Cybersecurity

THE ENVIRONMENT, ENERGY, AND INFRASTRUCTURE (EEI)

Photo Credit: USAID Energy

Why Does Cybersecurity Matter for EEI?

The environment, energy, and infrastructure (EEI) sectors increasingly use digital technologies to capture data, improve and expand service delivery, and optimize system performance. However, as industrial systems continue growing their digital footprint while incorporating emerging technologies, they are increasingly vulnerable to cyber attacks. EEI systems are attractive targets for state and non-state cyber attackers precisely because they can cause severe damage. A 2019 Siemens/Ponemon Institute survey of over 1,700 gas, wind, water, and solar utility professionals found that more than half reported "at least one attack involving a loss of private information or an outage" in their operational technologies environment in the past 12 months. This statistic is particularly alarming because these utilities often constitute critical infrastructure—assets vital to the security, economic welfare, and the public health and safety of a state.

What is cybersecurity and why does it matter for international development?

As noted in USAID's Cybersecurity Primer, USAID defines cybersecurity as "*the activity or process, ability or capability, or state whereby information and communications systems that support or affect development outcomes, and the information contained therein, are protected from and/or defended against damage, unauthorized use or modification, or exploitation.*" As USAID partner countries further their digital transformation and continue to adopt new digital tools and systems, cyber risks and vulnerabilities proliferate. Cybersecurity failures pose material threats to USAID partner countries and undermine partner country government legitimacy. USAID must protect its digital investments by ensuring that its digital programming addresses cyber harms and includes cybersecurity mitigation measures.

Cybersecurity trends in EEI

Cyber attacks in EEI sectors are becoming higher profile and causing more damage. The rapidly growing use of digital technologies in EEI increases the number of potential origin points for a cyber attack. In recent years, prominent cyber attacks on critical infrastructure have included breaches of power systems in Ukraine, the national airline information systems in Vietnam, a state-owned energy company in Taiwan, a major telecommunications company in Japan, and the Colonial Oil Pipeline in the

United States. The cyber attack on the Colonial Pipeline—the country's largest—forced the pipeline to shut down for several days, spiking oil prices and leaving over 10,000 gas stations without gas.

State actors are committing cyber attacks on EEI. While sophisticated cyber criminal groups do conduct some cyber attacks on EEI targets, it is more often nation-states such as Russia, North Korea, China, and Iran that are behind these attacks. Ukraine has been the victim of state-sponsored cybercrime since December 2015, when a cyber attack knocked segments of the country's energy grid offline and left 225,000 people without power. This was the world's first confirmed cyber attack on sovereign energy infrastructure, and has been attributed to a hacking group affiliated with the Russian government. In a 2019 Siemens/Ponemon Institute study, 25 percent of surveyed utilities had been subject to cyber attacks "with expertise developed by nation-state actors."

Ransomware and supply chain attacks are popular types of cyber attacks in EEI sectors. In a ransomware attack, cyber criminals block victims' access to their own data and will release it only if the victim pays a ransom. Sometimes, the criminals will also threaten to release sensitive data publicly if the ransom is not paid. In February 2022, the United States, the United Kingdom, and Australia published a Joint Cybersecurity Advisory warning of "an increase in sophisticated, high-impact ransomware incidents against critical infrastructure organizations globally." In 2021, the FBI reported 649 ransomware incidents against critical infrastructure operators in the United States. Supply chain attacks—during which hackers gain access to their target through the computer systems of third-party vendors or other suppliers—are also becoming more common in the EEI sector. According to AXA, about "50 percent of… cybersecurity exposure risk can be attributed to using multiple security vendors, equipment, and services." Arguably the most notorious supply chain cyber attack against the United States was the 2020 SolarWinds breach. Thousands of businesses, organizations, and U.S. government agencies that used Orion software (manufactured by the SolarWinds software company) were affected, including critical infrastructure entities. U.S. officials have since attributed the attack to groups affiliated with the Russian government.

USAID-NREL partnership on cybersecurity

Under a partnership that supports clean, reliable, and affordable power in USAID partner countries, USAID and the U.S. Department of Energy's National Renewable Energy Laboratory (NREL) produced a Power Sector Cybersecurity Building Blocks framework in March 2021. The framework lists the 11 building blocks—Governance; Organizational Security Policy; Risk Management; Cyber Threat Intelligence; Laws, Regulations, and Standards; Compliance; Procurement; Technical Controls; Incident Response; Cybersecurity Awareness Training; and Workforce Development—required for electric utilities to have a resilient and mature cyber posture, and provides resources and references relevant to each building block. USAID and NREL are using these building blocks to conduct assessments of all partner energy sector stakeholders. In addition, NREL uses its Distributed Energy Resource Cybersecurity Framework (DERCEF) as a tool to assess the cybersecurity posture of Distributed Energy Resource (DER) systems.

Photo Credit: Jeffrey Michael Walcott

Climate change and cybersecurity are linked in complex ways. There is growing evidence that social and economic instability stemming from climate change can lead to the proliferation of cyber threats and cyber risks. Global efforts to combat the effects of climate change can increase opportunities for cyber attacks, particularly as countries pivot to smart grids or collaborate with new market players to add solar and wind generators, electric transportation equipment, and battery storage units into their existing power grids. Some evidence suggests that those developing these new technologies are not

doing so with cybersecurity in mind. According to a 2021 survey of professionals in the Danish energy, resources, and industrials sector, more than half of respondents reported that their companies did not take cybersecurity into account before the development phase for a new digital solution. Because climate change and cybersecurity are closely linked, it is important that solutions to address one challenge also address the other.

USAID and other donors are investing in building partner country resilience against cyber attacks on critical infrastructure sectors like energy, water, and transport. In recent years, bilateral and multilateral donors like USAID and The World Bank have prioritized investments that strengthen cybersecurity for partner nations and their EEI sectors. Some donor initiatives have focused on the national policy level, working with partner governments to develop cybersecurity strategies (including for critical infrastructure) and tailored multi-stakeholder governance structures to implement these strategies. Other donors, including USAID, are working directly with electricity utilities to build a more cyber-resilient internal infrastructure and workforce in places like Ukraine, Vietnam, Pakistan, Ghana, and the Balkans. However, these initial efforts represent relatively small investments in a handful of countries. Scaling up protections for the EEI sector around the globe will require considerable investment and commitment from a wide range of donors and funders.

Photo Credit: USAID Energy

USAID-USEA partnership on cybersecurity

USAID and the United States Energy Association (USEA) have developed and published the Electricity Sector Cybersecurity and Digitalization Handbook, which supports power sector utilities by detailing the modern cybersecurity threats, vulnerabilities, and risks they face. Published in June 2021, the handbook was based on and features practical recommendations from 15 webinars in the USEA and USAID-hosted Cybersecurity and Digitalization Webinar Series:

1. Strategies for Intelligence Integration: Connections Between Digitalization and Cybersecurity
2. Building Blocks to Support Cybersecurity in the Power Sector
3. Utility Digitalization Progress and Digitalization Strategies and Roadmaps
4. Cybersecurity and Distributed Energy Resources
5. The Corporate Culture and Importance of Cyber Hygiene
6. Introduction to the Cybersecurity Capability Maturity Model (C2M2)
7. Forging a Cybersecurity Defense for Utilities
8. Cybersecurity Standards and Best Practices: US Standards
9. Cybersecurity Standards and Best Practices: Utilities and ISO/IEC 27001 ISMS 2005/2013
10. Utility Data Protection Policies and Practices
11. The Importance of Supply Chain Security
12. Industrial Control System (ICS) and SCADA: Risks and Solutions
13. The Relationship Between Regulators and Power Utilities: Evaluating the Prudency of Cybersecurity Investments
14. Key Elements of Trusted Collaboration and Information Sharing
15. Communication Strategies for Before, During, and After Cyber Attacks