Adviser: Don't ignore the human element in reducing risks

By THOMAS F. ZYCH

Crain's Cleveland Business (7/29/2017 12:01 AM) -- The key to effective cyber defense is knowing your critical vulnerabilities. Whenever we use the prefix "cyber" to discuss data security, we think first about electronic systems. But that is not where the No. 1 data risk lies.

Walt Kelly's classic Pogo Earth Day 1970 comic tells us where to look first when assessing data risks: "We have met the enemy and he is us."

Cyber defense planning too often begins with data system review and upgrade, and typically ignores the human factor: Your own employees are the most easily exploited and hard to close holes in your defenses.

System security measures are critical components of effective data security. Your business would no sooner ignore the maintenance of secure processing environments than you would leave your car unlocked with the keys in the ignition or a bank vault open and unattended. That said, system defenses are necessary but not sufficient by themselves.

We recently have seen ransomware (and other viruses masquerading as ransomware) infect and even disable enterprise systems. While much attention focuses on failure to patch software vulnerabilities, the critical weakness necessary for the infiltrations to succeed is the carelessness of system users who open emails, attachments and other infected communications, letting the malware in. Of course, we don't necessarily accuse careless users of intending to harm the company (although malicious insiders certainly exist) or even of reckless disregard for the organization. As Shakespeare reminds us, "The fault, dear Brutus, is not in our stars, but in ourselves." We must look at the environment we create to understand the challenge.

First, in a connected world, we require everyone to communicate electronically, setting expectations that demand trust in the systems we use. No one gets rewarded for taking extra time to finish a task. Second, the old lines between the work and off-work contexts are gone. Our laptops, phones, tablets and other devices support both the business and private sides of our lives.

Third, trusting others is necessary simply to get anything done. It's not feasible to perform background checks on everyone you encounter. You often must trust someone based on who they represent. These assumptions are realities, and we cannot expect our people to ignore them. What we must do is recognize they exist, honestly admit the vulnerabilities and do our best to empower employees to be a real first line of defense. How do we do that?

Here are a few experience-based strategies:

Start with executive sponsorship. There is no substitute for clear communication from top management (and not just IT leadership) that vigilance is expected, encouraged and funded.

Align good practices with company values. For example, in a law firm environment, protecting confidential client information is a baseline ethical obligation, and maintaining security consciousness can be explained as part of that ethic. Indeed, for most commercial enterprises, not harming customers or employees is a necessary business value. In other words, good data hygiene cannot be sold as a "nice to have" but, rather, it has to be articulated as core to your organization's mission. Address everyone who touches your information, including all employees as well as contractors and service providers (including business advisers). Any one of these people can be your weakest link. Train, train, train. It's not an employee's fault if she or he hasn't been given timely, accurate and practical advice. Your entire team should receive regular (and mandatory) data security training. While you may have good trainers on your staff, there also are many cost-effective training resources available to provide the full range of in-person, online and repeated messaging assistance.

Enable effective response. In the end, you can't prevent every incident — it's a matter of when, not if. Every business should have a clear, written plan for responding to a data breach, but that plan will be effective only if your employees are aware of it and their responsibilities. While your response team is specifically tasked with addressing a breach, everyone in the organization has a role in protecting the company's data. "If you see something, say something" applies as much to cybersecurity as national security. Employees should know how and to whom to report a suspected incident, even if it's their own mistake. In fact, if the person who accidentally opens a questionable email attachment knows she or he won't be punished and complies with the expectation to report what happened, the chances of corralling the infection are much greater than if it lingers in the system.

We're all human, and we can be careless or fooled into communications we ought not have. By acknowledging and addressing the human factor vulnerabilities, we can minimize the risks, and perhaps the enemy won't be us, at least not this time.

Thomas F. Zych chairs Thompson Hine's emerging technologies practice and heads its privacy and cybersecurity team.