Inside Cybersecurity: The Vulnerabilities and Opportunities

Date : October 2, 2019

A while back Phalguni Miraj, a high school sophomore in New Jersey, was working on a school assignment in Google Drive. When he logged in, he was redirected to random tabs urging him to click in exchange for financial rewards. Miraj immediately closed the tabs, but wondered what had lurked behind them. “I was curious about how I could protect my computer’s security and the information stored in it. However, I still felt vulnerable,” he says.

Therein lies the lifeblood of cyber crime: finding online ways to attack and make money from vulnerabilities, whether they are on our laptops or within the more complex systems of multi-million-dollar companies. Once they gain access, cyber criminals steal everything from personal information like credit card numbers to sensitive company data. A hack on your personal computer might compromise your list of contacts, who suddenly receive emails from you requesting money. High-profile corporate cases have put the information for millions of consumers at risk, including the Marriott data breach, the Capital One data breach, and hackers targeting unsuspecting Fortnite players for money (*see Related Links for details*).

A Leading Business Risk

Cybercrime has taken on a financial life of its own, characterized these days as an actual economy, not just a collection of cyber attacks. Recent research quantifies worldwide cybercriminal revenues at more than $1.5 trillion, coming from sources like illicit markets for stolen information, the theft of intellectual property and trade secrets from companies, data trading and ransomware, where criminals hijack files and hold them for ransom. According to the Internet Society’s Online Trust Alliance, more than 2 million cyber incidents in 2018 caused $45 billion in losses. A World Economic Forum survey of business leaders named cyber attacks as the leading risk for business executives in the U.S., Canada and Europe. And back to that economy – if cybercrime were a country, it would have the 13th highest GDP in the world.

Cybercrime is very much a global problem, observes Andreas Haeberlen, an associate professor of computer and information science at the University of Pennsylvania. “We’ve seen examples of nation states hacking each other’s infrastructure, and also many examples of criminals from one state attacking citizens of another. This makes sense: if I am on another continent, physical-world crime is hard. I can’t physically pick the pockets of someone in the U.S. But cybercrime is easy. All I need to scam someone is an Android phone and some basic English skills. The OPM [U.S. Office of Personnel Management] hack is thought to have originated in China, the Sony hack in North Korea, and so on. And there is an entire market for stolen credit card numbers, drugs, and more.” During a gathering at the United Nations in late September, 27 countries signed a joint agreement on what is considered fair and foul play in cyberspace, trying, in part, to get ahead of this exploding issue.

> “There is only so much that technology can do if people choose the password “12345,” share their credentials with their friends, or post all their personal information in online forums.” — Sebastian Angel, Professor of Computer and Information Science

Fourteen-year-old Miraj, increasingly aware of all these headlines, spent a week this past summer studying cyber threats at the ISTS GenCyber Introductory Camp at Dartmouth College in New Hampshire. He left with a much clearer understanding of the issues. “People who work in the field of cybersecurity have faced many difficulties trying to prevent wide-scale and even minor attacks because of increased interactions online, especially through smartphones and social media,” says Miraj, who learned everything from the different types of cyber threats to how big companies can defend against cyber attacks. “Increasingly complex systems mean more room for vulnerabilities, meaning more cyber

attacks."

In other words, cybercrime is a field where problems need to be solved. "Cybersecurity," adds Miraj, "is truly a great career choice."

The cybersecurity industry, the protection of computer systems against costly cyber threats, is a dynamic field these days as computer scientists and other experts work to combat system hackers and other cybercriminals and stop the flood of money into this dark economy.

Sebastian Angel, also an assistant professor of computer and information science at the University of Pennsylvania, notes that cybersecurity is very complex because designers of systems need to be right every time in order for a system to be secure. In contrast, attackers only need to be right or get lucky once. Therefore, the more devices and applications we have, the more chances for attackers to be right.

Cybersecurity, Angel suggests, has become incredibly important. "Cybersecurity studies how our computer systems and networks behave in the presence of an intelligent and adaptive adversary, as opposed to how these systems behave in nature," says Angel. "Specifically, in nature some "bad" event might happen, like an earthquake might cause a power loss to a data center. But we can reason about what to expect and usually have some idea of why or how often these bad events happen. As a result, we can build our infrastructure to tolerate these bad events with solutions, like backup generators. In an adversarial setting, the adversary might notice that the data center has backup power generators, so instead of shutting off the power, the adversary might instead use its resources to corrupt a router and cause it to drop important packets (collections of data)."

We hear so much about cyber attacks these days for a number of reasons, Angel notes. In addition to security gaps in really large systems and a growing number of hackers with the knowledge and technology to do some damage, companies don't always want to pay the ever-growing expense of defending against attacks. "A company can spend a near infinite amount of money securing their infrastructure, but very little of that translates into new customers or revenue streams," says Angel. "As a result, security is often seen as an insurance problem. In fact, companies have insurance policies that cover data breaches or other hacks…this is less costly than preventing these attacks in the first place."

The Role Humans Play

Angel confirms that the industry has "very interesting work, high-paying career opportunities, and high demand." And the need for experts will only increase, adds Haeberlen. "You need a good education in computer science to understand the systems that are being attacked and how the attacks work," Haeberlen says. "And also some breadth. There are typically many 'offline' factors that are involved as well, such as economics (in black markets, for instance), social sciences (how people behave), political science, network science, and so on. Cybersecurity is a very interdisciplinary field."

In addition, Angel hopes that students prepare for the future of this industry by truly understanding what it means to be cyber secure. "Cybersecurity is partially a technical problem and partially a social problem," Angel says. "There is only so much that technology can do if people choose the password "12345," share their credentials with their friends, or post all their personal information in online forums like Facebook and Instagram. A lot of cybersecurity attacks exploit the role that humans play in these systems and their weaknesses, rather than some vulnerability in the code."

Which brings us back to Miraj's concern with protecting his computer's security and the information stored there. Angel suggests that a safer cyber life for individuals begins with "threat modeling," to identify the following three things:

- What assets – like pictures, devices and smartphones — do you want to keep safe?
- What policies will you put in place to make sure they're safe? Maybe only your friends can see your pictures, or you want a guarantee that nobody else can access your cellphone.
- Who are your potential adversaries? Are you worried about your high school frenemy accessing your pictures? Are you worried about your parents unlocking your phone? Are you worried about a remote hacker somewhere in a basement in Eastern Europe?

Thinking more about your online vulnerabilities will help you implement effective cyber protections. "The Internet is a more dangerous place than we think it is," warns Miraj. "All of us have the possibility of becoming victims of cyber attacks."