By Matt Ottinger

BEHIND THE CYBER CURTAIN

Beware of Risky Behaviors, Sophisticated Threats

WannaCry. It's the aptly-named computer virus that, according to European law enforcement agency Europol, hit 150 countries and infected 200,000 machines in May. The ransomware cryptoworm attack targeted computers using the Microsoft Windows operating system by encrypting data and demanding users pay to recover it.

Ransomware is just the latest iteration of computer hacking that has businesses – both large and small – searching for advice and protection.

"For the bad guys, it's a low-risk, potentially high-reward endeavor," contends Chuck Cohen, Indiana State Police captain and director of the Indiana Intelligence Fusion Center (IIFC). "It's a phenomenon we've seen with regularity over the last several years. But Indiana businesses and government organizations tend to be high-value targets because they hold information that is critical to run their operations."

Trojan viruses, phishing, malicious bait and switch programs and cookie theft are other common hacking techniques. Denial of service attacks can also be an instrument of destruction for businesses.

Sid Bose, an attorney in Ice Miller's Litigation and Intellectual Property Group, tells the story of such an attack.

"In a smoke screen situation, a company was getting bombarded with millions of requests through its online web portal from different computers that had been compromised by malware, which essentially made them little drones," he recalls. "It basically brought their network to a grinding halt because it couldn't handle the load from these attacks.

"On its face, the motivation was thought to disrupt the operation of the portal, but an investigation showed that the attack was a smoke screen to pull money out of the company's bank account. Those are sophisticated attacks."

Breaking bad behavior

Vulnerability is often most evident in human frailties rather than technical weaknesses, according to experts.

"There's a popular saying: Amateurs hack computers but professionals hack people," Bose relays. "Phishing is so successful because it takes advantage of our behaviors and the desire to want to be useful when someone makes a request of you."

Bill Mackey, an assistant professor at Indiana State University (ISU), is launching new courses (Intelligence Analytics and Cybercriminology) to train students in the behavioral aspects of cybersecurity. Mackey also owns Alloy Cybersecurity – a firm that's hiring ISU students as interns to offer real world experience in the field. He outlines behavioral-based approaches to exposing a company's vulnerabilities.

"We look at names, email addresses and basic information from web sites," Mackey notes, explaining phishing efforts will often relate to a person's hobbies or a company's industry. "Using open source intelligence, we'll find out how active you are online and how much information you've divulged that we can access. Then we'll try to use that against you. It might go beyond just the standard phishing email from corporate saying, 'Click on this link.'

"We can get incredibly personal," he adds. "If we know John Doe drives a certain car or eats at a certain place or donates money to a certain group, that will be exploitable and a vulnerability we could attack."

Mackey also says training ISU students to be behavior analysts will help close a critical knowledge gap.

"What I've found is that businesses are

"A problem we see is that a business may have taken great steps toward security and computer hygiene but their vendor hasn't."

– Bill Mackey

incredibly interested in getting a graduate of our program to come in with knowledge of the psychological, the criminological business and technological sides of cybersecurity and bringing that in one package," he summarizes. "The technology piece is just the ability to speak the language. We want our graduates to work hand-in-hand with IT people, but what we're developing here is the idea that we don't want your IT person trying to solve behavioral issues."

Cohen points to positive trends and lauds organizations that have made data protection a priority by reorganizing their workforce.

"We're starting to see companies hire chief information security officers, not just chief information officers; it's a different skillset," he delineates. "We're also seeing companies recognize the need to have pre-existing relationships with law enforcement entities so they're not cold calling State Police, the FBI or the Fusion Center. They have a relationship and part of our job is to have that with those companies. And we want relationships not just with the chief security person, but the person in charge of the networks."

Should you pay the cyber piper?

"We don't negotiate with terrorists" has long been the preferred posture by some governments across the globe. But when your company is hacked, should you apply that hardline stance as well? Or should you pay up and get it over with?

A large Los Angeles hospital did just that in 2016, paying about $17,000 in Bitcoin currency to regain access to its network following an attack.

"It was unique because it was one of the most public ransomware incidents," Bose says. "It put hospitals and the health care industry on the front lines and brought scrutiny to their security practices."

Experts generally advise not to pay in these situations, but Bose understands why a hospital with such vital operations would feel pressured to give in.

"Yes, the general sentiment is that you never pay hackers but sometimes that sentiment is overcome with business need," he points out. "For example, let's say a company has just been hit with ransomware. Ideally, the company would have backups of its systems to recover and have minimal impact to its operations. Let's say, however, that those backups are not viable. In such situations, if the ransom is reasonable enough in view of the circumstances, then payment might be the simplest out."

Yet he reinforces why the best advice in the long run is to avoid succumbing to hackers' demands.

"We always counsel clients that there is no guarantee that your data will be released upon paying the ransom," Bose discloses. "And it could be bad precedent. After paying, your organization might become known to pay ransoms, which can put you increasingly at risk for being targeted. Also, paying up plays into incentivizing such attacks to begin with."

Are you protected? Are you sure?

Security is coveted but a false sense of security can be devastating.

"Nobody can stop it 100% but all it takes is one weak link," Mackey surmises. "A problem we see is that a business may have taken great steps toward security and computer hygiene but their vendor hasn't. Those people have access to their systems so that's indirect access through the weakest link. It's good to talk to your vendors before you hire them and ask what they've done for cybersecurity."

Bose concurs that risk evaluation is critical.

"It's really important to be able to understand your risk exposure and how you want to mitigate that," he says. "What level of risk are you willing to accept? Just because you have a type of risk, maybe implementing something to address that is cost prohibitive. Some small companies can't do what the big guys are doing – or they can't do the industry best. I was talking to a company (whose representative) said, 'I don't have to be in the front of the pack; I just don't want to be in the back of the pack.' "

Cyber risk insurance has grown in popularity in the last couple of years, according to Bose. He touts its benefits but cautions businesses to be fully aware of what they're buying.

"I've seen situations where companies thought they were covered for a certain type of event and they weren't at all," he advises. "It's important to make sure the coverage they have contorts to their specific type of risk."

While hospitals or financial institutions are obvious targets, many sectors are at risk.

"Ransomware has impacted a lot of different industries across the board," Bose offers. "In other areas, you have specific problems affecting specific industries. In financials, you have things like business email compromise and sophisticated phishing attacks. In the energy utilities sectors, you have nation-state threats as well."

Unknown resource

Cohen reinforces that the IIFC exists to help the citizenry and businesses. The first step in prevention, however, begins with cultivating that relationship.

"The vast majority of businesses don't reach out to us or know we're there as a resource," he imparts. "Giving them (examples of) IP addresses that distribute malicious code, for example, is something we can do. We want to be giving bulletins out to as many organizations as possible, but I can't be putting it out in the media. So we need that relationship."

However, if hacking occurs, Cohen says the attack should be treated as a crime and a company's first response should be to contact police.

Ransomware Tips

The state of Indiana's Information Sharing and Analysis Center offers the following information on removing ransomware from your computer:

One method is by using "system restore" to load your system's last known working configuration. There may be variations in the exact steps to be followed depending on the manufacturer of your computer, but the following is a process that sometimes works on many systems using Windows:

- Restart the computer and press F8 repeatedly as soon as you see anything on the screen
- Use the arrow key to select "safe mode" and press enter
- Open "system restore" by clicking the "start" button. In the search box, type "system restore," and then, in the list of results, click "system restore." If prompted for administrative access, provide confirmation
- Choose a restore point and then click "next"
- Review the restore point and then click "finish"
- Restart your computer and let Windows start normally

If "system restore" doesn't help, one may try running Microsoft Safety Scanner, Windows Defender or other antivirus software. To do that, once you are in the safe mode, try to run the antivirus software – performing a full-system scan to detect any malicious activity.

RESOURCES: Sid Bose, Ice Miller, at www.icemiller.com | Chuck Cohen, Indiana Intelligence Fusion Center, at www.in.gov/iifc | Bill Mackey, Indiana State University, at www.indstate.edu