3-2015

Cybersecurity in the Information Age

Follow this and additional works at: https://via.library.depaul.edu/depaul-magazine

Part of the Data Storage Systems Commons, and the Digital Communications and Networking Commons

Recommended Citation

(2015) "Cybersecurity in the Information Age," DePaul Magazine: Vol. 1 : Iss. 12015 , Article 4. Available at: https://via.library.depaul.edu/depaul-magazine/vol1/iss12015/4

This Article is brought to you for free and open access by the Alumni Publications at Via Sapientiae. It has been accepted for inclusion in DePaul Magazine by an authorized editor of Via Sapientiae. For more information, please contact digitalservices@depaul.edu.
In the past 18 months, the databases of an alarmingly long list of companies have been compromised, including household names Target, Home Depot, Sony Pictures, Michael’s, JPMorgan Chase and UPS. According to the Identity Theft Resource Center, more than 750 breaches occurred in 2014, exposing over 83,000,000 records. The IBM Security Services 2014 Cyber Security Intelligence Index calls these attacks “the problem that isn’t going away.” Faced with this reality, consumers and companies may wonder if it’s even possible to protect their personal and financial data.

“Huge breaches were much less common half a dozen years ago,” says Jacob Furst, professor of computer security and visual computing in the College of Computing and Digital Media (CDM). “Today, they’re happening on a regular basis.” Furst is one of several faculty members whose expertise makes them frequent contributors to media outlets reporting on the rise of hacking. In the classroom, Furst and his colleagues in CDM’s School of Computing lead the charge in training the next generation of cybersecurity experts (see sidebar on page 15).

The challenges to cybersecurity are daunting, but as DePaul’s experts explain, the situation isn’t hopeless.

By Kelsey Schagemann
Putting hacking into context

At a basic level, data breaches can be traced to two primary motivations. “Breaches occur because people have discovered that there’s money to be made from stealing corporate and customer information,” Furst says. His colleague, Instructor Jean-Philippe Labruyère, summarizes the second reason: “Why do they breach the data? Because they can.”

While credit card fraud is nothing new, the advent of online banking and buying has changed the game. “Before computers, a classic example of credit card fraud would be a waiter who steals 20 or 50 cards per day,” Labruyère explains. “Now you can steal 1 million cards in a minute.” Compromised cards are sold through an online black market, and at roughly $20 per card, the financial payoff is high.

The hackers behind cyberattacks differ from old-school thieves in other ways as well. “Years ago, it was common for criminals to immediately try to charge as much as they could on stolen cards,” explains Nick Graf (CDM ’05, MS ’06), the consulting director of information security for risk control at CNA Financial. “These days, they’ll charge a couple dollars here, a couple dollars there—when a million credit cards have been breached, charging a few dollars on each can still bring in a lot.” This tactic is particularly insidious, because consumers might not contest or even notice small charges on their account statements.

Many major breaches are the work of international organized crime. “You need to have a certain level of funding and expertise, which means the larger attacks aren’t usually instigated by small groups,” Furst says. The global nature of cybercrime makes it especially difficult to combat, as laws vary and may be unenforceable from country to country.

Hacking strategies

Furst and Labruyère outline two main hacking strategies. In a phishing attack, a hacker will send an email asking individuals in an organization to click on a link. “If you disguise the email well enough, someone will click on this malicious link—the hackers only need one person to do it,” Furst explains. This action will install malware, such as a key logger that can be used to decipher passwords. Once hackers have the user’s administrative privileges, they can employ these legitimate credentials to access data.

The other common cyberattack targets exploits—known vulnerabilities in software operating systems—which can be eliminated through coding in a process called patching. “All software has exploits. These exploits are typically found and solutions made public, but organizations are not always current on patching,” says Furst. Up to 70 million Target customers were victims of this type of hacking in December 2013. Most likely, the breach occurred through the point-of-sale device—the credit card reader. “The credit card readers are still running an operating system, but because of their limited role, they may not receive patches like a normal computer would,” Graf explains. This oversight allowed hackers to install malware that effectively siphoned off each credit card number that was swipe through the machines.

“Huge breaches were much less common half a dozen years ago. Today, they’re happening on a regular basis.”

–Professor Jacob Furst

Human error

Whether individuals succumb to phishing attempts or fail to notice or fix vulnerabilities in their systems, these breaches can largely be attributed to human error. In fact, the IBM Security Services 2014 Cyber Security Intelligence Index blames human error for 95 percent of information technology breaches. Combating this root cause is not necessarily easy, effective or cost-efficient.

Education is one solution. “With a phishing attack, it doesn’t matter how good your technological security is because [it relies on] human action,” Furst says. Installing a firewall might seem like an easier and cheaper response than hiring someone to lead a comprehensive security education awareness program, but this could be less beneficial in the long run. Graf, who advises CNA on the level of risk they’ll assume when writing a new cybersecurity insurance policy, stresses the importance of regular employee training. “When I’m reviewing a company’s overall security and technology programs, I’ll look to see if they have user education in place,” he says. “I’ll check if they have security leadership—someone who can implement a security program strategy.”

For some companies, the cost of security precautions—whether for staff, training, system tests or even the creation of a data breach plan—can be prohibitive. “We’re storing more information online and the complexity of the systems is increasing, but the resources given to protect the systems are not necessarily increasing at a comparable rate,” Labruyère says. “At some point, a company may decide that the cost of protecting against every possible attack is too high.” Both Labruyère and Furst emphasize that this isn’t necessarily a fully conscious decision about a company’s bottom line, but rather due to limited human capacity and competing priorities.

Data protection strategies

Thankfully, several different options exist for consumers seeking enhanced security, and they don’t require going off the grid. Both professors recommend using cash whenever possible, but they acknowledge the obvious limitations of this suggestion. When it comes to debit versus credit cards, the experts prefer the latter. Not only do many credit card companies monitor patterns of use and alert consumers when fraudulent activity may have occurred, but also, the industry has protections that make it less of a hassle to redress the situation.

Some credit card companies offer one-time use numbers, which can be helpful for online transactions. Consumers enter their desired limit and the length of time the card is valid. Once the limit is reached or the time period passes, the card number is rendered useless. Europay, MasterCard and Visa (EMV) cards operate similarly. Transactions are approved
via a unique authentication code that cannot be reused. “Other parts of the world have had this in place for years, so it isn’t a new technology. It won’t solve everything, but it’s a huge step in the right direction,” Graf says. “For one thing, it will be much more difficult for forged credit cards to be created, since they use an embedded chip rather than a magnetic stripe.”

Graf also recommends using a password manager. He stores all of his passwords behind one long, complex master password on a secure online site; additionally, Graf takes advantage of the service’s second factor of authentication, which entails entering a random number that is sent to his phone. “Even if someone got my master password, they still wouldn’t be able to access my account unless they also had my phone,” he explains. It’s also a good idea to change passwords frequently and use different passwords for every site.

All three experts emphasize the importance of monitoring account statements. “You have to be aware,” Furst states. “If you see suspicious activity, report it right away.” Furst, who had shopped at Target when the company was breached, recalls that he never saw any fraudulent charges but his credit card company sent him a new card almost immediately as a precaution. Often, a company whose data have been compromised will offer a free credit monitoring service. “We only see about 10 percent of customers sign up for these services,” Graf says. “That’s a missed opportunity, because those companies will do the legwork to help you restore your credit.” Consumers should check their credit regularly at annualcreditreport.com, which is the official, government-authorized website for free, annual credit checks.

While it’s important to be vigilant, consumers needn’t feel paralyzed with fear. “It comes down to education and awareness,” Furst says. “We have to take sensible precautions and then get on with our lives.”

---

DePaul Prepares Next Generation of Cybersecurity Experts

In the ever-changing technology field, there’s only one solid way to prepare students for future careers. “You have to teach fundamentals,” says Jacob Furst, professor of computer security and visual computing in the College of Computing and Digital Media. After all, by the time students graduate, new operating systems and structures may already be in place, not to mention new hacking techniques. In his courses on host-based security, Furst focuses on the building blocks, such as authentication and access control. “We don’t teach the technology, even though we use the most current technology,” he says. “If students learn the basics and how to put them in action, they’ll be in good shape.”

Nearly 10 years after graduating, Nick Graf (CDM ’05, MS ’06), the consulting director of information security for risk control at CNA Financial, still relies on the skills he developed in the classroom. “Information security requires constant learning, and DePaul gave me the ability to learn and to teach,” he explains. “My professors taught security design, how to educate your users, human-computer interaction, system management—these are all relevant to my current position.” Jean-Philippe Labruyère, an instructor in the School of Computing and Graf’s former mentor, spent 16 years in the industry. “I always tell students, if you like to learn and are excited by different challenges every day, this is a good field for you,” Labruyère recalls. “It’s not a nine-to-five job, that’s for sure.”

When graduates of DePaul’s information assurance and security engineering program enter the job market, their resumes benefit from a special designation held by a select number of universities. The National Security Agency and the Department of Homeland Security recently reappointed DePaul as a National Center of Academic Excellence in Information Assurance/Cyber Defense. “We were one of the early universities to achieve this about 10 years ago,” Furst says. “We’re evaluated on the rigor of our curriculum and whether we meet a certain set of standards,” Labruyère explains. “Our program is truly one of the best.” Furst notes that it’s not uncommon for applicants to apply to DePaul specifically for the information assurance and security engineering program, which enrolls more than 200 students. “We’re pretty excited about what we offer,” he says. “When our students graduate, they don’t have any trouble finding work in the field.”

---

ONLINE EXTRAS

View a visual summary/infographic of the “problem that isn’t going away” and read about “After the Breach,” DePaul’s recent cyberrisk conference featuring keynote speaker Peter W. Singer, at depaulmagazine.com.