efforts.

The hydropower-specific goals identified for the hydropower roadmap address needs similar to those of the entire energy sector. The alignment between the goals identified herein and the CESER Blueprint goals is shown in Table 3.1.

[1] https://www.nccoe.nist.gov/zerotrust
[2] https://www.nccoe.nist.gov/news/nccoe-announces-technology-collaborators-demonstrate-zero-trust-architectures
[3] https://csrc.nist.gov/publications/detail/sp/800-207/final
[4] https://www.energy.gov/eere/articles/wpto-releases-rfi-testing-capabilities-and-facilities-validate-hydropower-technology

Table 3.1. Alignment of Roadmap Goals to CESER Blueprint Goals. An uppercase X indicates primary alignment, and a lowercase x indicates secondary alignment.

Roadmap goal	Advance cyber discovery, vulnerability assessment, and rapid risk mitigation	Pursue game-changing R&D and technology transition	Build capacity in the energy sector to understand risks, assess priorities, and identify cost-effective security and resilience improvements	Enhance sector-wide situational awareness to inform decision-making in the energy sector	Ensure effective and efficient emergency response and recovery efforts
Foster Actionable Information Sharing	**X**			x	
Develop Guidance Tailored to Common Plant Types	x		**X**	x	x
Grow Workforce Development and Cybersecurity Training	x		**X**		
Develop and Demonstrate Technologies	x	**X**		x	x

In a progression of roadmaps relevant to hydropower (Table 3.2), critical infrastructure is a primary focus. Avoiding consequences to critical infrastructure is an appropriate focus to protect public interests and public safety, but other interests are also worth protecting. Cyber incidents that may affect only the facility or business operations may have few immediate consequences for the public good, yet may be of great importance to the owner or operator. The consequences of such incidents can make power generation more costly, less flexible, or less predictable. These changes affect the viability of smaller facilities and are counter to WPTO's vision.

Table 3.2. Prior Cybersecurity Roadmaps Relevant to Hydropower

Document	Agencies	Scope	Sectors
2006 Roadmap to Secure Control Systems in the Energy Sector	DOE, DHS, and Canada	Critical infrastructure	Electricity, oil, and natural gas sectors
2011 Roadmap to Achieve Energy Delivery Systems Cybersecurity	Energy Sector Control Systems Working Group	Critical infrastructure	Electricity, oil, and natural gas sectors
2015 Roadmap to Secure Control Systems in the Dams Sector	DHS	Critical infrastructure	Dams sector
2018 Multiyear Plan for Energy Sector Cybersecurity	DOE/OE	Critical infrastructure	Electricity, oil, and natural gas sectors
2021 CESER Blueprint	DOE/CESER	Critical infrastructure	Electricity, oil, and natural gas sectors
2021 This Document	DOE/EERE/Water Power Technologies Office	Any hydropower plant	Hydropower

3.2.1 Tiered Cybersecurity Requirements

Cybersecurity requirements apply differently, depending on the type of plant and the risk to public safety or electric system reliability. Table 3.2 above reveals an emphasis on protecting plants classified as critical infrastructure. Hydropower facilities that play a pivotal role in the bulk electrical system (BES) are classified as critical infrastructure. This classification initiates a set of requirements known as North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards to ensure that those facilities are secured to avoid negative impacts on the reliability of the electric grid or on public safety.

The NERC develops and enforces reliability standards under the oversight of the Federal Energy Regulatory Commission (FERC) in the U.S. and governmental authorities in Canada. The NERC-CIPs apply to hydropower as they do to other components of the BES. Inclusions and exclusions add some complexity, generation facilities that connect to the electric grid at voltages below 100 kV are not considered part of the BES and are not subject to NERC-approved reliability standards.

For plants considered part of the BES, requirements for compliance differ according to the level of impact that an outage would have on the BES. The NERC CIP high-impact category applies to control centers that coordinate reliability, energy balancing, or transmission across a broader system. Generation facilities or groups of facilities operated together that have a capacity of at least 1,500 MW are considered medium impact. Other facilities considered part of the BES would fall into the low-impact category. This creates three categories—NERC Medium Impact, NERC Low Impact, and Non-BES—that cover the bulk of the hydropower fleet. Each facility must determine which category they fall in using the full set of criteria, but in simple terms, smaller facilities have a greater likelihood of falling into the Non-BES category and medium and large facilities are likely to fall into one of the NERC impact categories.

Hydropower facilities that fall into the NERC high or medium impact category must review and obtain approval every 15 calendar months for documented cybersecurity policies addressing the topic areas below. The CIP standard referenced parenthetically provides additional detail about what the policies must address. The areas are:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BES Cyber Systems (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BES Cyber Systems (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

NERC CIP low impact generation facilities must document policies addressing the following topic areas:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets and Removable Media malicious code risk mitigation; and

1.2.6. Declaring and responding to CIP Exceptional Circumstances.

Facilities that do not meet criteria requiring compliance with NERC standards may find it difficult to justify voluntary compliance with those requirements. NIST has developed a framework for cybersecurity (NIST Cyber Security Framework [CSF]) that is applicable to any organization, whether or not they are considered critical infrastructure. Hydropower facilities not required to comply with NERC reliability standards may choose to adopt the NIST CSF approach. Implementing the NIST CSF is not without cost, but it can be a helpful tool for managing cybersecurity risks.

Hydropower facilities that have limited influence on the BES are not classified as critical infrastructure. Fewer requirements are imposed on these facilities, but the consequences of a disruption at these facilities may still be of great importance to the operator of the facility, so they also have a keen interest in avoiding cyberattacks.

3.3 Strategies for Securing Hydropower

Achieving a conspicuously improved cybersecure U.S. hydropower fleet within a decade is a challenge. A suggested 10-year timetable of milestones is given in Table 3.3. But because cyber threats emerge or change continuously, it should be viewed with an eye to flexibility. The stated goals are to be both measurable and adaptable to fluctuating funding and priorities.

The strategies and goals making up this roadmap are based on conclusions drawn from both hard data and from discussions with the hydropower community. The roadmap encompasses a general set of capabilities that WPTO can address with future R&D money; it does not address specific solutions or specific products. General recommendations for ways WPTO may choose to implement the strategies to reach the goals are mentioned, but it should be borne in mind they are suggestions. WPTO is expected to take them under advisement when making its own determinations.

In giving thoughtful consideration to the hydropower community’s unique operational needs and challenges, the following questions were posed to enable choosing the best-fitting set of strategies and goals:

- Are a significant number of hydropower facilities helped? (community propagation)
- Are cybersecurity risks substantially reduced (impact)
- Is there a clear path and short time to put in place? (speed to adoption)
- Is the maintenance burden minimal? (ease of ownership)

Strategies for accomplishing the five goals presented in in Table 3.3 are summarized in Table 3.4 through Table 3.7. Each goal presents distinct challenges that must be overcome, may require deliverables to be completed on an established timetable, and must be prioritized in the face of unknown year-to-year budgets. Priorities are organized around four areas critical to improving cybersecurity—Policies, People, Process, and Technology. These solutions represent examples of potential projects, initiatives, and activities that were identified. They are not intended to be an exhaustive list.

Table 3.3. Roadmap for Markedly Improved Cybersecurity in Smaller Hydropower

Vision			
Within 10 years, the U.S. hydropower fleet shall be conspicuously modernized, well-maintained, and a cybersecure source of value for the nation.			
Goals			
Foster Actionable Information Sharing	**Develop Guidance Tailored to Common Plant Types**	**Grow Training & Workforce Development**	**Develop and Demonstrate Technologies**
Milestones			
Near Term (0-2 Years)			
OT device advisories include seriousness based on distance from IT/OT border, whether vulnerability warrants an unplanned outage, and reasonable (for OT) workarounds if updates/patches can wait for scheduled outage.	Facility typologies are identified and checklists to secure each are written, and resources identified and listed.	Cybersecurity training resources are binned according to roles and responsibilities. Programs to develop and recruit talent to hydropower are initiated.	A process is in place to identify OT-specific cybersecurity technology gaps. A plan to periodically fund R&D for identified cybersecurity technologies is initiated.
Mid-Term (3-6 Years)			
Owners/operators are enabled to use threat OT-specific threat advisory steps. Operators are aware of peer-to-peer information sharing conduits and use them.	Typologies and resources are permanently housed at a location accessible by operators that is secure from threat actors who might misuse such information.	Right-sized, role-based, affordable cybersecurity training resources are used effectively. Talent pipelines are in place for hydropower cybersecurity	Periodic funding opportunities are awarded to develop OT-specific cybersecurity tools easily adoptable by hydropower, A periodic process is established for demonstrating and vetting technologies and approaches,
Long Term (7-10 Years)			
Operators have access to cyber-threat information that conveys the applicability and urgency of cyber threats to hydropower OT systems, and that includes detailed and realistically actionable mitigations implementable in OT systems. Plant operators have trusted conduits by which to share their knowledge and experiences peer-to-peer and facility-to-sector.	Operators have a curated single-sitting resource that enables them to identify their facility type, steps to cybersecure it, and materials for routine staff cybersecurity training and behavioral enforcement of good cyber hygiene, which is protected from misuse by threat actors.	Hydropower facility operators have access to curated cybersecurity awareness curricula consumable by all facility staff, including initial training and subsequent knowledge reinforcement exercises. Students are aware of hydropower as a desirable career choice for many fields, including cybersecurity. Pipelines are in place at vocational schools and colleges. Students from nontraditional backgrounds can see themselves in careers as hydropower professionals.	Operators have devices and tools they specifically need as a direct result of R&D investments and the technology transfer pipeline. Existing candidate technologies are tested in volunteer facilities or representative test beds and results are communicated, enabling facility owners to make wise choices and enabling vendors to modify and improve offerings specifically benefiting hydropower facilities.
End State (2031)			
Operators have cyber-threat information about the applicability and urgency of cyber threats to hydropower OT systems, which includes mitigations implementable in OT systems. Operators have trusted conduits by which to share knowledge peer-to-peer and facility-to-sector.	Operators have a curated single-sitting resource enabling them to identify their facility type, steps to cybersecure it, and materials for routine staff cybersecurity training and behavioral enforcement of good cyber hygiene.	Students are educated about hydropower cybersecurity. Students are offered a clear path into hydropower cybersecurity careers. Curated cybersecurity curricula are available to all staff.	Operators have devices and tools they need as a direct result of R&D investments and an effective, repeatable technology transfer pipeline.

3.3.1 Goal: Foster Actionable Information Sharing

Operators have cyber-threat information about the applicability and urgency of cyber threats to hydropower OT systems, which includes mitigations implementable in OT systems.

Operators have trusted conduits by which to share knowledge peer-to-peer and facility-to-sector

3.3.1.1 Challenges

These challenges are described in depth in Section 2.6.1.1 Bi-directional Cyber Risk Information Sharing, in Section 2.6.1.4, Cyber Assistance: Threat Advisories and OT Systems, and in Section 3.1.1, Foster Actionable Information Sharing.

There is a lack of efficient means for connecting public threat advisories to a facility's operational devices, and a failure of threat advisories to be automatically ingestible by facilities' asset management software, which could then alert facility operators.

There is a lack of a single asset management software solution that does everything facilities need; facilities report having more than one but even then must maintain spreadsheets, requiring considerable staff time to use and keep updated.

Publicly available threat advisories give poor indications of whether a threat is serious enough to require facilities to schedule emergency downtime to take equipment out of service for emergency patching.

Advisories lack mitigation advice for ICS environments; simply advising to "patch now" is easily implemented by IT network administrators, but fails to take into account facilities' requirement to first test changes for operational consequences and human safety and then schedule downtime. Interim mitigation alternatives should be included in threat advisories for equipment expected to reside in ICS environments.

Peer-to-peer and facility-to-sector information sharing are both challenging due to the plethora of communications conduits and the haphazard nature of one-on-one encounters via which knowledge is shared. Facility owners currently have poor means to consistently associate their plant type with others requiring similar protections. If such an association could be made, there is currently no community of practice that supports the planning and implementation of a program to secure their type of facility.

I some cases a security clearance is required in order to learn about the existence of a threat. Other times a clearance is needed to obtain sufficiently meaningful details to enable putting in place effective mitigations. Creating a means for hydropower operators to receive security clearances is seen as a way to correct this problem.

3.3.1.2 Priorities

Priorities summarized here are viewed through the lens of having foreknowledge of emerging threats, the ease of knowing how to quickly reposition in response, and the resulting lack of successful cyberattacks. Additional guidance that helps operators understand the applicability and severity of threats to hydropower facilities needs to focus on the following:

- Helping existing threat intelligence become more ICS-friendly by including ICS-specific severity scores and workaround mitigation steps pending facilities' maintenance outage for patching.
- Monitoring classified threat intelligence and preparing curated summaries of declassified versions deemed important and requiring a response in smaller hydropower facilities.
- Billeting a group of hydropower industry professionals with security clearances, thereby enabling hydropower staff themselves to take on the intelligence tasks above for their own industry.

Table 3.4. Goal: Foster Actionable Information Sharing

Goal		
Foster Actionable Information Sharing		
Challenges		
• Threat advisories are not correlated with a facility's operational devices. • Threat advisories are not easily actionable by OT system operators. • Peer-to-peer information sharing is primarily ad hoc. • Facility-to-sector information sharing paths are not well developed.		
Milestones		
Near Term	**Mid-Term**	**Long Term**
• OT device advisories include information about the seriousness based on distance from the IT/OT border, whether vulnerability warrants an unplanned outage, and reasonable (for OT) workarounds if updates/patches can wait for scheduled outage.	• Owners/operators are enabled to use OT-specific threat advisory steps. • Operators are aware of peer-to-peer information sharing conduits and use them.	• Operators have access to cyber-threat information that conveys the applicability and urgency of cyber threats to hydropower OT systems, and that includes detailed and realistically actionable mitigations implementable in OT systems. • Plant operators have trusted conduits by which to share their knowledge and experiences peer-to-peer and facility-to-sector.
Selected Priorities		
Policy • Threat advisories concerning OT devices contain information specifically addressing how OT owners/operators must implement workarounds and schedule maintenance advisories **Process** • Create conduits, environment, and culture encouraging peer-to-peer information sharing. • Create conduits, environment, and culture encouraging facility-to-sector information sharing.		

3.3.2 Goal: Develop Cybersecurity Guidance Tailored to Common Plant Types

Operators have a curated single-sitting resource enabling them to identify their facility type, steps to cybersecure it, and materials for routine staff cybersecurity training and behavioral enforcement of good cyber hygiene.

3.3.2.1 Challenges

These challenges are described in depth in Section 3.1.2 Develop Guidance Tailored to Common Plant Types.

Facility operators struggle to allocate the resources needed to improve their cybersecurity maturity. Hydropower facilities are often tailored to the physiography of a site, the available water and storage, and an array of other purposes such as recreation and water supply. That approach results in facilities, equipment, and operations that are rarely duplicated. Ham et al.

(2021) found that plants could be grouped into nine types, based on their cyber-physical configurations. Hydropower operators would benefit from being able to identify their plant's type, such that they could benefit from shared lessons learned. Those type designations could also form the framework within which cybersecurity resources could be organized. For example, tailored sets of training could be identified from commercial or community offerings. Guidance on the steps required to improve the security posture of each type of plant would also be a time-saver for staff.

3.3.2.2 Priorities

To provide cybersecurity resources better suited to a plant, it is necessary to organize plants into types that are relevant to their risks and mitigation options. To accomplish this, operators need a simple way to identify their type of plant. Resources need to be curated and made available for each plant type to make time spent on cybersecurity efficient and effective. Rubrics and guidance need to be securely located so that only the appropriate individuals have access to them, and the information needs to be updated and maintained to remain relevant.

Table 3.5. Goal: Develop Guidance Tailored to Common Plant Types

<table>
<tr><th colspan="3">Goal</th></tr>
<tr><td colspan="3"><b>Develop Guidance Tailored to Common Plant Types</b></td></tr>
<tr><th colspan="3">Challenges</th></tr>
<tr><td colspan="3">• Facility operators have no single site enabling identification of their facility type.
• Facility operators cannot easily identify resources and a checklist enabling them to implement a plan to secure the cyber assets common to their facility type.</td></tr>
<tr><th colspan="3">Milestones</th></tr>
<tr><th>Near Term</th><th>Mid-Term</th><th>Long Term</th></tr>
<tr><td>• Facility typologies are identified and checklists to secure each are written, and resources identified and listed.</td><td>• Typologies and resources are permanently housed at a location that is accessible by operators secure from threat actors who might misuse such information.</td><td>• Operators have a curated single-sitting resource that enables them to identify their facility type, steps to cybersecure it, and materials for routine staff cybersecurity training and behavioral enforcement of good cyber hygiene, and that is protected from misuse by threat actors.</td></tr>
<tr><th colspan="3">Selected Priorities</th></tr>
<tr><td colspan="3"><b>Process</b>
• Facility cyber-physical types can be identified using a common tool.
• Resources and checklists can be chosen for each typology.

<b>Technology</b>
• Rubrics and associated guidance are securely located and maintained.</td></tr>
</table>

3.3.3 Goal: Grow Workforce Development and Cybersecurity Training

Students are educated about hydropower cybersecurity.

Students are offered a clear path into hydropower cybersecurity careers.

Curated cybersecurity curricula are available to all staff.

3.3.3.1 Challenges

These challenges are described in depth in Section 3.1.3. Grow Workforce Development and Cybersecurity Training.

Hydropower staff is aging, young vocational and professional workers are largely unaware of the large array of hydropower career paths available to them. Reaching nontraditional workers from diverse backgrounds requires special focus and effort.

Competition for recruiting cybersecurity talent is acute. Barriers to hiring cybersecurity professionals must be understood and overcome.

Right-sized, affordable, and easily accessed cybersecurity training, knowledge reinforcement, and ongoing awareness are not widely available for operators wishing to provide them to staff in group settings or on-demand.

3.3.3.2 Priorities

To ensure a hydropower workforce of sufficient size and which has the right skills, outreach programs and clear pathways to entering the hydropower workforce must be in place. Right-sized cybersecurity training and ongoing awareness programs that are within facilities' budgetary constraints must be available and not burdensome to locate and implement.

Table 3.6. Grow Workforce Development and Cybersecurity Training

<table>
<tr><th colspan="3">Goal</th></tr>
<tr><td colspan="3"><b>Grow Workforce Development and Cybersecurity Training</b></td></tr>
<tr><th colspan="3">Challenges</th></tr>
<tr><td colspan="3">• Right-sized, affordable, and easily accessed cybersecurity training, knowledge reinforcement, and ongoing awareness are not widely available for groups or on-demand.
• Hydropower staff is aging; young vocational and professional workers are unaware of the large array of careers available to them.
• Competition for recruiting cybersecurity talent is acute.
• Awareness of hydropower career paths is limited among some groups; reaching nontraditional workers from diverse backgrounds requires special focus and effort.</td></tr>
<tr><th colspan="3">Milestones</th></tr>
<tr><th>Near Term</th><th>Mid-Term</th><th>Long Term</th></tr>
<tr><td>• Curated collections of cybersecurity training resources are binned according to cybersecurity roles and responsibilities.</td><td>• Right-sized, role-based, affordable cybersecurity training resources are being used effectively.</td><td>• Hydropower facility operators have access to curated cybersecurity awareness curricula consumable by all facility</td></tr>
</table>

• Programs to develop and recruit talent to hydropower positions are initiated. • Programs to raise general awareness of hydropower are initiated.	• Talent pipelines are in place for hydropower in general and specifically for hydropower cybersecurity.	staff, including initial training and subsequent knowledge reinforcement exercises. • Students are aware of hydropower as a desirable career choice for many fields, including cybersecurity. • Pipelines are in place at vocational schools and colleges. • Students from nontraditional backgrounds can see themselves in careers as hydropower professionals.
Selected Priorities		
Policy • Establish role-based cybersecurity training that is standardized for all staff. **People** • Establish well-defined cybersecurity roles and responsibilities that are identified and assigned. • Develop a pipeline that recruits talent from all sectors of society to hydropower cybersecurity careers. • Develop cooperative hydropower STEM outreach opportunities and internship pathways to recruit cyber talent. **Process** • Curate training resources. • Match training to needs. • Provide ongoing cybersecurity training across the organization. • Define and standardize organizational cybersecurity policies and procedures for all staff. **Technology** • Deliver training effectively.		

3.3.4 Goal: Develop and Demonstrate Technologies

Operators have devices and tools they need as a direct result of R&D investments and an effective, repeatable technology transfer pipeline.

3.3.4.1 Challenges

WPTO develops advanced technologies to address many hydropower needs. For cybersecurity, technologies are needed to ease the burden of navigating cybersecurity information that is voluminous but not focused on the types of equipment and protocols that control hydropower operations. Developing technologies that facilitate mitigating vulnerabilities would increase the effectiveness of cybersecurity efforts while reducing their cost. WPTO R&D investments could be directed toward developing or adapting tools to provide that functionality for hydropower operators.

While sources of information about cybersecurity vulnerabilities are now commonplace, converting the information to practice can be complex. Operators struggle to automate asset management, to better understand the equipment and versions of firmware or software that might be the subject of a vulnerability. Matching known vulnerabilities to the set of on-site equipment is not always straightforward. If these information gathering tasks could become more automated, fewer staff hours would be required to accomplish the fixes that improve security.

Anecdotal accounts from one-on-one interviews with operators reveal a substantial gap in salaries cybersecurity professionals command versus what hydropower is accustomed to or able to afford. Solutions must be found, including development of new technologies or ways of supplying cybersecurity assistance.

Needs in the dam sector's sister sector, the water and wastewater sector, are similar to those of hydropower: water utilities' top four most-asked-for requests for assistance are training and education specific to the water sector; technical assistance, assessments, and tools; (usable) cybersecurity threat information; and federal loans and grants (to help pay for cybersecurity education, training, and tools).

Hydropower facilities may be reluctant to adopt new advances in cybersecurity technology until they are proven to function well in the ICS and OT environments. WPTO could accelerate the evaluation and adoption of promising cybersecurity technologies by sponsoring operational tests of those technologies in a hydropower environment. This testing could be accomplished in volunteer facilities or representative test beds. Communicating test results to facility operators would enable them to make wise choices and enable vendors to modify and improve offerings in ways that benefit hydropower facilities.

Hydropower operators take a conservative approach to adopting new tools and approaches. When a promising tool or approach originates in another sector of industry, operators may delay adoption until it is proven to work in a hydropower situation. Tools that provide the appropriate amount of visibility and control over IT/OT assets could provide significant benefits, so it would be helpful if they could be identified, evaluated, and adopted more quickly. To accomplish that, industry-standard technologies need to be vetted for use with non-standard OT communication protocols in a hydropower environment using established procedures that address concerns that delay adoption.

3.3.4.2 Priorities

To improve the effectiveness of cybersecurity efforts in hydropower, it is necessary to first identify the needs that technology could address. With that information in hand, it would be possible to develop funding opportunities that foster the innovation necessary to create impactful new technologies. A forward-looking perspective would ensure that development addresses trends such as the convergence of IT and OT systems to achieve operational efficiency, but that in turn pose new risks in need of new mitigations.

To improve the rate of adoption of advanced cybersecurity tools in hydropower, standards need to be developed and adopted for vetting technologies. The process for vetting technologies needs to result in communicating the capabilities and limitations of that technology. With reliable information about the benefits these technologies can provide, adoption rates and timelines should improve.

Table 3.7. Goal: Develop and Demonstrate Technologies

<table>
<tr><th colspan="3">Goal</th></tr>
<tr><td colspan="3"><b>Develop and Demonstrate Technologies</b></td></tr>
<tr><th colspan="3">Challenges</th></tr>
<tr><td colspan="3">• Asset management capabilities are incomplete or inadequate.
• Vulnerabilities are difficult to match with equipment on-site.
• Automated tools are needed to compensate for limited pool of cybersecurity practitioners.
• A recurring process to discern the community’s year-by-year cybersecurity technology needs is wanting.
• Operators may not be aware of useful tools and approaches developed in other sectors.
• Tools that can provide the appropriate amount of visibility and control over IT/OT assets are lacking.
• Industry-standard technologies need to be vetted for use with non-standard OT communication protocols.</td></tr>
<tr><th colspan="3">Milestones</th></tr>
<tr><th>Near Term</th><th>Mid-Term</th><th>Long Term</th></tr>
<tr><td>• A process is in place to identify OT-specific cybersecurity technology gaps.
• A plan to periodically fund R&D for identified cybersecurity technologies is initiated.
• Promising technologies and approaches that have yet to penetrate the hydropower industry community of practices are identified.</td><td>• Periodic funding opportunities are awarded to develop OT-specific cybersecurity tools easily adoptable by hydropower.
• A periodic process is established for demonstrating and vetting technologies and approaches.</td><td>• Operators have devices and tools they specifically need as a direct result of R&D investments and the technology transfer pipeline.
• Technologies are tested in volunteer facilities or representative test beds and results are communicated, enabling facility owners to make wise choices and enabling vendors to modify and improve offerings specifically benefiting hydropower facilities.</td></tr>
<tr><th colspan="3">Selected Priorities</th></tr>
<tr><td colspan="3"><b>Policy</b>
• Identify and adopt standards and requirements for vetting technologies.
<b>Process</b>
• Develop funding opportunities to address evolving needs for OT cybersecurity.
• Improve processes for vetting technologies prior to their deployment.
• Communicate the technical requirements to hydropower owners and vendors.
<b>Technology</b>
• Identify technology needs for OT cybersecurity.
• Establish IT-OT convergence that improves operational efficiency and reliability.
• Demonstrate promising cybersecurity technologies to improve adoption rates and timelines.</td></tr>
</table>

4.0 Bibliography

[1] ORNL database of Existing Hydropower Assets (https://hydrosource.ornl.gov/dataset/existing-hydropower-assets-eha-2020) was used to develop Figure 2.1 and Figure 2.2.

[2] Ham, KD, C Eppinger, D Thorsen, C Powell, P Boyd, A Somani, M Ingram, V Koritarov. 2021. “Hydropower Cyber-Physical Configurations (DRAFT): A typology for understanding the fleet of hydropower plants.” Report to the Water Power Technologies Office by Pacific Northwest National Laboratory. PNNL-31483. Richland, WA. Figure 2.3 is taken from this report with permission.

[3] The VERIS community database was used to develop Figure 2.4, http://veriscommunity.net/vcdb.html

[4] “Trends in Overall Cybersecurity Breaches Over Previous 6 Years.” Verizon, Verizon Data Breach Investigations Report, 14 Sept 2020, https://www.verizon.com/business/resources/reports/dbir/

[5] ENISA, https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends

[6] Miller, T. et al. “Looking back to look forward: Lessons learnt from cyberattacks on Industrial Control Systems.” Journal of Critical Infrastructure Protection, https://doi.org/10.1016/j.ijcip.2021.100464

[7] The following sources were used to construct the cyber-attack timeline effecting ICS shown in Figure 2.7:

— “Attacks on Industrial Control Systems.”, International Journal of Critical Infrastructure Protection Volume 35, December 2021, 100464

— “Worldwide Attacks Against Dams: A Historical Threat Resource for Owners and Operators.” DHS HSIN-CS (registered users only), alternately from Association of State Dam Safety Officials (ASDSO) https://damfailures.org/wp-content/uploads/2019/04/Worldwide-Attacks-Against-Dams.pdf

— Abrams, M. et al. “Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia.” https://www.mitre.org/sites/default/files/pdf/08_1145.pdf

— Slay, J. et al. “Lessons Learned from The Maroochy Water Breach.” Critical Infrastructure Protection, Post-Proceedings of the First Annual IFIP Working Group, March 19-21, 2007

— MITRE. 2017b. “BlackEnergy.” Modified June 2019. Accessed January 22, 2020 at https://attack.mitre.org/software/S0089/

— NJCCIC. 2017. “Stuxnet.” New Jersey Cybersecurity and Communications Integration Cell. Accessed January 22, 2020 at https://www.cyber.nj.gov/threat-profiles/ics-malware-variants/stuxnet.

— Zetter, K. “Countdown to Zero Day.” https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ (book excerpt)

- Kushner, D. “The Real Story of Stuxnet”, IEEESpectrum, 26 Feb. 2013, https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

- Langner R. 2013. “To Kill a Centrifuge: A Technical Analysis of What Stuxnet’s Creators Tried to Achieve.” The Langner Group. Accessed January 22, 2020 at https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf .

- NJCCIC. 2017. “Stuxnet.” New Jersey Cybersecurity and Communications Integration Cell. Accessed January 22, 2020 at https://www.cyber.nj.gov/threat-profiles/ics-malware-variants/stuxnet

- F-Secure Labs, “BLACKENERGY & QUEDAGH The convergence of crimeware and APT attacks.” Security Response Malware Analysis Whitepaper, Oct. 2019, https://blog-assets.f-secure.com/wp-content/uploads/2019/10/15163408/BlackEnergy_Quedagh.pdf

- Department of Justice Office of Public Affairs, “Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector.” 24 March, 2016, https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged

- NJCCIC. 2017. “Havex.” New Jersey Cybersecurity and Communications Integration Cell. Accessed January 22, 2020 at https://www.cyber.nj.gov/threat-profiles/ics-malware-variants/havex

- ICS-CERT. 2014a (rev 2018). “ICS Focused Malware,” ICS Advisory, ICSA-14-178-01. Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security. Accessed January 22, 2020 at https://www.us-cert.gov/ics/advisories/ICSA-14-178-01

- ICS-CERT. 2014b (rev 2018). “ICS Focused Malware,” ICS Advisory, ICSA-14-178-02A (update to ICS-CERT 2014a). Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security. Accessed January 22, 2020 at https://www.us-cert.gov/ics/alerts/ICS-ALERT-14-176-02A .

- “Bericht zur Lage der IT-Sicherheit in Deutschland 2014.” 15 Dec. 2014, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile%20

- Lee, R.M. et al. “ICS CPPE Case Study 2 German Steelworks Facility.” 30 Dec. 2014

- Oueslati, N.E. et al. “Comparative Study of the Common Cyber-physical Attacks in Industry 4.0.”, *2019 International Conference on Internet of Things, Embedded Systems and Communications (IINTEC)* , 20-22 Dec. 2019, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9112097&tag=1

- ICS Alert (IR-ALERT-H-16-056-01) Cyber-Attack Against Ukrainian Critical Infrastructure, Released: 25 Feb. 2016 | Revised: 20 Jul. 2021, https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

— “Half of Ivano-Frankivsk Region Was De-Energized Due to Hacker Attack.” TCN 24 Dec. 2015, http://ru.tsn.ua/ukrayina/iz-za-hakerskoy-ataki-obestochilo-polovinu-ivano-frankovskoy-oblasti-550406.html

— “Analysis of the Cyber Attack on theUkrainian Power Grid Defense Use Case.” 18 Mar. 2016, available from multiple sources https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

— Lacy, E. “Safer? BWL Loses 13 IT Employees After Cyberattack.” 19 May. 2017, https://www.lansingstatejournal.com/story/news/local/2017/05/19/bwl-cyberattack-employees/327299001/

— Chirgwin, R. “Michigan electricity utility downed by ransomware attack.” 3 May 2016, https://www.databreaches.net/michigan-electricity-utility-downed-by-ransomware-attack/

— Industrial Control Systems: The list provided below is meant to provide an overview of the most prevalent industrial control system variants currently impacting US victims. https://www.cyber.nj.gov/threat-center/threat-profiles/industrial-control-system-variants/

— Threat Activity Group: Electrum. https://www.dragos.com/threat/electrum/

— Slowik, J. “CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack.” 15 Aug. 2019, https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf?hsCtaTracking=aa9179e5-48b0-464b-9b78-ffd6242fb635%7C30d0dd95-4a2b-4045-a7cc-c6bfa1be5e2d

— Greenberg, A. “'Crash Override': The Malware That Took Down a Power Grid.” Wired, 6 Dec. 2017, https://www.wired.com/story/crash-override-malware/

— “Found: “Crash Override” malware that triggered Ukrainian power outage.” ARSTechnica, 12 Jun. 2017, https://arstechnica.com/security/2017/06/crash-override-malware-may-sabotage-electric-grids-but-its-no-stuxnet/

— “ICS-CERT Releases WannaCry Fact Sheet.” Released 17 May 2017, Revised 9 Jun. 2019, https://us-cert.cisa.gov/ncas/current-activity/2017/05/17/ICS-CERT-Releases-WannaCry-Fact-Sheet

— “Alert (TA17-132A) Indicators Associated With WannaCry Ransomware.” Released 12 May 2017, Revised 7 Jun. 2018, https://us-cert.cisa.gov/ncas/alerts/TA17-132A

— “WannaCry.” NJCCIC Threat Profile, 13 May 2017, https://www.cyber.nj.gov/threat-center/threat-profiles/ransomware-variants/wannacry

— “What is WannaCry Ransomware Attack?” Fortinet https://www.fortinet.com/resources/cyberglossary/wannacry-ransomeware-attack

— Katz, J. "DOJ charges three in WannaCry attacks, attempts to steal $1.3B" Federal Computer Week, 17 Feb. 2021, https://fcw.com/articles/2021/02/17/doj-dprk-wannacry-indict.aspx

— Threat Activity Group: Xenotime. https://www.dragos.com/threat/xenotime/

- MITRE. 2019. “TEMP.Veles.” Created April 16, 2019, Updated April 29, 2019. Accessed January 22, 2020 at https://attack.mitre.org/groups/G0088/

- MITRE. ND. “Groups.” Accessed January 22, 2020 at https://attack.mitre.org/groups/

- Bing, C. “Trisis has mistakenly been released on the open internet." Cyberscoop, 16 Jan. 2018, https://www.cyberscoop.com/trisis-virus-total-schneider-electric/

- "A Cyberattack Hobbles Atlanta, and Security Experts Shudder." New York Times (paid content), https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html

- Kearney, L. "Atlanta takes down water department website two weeks after cyber attack." Reuters, 5 Apr. 2018 https://www.reuters.com/article/us-usa-cyber-atlanta-water/atlanta-takes-down-water-department-website-two-weeks-after-cyber-attack-idUSKCN1HC2WB

- Emergency Directive 21-01 - Mitigate SolarWinds Orion Code Compromise, Released 13 Dec. 2020, Revised 15 Apr. 2021, https://cyber.dhs.gov/ed/21-01/#supplemental-guidance

- "Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor." FireEye, 13 Dec. 2020, https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

- MS-ISAC ADVISORY NUMBER:2021-021, Multiple Vulnerabilities in SolarWinds Orion and ServU-FTP Could Allow for Remote Code Execution, 4 Feb. 2021 https://www.cisecurity.org/solarwinds/

- SEC Filing: https://d18rn0p25nwr6d.cloudfront.net/CIK-0001739942/57108215-4458-4dd8-a5bf-55bd5e34d451.pdf

- "Brazil's Eletrobras says nuclear unit hit with cyberattack." Reuters, 4 Feb. 2021 https://www.reuters.com/article/us-eletrobras-cyber/brazils-eletrobras-says-nuclear-unit-hit-with-cyberattack-idUSKBN2A41JN

- Weber, D. "ICS Hot Take: Oldsmar, FL Water Facility Event." SANS, 25 Feb. 2021 https://ics-community.sans.org/media/download/36f72g/Water_Facility_Event_V1.pptx

- https://ics-community.sans.org/t/p8hz54d/water-facility-event

- Impelli, M. "Hackers Infiltrate Florida Water Supply, Attempt to Raise Chemical Levels to Dangerous Amounts." Newsweek, 8 Feb. 2021, https://www.newsweek.com/hackers-infiltrate-florida-water-supply-attempt-raise-chemical-levels-dangerous-amounts-1567716

- Greenberg, A. "A Hacker Tried to Poison a Florida City's Water Supply, Officials Say." Wired, 8 Feb. 2021 https://www.wired.com/story/oldsmar-florida-water-utility-hack/

- "Cybercriminals are interested in your SCADA systems." Intel471, 12 Feb. 2021 https://intel471.com/blog/scada-oldsmar-florida-water-treatment-plant-hack/

This Page Intentionally Blank

Pacific Northwest
National Laboratory

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99354
1-888-375-PNNL (7665)

www.pnnl.gov

https://www.energy.gov/eere/water/water-power-technologies-office

Pacific Northwest National Laboratory

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99354
1-888-375-PNNL (7665)

www.pnnl.gov