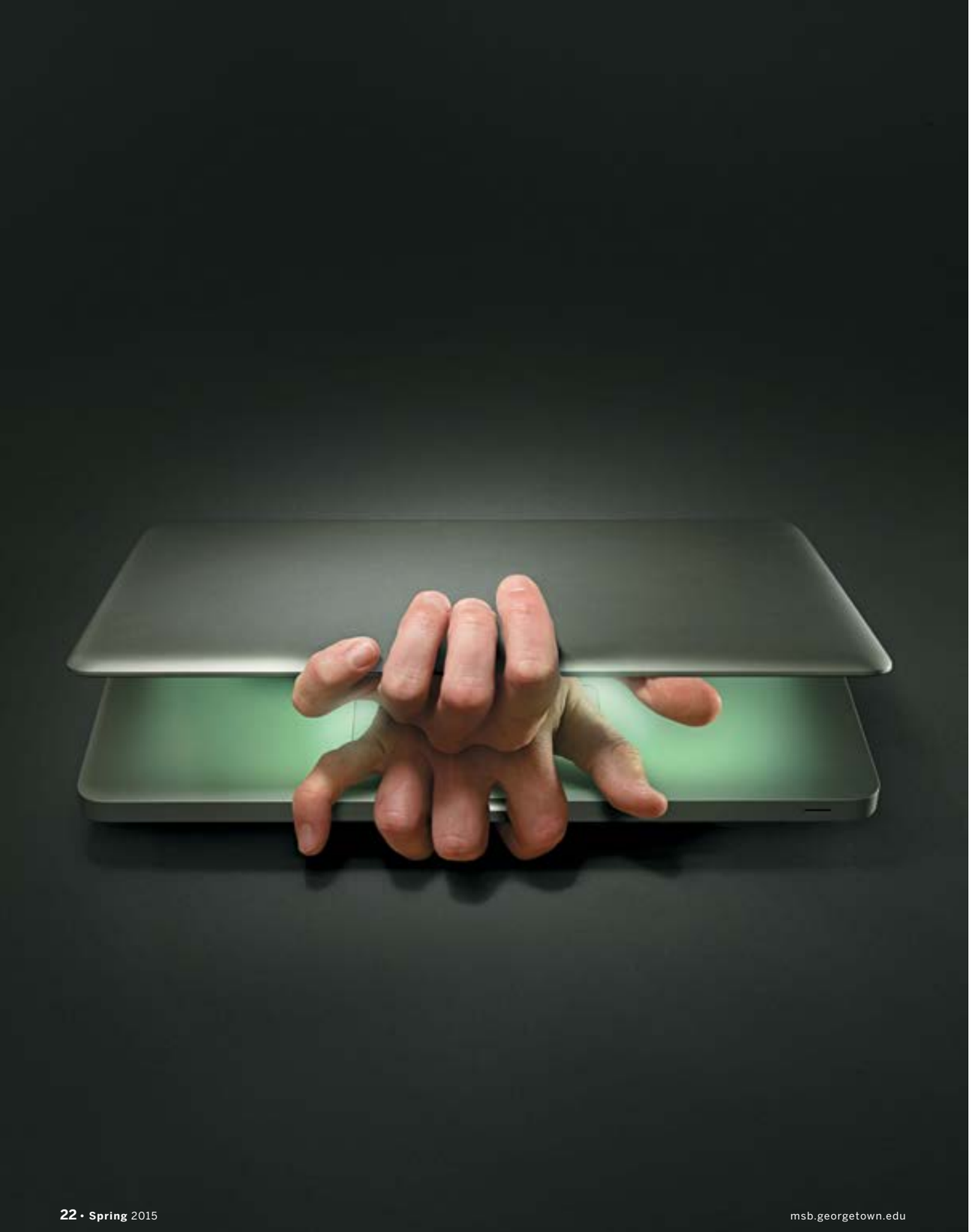






By Melanie D.G. Kaplan

# Cyber (In)Security

## Barely a week goes by without a headline about cybercrime. What should businesses be doing to tighten security?

**One weekend in** February, McDonough School of Business Associate Professor Robin Dillon-Merrill sat down at home with her laptop and an MP3 file. She needed to edit a podcast and was in a hurry to finish the task. Although she didn't have the right editing software, she dismissed the idea of waiting until Monday, when she could use a reliable program at Georgetown. >>

C.J. BURTON

She searched cautiously for free software, aware that she was taking a serious risk. In fact, she had just been working on a paper about behaviors related to cybersecurity decisions, in which she had written, "Beware of high pressure situations, i.e., if I had more time and more resources, would I make the same decision?" Yet she downloaded the software; her motivation to finish the work trumped the risk of downloading a virus.

Dillon-Merrill admits she, of all people, should have known better.

"I'm one of the most vigilant people, and I still managed to completely corrupt my laptop with malware," she says.

Dillon-Merrill is still kicking herself for the mistake; not only did she thwart any further attempts to work that weekend, but she lost more time on Monday when technicians took *their* time to clean up the laptop. However, she also acknowledges that her painful ordeal illustrates how common hacking is today — and how cyber attacks can inflict damage on even the most vigilant targets. Furthermore, the incident gave her an insider's perspective for her research, in which she looks at why people, fully aware of risks, still click their way into potential cyber disaster.

> "Predictive analytics can look at changes in behavior across hundreds or thousands of activities and unearth specific patterns not visible to a human."
>
> *—Chris Checco (EMBA '05)*

Barely a week goes by without a headline about theft of personal information, intellectual property, or financial data. In less than two years, an attack on Target yielded an estimated 110 million customer records; a JP Morgan breach affected nearly 80 million households and 7 million businesses; thieves stole up to 60 million credit card numbers from Home Depot; health insurer Anthem had as many as 80 million records stolen; and a hack on Sony led to the cancellation of a movie release and served as yet another stark reminder of the power evil-doers can wield.

In January, Sen. Ron Johnson chaired a Senate Homeland Security and Governmental Affairs Committee hearing on cybersecurity. Private-sector experts talked about the importance of information-sharing, a national data breach notification policy, and privacy concerns. Johnson cited a 2014 study by the Center for Strategic and International Studies that estimated the total economic loss from cyberattacks as high as $100 billion a year.

"Cybercrime is a growth industry," the report states. It goes on to say that the biggest cost of cybercrime comes from its impact on company performance and national economies. "Cybercrime damages trade, competitiveness, innovation, and global economic growth."

## Cyber Threats, Human Behavior

At Georgetown McDonough, Dillon-Merrill is working with management professor Catherine Tinsley on a Department of Homeland Security (DHS)-funded project that looks closely at the nontechnical side of cybersecurity. In other words, what are the behavioral aspects, rather than algorithms and firewalls? In June, they will host the Security and Human Behavior Conference at Georgetown.

"The people side of cyber is the challenge. People fundamentally don't understand the different parts of technology that are involved," Dillon-Merrill says, noting that during a congressional hearing, Rep. Joe Barton asked Target executives what happened when criminals came into the stores and infected the card-swipe machines.

But after you have enough understanding of technology to protect yourself, she says, it is equally important to avoid getting caught up in behavioral biases that affect how we take risks and interpret warnings. Even the best technology can't make up for flawed human behavior.

Dillon-Merrill likes to compare cyberthreats to prohibited items at the airport. TSA, she says, encounters warnings all the time — toothpaste that's over the three-ounce limit, for instance. It's a genuine warning, and it's real contraband, but it's not a bomb. If a bomb exploded every time that warning was tripped, people would adopt a certain mindset. "But over time, when people see these warnings," she says, "they add their own interpretations, like, 'Oh, that's just toothpaste.' That reinforces the idea that you can ignore warnings."

Target offers one example of a company that invested in the best detection software, which generated all the right alerts, yet personnel still ignored the warnings, Dillon-Merrill says.

"You have to assume it was some of these cognitive biases at play," she says. She doesn't yet have the data to prove that people are relaxing about warnings, but that's what she is trying to understand: whether the lapses take place on a personal computer or at the corporate level.

While cybersecurity tends to focus more often on external threats, Edward Snowden's decision to leak NSA data nearly two years ago is still an acute reminder that employees and contractors also can cause massive security breaches.

> "I'm one of the most vigilant people, and I still managed to completely corrupt my laptop with malware."
>
> *—Robin Dillon-Merrill*
> *Associate Professor of Operations and Information Management*

"It's not just the disgruntled employee," says Chris Checco (EMBA '05), president and chief analytics officer of Virginia-based Razorsight, which provides cloud-based analytics to communications companies. "The person might be going through a tough credit period, or something is going on outside the workplace. It's a multidimensional challenge."

Checco's experience using advanced analytics to reduce fraud in his previous job at Accenture gave him a deeper understanding of insider threats to data security. The first defense against these breaches is having policies and procedures in place, he says, but a sound protocol goes far beyond a written strategy. Checco recommends wider use of background checks before hiring and use of technology to recognize danger signs. By tracking patterns of downloads, email, and messaging, organizations can help identify anomalous behavior for individuals who have rightful access but who are using it in unusual ways.

"Predictive analytics," Checco says, "can look at changes in behavior across hundreds or thousands of activities and unearth specific patterns not visible to a human."

Yet even if an employee is suddenly downloading sensitive information, it's important to look at other factors — human resource issues and recent performance reviews, for example — and use human judgment. "You won't bring someone into your office saying, 'You're fired because you have some strange behavior lately,' " Checco says, comparing that mindset to the movie *Minority Report*, in which people were apprehended even before they committed crimes. "If they've had issues, you take a positive approach and try to help them. Talk to that person's manager and keep a closer eye on them. Or restrict their access to data so you can nip it in the bud before it becomes an issue."

Naturally, as security tightens, an individual's level of behavior becomes more accessible to their organizations. This battle between security and privacy has come to the forefront as employees are increasingly concerned about their own personal information. But Checco says in the case of tracking an individual's behavior, companies can put measures in place, such as simple data anonymization,

## What Can Consumers Do?

When it comes to cybersecurity, the risks to businesses affect consumers in the end. Here are nine steps to take to protect yourself:

1. **Remember**, when you put something onto the Internet, it's out there, even if you think it's secure or encrypted, says Bill Jones (MBA '09), with the CERT Division of Carnegie Mellon's Software Engineering Institute.
2. **Keep an eye out for chip and PIN authentication** technology, common in Europe and slowly rolling out in the United States; it significantly decreases the risk of credit card theft.
3. **Expect to be hacked**, and consider what you share online. You may not be targeted individually (most of us have security through obscurity), but chances are, you'll be targeted through your connection to a corporation that is hacked.
4. **Stay vigilant about checking your bills** when they arrive and credit reports annually so you can catch problems early.
5. **Keep your virus software up to date.**
6. **Pets' and kids' names are easy to find online**, so do not use them in your passwords, advises Brenda Fischer (B '90), bureau chief of New York City's Cybercrime and Identity Theft Bureau. "Make your password unique, and change it often." In addition, tools such as Google's 2-Step Verification make sign-in more secure, requiring the user to prove identity in two ways.
7. **Beware of emails impersonating** someone you know. It's easy to learn a name and create an email that's just one character removed from the real address.
8. **Read the small print** and ask businesses where they'll use your information. "Be aware what you're signing up for," Jones says, "especially with free apps."
9. **If you truly don't want to be hacked**, Jones says, use the U.S. Postal Service or share information in person.

so only people with a "need to know," such as an investigator, have access to a person's identity.

Brenda Fischer (B '90)

## The Risk Assessors

Bill Jones (MBA '09), an Army reservist who spent five years at the FBI supporting cyber investigations and who recently became a member of the technical staff in the CERT Division of Carnegie Mellon University's Software Engineering Institute in Virginia, thinks the leadership of most companies doesn't understand the risks associated with being online.

"One of the biggest problems is that the CISO (chief information security officer) doesn't have a seat at the table," says Jones, who works on federally funded Internet security research, largely with the Department of Defense and DHS. He stresses that his comments are based on his own opinion, not those of his employer or customers.

He explains that a chief information officer's (CIO's) job is to make sure a system functions; a CISO protects it and keeps the bad guys out. "The CISO needs to be a peer to a CIO, and in most cases, the CISO reports to the CIO," he says. Among a CISO's tasks are prioritizing what needs to be defended, making a risk calculation (since you can't afford to defend everything), and understanding the normal business flow, so a red flag is detected when the pattern changes.

The risks, as we know, are considerable. Hackers can overtake a machine, steal information, encrypt the system, destroy the network, or alter data. Jones suggests one chilling example: the implications of a cyberattack on the air traffic control system. Suppose a hacker removes a zero from the number of feet remaining before landing, so when a plane is 100 feet out, the pilot reads that he's just 10 feet off the ground.

Jones recommends companies take technical and personnel precautions to fortify their cyberdefense, and he stresses the importance of understanding internal networks. Imagine a startup company adding routers, servers, and fiber optics as it grows.

"If that addition of capabilities isn't managed, you end up with a hodgepodge," Jones says. "The CIO and CISO should know what that hodgepodge is, but then you merge with another company, and before you know it, you're a multinational corporation, and you don't have a clue what's going on with the networks." In this scenario, the company is left with vulnerabilities, and hackers come in through channels the executives didn't even know existed.

Jones also encourages information sharing between the private sector and public agencies, a view shared by Brenda Fischer (B '90), bureau chief of the Cybercrime and Identity Theft Bureau in the New York County District Attorney's Office. Fischer says she's encouraged that corporations are talking more about public-private partnerships, but much work remains.

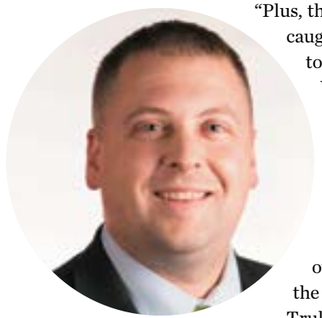
"At the end of the day, private organizations are bottom-line driven," she says. "They want to be good corporate citizens, but their primary focus is making money." Most larger companies do disclose security breaches, she says, because it would be hard to hide them from the media. But smaller companies don't always disclose, and most are fearful of a damaged reputation once shareholders, regulators, and customers learn that customer information may not have been adequately protected.

After Fischer graduated from Georgetown, she went to Brooklyn Law School and has been at the D.A.'s office for nearly two decades. Her bureau handles more than 25,000 cybercrime and identity theft cases per year for Manhattan alone.

These days, she sees trends with young thieves overseas selling credit card numbers to criminals — complete strangers — in New York, who are re-coding plastic cards, cashing out at an ATM, or shopping online. The Internet, she says, has become the crime scene of the 21st century.

Fischer says many people who once dealt drugs and were involved in violent criminal activity have now turned to cybercrime and identity theft. Why? It's easier, it's safer, and they can do it in the comfort of their own homes.

"Plus, the criminal punishments haven't quite caught up to speed," she says. "There is little to no case law in the area of cybercrime. We are making law as we proceed to prosecute these cases."



Bill Jones (MBA '09)

Companies can't afford to ignore these threats, Fischer says. "If you're the CEO of a major company, you have a big target on your back. You have to pay attention, if only to protect your own customers. These major breaches hit the news and scare the heck out of people."

Truly scary, she adds, are the issues of national security. "In some cases, you're not talking about people losing dollars," Fischer warns. "It's about people losing lives. That's when it gets really frightening. When you talk about the ability of cybercriminals to take down electric grids and government networks, it ramps up to be very serious very quickly." GB

**ON THE WEB**

LEARN ABOUT THE GEORGETOWN CENTER FOR BUSINESS AND PUBLIC POLICY'S WORKSHOP ON SECURITY AND HUMAN BEHAVIOR AT **CBPP.GEORGETOWN.EDU/ACADEMIC-CONFERENCES**.