ENERGY

Energy Companies Face Growing Cyber Threats, Matrix Of Solutions

Dipka Bhambhani Senior Contributor
I distill energy policy and technology movements.

Follow

Sep 30, 2021, 08:00am EDT

Listen to article 11 minutes

Cybercrime and threats to U.S. energy companies have surged in the past year, costing millions of dollars in losses and ransoms paid, billions of dollars of investment in cybersecurity software, and executive and legislative branch intervention.

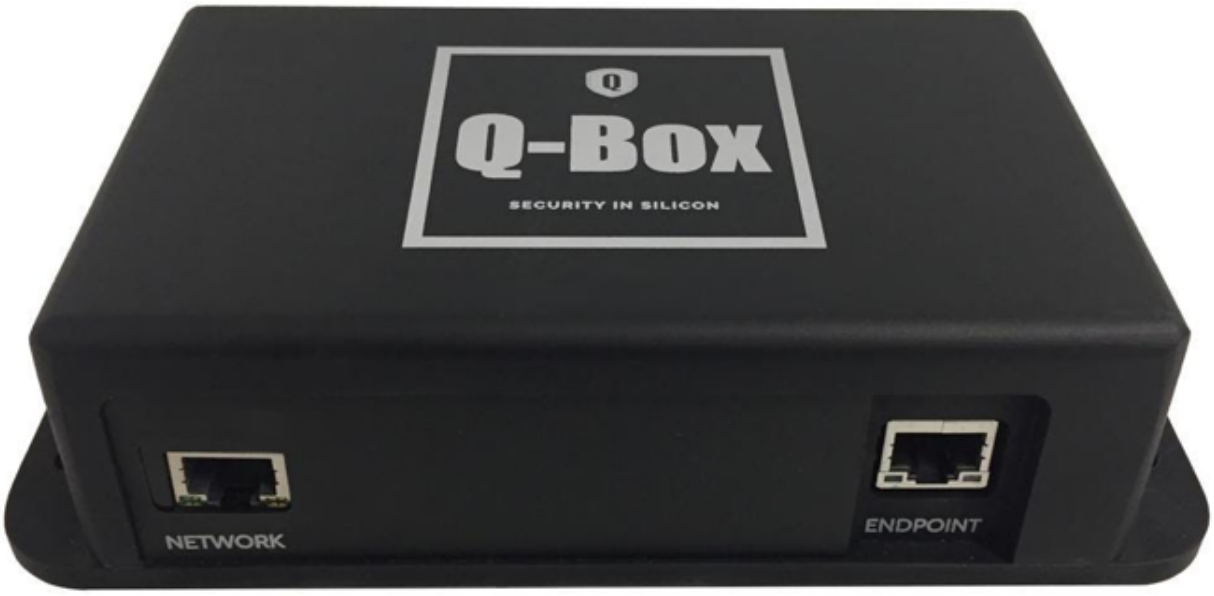
In 2020, investor-owned utilities spent $120 billion for capital investment for the grid, which includes cybersecurity, money for resilience and grid modernization.

Meanwhile, more than 3,000 U.S. cyber software companies have entered the market.

But a former professor of Washington University in St. Louis says the answer to cybercrime is in a little black Q-Box manufactured in Southern Illinois.

Ron Indeck, PhD, founder and CEO of Q-Net Security, which developed the Q-Box, has been working on testing and improving cybersecurity protection for 35 years.

He's now "evangelizing" security executives to a new mantra: hardware, not software, is the way to protect a system from cyberattacks.



St. Louis-based Q-Net Security has developed the Q-Box equipped with an Intel chip programmed with ... [+] Q-NET SECURITY

Indeck recently signed a $3 million deal with the U.S. Air Force to supply Q-Boxes for various devices, and he's inked agreements with half a dozen utilities, including Berkshire Hathaway Energy BRK.B -3.7%, which oversees 11 energy companies.

"Software systems are not secure. Full stop," Indeck said.

Though he admits there's still room in the market for malware detection software, he said his technology obviates the need for firewall protection and virtual private networks which can cost an organization millions of dollars a year.

MORE FOR YOU

Here's The List Of 317 Wind Energy Rejections The Sierra Club Doesn't Want You To See

Revisiting The Blame For High Gas Prices

Why Do 'Fracking' Opponents Ignore Its Moral Benefits?

Q-Box uses Intel INTC -3.4% chips programmed with physical pins; none of the technology runs on software.

"This technology provides protection without requiring changes or additions to an endpoint's legacy code and with no modifications to existing equipment," according to a Q-Net Security press release.

Forbes Business

READ MORE

The company is feeling the momentum. Its factory in Carbondale, Illinois, is building 500 Q-Box devices with another 500 expected to be delivered by year's end.

The National Academies of Science has endorsed the security of the Q-Box.

In a 2018 NAS report, "Quantum Computing: Progress and Prospects," authors found that encrypted data from the Q-Net box would take an assumed quantum computer running the most efficient algorithm known to crack encryption.

Indeck said it would take "over 200 billion-billion-trillion years to decipher the data…longer than the age of the universe."

The box has two outlets—one connects to a company's network, the other plugs into the device that requires protection. Devices are typically part of the Distribution Energy Resource System. A Q-Box can connect to up to 2,000 devices.

"We have thousands, millions of devices [on the network], creating that [critical] infrastructure," Indeck said, describing the electric grid.

That includes wind turbines, solar arrays, substations, control units, pumps, and electronics that are accessible from the network, which creates vulnerability, he said.

Scott Aaronson, Vice President of Security and Preparedness for the Edison Electric Institute (EEI), said he's not convinced there's a "silver bullet" to protect the electric grid from cyberattacks.

"Yes there is inherent vulnerability in all computer systems, but by prioritizing high-value targets, by prioritizing ability to defend and respond, you begin to buy down some of that risk," he said.

Utilities are focused on preventing an incident, addressing the vulnerability, and isolating the vulnerability so it does not have

meaningful impact, Aaronson said.

Cyber risks have multiplied as the electric grid becomes more digital and interactive where customers are increasingly given control through smart grid systems. The risk is changing, evolving because the nature of infrastructure is changing, he said.

“We are deploying more clean energy capabilities…more digitization… more customer controls, which by definition expands the attack surface,” Aaronson said.

“But simultaneously we’re expanding visibility and monitoring of these technologies, which is giving us a better picture of where our vulnerabilities are and what the adversaries are doing,” he said.

“This is one of the top priorities for the chief executives and their boards in the industry,” Aaronson said.

What’s being used now is “not working,” Indeck said. “We’ve seen water supplies compromised. We’ve seen oil and gas delivery systems compromised, and we’ve seen the electrical grid compromised.”

The Federal Energy Regulatory Commission manages cybersecurity standards for the bulk power system, which includes physical assets—plants, wires, and their control systems for the interconnected grid.

State regulators at public utility commissions oversee investor-owned utilities and decide what percentage of profits utilities can retain. They also authorize which investment costs can be passed on to customers.

“Q-Box units would be considered an investment due to the fact that the economic life of the units is in years and not months,” said Branko Terzic, former Federal Energy Regulatory Commission member, now

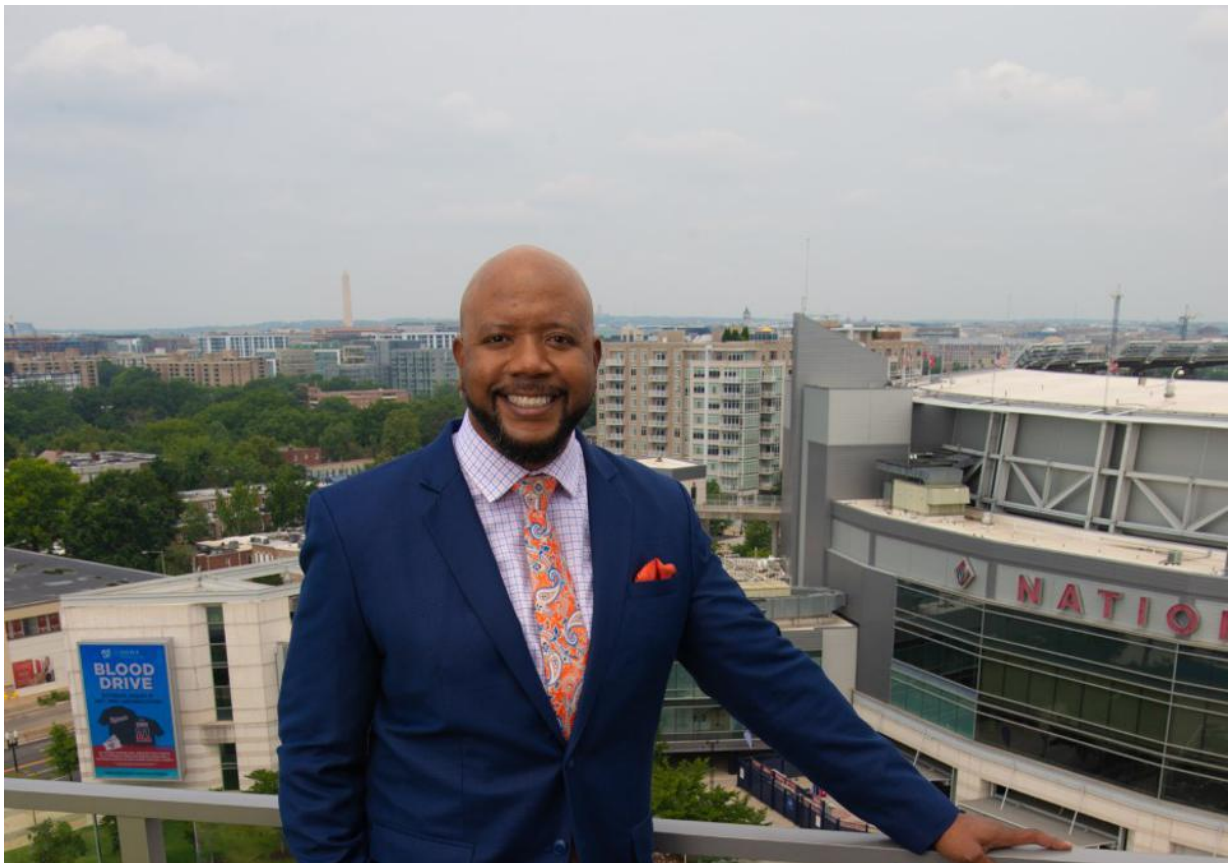
managing director of the energy practice at Berkley Research Group in Washington.

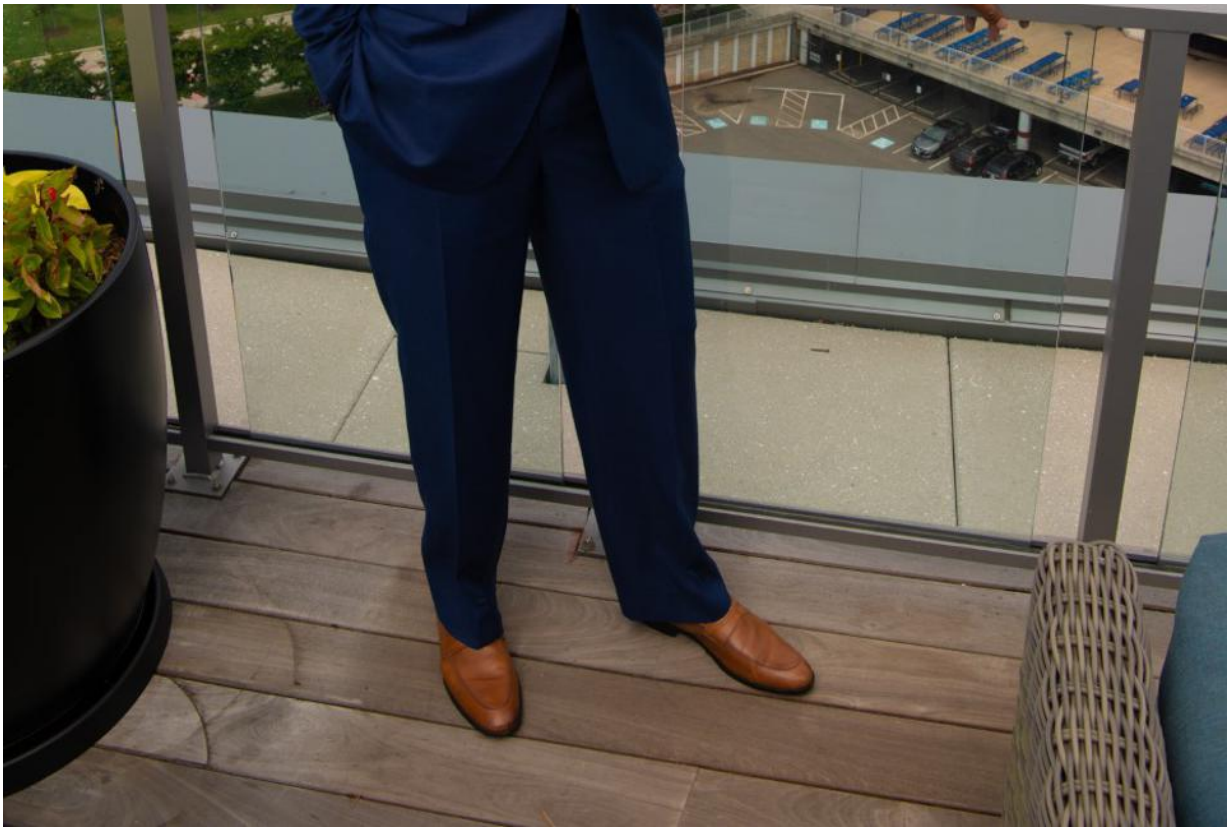
“They would be plant in service [rate base] and be depreciated over their economic lives. The cost of the Q-Box like other assets is part of the revenue requirement upon which rates are based. As rate base the Q-Box both earns a return and creates a depreciation expense,” Terzic said.

Who Can You Trust

Retired U.S. Marine Corps. Gunnery Sgt. Omar Dennis, CEO of Sedulous Consulting Services, which provides cybersecurity to the federal government, said, “Saturation of software solutions leaves companies in a bind because those companies don’t know which software solution is best.”

“That leaves our country vulnerable,” he said.





Retired Marine Corps. Gunnery Sgt. Omar Dennis is CEO of Sedulous Consulting Services. He founded ... [+] SEDULOUS CONSULTING SERVICES

Instead, companies should get tailored solutions which ideally comes with a person embedded in an organization to monitor threats and run the software solutions, Dennis said.

Sedulous provides risk management, cybersecurity architecture and engineering services to the private sector and the U.S. government. The Defense Department is a primary client, but Dennis also has worked on protection for the Transportation and Energy departments.

In the past eight months alone, Sedulous has grown 200% as its number of clients jumped from 5 to 15. The company in August acquired Infinity, a large logistics and security company, to bolster offerings.

“We hear about Colonial [pipeline hacking] but those in the news are only a quarter of what’s really going on,” Dennis said.

Recent attacks on U.S. energy infrastructure, including the 2021

cyberattack on the Colonial Pipeline, which temporarily paralyzed movement of fuel throughout parts of the Southeast, and the 2020 attack on IT giant SolarWinds Corp. SWI -1.9% have fomented fears and sparked swift action in the public and private sector to coordinate protective measures.

EEI does not track incidents, but Aaronson said, "We hear all the time that a company is likely being hit millions of times per day, but these are not material incidents."

Dennis isn't convinced the grid or any energy infrastructure is secure.

Industrial control systems, including those in the country's fuel, oil, water, and electricity systems—are overseen by the private sector and operating using six-year-old guidelines.

"[Software companies] using National Institute of Standards and Technology (NIST) guidelines [circa 2015] are trying to create one-size-fits-all solutions," Dennis said.

"If you're wearing a winter coat that's three sizes too big, you're not going to be as warm as if you had the correct-fitted coat," he said.

By November, DOD could add Sedulous to its list of four U.S. companies certified by the U.S. government to judge the capability and integrity of other cyber software companies. Sedulous would then parse out the reliable software providers drowning in the "saturated" market of more than 3,000 software companies.

Unlike industrial control systems, information systems (IS) are largely controlled by the U.S. government. NIST guidelines for protecting IS and privacy information were released in September 2020.

The new IS standards are sending a message. “We have a higher priority for protecting government,” Dennis said.

The Government’s Role

“On the federal side, there are minimum [software and technology] standards you have to meet before you can even be awarded work to manage or provide services to the federal government. Those standards don’t exist on the private side,” Dennis said.

About 90% of U.S. energy infrastructure is under the purview of the private sector.

EEI’s Aaronson said, “The electric power sector does have mandatory cyber and physical security standards and other regulations that dictate reliability policy, effectively mandates to keep the lights on.”

As for the government, EEI sees its role as diplomacy.

Aaronson said the government can do things that help deter adversaries, like gather intelligence to understand what the adversaries’ capabilities are.

“Infrastructure that is critical to national security is infrastructure that is critical to life, health and safety of communities. By definition, industry and government have a shared responsibility,” Aaronson said.

“Industry is very good at operating our system, engineering defenses and solutions and redundancy and resilience. Where we benefit from government, which is not actually good at all of those things, is with intelligence gathering, law enforcement.”

The government can help industry prioritize threats, focus its attention,