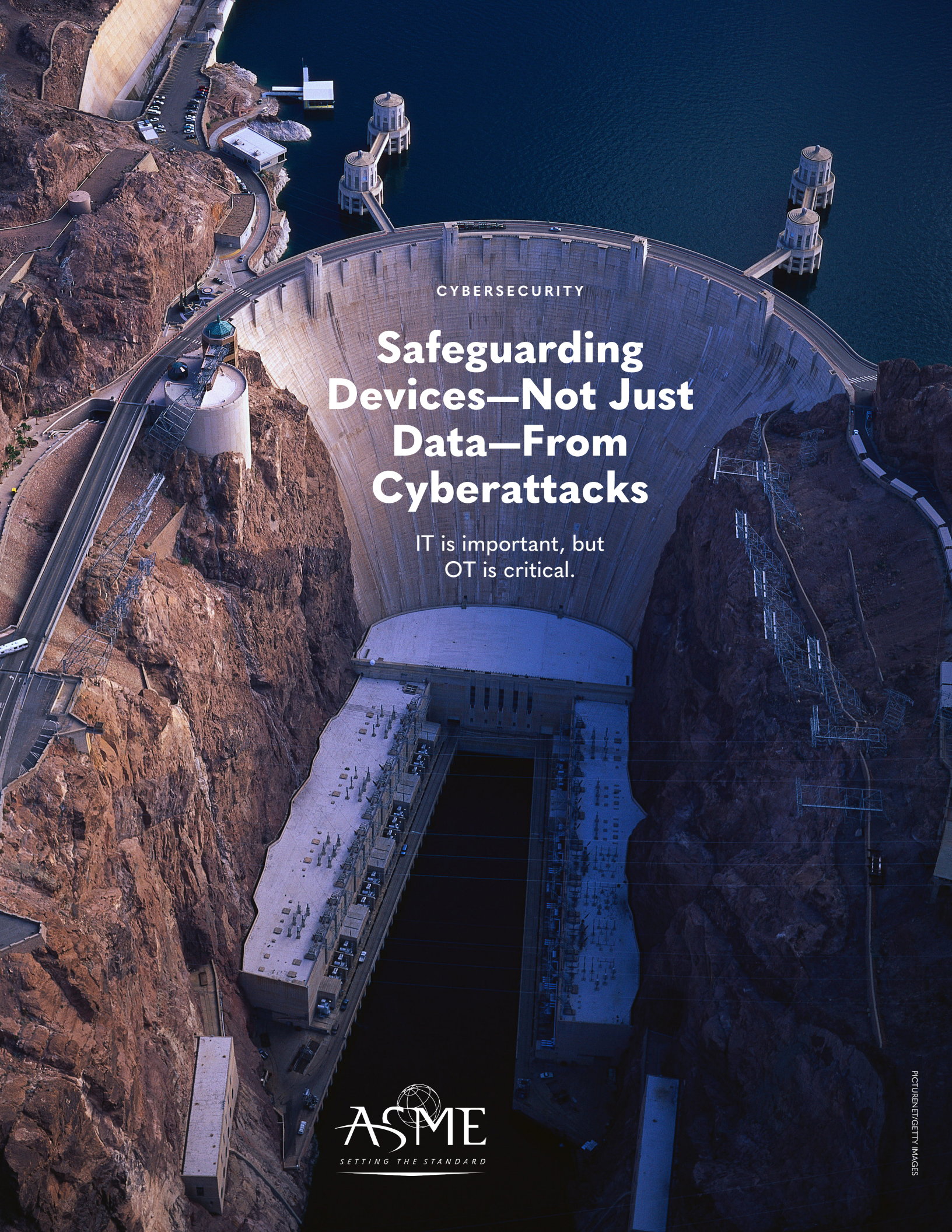


CYBERSECURITY

Safeguarding Devices—Not Just Data—From Cyberattacks

IT is important, but OT is critical.

ASME
SETTING THE STANDARD

PICTURENET/GETTY IMAGES

Speaking at the sixth annual Boston Conference on Cyber Security at Boston College in June 2022, FBI Director Christopher Wray revealed that the agency had thwarted a planned cyberattack on Boston Children's Hospital the previous summer. • As the *Boston Globe* reported, the FBI, working with the U.S. Cybersecurity and Infrastructure Security Agency, the Australian Cyber Security Centre, and the U.K's National Cyber Security Centre, discovered that "hackers associated with the Iranian government" had accessed the environmental control network in an effort to breach its data networks through its third-party HVAC system or to commandeer the facility's temperature control system.

Detected early enough to prevent any damage to the network or the hospital's data, the attack could have been an extortion attempt using ransomware. Whatever the intent, this malicious act underscored the vulnerability of both operational technology (OT) and industrial control systems (ICS)—in this case the monitors and controls of the hospital's HVAC system—to hijacking by cybercriminals and rogue nation-states.

A WIDER ATTACK SURFACE

Once, industrial equipment, assets, and processes operated in isolation and were vulnerable only to physical attack. In today's digitized world, however, barbed wire, concrete walls, checkpoints, and other traditional safeguards are only part of the infrastructure security playbook. Exponentially expanded by the network-connected and ubiquitous agglomeration of Industry 4.0 and Industrial Internet of Things (IIoT) sensors and data processing engines, the attack surface extends to environments that include manufacturing facilities, supply chains, and most alarmingly, critical infrastructure sectors.

Moving well beyond extortion and selling stolen data, sophisticated malicious actors are increasingly targeting takeovers of physical equipment for more insidious ends.

Healthcare and public health are among the 16 critical sectors classified and overseen by CISA (see sidebar, page 4). Others include dams, energy, nuclear reactors, transportation, and water and wastewater systems. All are ripe targets for government-sponsored APT (advanced persistent threat) groups such as the Iranian hackers in Boston. Moving well beyond extortion and selling stolen data, sophisticated malicious actors are increasingly targeting takeovers of physical equipment for more insidious ends, such as causing power blackouts and poisoning water systems.

The control systems and devices that monitor and regulate everything from the HMIs (Human-Machine Interfaces) and controllers embedded in ICS architecture to centrifuges, turbines, pumps, transformers, reactors, and other vital large-scale machinery demand the most vigilant and uncompromised safeguards. Yet, as many observers have pointed out, this equipment is glaringly insecure.

"Before the Stuxnet computer worm attack against Iran's uranium enrichment facility in 2010, nobody considered nation-state attacks on infrastructure," says Joseph Weiss, managing partner at Applied Control Solutions in Cupertino, California, and an international authority on cybersecurity, control systems, and system security with more than 40 years of experience



Dams (as on the cover) and water and wastewater systems (above) remain vulnerable to cyberattacks.

in the energy industry. "We were only worried about operational safety and unintentional failure modes. But as malicious and unintentional control system cyber incidents proliferate, our guard remains down."

For mechanical and other engineers, this urgent situation offers an unprecedented—and especially critical—opportunity to reexamine, reimagine, and reengineer cybersecurity solutions for the machines and infrastructure that run the world.

WAKE-UP CALLS

According to Weiss, whose experience on the forefront of ICS and cybersecurity includes leading nuclear and fossil fuels instrumentation and diagnostics along with other critical infrastructure programs at the Electric Power Research Institute in Palo Alto, California, ICS cyberattacks on critical infrastructure have been rampant for years—and continue to go largely unchallenged.

The attack surface now extends to environments that include manufacturing facilities, supply chains, and most alarmingly, critical infrastructure sectors.

"In 2000, when I helped start the control system cybersecurity program for the electric utilities," he recalls, "I started amassing a database of actual control system cyber incidents, both unintentional and malicious." Since then, he has recorded more than 11 million control system cyber incidents, which have, he says, "collectively resulted in tens of thousands of deaths and more than $90 billion in direct damage."

However, unlike the widely publicized cyberattacks on computer networks, information systems, and personal devices, the true scale of OT and ICS cyberattacks goes largely underreported. Given that, Weiss and others suggest that the incidents that do make the headlines should serve as an urgent call to action.

For example, a recent report in Dark Reading, a cybersecurity news site, described how Ukraine's computer emergency response team (CERT-UA), in collaboration with researchers from Microsoft and the Slovakian internet security firm ESET, stopped an April 2022 cyberattack on an energy company that aimed to disconnect several high-voltage substations from a section of Ukraine's electric grid.

This recalled incidents in 2015 and 2016, when the same attackers, Russia's notorious Sandworm group, struck the Ukrainian grid with its Win32/Industroyer malware, creating temporary blackouts. In a 2017 white paper, ESET described Win32/Industroyer as "a sophisticated piece of malware designed specifically to disrupt the

JUPITERIMAGES/GETTY IMAGES

working processes of industrial control systems used in electrical substations."

The highly configurable malware consists of multiple modules and tools, including a destructive data wiper component. This gives threat actors remote control of switches and circuit breakers in high-voltage substations, which they can manipulate to trigger disruptions. Noting that this incident serves as a reminder that securing human assets is equally critical, ESET added that "it seems very unlikely anyone could write and test such malware without access to the specialized equipment used in the specific, targeted industrial environment."

These incidents, of course, were hardly isolated. Consider, for example, the massive Russian cyberattack in December 2020 on Tulsa, Oklahoma-based software company SolarWinds. Going undetected for months, the breach of SolarWinds' IT performance monitoring system exposed sensitive data from thousands of client organizations—Microsoft among them—along with top branches of the U.S. government, including the Department of Homeland Security and the Treasury Department.

While SolarWinds was a major attack on IT infrastructure that ostensibly was cybersecure (IT itself is classified as a critical infrastructure sector), Weiss notes that the high rate of attacks on critical OT—and their vulnerability to attack in the first place—stems from a combination of misunderstood terminology and "cultural conflict" between the worlds of OT and IT.

FULL STEAM BEHIND

Defined as "the science of communications and automatic control systems in both machines and living things," the feedback loop principle of cybernetics informed the earliest advancements in mechanical engineering, including Scottish mechanical engineer James Watt's groundbreaking advancement of steam engine technology in the 1770s. Watt's innovative step forward forever changed the way people interface with, learn from, manage, and improve mechanics.

At the time, operators of automated machinery such as water-powered sawmills relied on their senses to regulate mechanical action. Watt's steam engine, with its revolutionary external condensing chamber, broke that mold entirely. As engineers often perilously experienced, attempting to measure and control the engine's combustion chamber temperature and boiler pressure by sight, sound, smell, and feel could go explosively wrong. The solution was the development of physical devices such as the overpressure valve, which set in motion the evolution of the industrial control systems that operators now rely on to monitor and control machines, devices, and other physical assets.

In the modern age, the word cybernetics was shortened to cyber, creating a term that Weiss claims is not only misunderstood but may be, in fact, the underlying reason why there has been a lack of significant progress in securing critical infrastructure.

"As 'cyber' became synonymous with IT and information systems," Weiss explains, "OT took a back seat in the cybersecurity context." He notes that before 9/11, engineers focused solely on reliably and safely keeping the lights on and the water flowing, but that "after 9/11, when cybersecurity became national security, all the attention went to securing IP networks and data. Cybersecurity was yanked away from every engineering organization including suppliers and end-users, and, to this day, despite mounting

Matters of National Security

Working in close partnership with the Office of Management and Budget, which is responsible for federal cybersecurity overall, the Cybersecurity and Infrastructure Security Agency (CISA) "quarterbacks the federal cybersecurity team, protecting and defending the home front."

CISA oversees 16 critical infrastructure sectors "whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." Consider the damage that could be sustained by cyberattacks on any of these sectors:

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials, and Waste
- Transportation Systems
- Water and Wastewater Systems

and increasingly consequential attacks, critical infrastructure cybersecurity is primarily concerned with information assurance—not mission assurance."

POROUS PERIMETERS

The Win32/Industroyer and SolarWinds incidents alone show how far behind IT, OT and ICS have lagged. But in a showcase example, the Israeli Water Authority demonstrated that taking action to bolster ICS cyber defenses is as achievable as it is critical.

In April 2020, a suspected Iranian group attempted to exponentially increase the level of chlorine in a facility supplying water to residential areas in central Israel by changing the system's programmable logic controllers (PLCs) and hiding the subterfuge from system detection. That June, malicious actors struck twice again, hitting water pumps and waste treatment facilities in Upper Galilee and in the regional council of Mateh Yehuda.

PLCs, which were the focal point of the Stuxnet attack, are integrated in a broad swath of industrial and infrastructure operations, including liquefied natural gas, food production, power plants, and electric facilities. As such, they are a popular and frequent target for hackers, which prompted CISA, along with the Energy Department, the National Security Agency, and the FBI, to issue an official alert in April 2022.

All three of the Israeli attacks involved vulnerable cellular routers, which allow organizations to remotely connect to their industrial systems. In a security alert, the Israeli National Cyber-Directorate urged operators of water, cellular communications, and energy infrastructure to change passwords for all their internet-connected systems or to take those systems offline until proper defensive systems could be installed.

But when the operators were slow to respond, the government issued a report stating that "Israel's water infrastructure is not ready to withstand a possible cyberattack by Iranian hackers" because "water companies in Israel have largely failed to step up digital defenses of their infrastructure." In July 2021, the Israel Water Authority hired Israeli cybersecurity firm SIGA OT Solutions to protect water utilities from ICS and OT cyberattacks on their machinery and equipment. Solutions included monitoring the electrical characteristics of process sensors to detect changes or anomalies.

"As 'cyber' became synonymous with IT and information systems, OT took a back seat in the cybersecurity context."

Though Israel may have successfully installed safeguards, other water utilities around the globe remain vulnerable to attack. In February 2021, an unknown hacker increased the levels of sodium hydroxide—the main ingredient in liquid drain cleaner—in the water treatment system of Oldsmar, Florida, just west of Tampa, by more than a hundred times. Alerted to the intrusion as the hacker accessed the system remotely, an operator immediately reduced the sodium hydroxide to normal levels and thwarted the attack.

DANGER LURKING IN A COFFEE POT

The transportation sector is another popular target of government-sponsored APT groups. Railways, for example, offer multiple attack vectors. In a recent article from the International Society of Automation Global Cybersecurity Alliance (ISAGCA) on the state of cybersecurity in the world's increasingly digitally controlled rail networks, the author identified "signaling systems, traction systems, train control systems, passenger information systems, and station infrastructure" as targets, such as happened when an Iranian cyberattack in 2020 caused significant equipment and infrastructure damage at train stations throughout Israel.

Those are not the only points of attack, however. Far less obvious, but no less vulnerable, are such seemingly innocuous IoT-connected devices as the "smart coffee pot" in the buffet car. "These are often very cheap systems, with little or no security," the author noted. "In these cases, where the signaling network can be accessed through the passenger network, the 'smart coffee pot' network access becomes an entry point for hackers."

The truth is that hackers can access virtually any smart, web-connected device at will, no matter how mundane. They are barely challenged by operational equipment and devices. In April 2022, Dutch researchers Daan Keuper and Thijs Alkemade won the annual Pwn2Own hacking championship in Miami by accessing the software that runs the world's power grids, gas pipelines, and more. The duo, whose previous triumphs at the world's largest hacking event included successfully hacking a brand-new iPhone (2012), a car (2018), and videoconferencing software and coronavirus apps (2021), described the challenge as "their easiest yet." Underscoring that point, Keuper noted that "In industrial control systems, there is still so much low-hanging fruit. The security is lagging behind badly." What all mission-critical infrastructure has in common, the author of the ISAGCA article emphasized, is "the need to implement appropriate



Steps for Thwarting Tomorrow's Threat Actors, Today

In a June 2022 article for the global news site Insider, Charles Henderson, global managing partner and head of X-Force at IBM Security, discussed how "the real-world repercussions of cyberattacks will usher in a security renaissance."

Citing the fact that "the FBI, CISA, and NSA observed ransomware incidents against 14 of the 16 U.S. critical infrastructure sectors in 2021," Henderson prescribed exacting countermeasures such as "moving to a Zero Trust model where everything and everyone is scrutinized and iteratively validated."

Stating that "no single solution" exists to counter ransomware and other cyberattacks, Henderson advocated for a comprehensive approach. "AI, analytics, and advanced detection capabilities are gaining focus, but these technologies will fall short if they are not coupled with adversary simulation, threat hunting, training, response playbooks, and reliable threat intelligence to inform these processes," he wrote.

Another key strategy is Defense in Depth (DiD). Prominent in the world of nuclear engineering, DiD employs a multi-layered approach with multiple redundancies to guard entire systems from different attack vectors. By analogy, this strategy functions like such defensives of a medieval castle as moats, drawbridges, ramparts, towers, and battlements.

The Department of Homeland Security outlines seven strategies to counter cyber intrusions into U.S. critical infrastructure systems. These include reducing the attack surface area by isolating ICS networks from untrusted networks, especially the internet; limiting and securing remote network access; and building defendable environments that "limit damage from network perimeter breaches" and "segment networks into logical enclaves and restrict host-to-host communications paths."

proactive, rather than reactive, security practices." As Israel found, changing passwords, adding two-factor authentication, and adopting other measures provide one line of defense. But, if they are to keep bad actors at bay, engineers must holistically rethink and prioritize a multi-layered, integrated approach to security that shields devices and equipment from malicious efforts to hijack and reprogram critical infrastructure networks.

OUT-RESOURCED, OUTPACED, OUTDISTANCED

How far behind are we in the effort to protect critical infrastructure from escalating cyberattacks? To find out, leading cybersecurity firm Tenable analyzed 200,000 vulnerability assessment scans over a three-month period in late 2017 and found that "with an average seven-day head start … threat actors are sprinting ahead, exploiting vulnerabilities before security teams have even left the starting blocks."

Tenable built upon this finding two years later when it partnered with the Ponemon Institute, a preeminent center for research into privacy, data protection, and information security, to look closely at the state of OT cybersecurity. Surveying more than 700 IT and IT security decisionmakers in the U.S., U.K., Germany, Australia, Mexico, and Japan from the energy and utilities, industrial and manufacturing, health and pharmaceutical, and transportation sectors, the study found that nearly all (90%) respondents had experienced at least one damaging OT or IT infrastructure security event over the preceding two years, and 62% said they had experienced two or more attacks. Half of all attacks resulted in plant or operational equipment downtime. And significantly, nearly one-quarter (23%) "were able to attribute an attack to a nation-state."

With threats and incidents proliferating, the situation is getting worse. In the 2022 edition of its annual Global Risks Report, the World Economic Forum stated that "cybersecurity threats (including against critical infrastructure) are growing and outpacing societies' ability to effectively prevent or respond to them."

CONFRONTING THE CULTURAL DIVIDE

For Weiss, bridging this chasm starts with confronting the cultural divide between OT and IT. "The grid and other critical infrastructure are in fact operable without IP networks," he notes,

THOMAS BARWICK/GETTY IMAGES

There is a "burning need for OT cybersecurity organizations to include engineers responsible for the design and operation of ICS and the processes they monitor and control."

citing the aftermath of the 2015 cyberattack on the Ukrainian power grid during which Ukrainians ran the grid manually for months. But, he cautions, "get to the devices, and you can cause the Iranian centrifuges to spin out of control." His point is that the persistent approach of securing critical infrastructure by securing the networks is "simply not working." With malicious cyberattacks against control systems occurring since the late 1990s, he wonders "how many more people will die before control system cybersecurity is treated as a systems engineering issue?"

Encouragingly, the issue is now getting the attention it demands. In May 2022, Lauren Zabierek, executive director of the Cyber Project at Harvard University's Kennedy School's Belfer Center, and Sean Plankey, former principal deputy assistant secretary in the Office of Cybersecurity, Energy Security, and Emergency Response at the Department of Energy, gave a presentation entitled, "We Must Regulate Water and Wastewater Cybersecurity—Here's How."

The discussion produced a set of "clear, actionable ways to enhance cybersecurity in the water sector" and critical infrastructure more broadly in three categories: cybersecurity legislation, continuity of economy, and steps specific to water and wastewater. Among the recommendations: "Create North American standards for OT sensors and actuators. Require engineering firms to incorporate cybersecurity into their device engineering design and require acceptance and testing."

Among the notable recommendations to "address specific regulations based on common cyberattack behaviors" were the following:

- Restricting remote access and externally accessible services
- Requiring access controls on IT and OT assets
- Immediately revoking access to outgoing employees
- Maintaining a resilient control system in which pressure and treatment functions can be manually run
- Incorporating protective technology

As these and other initiatives move forward, mechanical engineers will have their own critical role to play in securing the future.

BACK TO THE FUTURE

With operators and engineers rallying around protective strategies such as Defense-in-Depth (see sidebar, page 6), the opportunities to secure critical equipment and machinery from OT and ICS cyberattacks are as expansive as the collective attack surface itself.

Weiss suggests that finding the truest safeguards may be a matter of circling back to the past. "Returning to the early principles of cybernetics and recognizing that problems can be induced in any feedback loop, whether networked or not, offers real possibilities to reengineer and solve many control system vulnerabilities," he concludes. "That goes with the burning need for OT cybersecurity organizations to include engineers responsible for the design and operation of ICS and the processes they monitor and control in the security process. Remember, the field control system equipment keeps the lights on and the water flowing, and for mechanical engineers, I would say this is a major opportunity to make a difference not only to your career, but to civilization itself."

About the American Society of Mechanical Engineers (ASME)

Founded in 1880, ASME has a long history of helping engineers connect with colleagues and resources throughout the engineering industry. Our mission is to promote the vital role of engineers in society. ASME enables collaboration, knowledge sharing, and skill development across all engineering disciplines. Explore networking opportunities and become part of our worldwide community through an ASME membership.

FOR MORE INFORMATION, VISIT WWW.ASME.ORG