CYBERSECURITY

Building a culture of cybersecurity from the ground up

September 4, 2018 Betsy Loeff

Culture certainly eats strategy for breakfast. Culture also takes a big bite out of even the most strategic cybersecurity initiative.

Read on to find out how three public power utilities evangelize about cybersecurity throughout their organizations to step up cyber awareness and readiness.

Put every employee on alert

"Humans are the biggest weakness in the system," said Timothy Pospisil, director of corporate security and chief security officer for Nebraska Public Power District. "Anyone in your organization can be the

one individual who sees that phishing email, clicks that link, downloads malware, and lets people into your systems."

That's why NPPD — a public power provider with 90,000 meters on the retail side plus a wholesale power supply business serving most of Nebraska — has had a dedicated cybersecurity department since 2003. The department's emphasis is on training employees. "Teaching people to defend our systems and networks is the right place to focus cybersecurity energy," Pospisil said.

Pospisil isn't alone in believing that utilities must foster a culture of vigilance that puts every employee on alert.

"For a number of years, I think everyone assumed it was just the IT guys that needed to worry about cybersecurity issues and breaches," noted Jace Yancey, operations technology manager at Idaho Falls Power, the public power utility serving some 57,000 people in Idaho Falls, Idaho. "But typically many employees at the utility have access to systems that have sensitive information, and there are many different attack vectors that can move through those employees. From the top down, cybersecurity pertains to everyone."

Chad Schow is the information technology manager and security officer for Pasco, Washington's Franklin Public Utilities District, which serves about 30,000 meters. Once he got the nod from upper management, he formed a cyber team that spanned several departments.

"It involved operational technology — which included our industrial control system and our broadband network — as well as our purchasing department and our buildings and ground people, who are involved with physical security. For me, that demonstrated how people now accept that cybersecurity is cross-departmental, not just IT," he said.

"You have to have engagement all the way to the top of the organization. If the CEO and your vice presidents don't support cybersecurity programs, if they don't help you sell them, it will be harder for you to get buy-in from employees," said Pospisil.

Schow works on gaining leadership support this way: "Our commissioners, our senior managers, and our general manager really can't attend a meeting anymore without hearing about cybersecurity," he said.

Schow makes sure his presentations bring home the reality of the threat discussed in the training. "I'll try to find some utilities in the Northwest that have been hit with ransomware and explain what it did to them," he said. He added that a ransomware attack in Atlanta cost the city millions.

Train and engage

Employees at Franklin PUD undergo training each quarter, mostly through videos supplied by a

vendor. "The videos have to do with safe web browsing, safe email practices, phishing, purchasing … lots of different topics," Schow said.

Franklin PUD and Idaho Falls Power both offer in-person training.

At NPPD and Franklin PUD, phishing exercises occur regularly. "I'll send out an email that tries to trick people into clicking on a link or opening an attachment. If they fail — if they do click on the link or attachment — the link will take them to a landing page that says, 'You've been hacked,'" Schow explained.

"We do these exercises to make sure employees understand what to look for," said Pospisil. "Adversaries are getting craftier. Their tools are better, so they're able to make messages look more legitimate. It's harder now for employees to catch this stuff."

"We realize that all it takes is for one person to click on a malicious email link from a hacker to compromise our network with a Trojan horse or ransomware," Schow noted.

He added that repeat offenders — employees who click on a phishing exercise link more than twice in a calendar year – are sent to refresher training. NPPD has a similar policy, and the more employees click, the more they get training.

At NPPD and Franklin PUD, board members also undergo training through face-to-face presentations. "We do it a little bit differently with the board because I like to have a more hands-on approach rather than just run them through computer-based training or a video," Pospisil said. He provides in-person instruction and also updates the board on cybersecurity matters each month. While Idaho Falls Power's Yancey keeps his board apprised of cybersecurity issues on a regular basis.

Pospisil also advocates adding an element of humor to training. "If I just give you death by PowerPoint, you're going to forget what you saw," he said. Instead, his team hams it up with goofy videos and creates timely themes to tie campaigns together.

One NPPD video, for example, was zombie-based when *The Walking Dead* was the latest buzz. The group also has used a superhero theme featuring prominent employees dressed in tights and capes, and it has used a Western theme. In fact, the utility has won Telly awards, which recognize excellence in broadcast and non-broadcast programming such as corporate videos.

Encourage vigilance

Franklin PUD and NPPD use auto-reporting tools to help employees report phishing emails, including those that come through during utility-sponsored phishing exercises. NPPD's Pospisil said that the percentage of employees who report the phishing test as suspect email has gone up from some 20 percent when the utility first started the exercises to nearly 80 percent now.

Franklin's Schow said the exercises — combined with a "report phishing email" button installed on their email — have proven to be a strong preventive measure. "There have been numerous occasions where we got multiple reports of the same phishing email and it wasn't one of my tests," he noted. "When that occurs, there are a lot of things we can do."

Among the measures he takes are sending warning emails to all employees so that they'll be on alert, as well as blocking the phishing source through the utility firewall or putting a filter on the company email to block the sender.

Find your weaknesses

Effective engagement isn't only about teaching employees how to make the right choices; it is also about understanding the most pressing needs your organization faces.

Both Schow and Yancey have conducted password audits, and both determined that their organizations had to impose password-construction rules and teach employees how to make passwords secure.

Yancey made passwords the subject of his first training campaign. "We realized we could do a better job of helping individuals determine the complexity of their passwords," he said.

For a broader view of security at his utility, Schow went through the Department of Energy's Cyber Capabilities Maturity Model, or C2M2, assessment process, which he learned about through a workshop conducted by the American Public Power Association. Schow also helped the Association pilot the online Public Power Cybersecurity Scorecard, a shorter version of the C2M2 assessment.

Both assessments give a utility a snapshot of where it stands on key areas of cybersecurity, so it can prioritize issues that need attention.

"It gave us a benchmark of how mature we were," Schow recalled. "I was able to take those results, present them to our leadership team, and get that framework adopted at our utility. Management doesn't want to get into details — they just want to know how we're doing. We identified some of our risks, took necessary mitigation steps, and plugged a bunch of holes."

Knowing where your utility stands is not a one-time activity. "Cybersecurity is a moving target," Pospisil noted. "Make sure that your management knows it isn't a one-and-done thing. The threats change all the time. Refresh materials periodically."

Recognize the commitment

"The thing about cybersecurity is that it's very expensive," said Yancey. "Firewalls and routers cost a lot of money, and so do the individuals that have the knowledge and the skills to administer those

devices. Boards and general managers of utilities need to understand this when budgets come up. Cybersecurity is just as important as a transformer, as important as the poles and conductors you're putting up. That's just the reality of our industry."

"You don't have to do this on your own," Pospisil said. "There are a lot of very good tools out there and a lot of free resources, too." Resources he mentioned include free materials from the U.S. Department of Homeland Security and the SANS Institute. As part of a cooperative agreement with the Department of Energy, the American Public Power Association offers a number of free or discounted cybersecurity resources and programs for public power utilities as well.

"You can get a training program started without having to make a big spend," Pospisil added.