CYBERATTACKS and the DIGITAL DILEMMA

Recent high-profile hacks have renewed calls for improved security, but competing incentives pose a challenge

By Tim Sablik

Over the past year, Americans have been inundated with news of one large-scale cyberattack after another. The Democratic National Committee's email server was compromised during the 2016 election, and the organization's internal emails were posted publicly by WikiLeaks. An October 2016 attack temporarily disrupted service to many of the most trafficked sites on the Web, including Netflix, Amazon, and Twitter. Ransomware — malicious code that locks a computer's files until users pay for a decryption key — infected business, government, and personal computers around the globe in May and June 2017. And in September, credit bureau Equifax disclosed that hackers accessed personal data used to obtain loans or credit cards for as many as 143 million Americans — making it potentially the largest data theft in history. No digital system seems safe.

According to Symantec's 2017 Internet Security Threat Report, more than 1 billion identities were exposed due to data breaches in 2016 alone, and the number of large-scale breaches (those that exposed more than 10 million identities) crept up from 13 in 2015 to 15 in 2016. Ransomware threats have also ballooned. From 2015 to 2016, the average ransom demanded by attackers rose from $294 to $1,077.

In response to these threats, organizations are heaping significant sums at cyber defense. International Data Corporation, an IT market analysis consultancy, forecasts that worldwide spending on cybersecurity software and services will surpass $80 billion this year. They predict that number will grow to more than $100 billion by 2020. Despite that, successful attacks have shown no signs of slowing down. What makes cyber defense so difficult, and can economic principles shed any light on how to improve it?

More Connected, More Exposed

One reason cyberattacks continue to be a problem despite efforts to stop them is that there are simply more avenues of attack than ever before. For instance, a growing array of consumer devices — TVs, cars, ovens, and thermostats, to name a few — are now connected to the Web, making up what has been called the Internet of Things (IoT). One estimate holds that there will be more than 8 billion connected devices by the end of 2017 — more than one for every person on the planet. By 2020, this number is expected to grow to more than 20 billion. But these new devices come with a trade-off.

"The more technology we accumulate to make our lives easier, the more it opens us up to attack," says Timothy Summers, the director of innovation, entrepreneurship, and engagement at the University of Maryland's College of Information Studies.

That's the digital dilemma: With the power and convenience of greater connectivity comes more potential for vulnerability to intruders.

Last fall, hackers seized control of thousands of IoT devices to create a "botnet" — an army of infected machines. Botnets are typically used to launch what are known as distributed denial of service (DDoS) attacks where enslaved computers overwhelm websites with requests, enough to temporarily shut them down. The DDoS attack last October that hit numerous major websites was launched using a botnet of IoT devices. With that service knocked offline, many of the most highly trafficked sites on the Web became hampered or unreachable.

"Anytime you enable an operation, you're creating a potential path for a bad guy to carry out an operation as

well," says Martin Libicki, the chair of cybersecurity studies at the U.S. Naval Academy and a researcher at RAND Corp. "In the old days, if I wanted to set my thermostat, I had to actually put my fingers on the thermostat itself. That limits the amount of mischief someone can do. Now that you can change your thermostat using your phone, potentially everyone else can too. So in order for me to have my convenience, I have to enable capabilities that might get hijacked."

Just as connecting household devices through the IoT benefits consumers, interconnectivity offers firms many benefits as well. Sharing data and system access with regular business partners may improve supply chains. But expanding the range of trusted individuals or companies who have access to a firm's system increases the opportunities for bad actors to access it. For example, hackers were able to gain access to Target's payment information in 2013 by compromising a system of one of the company's contractors, an HVAC vendor. (See "Cybersecuring Payments," *Econ Focus*, First Quarter 2014.)

Automating updates can ensure that a computer system's defenses against hackers remain up to date — unless those automated updates become the gateway for malicious actors to enter the system. The ransomware attack that occurred this past June initially infected Ukrainian computers by corrupting an automatic update to widely used tax software.

Likewise, allowing employees to remotely access their files or emails at home or on the road can increase productivity and create a more flexible workforce but at the expense of more digital doors to defend.

Is it possible to reap the benefits of increased connectivity while minimizing our vulnerability?

Lack of Incentives

One often proposed solution to cyberattacks is to simply increase security spending. Economic theory does offer some insights into why individuals and firms might underinvest in cybersecurity from a social perspective. As the botnet used in the October 2016 DDoS attack illustrates, the owners of the breached systems are not necessarily the ones who suffer the most. This creates a potential externality problem, which can skew the incentives to demand or supply cybersecurity.

On the demand side, if consumers don't bear the costs of their devices being breached, they may demand more open devices in the interest of convenience. Additionally, they may believe their devices are more secure than they actually are. Manufacturers, who know more about the security of their products than buyers, may take advantage of this information asymmetry to sell cybersecurity "lemons." For example, Brian Krebs, a leading cybersecurity expert and blogger, has reported that many IoT devices come with weak security measures out of the box. A recent Senate bill seeks to address this situation by setting baseline security standards for any Internet-connected devices sold to the government.

Both positive and negative externalities also may skew the incentives for firms to invest in security. The Internet is designed to allow all machines on the network to interact with one another, and many devices share common software and operating systems. Once an exploit is implemented on one machine, it can quickly spread to others on the network. In this way, each firm's security depends both on its own defenses as well as the aggregate security of the entire network, what Howard Kunreuther of the University of Pennsylvania and Geoffrey Heal of Columbia University described in a 2003 article as "interdependent security." This interdependency may result in weaker network security for a couple of reasons. First, since firms benefit from the security investments of others, some may devote fewer of their own resources to security than they would in a vacuum. If enough firms do this, it weakens the security of the network as a whole, potentially undoing the benefits of the firms that invest more in cybersecurity. Second, even assuming each firm invests in a level of security appropriate for its own needs, it may still impose costs on other firms on the network that value security more highly.

On an individual level, firms also have incentives to limit cybersecurity spending. In a 2002 article, Lawrence Gordon and Martin Loeb of the University of Maryland developed an influential model of information security suggesting that firms maximize their benefits from cybersecurity by spending only a fraction of their expected losses from a breach, similar to the rationale for insurance. Often the most vulnerable systems or information are the most costly and challenging to defend. Moreover, defenders face a great deal of uncertainty about where attackers will strike. Attackers will always seek out the weakest link in a system, but it may be difficult to identify weak points ahead of time. Rainer Böhme of the University of Münster and Tyler Moore of the University of Tulsa argued in a 2016 article that it may therefore be rational for firms to wait for attackers to identify weak points for them and respond after the fact.

While these actions may be rational for individual consumers and firms, they could result in less security and more costly outcomes for society as a whole. In response to a 2013 executive order from President Barack Obama seeking to improve critical infrastructure cybersecurity, the Department of Homeland Security issued a report exploring the incentives firms have to provide adequate cybersecurity from the perspective of society and how the government might better align those incentives. Options included using carrots, such as grants tied to security improvements, and sticks, such as regulations that hold entities liable for failing to meet minimum security standards.

Private actors have also tried to solve the externality and interdependent security problems. After Google was hacked in 2009 through a flaw in Microsoft's Internet

Explorer browser, it began to examine its partners' software more closely. In 2014, Google revealed Project Zero, a team dedicated to notifying firms of flaws in their software. At times, Project Zero members have threatened to disclose flaws publicly in order to pressure firms to patch the holes in their programs.

Ultimately, better cybersecurity is unlikely to be simply a question of resources alone. "No doubt there are companies that should be devoting more resources to cybersecurity," says Josephine Wolff, a cybersecurity expert at the Rochester Institute of Technology who studies the costs of cyber incidents. "But often when you retrace where things went wrong after a breach, the problems arise not from how much or how little a victim spent on defending itself but rather from what they spent their resources on."

Hackers for Hire

There is certainly no shortage of cybersecurity options for firms, governments, and individuals to choose from. Firewalls, antivirus software, and encryption, to name a few, are all aimed at keeping bad actors away from sensitive systems and data. As with the walls, gates, and moat of a castle, firms often invest in multiple layers of cyber defenses — a strategy known as "defense in depth."

"We add as many barriers as we can in hopes that maybe the hackers won't be able to get in," says Summers of the University of Maryland. "And when they finally do get in, we always say that if we just had one more barrier, they wouldn't have been able to get through. But there's always going to be a way in."

In a 2016 article, Wolff described another potential problem with simply accumulating multiple layers of cyber defenses: It can be counterproductive. Different security programs may interact poorly or prompt responses from human users that defeat the purpose of the security. For example, requiring users to regularly update passwords can make systems harder to breach — unless it prompts users to keep track of a multitude of passwords on notes at their desk or to choose shorter, simpler passwords that are easier to remember.

Therefore, it is important to have contingency plans in place for when attackers do get through, says Summers. One way firms have tried to do this is by hiring skilled security personnel who can identify holes in defenses and respond to attacks in real time. These "white hat" hackers have many of the same skills as their criminal "black hat" brethren, and demand for those skills is high.

White hat hackers may work for firms or government agencies directly or freelance in the growing "bug bounty" market. A number of third parties manage payouts offered by tech companies for finding and reporting various types of software flaws. Rewards vary based on the severity of the flaw, from hundreds or thousands of dollars to over a million dollars in some cases. HackerOne, one of the largest platforms for bug bounties, has paid out more than $20 million since 2012. Other platforms also report year-over-year growth. Bugcrowd's total payouts grew 211 percent since 2016 to more than $6 million, and its average payout per bug rose to $451 from $295.

"It's a big market," says Libicki of RAND Corp. But it isn't the only market for hackers' services.

Understanding Cybercriminals

As is the case with physical security, cyber defense is inherently more difficult than offense. Defenders have to protect every conceivable entry point into a system; attackers only need to find one opening to succeed. And as the market for cyber defense has evolved, so has the market for cybercriminals.

"The hacker market — once a varied landscape of discrete, ad hoc networks of individuals initially motivated by little more than ego and notoriety — has emerged as a playground of financially driven, highly organized, and sophisticated groups," according to a 2014 RAND report.

Today's cyberattackers don't even need to be particularly tech savvy themselves. They can buy exploit kits designed by someone else and rent botnets by the hour to launch DDoS attacks, another source of revenue for skilled hackers. Such services, which sell for hundreds or thousands of dollars on the black market, can be broadly affordable for attackers and lucrative for underground coders. (See table.)

Just as the incentives for defenders matter for cybersecurity, so too do the incentives faced by attackers. In a seminal 1968 article, the late Nobel laureate in economics Gary Becker argued that criminals are rational economic agents, weighing the costs and benefits of their actions. For firms and governments concerned about cyberthreats, there are a variety of ways they might attempt to change the criminal calculus. For instance, given the right incentives for legal hacking, some hackers might be persuaded to trade in their black hats for white ones.

As a self-described ethical hacker himself, Summers has interviewed hundreds of hackers to better understand

what motivates them. "Many times, it's really the challenge that drives them more than anything else," he says. "I think that the bug bounty programs are just a little too focused on the monetary aspects. If you think about our economic system, there are many mechanisms that motivate people. Multilayered incentives for cybersecurity are really lacking."

Giving hackers more freedom to explore system exploits in a legal setting could bolster defense against malicious actors, but it might not necessarily reduce criminal activity. The anonymity of the Internet makes it hard to be certain that hackers aren't "double-dipping" in both legal and illegal markets. For example, Marcus Hutchins, a British hacker who helped stop the spread of the "WannaCry" ransomware attack in May, was recently arrested by the FBI and charged with developing and distributing other malware. (Hutchins has pleaded not guilty to the charges.)

Of course, carrots aren't the only way to change criminal incentives. Law enforcement can also raise the costs of cybercrime. In a 2016 operation, U.S. and European law enforcement agencies worked together to shut down thousands of domains associated with the Avalanche network, a major global provider of malware. Authorities also identified and apprehended key administrators of the network to ensure it couldn't immediately rebuild. According to a study by the Center for Cyber & Homeland Security at George Washington University, the Avalanche takedown operation temporarily disrupted the entire cybercrime ecosystem.

In addition to apprehending and prosecuting cyber criminals, law enforcement — through anti-money laundering laws and "know your customer" laws in the banking system — can also make it more costly for them to get at their profits. Hackers have also become victims of their own success and the forces of supply and demand within black markets. For example, the average value of a stolen credit card on the black market plummeted from $25 in 2011 to $6 in 2016, according to Intel Security. This may help explain the recent rise of ransomware, which seeks to sell stolen data back to the person often willing to pay the most for it — the victim.

Carefully weighing security options and reducing incentives for crime are two methods of managing cyberattacks. A third option is simply to reduce the opportunities criminals have to access sensitive data in the first place.

Something for Everyone

Black market prices for cybercrime tools and stolen data

Malware and Services	Price
Basic banking Trojan kit with support	$100
Password stealing Trojan	$25-$100
Android banking Trojan	$200
Ransomware kit	$10-$1,800
DDoS service, short duration	$5-$20
DDoS service, more than 24-hour duration	$10-$1,000
Consumer data	
Single credit card	$0.5-$30
Airline frequent flyer miles account (10K miles)	$5-$35
Identity (Name, SSN, and DOB)	$0.1-$1.5
Scanned passports and other documents	$1-$3

SOURCE: Symantec *2017 Internet Security Threat Report.*

Openness vs. Security

Rethinking who should have access to data and what should be accessible from the Internet lies at the heart of the digital dilemma.

"Today's attitude is largely that we want to have access to everything, and if that creates security problems, that's what we have firewalls for," says Libicki. "When an attack happens, the response usually isn't that we've made our systems too accessible, it's that we need to double down on security."

To be sure, reducing accessibility and interconnectivity would have costs, too, which would need to be weighed against the costs of cybersecurity and the costs of breaches. There is no doubt that the openness of the Internet has had tremendous economic and social benefits. Weighing the benefits of openness and interconnectivity against the need for security will likely be a matter of continuing deliberation in the coming decades.

"Cybersecurity is really a matter of three trade-offs," says Libicki. "How much are you willing to invest in security? How much loss are you willing to accept? And how much are you willing to change the way you do business?" **EF**

Readings

Ablon, Lillian, Martin C. Libicki, and Andrea A. Golay. *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*. Santa Monica, Calif.: RAND Corp., 2014.

Böhme, Rainer, and Tyler Moore. "The 'Iterated Weakest Link' Model of Adaptive Security Investment." *Journal of Information Security*, March 2016, vol. 7, no. 2, pp. 81-102.

Kunreuther, Howard, and Geoffrey Heal. "Interdependent Security." *Journal of Risk and Uncertainty*, March/May 2003, vol. 26, no. 2/3, pp. 231-249.

Wainwright, Robert, and Frank J. Cilluffo. "Responding to Cybercrime at Scale: Operation Avalanche — A Case Study." Center for Cyber & Homeland Security Issue Brief No. 2017-03, March 2017.

Wolff, Josephine. "Perverse Effects in Defense of Computer Systems: When More is Less." *Journal of Management Information Systems*, October 2016, vol. 33, no. 2, pp. 597-620.