Cybersecurity and public works

An overview of cybersecurity challenges for public works, cyberattack impacts, and potential solutions

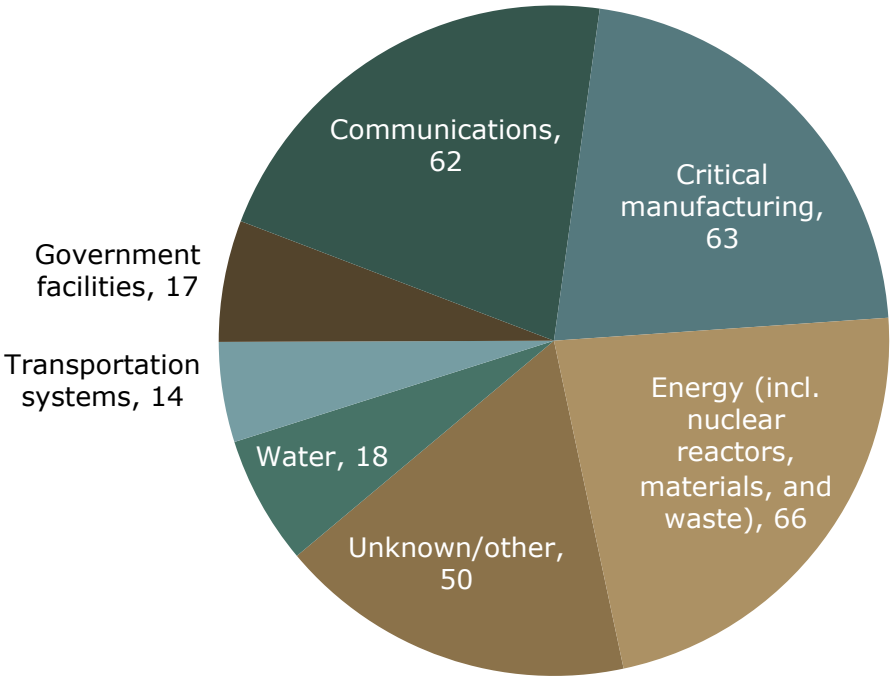
April 30, 2020

Roadmap

- Background on cybersecurity concerns for public works
- Impact of cyberattacks on public works
- Challenges and solutions for protecting public works from cyber threats
- Outlook for cybersecurity and critical infrastructure

Cyberattacks affect many public works projects

Reported cyber incidents by critical infrastructure sectors, 2016



Technology is involved in the construction, operation, and maintenance of infrastructure, as highlighted by drinking water systems and smart cities

- Databases can store information gathered by street or pipeline sensors
- Supervisory control and data acquisition (SCADA) systems monitor and operate drinking water systems
- Control systems turn processes such as water flow or lighting on and off

Sources: Energy.gov, HS Today, Webopedia, Tech Republic.

Roadmap

- Background on cybersecurity concerns for public works
- Impact of cyberattacks on public works
- Challenges and solutions for protecting public works from cyber threats
- Outlook for cybersecurity and critical infrastructure

Cybersecurity intrusions have come from multiple sources

Recent cybersecurity intrusions on the U.S. electric grid:

March 2016

- The Bowman Avenue hydroelectric dam in suburban New York was targeted by seven Iranian hackers on behalf of Iran's Revolutionary Guard Corps (IRGC)
- The IRGC also made successful breaches at 46 U.S. financial institutions
- It is believed that the New York dam was targeted accidentally, and that the IRGC had confused it with the Arthur R. Bowman dam in Oregon, which is much larger

October 2017

- North Korea is believed to be responsible for several October 2017 cyber-intrusions at several U.S. power companies
- There was no evidence that the hackings were successful in their attempts

March 2018

- The U.S. Computer Emergency Readiness Team issued an alert to several critical energy and infrastructure companies regarding a potential cyberattack
- The Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) concluded that there was a multi-attempt intrusion campaign by the Russian Government

Sources: Congressional Research Service, New York Times, NBC News, TIME, NPR.

Spotlight: cyberattacks on public utilities in 2019

Even small utilities are targets of cyberattacks

Overview

- In August of 2019, researchers at a Silicon Valley cybersecurity company reported that over a dozen utilities had been targeted in a series of cyberattacks using a malware called “Lookback”
- Some of the utilities are near dams, locks, and other critical infrastructure
- Most were relatively small utilities
- Hackers used phishing emails to attempt to breach utilities’ computer systems

Impact on large utilities

- None of the utilities publicly identified as impacted in the Lookback attacks are in the top ten largest U.S. utilities by customer count

Impact on small utilities

- Historically, municipally-owned utilities serving a relatively small number of customers were thought to be less susceptible to attack
- The 2019 wave of attacks demonstrated that small utilities are hacking targets
- Small utilities often lack large budgets for security

Sources: GovTech, Wall Street Journal, Energy Information Administration.

Roadmap

- Background on cybersecurity concerns for public works
- Impact of cyberattacks on public works
- Challenges and solutions for protecting public works from cyber threats
- Outlook for cybersecurity and critical infrastructure

Challenges of protecting public works systems from cyber threats

Technology, management, and training pose key challenges

Inconsistency in the role of technology across public works projects

- Variability in the ways systems are connected to networks can present both hardware and software barriers
- In some systems, any one computer can serve as a potential failure point
- In some systems, networks connecting critical infrastructure can fail

Inconsistency in who manages public works projects

- Public and private sector employees both often have a stake in public works projects
- Permitting and utility locating processes can vary across communities

Inconsistency in training opportunities

- Some utilities lack the resources for information technology and security specialists to start a formal cybersecurity program
- The Environmental Protection Agency (EPA) notes that utility staff may feel that they do not have the technical capacity to improve their security, including through training

Sources: HS Today, EPA.

Solutions to protect against cybersecurity attacks

Collaboration and awareness are key

Evaluating cyber threats and vulnerabilities across public works

Collaboration between public and private sectors on cybersecurity initiatives

Spreading awareness about the importance of cybersecurity

Conducting regular cybersecurity trainings for staff and contractors

Sources: HS Today, EPA.

Slide last updated on: April 29, 2020

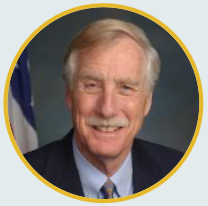
Roadmap

- Background on cybersecurity concerns for public works
- Impact of cyberattacks on public works
- Challenges and solutions for protecting public works from cyber threats
- Outlook for cybersecurity and critical infrastructure

Spotlight: S. 174 – Securing Energy Infrastructure Act

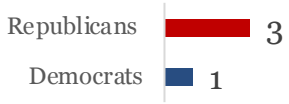
Bill at a glance

Introduced 1/17/19 → Passed Senate → Passed House → To president → Signed into law



Sen. Angus King (I-ME)
Bill sponsor

Co-sponsors: 4



Bill overview

- Senators Angus King (I-ME) and Jim Risch (R-ID) reintroduced the Securing Energy infrastructure Act in the 116th Congress
- The bill aims to secure the U.S. energy grid against cyberattacks
- The same bill passed the 115th Senate unanimously in December 2018
- The legislation was inspired by the hacking of the Ukrainian energy grid by Russia in 2015

Status in Congress

- Introduced in the Senate and House as identical bills
- Referred to the Senate Committee on Energy and Natural Resources
- Referred to the House Science, Space, and technology subcommittee on Energy

"Securing our energy infrastructure is not an abstract policy idea, it is an immediate need to protect our grid from the real threat of malign actors. … So far, the federal government has not matched this serious threat with the necessary action. Our bipartisan bill has broad support, as evidenced by its passage in the Senate last December, and I hope the new Congress will take swift action on it so we can proactively protect our country's critical infrastructure from cyberattacks." – Sen. Angus King

Sources: U.S. Congress, Senator Angus King Press Releases.

Slide last updated on: April 29, 2020

The outlook for cybersecurity and public works depends on government and industry action

1. Critical infrastructure remains vulnerable to power disruptions

2. The scope and duration of a future cyberattack on the electric grid or on another critical infrastructure sector depends on preparedness and response plans

3. The U.S. needs government and industry partners to close identified gaps in cybersecurity preparedness and response

Sources: Energy.gov.