Creating Value by Preventing Cyber Crime

November 2016 SE

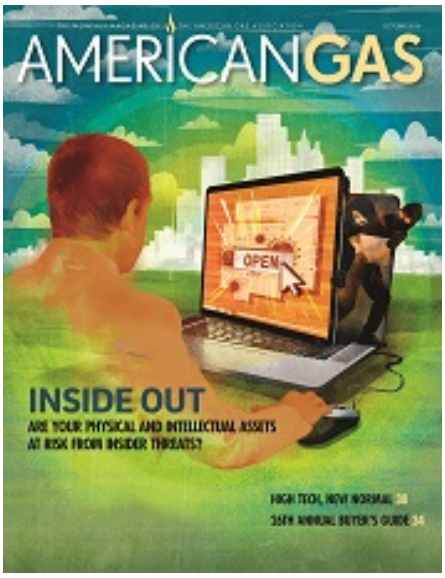
Credit: iStock image 518897996

I've become more anxious, even a little fearful, about the future.

My heightened anxiety has nothing to do with the Zika virus, the threat of domestic terrorism or the results of this month's presidential election. Rather, it is tied directly to my work as a communications resource for utilities.

I've become very worried about insider threats to cybersecurity at our electric and gas utilities. And if I'm worried, I can only imagine what's going through the minds of the people responsible for protecting the digital and physical assets at electric and gas companies.

I recently wrote the cover article for *American Gas* magazine on the potential threats utility-company "insiders" — employees and contractors — pose to their employer's cyber and physical assets. What I learned as I reported and wrote that article was very disturbing.



As communicators, we all have a **vital role to play in combatting insider threats** to cybersecurity at our companies.

We've probably all seen news stories about cyber-crooks who hacked into the computer networks of companies like Yahoo, Target, J.P. Morgan, Anthem and others. And, of course, thanks to WikiLeaks, we know more than we should about emails involving Hillary Clinton's staffers.

Credit: iStock image 483978146

Last December, the Ukrainian electric grid was hacked, turning off the lights to as many as 200,000 people for as long as six hours. More recently and closer to home, the systems of Lansing Board of Water & Light, a Michigan public power utility, were held hostage earlier this year after an employee unknowingly opened an email with a malicious attachment that encrypted files across the utility's network.

Until it paid a ransom, the Michigan utility lost access to its accounting system, email, phone lines, printers and other technology. So now we have a new word in our cyber vocabulary: "ransomware."

Given the critical role that data and digital systems play in utilities and every other business venture, what company would refuse to pay a ransom to get its data and systems back?

"Click here" has become one of the scariest phrases in the English language.

Experts I interviewed for the magazine article agreed that, across industries, most cyber breaches originated when a careless employee or contractor clicked on an attachment or link in an email from an unknown sender. That attachment or link could contain malware, viruses or ransomware that could do great harm to a utility's networks.

Credit: iStock image 501674170

When reporting that article, more than a dozen gas utilities declined my request for an interview. One utility that did agree to speak with me, Colorado Springs Utilities, told a refreshing story about what they were doing to educate employees so they don't make a mistake that could expose the utility networks and systems to cyber crooks.

As I wrote in the article:

> *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.*

While visiting a client recently, I noticed posters on the walls warning employees against clicking on messages from unknowns senders. When utility employees respond to my emails, a growing number of them have large prominent warnings at the top of the email: **“WARNING: This mail is from an external sender. Don’t click on a link or open an attachment unless you know the sender.”**

Cyber crime represents an opportunity for utility communicators to demonstrate the value of what they do. A quote I heard many years ago — “War is too important to be left solely to the generals” — certainly applies here. Cyber security has become every utility-company employee’s business. It’s not just the purview of the Information Security or Information Technology departments.

Communicators have a **critical role to play** in protecting their utility’s data and systems. By educating employees about the dangers of hacking and the need for ongoing digital vigilance, you can make a meaningful contribution to keeping your utility’s data and systems safe from hackers. There’s a ton of value in preventing a cyber attack. Executives will remember communicators’ work (or lack of it) to protect their utility’s data and systems the next time they make budget decisions.