SmartFocus on Cybersecurity in Business

A **Smart**Brief Education Update

SPONSORED BY VIRGINIA TECH

WINTER 2017

BUILDING THE BRIDGE TO A CYBERCULTURE

Recent security attacks have signaled the need for a new organizational culture that bridges cybersecurity and business operations. Here's how to make that happen.

If we learned anything from the Equifax hack that affected 143 million people, it's that the CEO (along with the rest of the C-suite) needs to be concerned as much about cybersecurity as the chief information security officer (CISO). More organizations realize that they need to better integrate security practices into their business operations to help combat the increasingly complex threats attacking their networks — and their brand reputations. This shift has given rise to the concept of the cybersecurity culture, in which all users, from entry-level personnel to executive leadership, are responsible for helping maintain the integrity of data assets.

WHERE THREATS ORIGINATE

Wade Baker, an associate professor of integrated security and a cybersecurity researcher in Virginia Tech's Online Master of Information Technology program, describes today's breed of cybersecurity threats as falling into four categories:

- Insiders, either employees of the company or employees of trusted partners and contractors;
- Cybercriminals, the people who send out spam and phishing emails to gain entry to the corporate networks;
- Cyberespionage, including nation against nation, nation against company and even company against company, with the intent of stealing intellectual property or other confidential information; and
- Activists, people who use the internet to launch a protest or deface websites of organizations they oppose.

That's a wide swath. What makes fighting the bad guys a "whole company issue," says Baker, is that everybody's a target. "Take a phishing email, which is used in cybercriminal activity and cyberespionage campaigns. If the employee clicks on it, then their computer is infected, and it spreads from there to compromise other computers and servers throughout the network."

DEVELOPING THE CYBERSECURITY CULTURE

Smart companies have learned that helping employees understand that they're part of the security picture is much more effective than, for example, making them sit through an annual slideshow about security. That practice isn't going to change behavior, he insists.

Baker, who for many years led development of Verizon's annual Data Breach Investigations Report, points to a specific data point that surfaced in that research. "When you look at how data breaches are detected, what has found more breaches than intrusion detection systems were employees happening to notice things that were suspicious [and] then investigated," he says.

TIP: "If you can help employees feel like [they're] part of the defense of the organization ... you get more buy-in and more of a security culture."

As an example, Baker advises adding gaming elements in training to make it more engaging.

TIP: One example: to stop "tailgating" — the practice of one badged person allowing others to follow right behind when going through a locked door (a physical security data breach) — "gamify it a little bit and say, 'We're going to be walking through the building and someone will try to tailgate you, and you'll get $100 if you challenge them.'" That changes the conversation, he explains, from "I'm challenging you because I don't trust you and don't like you and I'm a jerk," to, "Hey I'm just trying to win $100."

"Everybody has that shared understanding," he says.

Retired US Navy Rear Admiral David Simpson, who will be instructing Virginia Tech students in a course on cybersecurity risk in the spring, advises "judicious deployment of 'red teams.'"

TIP: "These are third-party or in-house experts who play the role of white-hat hackers to uncover ways systems and services in the company can be compromised [by] extracting data, denying availability of critical services or "replacing truth with an agenda that would be harmful."

The reason Simpson likes the red team approach is that it helps "capture the attention of your various divisions in a language they understand: 'You couldn't get the car off the assembly line for three days because you lost control of your robotic arms? Hey, I understand that. No cars off the assembly line. Really bad.'"

FROM MASTER'S EDUCATION TO THE WORKPLACE

Armed with an IT degree, Whitney Dano had been on the job for a year when she decided that earning her master's degree would help her fill in learning gaps surfacing at work with an American insurance company. She chose Virginia Tech's MIT program because it would allow her to tackle studies online, it provided a security focus, which met her interests, and she could continue working full time. "It was a perfect situation for me," she says.

Since earning her new degree, Dano has been promoted into an operation engineer role at the firm, as part of the security team. "I'm the one who says, 'These systems are old, they're end of life, they're going to have vulnerabilities and will need to be moved in the next year, so we want to stay on top of that,'" she explains. But she'd like to keep moving forward, working not so much to assess risk as to prove it out. Demonstrating the risks makes it real for people in a way that just talking about it doesn't, she says.

Dano's advice to others considering a master's degree in IT: "Try to think about what your goal would be when you come out of the program. Think about what you're going to use it for and what you're going to do. I knew going in that my end goal would be having this on my resume to really give me that next boost to be able to move into a security role."

WHAT TO DO ABOUT THE INTERNET OF THINGS

Not everyone who is pursuing a master's degree in IT wants to commit to becoming a cybersecurity professional, says Kendall Giles, an assistant professor of practice in Virginia Tech's MIT program. "Yet in today's world, I think certainly every MIT student should come out of the program with a basic understanding of security."

To provide that foundation, Giles teaches a semester-long security fundamentals course titled Cybersecurity and the Internet of Things, which uses a case study approach to concentrate on the main principles. As he explains, IoT is the common lingo we use to describe taking internet-connected sensors and putting them on devices that can compute and gather data. Yes, he acknowledges, sensors allow companies to gather data more easily, but IT and business leaders also need to remember that each of those devices possibly has vulnerabilities.

"[I]f it's easier for you to gather data, it's easier for the malicious hackers to gather that same data and use it," Giles says.

Because IoT involves physical devices, the traditional cybersecurity principles that stress confidentiality, integrity and availability also need to encompass safety now. That changes how companies should approach security, Giles says.

TIP: For one, the chief information security officer in charge of cybersecurity needs to work with the chief security officer in charge of physical security to develop a coordinated plan of action in the event of an attack. Second, given limited resources, organizations need to prioritize their critical assets and put in control mechanisms to protect those above all others.

But the most effective way to address security concerns is to become educated, Giles says.

TIP: "Everything in our lives is online," he stresses. "We can no longer afford not to understand the basic principles of security."

TIP: When that's the lesson, he adds, nobody needs to be a cyber expert to know they have a responsibility to mitigate such potential failures.

David Raymond, a faculty member for VT-MIT's online graduate program as well as deputy director of the university's IT Security Lab, urges his master's students to understand that business and cybersecurity need to work together.

TIP: While the cybersecurity team is busy putting together a layered approach with multiple levels of defense and checks and balances, the business side needs to help them prioritize the risks so they know where the work needs to focus.

TIP: When a security event occurs, too often he sees organizations treat them as natural disasters, something out of the control of the company. Better, he asserts, to "treat it as some level of failure. Somebody failed to do something that caused it to happen." In the case of Equifax, a web application vulnerability that wasn't fixed in March, when the patch was available, led to the May break-in and theft. Former CEO Richard Smith blamed a single employee for the problem to a Congressional committee. That response led to plenty of nonpartisan condemnation. As one representative asked during the hearing, according to The New York Times,

"How does this happen when so much is at stake? I don't think we can pass a law that, excuse me for saying this, fixes stupid. I can't fix stupid."

Raymond likens such mass cyber break-ins to a bridge falling into the water. "That is going to cause investigations [and] lawsuits, and the company that built that bridge is going to be out of business." In civil engineering, he says, "there's a compliance infrastructure and requirement that these things be engineered in a certain way. Security engineering just hasn't gotten to that level of maturity."

TIP: How can companies mature? One step Raymond recommends is adopting a "robust security framework" — a strong process for securing systems. An example is CIS Controls, produced by the Center for Internet Security, which is a prioritized set of actions for securing the organization's infrastructure and its data.

TIP: "It starts with relatively simple things — like having a full inventory of computing devices that should be connected to your network and then periodically auditing your network to make sure there aren't any unauthorized computing devices connected to it," he says. The point is to pick something and then do it. "You shouldn't be making it up as you go along," he says.

FORMING BRIDGES

TIP: The most important driver for changing culture, however, is getting the two sides — business and information security — to work better together. Baker's research has shown, for example, that while company boards understand and value the business-level metrics for cybersecurity at high levels, the same isn't true for the CISO.

"The board is craving this information. They need to know the organization is secure," Baker says. "The CISO doesn't really know how to explain it to them in a way they understand." That, in turn, leads to a lack of trust, confidence and willingness to fund what needs to be done. As a result, he adds, cybersecurity initiatives don't end up "in the right place."

That's why education programs that blend technical and business training — with a major dose of cybersecurity instruction — are so critical, Baker says. "It's common that you have pure business with no technical and technical with no business. When you have people who live in both worlds, they're valuable in an organization because they form a bridge." ■

> " The most important driver for changing culture, however, is getting the two sides — business and information security — to work better together. "