INSIDE OUT

Since 1996, Carnegie Mellon's cybersecurity experts have collected at least 1,200 publicly reported cases of insiders causing harm to companies and other institutions — but that might only be the tip of the iceberg. As physical and cyber threats become a company priority across all industries, here's how natural gas utilities in particular can protect their physical and intellectual assets. BY JOHN EGAN

ILLUSTRATION BY IAN DODD

The greatest potential physical and cyber threats to the integrity of gas utility networks, systems, assets and operations may not be coming from a cell located somewhere on the other side of the world. They might be walking in the door at the start of each work day.

Popular movies including *Live Free or Die Hard, Blackhat* and *Swordfish* focus on cybercriminals breaking into corporate networks from the outside to steal sensitive information, interrupt daily operations or cause financial or reputational harm. But unwary insiders can pose a potentially greater threat to your digital and physical assets, gas utility officials, consultants and academic experts tell *American Gas.*

Most employees and contractors, known collectively as insiders, don't realize they are a potential threat. But each time they fire up their laptop, log onto the network or insert a USB thumb drive into their terminal, they could inadvertently be injecting malware, viruses or ransomware into your network. And if they click on the wrong phishing email, they might accidentally be sending the keys to your network to cybercriminals.

There's even a chance your employees could be motivated by malicious intent, though there have been no confirmed reports of that among local distribution companies. Yet.

The Tip of the Iceberg

Utility companies around the world responding to PricewaterhouseCoopers' 18th annual Global State of Information Security® Survey for 2016 reported a surge in cyber incidents of all kinds—not just

insider threats—in 2014 (from 1,179 in 2013 to 7,391 in 2014), followed by a big decline in 2015 to 4,694.

The PwC survey includes responses from 129 power and utility executives around the world, 43 percent of whom are located in North America. The survey was sent to leaders at gas utilities, electric utilities and merchant generators; PwC did not specify how many gas utility executives responded to the survey.

Although 4,694 cyber incidents are better than 7,391, the numbers are still worrisome.

In other industries, employees and contractors acting with malicious intent have been behind some of the reported high-profile cyberattacks of recent years, typically attacking financial institutions, health care companies or government agencies. Randy Trzeciak, technical director of the insider threat center at Carnegie Mellon University's Software Engineering Institute, told *American Gas* that its CERT division has collected, coded and analyzed at least 1,200 insider incidents that have occurred since 1996 across all sectors of the economy where insiders intentionally caused harm to their employer.

But that number might be only a fraction of the real number of actual insider attacks since, according to Trzeciak, as many as 75 percent of the victim organizations do not involve law enforcement or take legal action when an insider incident happens, preferring to handle it internally and without filing charges. Adding in that 75 percent would put the total at about 5,000 insider attacks done with malicious intent across all industries over the last two decades.

Huge Potential, Pointed Response

"All industries, including gas utilities, need to recognize the potential of insider threats," Trzeciak told *American Gas.*

For example, Forrester Research surveyed 200 technology decision-makers who experienced a data breach in the previous 12 months in its report, *Understand the State of Data Security and Privacy: 2014 to 2015.* Nearly half—46 percent—said an internal incident was the source of their compromise. Of those 46 percent, more than 4 in 10—42 percent—said the incident stemmed from accidental misuse of company property, while 46 percent claimed the breach occurred because of deliberate, malicious abuse by an insider.

"Across all industries, over 95 percent of the cyber incidents we see are accidental malware infections caused by employees or contractors," said Del Rodillas, a lead for industrial control systems and supervisory control and data acquisition solutions at Palo Alto Networks. "I imagine it's not all that different for gas utilities. Attacks inadvertently facilitated by employees are far more numerous but less harmful than malicious attacks launched by insiders."

Brian Butler, a corporate systems engineer manager with Lancope, now an Oracle subsidiary, blogged about insider threats last year. He said there are five signs that a company could have an insider threat:

- Unusual data movement
- Unauthorized access attempts
- Suspicious employee behavior
- Stolen credentials
- Policy violations

The move to digitization has also made it easier for these threats to occur.

"There has been a massive digitization of information assets over the last few years, as gas utilities have put paper-based information into enterprise resource planning systems and document management systems," said Dan Bowman, a principal in PwC's Power & Utilities practice.

"Having that data digitized makes it easier to extract useful information using various analytic tools," he continued. "But with greater digitization comes greater risks. Data that used to exist on a piece of paper in a drawer now resides in a server, which can be vulnerable to a breach."

His colleague Brad Bauch, security principal in the firm's U.S. Power and Utilities practice, recommended gas utilities protect their cyber and physical assets by following the five-step cybersecurity framework laid out by the National Institute of Standards and Technology:

- Understand what's important.
- Install controls and safeguards.
- Monitor and detect anomalies on your network.
- Create incident response capabilities.
- Build capabilities surrounding resiliency and recovery.

"Gas utilities are in a relatively early stage of adopting the NIST CSF," Bauch said. "Over the last two or three years there has been a sharp increase in focus on this framework, but not all gas utilities are there yet."

Don't Get Hooked by a Phisherman

Most inducements to unwary employees and contractors come in the form of phishing, which is why Colorado Springs Utilities implemented a phishing security initiative a year ago. Each month, a randomly selected group of employees receives a fake phishing email sent by the utility's security team. Over the course of a year, each employee and contractor can expect to receive at least three such emails.

Anyone who clicks on the phishing email will be notified that they could have placed the utility's cyber and physical assets at risk. They also receive a link to educate them to the dangers of phishing. This mandatory training has cut the number of employees who click on a phishing email by 74 percent, said Rick Bustillos, a cybersecurity supervisor and cybersecurity architect at the Colorado utility.

"We take phishing very seriously, and we have implemented these measures to better protect our assets and our customers," Bustillos said. "Any company on the planet that is connected to the internet has to worry about phishing. Using a fake email to get a company insider to perform a specific action that gets outsiders into the network is the highest and most common cyber threat we face."

Phishing emails commonly contain macros, scripts, malware or ransomware. Bustillos noted that phishing was one of the methods outsiders used to get access to the Ukrainian power grid last year, turning out the lights for as many as 225,000 Ukrainians for as long as six hours.

RANSOMWARE: A GROWING THREAT

Del Rodillas of Palo Alto Networks warned that a relatively new threat, ransomware, should be keeping corporate information security officers at gas utilities up at night.

"Ransomware has evolved as a business model," he said. "Rather than hold an individual's computer hostage for $200, cybercriminals are finding it more profitable to hold the networks and data of large companies hostage for a much larger payout. Ransomware has escalated as a cyber threat."

According to news reports, the Lansing Board of Water & Light, a Michigan public power utility, was victimized by ransomware earlier this year after an employee unknowingly opened an email with a malware-infected attachment.

"Hospitals, school districts, state and local governments, law enforcement agencies, small businesses and large businesses are just some of the entities impacted recently by ransomware, an insidious type of malware that encrypts, or locks, valuable digital files and demands a ransom to release them," according to a warning issued this year by the Federal Bureau of Investigation.

"The inability to access the important data these kinds of organizations keep can be catastrophic in terms of the loss of sensitive or proprietary information, the disruption to regular operations, financial losses incurred to restore systems and files, and the potential harm to an organization's reputation," the FBI warning continued. —*J.E.*

New Safeguards

Since October is National Cybersecurity Awareness Month, it's a good time for all gas utilities to take a hard look at their cybersecurity, evaluating both information technology and operations technology, including their ERP and SCADA systems.

Colorado Springs Utilities, for example, has implemented the five-step cybersecurity framework laid out by NIST and emphasized the importance of educating employees about phishing and other scams that could expose a gas utility's networks and assets to exploitation by cybercriminals.

"Cybersecurity is not only about spending money for new hardware, software and systems," Bustillos said. "It's also about more effectively leveraging your employees to spot something anomalous and report it. If they see something, they should say something. This is a discipline you have to build internally. It's not something you can buy off the shelf. The cultural elements of cybersecurity are indispensable to keeping the bad guys away."

One easy step gas utilities can take: Affix a prominent banner that flags incoming emails that originate from outside the network and reminds employees not to click on any attachment

or link if they don't know the sender. These email banners have become increasingly common at gas utilities in recent years, but their use is not yet universal. One company's banner reads, in bold red type: "SECURITY NOTICE: This email originated from an external sender. Exercise caution before clicking on any links or attachments and consider whether you know the sender. For more information please visit the Phishing page on [the company website]."

Gas utility executives and board members also can obtain more information on insider threats to cybersecurity from the FBI, Homeland Security and Carnegie Mellon's CERT, among other sources.

That information is as eye-opening as it is disturbing. Employees who suddenly start living beyond their means could be demonstrating important early warning signs that something is amiss. Disgruntled employees also might bear watching. For their own protection, gas utilities should develop programs and procedures for fellow employees to raise a red flag on their colleagues who might be up to no good.

There are various types of behavioral analytic systems that gas utilities can install on their networks to flag anomalous employee behavior as well.

"I'm a consultant and I do a lot of travel in the U.S.," said PwC's Bauch. "So it is not unusual for me to access my company's networks anytime between 6 a.m. and midnight from anywhere in the U.S. But for an accounting clerk who works a 9-to-5 shift at the company headquarters, it would be unusual if he tried to access his company's network at 3 a.m. from Iceland."

Behavioral analytic software has come into vogue over the last few years for companies in a wide variety of industries, said Ryan Frillman, director of information security and compliance at Spire (formerly The Laclede Group) in St. Louis. Spire is investigating behavioral analytic software.

"Behavioral analytics help detect and deter insider threats by flagging employee behavior that's out of the norm," he told *American Gas*. "Is the time of accessing the network out of the ordinary? Is the location from which they access the network out

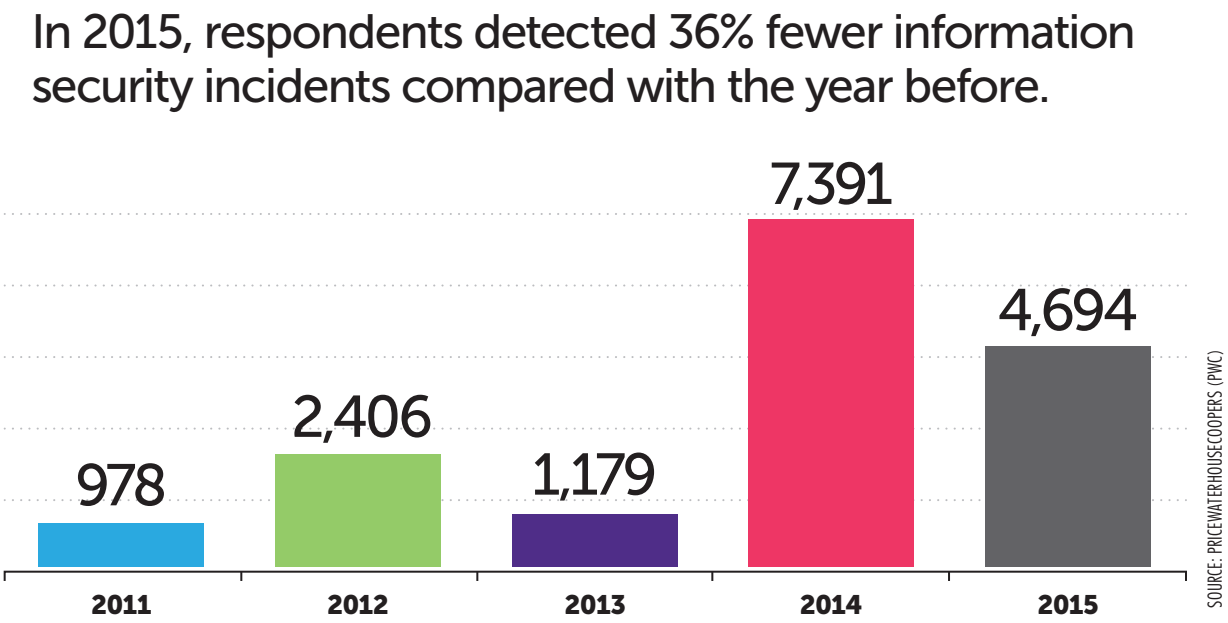

Figure 1: According to PricewaterhouseCoopers' Global State of Information Security® Survey for 2016, the number of cyberattacks across utilities decreased by nearly 3,000 in 2015. But utilities should remain on their guard.

of the ordinary? Are the actions they are trying to perform out of the ordinary? The network's logs will capture all of that information. Once the anomalous behavior is flagged, then you have to decide if it is a concern."

Depending on their size, gas utilities are able to track employees accessing the network using one of two types of systems: a System Information Event Manager, which large utilities would use, or a System Log Server for smaller utilities. Either can have behavioral analytics software installed.

Behavioral analytics "can be misunderstood," Frillman said. It is not Big Brother tracking every employee's keystrokes.

"Behavioral analytics doesn't look at everything an employee does on the job," he said. "It doesn't allow us to read employees' email. It is not monitoring the day-to-day, minute-by-minute activities of an employee. Behavioral analytics simply allow us to see how employees are accessing the network and what they're trying to do on it."

Every organization has the right and responsibility to protect itself, its employees and its customers from insider threats, said Colorado Springs Utilities' Bustillos. In fact, organizational factors are one of three factors the FBI suggests industries examine to prevent insider threats, along with personal factors and behavioral indicators.

Organizationally, gas utilities should institute a least-privilege protocol, where employees are only granted access to the systems and data that are directly relevant to their jobs. That means an accounting clerk would not have access to the company's SCADA system or its customer information system.

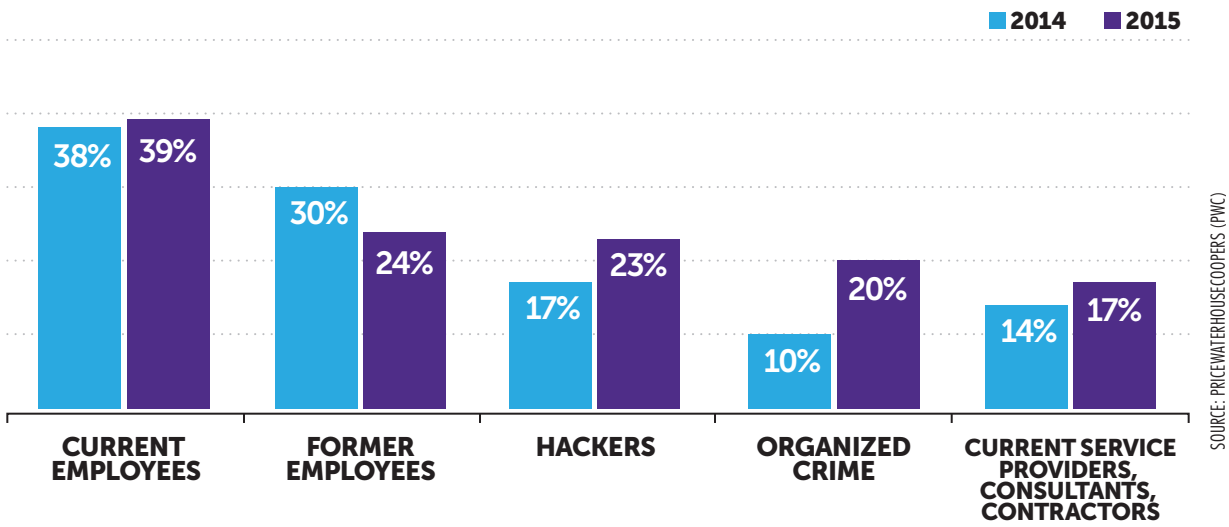

Figure 2: Survey data from PwC consultants also show employees are the leading threat vector to utility companies. Current utility company employees accounted for 39 percent of cyber incidents in 2015, up from 38 percent in 2014.

"It's easier for IT to give all employees credentials to access all parts of the network," said one industry source, "but the fewer people who have access to sensitive parts of the network, the less you have to worry that someone is accessing data they don't need. More and more gas utilities are implementing least-privilege protocols."

Network segmentation is another step gas utilities should take to guard against insider threats. Network segmentation means different sets of credentials are required to access different parts of the network. Segments that utilities could implement include requiring two-factor logon authentication, installing fingerprint scanners or embedding commands limiting machine-to-machine transfer of certain data.

Gas utilities also can guard against known network-borne threats with an intrusion detection system or intrusion prevention system, recommended Palo Alto Networks' Rodillas. An IDS runs in the background of a network and flags malicious traffic, such as malicious software like the Stuxnet or BlackEnergy payloads, which exploit vulnerable IT- and SCADA-specific systems and command and control communications. Using a more prevention-focused approach, the more robust IPS blocks the flow of malicious payloads and communications.

Industrial control systems and SCADA environments are more vulnerable than IT environments to malicious software and exploits because of infrequent patching and extended use of legacy, unsupported software. The use of IDS or IPS helps asset

BEST PRACTICES FOR NEUTRALIZING INSIDER THREATS

Randy Trzeciak, technical director of the CERT Insider Threat Center at Carnegie Mellon's Software Engineering Institute, recommends these steps for mitigating insider threats.

POLICIES

- Clearly document and consistently enforce policies and controls.
- Institutionalize system change controls.
- Implement strict password and account management policies and practices.
- Consider threats from insiders and business partners in enterprisewide risk assessments.
- Enforce separation of duties and least-privilege protocols.
- Be especially vigilant regarding social media.
- Implement secure backup and recovery processes.

WORKFORCE

- Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.
- Incorporate insider threat awareness into periodic security training for all employees.
- Anticipate and manage negative issues.
- Develop a comprehensive employee termination procedure.

MONITORING

- Use a log correlation engine or security information and event management system to log, monitor and audit employee actions.
- Institute stringent access controls and monitoring policies on privileged users.
- Monitor and control remote access from all end points, including mobile devices.

OTHER

- Know your assets.
- Develop a formal insider threat program.
- Establish a baseline of normal network device behavior.
- Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.
- Close the doors to unauthorized data exfiltration.

owners cope with this dynamic by serving as a compensating control.

"IPS is a must-have system, but it's not too common with gas utilities right now. It's more common for those companies to have an IDS," said Rodillas.

All of the Above

Experts agree that guarding against insider threats at gas utilities is not a case of "either/or"—invest in either systems or employees. Rather, it is a case of "both/and." Gas utilities need both vigilant employees and cutting-edge software to help ensure their networks, data and physical assets are safe.

"We can put systems in place, but we can't tell what's in someone's heart," said one source. "That's where the human intelligence comes in. Employees are critical to prevention or early detection of insider threats."

"It all comes down to hiring," another industry source said. "Find people who have integrity and verify they have integrity with background checks or criminal checks. A number of gas utilities are doing this, and those that aren't are considering it."

"It is absolutely critical to hire the right people, conduct background checks and then periodically perform those checks once they are employees," said PwC's Bauch. "The NERC Critical Infrastructure Protection standard calls for criminal background checks for employees in certain positions every seven years. There's nothing comparable for gas utilities at this point. But would anyone argue that the nation's gas pipeline and delivery network is not part of our nation's critical infrastructure that requires protecting?" ◆