To Improve Cybersecurity, Think Like a Hacker

JOSÉ ESTEVES, ELISABETE RAMALHO, AND GUILLERMO DE HARO

If you have any doubts about the need for a new corporate cybersecurity mindset, the daily news contains plenty of sobering evidence. Recently, Yahoo Inc., which was in the midst of a planned transaction to sell its core businesses to Verizon, disclosed that it had been the target of two of the biggest data breaches ever, with sensitive information stolen involving more than 1 billion user accounts in 2013 and 500 million in 2014[1]. In addition to highlighting Yahoo's cybersecurity vulnerability, the attacks have resulted both in a delay in the planned acquisition by Verizon and in a probe by the U.S. Securities and Exchange Commission about the disclosure of the breaches. [2]The incident raises broad questions about how cyberthreats affect mergers and acquisitions deals, and it could have an impact on disclosure guidelines and regulations.

In the past several years, the list of companies whose internal systems have been hacked has grown rapidly. In addition to hundreds of small and medium-size companies, it now includes such high-profile businesses as Target, JPMorgan Chase, Home Depot, Sony Pictures, Ashley Madison, and Yahoo. In many cases, cybersecurity breaches go on for weeks or months before they're discovered. Cybersecurity breach response times can be a crucial factor in the data breach scale, its mitigation, the determination of its source, and also future legal issues involving the disclosure period. Not only have the attacks in the past few years been costly for the companies, but they also shake the confidence of customers, shareholders, and employees. And no industry appears to be safe from attacks, regardless of the specific measures individual companies use to defend themselves.

As a result, spending on cybersecurity is poised to accelerate. Gartner Inc., the information technology (IT) research and advisory firm, has estimated that global spending on information security would reach $81 billion in 2016 and may grow to $101 billion by 2018, with the highest growth in security testing. [3]Unfortunately, investment in security measures is only part of the answer; traditional methodologies can only do so much. To be effective, executives in charge of cybersecurity need to adjust their mindsets and become as open and adaptive as possible.

To help companies respond to new types of threats, we have developed a framework that is informed by our understanding of the process hackers employ to attack an organization. We designed this framework in collaboration with expert hackers using the Delphi method, a structured technique that draws on the knowledge and opinions of experts. [4]We also relied on in-depth interviews with more than 20 experienced hackers. (See "About the Research.")

About the Research

We conducted a web-based study consisting of two rounds of surveys with 23 experienced hackers through an anonymous consensus-building process. The hackers list was obtained through a variety of methods: screening hackers offering their hacking

and cybersecurity services on the internet, people mentioned in the media, introductions from other hackers, recommendations from chief security officers who knew hackers, and individuals whom the research team knew. We asked hackers to label and prioritize the steps to perform a successful cyberattack. We subsequently conducted 17 in- depth interviews with panel experts to get more detail on the different phases of cyberattacks. The article is based on insights from our study, the interviews, and our own experience in cybersecurity and digital and information technology. In conducting our study, we used the Delphi method, which has been employed since the 1950s to obtain real-world knowledge. The method is based on several iterative rounds of questionnaires among experts to obtain data or test hypotheses. We used this approach to uncover the policies followed by hackers and to define what an adaptive cybersecurity strategy should be.

The Hacker Mindset

If organizations want to reduce the risk of external hacking attacks, they need to understand the hacker mindset. [5]In other words, companies need to comprehend the expertise of successful hackers to anticipate and confront attacks. Companies such as Facebook Inc. and Microsoft Corp., for example, have even hired hackers. [6]

To think like a hacker, you need to know the traits that characterize a competent and sophisticated hacker. Hackers tend to be highly skilled and intelligent and enjoy taking risks. They typically have backgrounds in computer science and have been labeled geeks for many years. Many successful hackers have good social and communication skills that enable them to manipulate people to release essential information or to perform critical actions. [7]

Many hackers are drawn to the possibility of earning thousands or possibly millions of dollars. They are accustomed to operating on the black market and committing crimes far away from where they live. They generally enjoy the adrenaline rush they get from taking high-stakes risks. Indeed, many hackers have nerves of steel — not much frightens them. Although it used to be common for hackers to work independently, few of today's hackers operate alone. They are often part of an organized hacking group, where they are members of a team providing specialized illegal services such as credit card or loan fraud, theft of intellectual property or personally identifiable information, identity theft, or counterfeiting documents. [8]

Thinking Like a Hacker

Fully protecting a company's data is no easy task. Dan Chenok, a former chairman of the Information Security and Privacy Advisory Board for the U.S. National Institute of Standards and Technology, has asserted: "The only way to 100% protect yourself from attacks is to turn off your computers.[9]" However, learning to think like a hacker can help your organization anticipate what a hacker might do and then take actions to reduce those risks. So, what is a hacking mindset, and how should it influence the way organizations approach cybersecurity?

We found that hackers actually have two different mindsets during different stages in an attack: explorative and exploitative. (See “How Hackers Approach an Attack.”) In the initial stages of an attack, hackers typically use an exploration mindset that combines deliberate and intuitive thinking and relies on intensive experimentation. For example, an experienced hacker will not attack a new system a company has just activated. He or she will prefer to wait and continue to search for the weakest link (such as a vendor, a new employee, or a situation that is not in compliance with the organization’s security standards). Once access to a system is gained, hackers rely on an exploitation mindset to meet their goals — for example, to gain as much information for profitable resale as they can. This strategy of exploration followed by exploitation typically involves four steps; the first two steps focus on exploration, and the third and fourth emphasize exploitation.

How Hackers Approach an Attack

To protect their organizations, companies need to understand how hackers go about their work. Our research suggests that hackers’ attacks typically involve four steps: identifying vulnerabilities; scanning and testing; gaining access; and maintaining access. The first two steps primarily emphasize an exploration mindset, and the third and fourth steps involve efficiently exploiting the access the hackers have gained.

Step 1: Identifying Vulnerabilities

Hackers are patient, studious, and clever. If they think your company is worth attacking, they will examine it thoroughly for weaknesses, surveying the network information, organizational information, and security policies. This process of gathering information is known among hackers as foot printing. They may also study your suppliers and other contractors that your company works with, as well as your subsidiaries. Before launching a cyberattack, hackers will map out the target network and systems and take note of all holes and vulnerabilities, potential entry points, and any security mechanisms that could be hurdles. At this stage, information such as server names, IP addresses, and user accounts can help them prepare the attack. As noted earlier, hackers also attempt to interact with company insiders who might have critical information that would not be easily obtained under normal circumstances and that could help the hackers gain access to company systems.

At this stage, a hacker’s most important characteristics are curiosity, patience, and communication and social skills. Recognizing this, you need to turn these characteristics to your company’s advantage: Be curious about your systems and how they relate to any vulnerability. In 2014, JPMorgan Chase & Co., one of the biggest U.S.-based banks, was reported to have suffered a cyberattack that compromised the data of 76 million households and 7 million small businesses. Although login information, passwords, user IDs, birth dates, and Social Security numbers were not compromised in this attack, other information that can be used for identity theft — names, email addresses, postal addresses, and phone numbers — was exposed. How did this happen? Most big banks use two-factor authentication, which combines static passwords with codes dynamically

generated by physical devices. Unfortunately, JPMorgan's IT security team failed to update one of its network servers to enforce two-factor authentication, leaving the bank vulnerable. [10] Hackers used this weakness, together with stolen credentials from a bank employee, to gain access to some 90 servers inside the company.

Companies can help protect themselves by adopting an iterative and adaptive process and making a point of conducting a high-level "footprint" of their systems on a regular basis. In addition, they should make sure that employees are well informed on policies regarding sharing of information and offer them periodic reminders about the various ways hackers obtain information. For example, if someone unknown begins to interact with a bank employee in a friendly way, maybe that person's purpose isn't so friendly.

Step 2: Scanning and Testing

After a hacker has broken into your network, weaknesses in the applications running on your systems could become avenues for further unauthorized access. Hackers often use scanning tools on applications running on a company's system once they enter. Cumulatively, small security vulnerabilities and design weaknesses can add up to major security holes.

To protect your company, you should identify potential weaknesses once you have created a footprint of your systems. Examine every element (hardware, software, and protocols) of the company's network. In testing your network's security, evaluate cases of use and misuse from as many angles as possible, and run penetration tests for your applications as a "power user" — or better yet, as a hacker — as opposed to as an average user.

Failure to take such measures could expose you to a cyberattack, which is what happened to TalkTalk Telecom Group PLC, one of the largest providers of broadband and phone service in the United Kingdom, in October 2015. The data breach exposed records of more than 150,000 customers. In the wake of the incident, the company lost customers, and it was hit with a £400,000 fine by the U.K. government. The government criticized TalkTalk's failure to implement basic cybersecurity measures such as software updates and regular system monitoring, thereby making it relatively easy for hackers to break in.[11]

Step 3: Gaining Access

Among the factors that influence a hacker's chances of gaining unauthorized access to a particular system are the system's architecture and configuration, the hacker's skill level, and the initial level of access the hacker is able to obtain. For example, hackers often contact organizations by telephone, a "phishing" email campaign, a forged email message, or instant messages asking individuals for login and password credentials, usually by pretending to be someone with credibility (for example, a senior company officer or a help desk technician).

At Target Corp., a retailer based in Minneapolis, Minnesota, hackers broke into the corporate network using stolen credentials from a third-party vendor who had provided air-conditioning services. They then installed malicious software (commonly called "malware") to siphon customer information from the company's networks and point-of-sale system in more than 1,800 brick-and-mortar stores in the United States. The malware the hackers of Target used is available on cybercrime forums for about $2,000. The hackers had explored a variety of ways to enter Target's system before identifying the entranceway through the vendor. Once inside Target's network, the hackers gained access to cash registers in stores.[12]

The tactics the hackers used against Target were unusual. At Anthem Inc., one of the largest health insurers in the United States, hackers used a stolen login and password to steal up to 80 million records of personal information pertaining to customers and employees — even the company's CEO — in 2015. [13] Once on the network, they obtained personal information such as names, Social Security numbers, birthdays, addresses, email addresses, and employment information (including income data) — all of which can be quite valuable in the black market for the purpose of identity theft.

To protect your company, you need to consider how a hacker could gain access to your organization's systems, based on the information you have collected in the first two steps. While those steps were designed to identify security vulnerabilities, this third step is geared toward exploiting them, or what's known in the hacker world as "owning the system." [14]

On Feb. 5, 2016, hackers sent emails with links to malware to employees of Hollywood Presbyterian Medical Center in Los Angeles. When an employee clicked on one of the links, the system locked and disabled the hospital's electronic communication. For more than a week, the hackers had unfettered access to Hollywood Presbyterian's data (although it was reported that no data was taken). The nightmare ended only after the hospital paid a ransom of 40 bitcoins, valued at the time at about $17,000, at which point the hackers sent them a digital decryption key to unlock the system.

Hackers tend to play on both sophisticated technical knowledge and communication skills to breach company security. If you are equally sophisticated in your knowledge of common hacker tactics, you can mount an effective defense. An awareness campaign that alerts your employees, contractors, and third-party users to common hacker strategies should be a critical component of that defense.

Step 4: Maintaining Access

Hackers try to retain their ownership of the system and access for future attacks while remaining unnoticed. Sometimes they "harden" the system from security personnel (and even from other hackers) by securing exclusive access and uploading a piece of code that's known as a "backdoor."

Once hackers "own" a system, they can use it as a base camp for launching new cyberattacks. [15] An owned system is often referred to as a "zombie" system. In the final

stages of an attack, hackers often cover their tracks to avoid detection by security personnel and remove evidence of hacking, to avoid legal consequences. Skilled hackers use to their own advantage their technical knowledge of how systems detect wrongful activity.

Therefore, it is critical for organizations to remain vigilant for suspicious activity in system logs and to ensure that monitoring systems are always up to date.

Putting the Hacker Mindset to Work

Once companies are familiar with the basic requirements, what should they do to protect the organization from cyberattacks? We believe effective cybersecurity practices need to be implemented both from the top down and from the bottom up. In support of this approach, we have developed five recommendations.

1. Get senior management on board. Sustained support from senior management is crucial to ensuring that action plans are in place to mitigate the risk of cyberattacks. The message needs to come from the top down that "we" as a company need to be more secure so that staff is more likely to engage. No matter how technically competent the IT department is, it can't change the vision of the company. Rather, senior management needs to ask for complete buy-in, hold periodic meetings with line managers, and deliver the message from the top down.

In order to get executive-level decision makers on board, it's important to emphasize the role of cybersecurity in addressing the market, privacy, technology, and regulatory risks and demands. To do this, top managers may need to explain how the cybersecurity strategy enables business objectives and initiatives and highlight how effective security governance can enhance the interests of all stakeholders (customers, business units, employees, and auditors) in a cost-effective manner.

It is also critical to demonstrate that the company's long-term profitability and resilience are contingent upon security. Companies should create a security communication plan for the whole organization that includes content aimed directly at executives and that gets updated on a regular basis. The material should include guidelines and processes on how to manage and communicate about security breaches that may arise.

2. Design a security strategy. As we have noted, technology alone is not enough. Companies must address cybersecurity from both technological and nontechnological perspectives. In many organizations, the people aspect of cybersecurity is one of the weakest links. Security experts recommend adopting a "threat- centric" and operational security model that looks at security from a hacker's perspective. This requires looking at cybersecurity from both inside out (to understand what employees, strategic business partners, and third-party vendors are doing within their organizations and how they are interacting with high- value assets such as systems, facilities, and data) and outside in (to consider what an enemy might see when scoping out weaknesses from the outside). The latter is often referred to as "turning the map around," and the goal is to ensure a

comprehensive approach to mission planning and to help the company prepare for actions an enemy may take in the future.[16]

Executives and information managers should examine how their information systems are currently managed to assess their level of cybersecurity, and they should determine how secure each asset needs to be. They need to assess whether they have the right competencies and whether they have the right organizational design to anticipate and respond to potential cybersecurity threats.

In developing strategies, companies need to make choices: whether to build full-fledged in-house security capabilities, rely on external experts, or adopt a hybrid approach. According to Stephan Somogyi, security and privacy product manager at Google Inc., "no company can do everything well." For many companies, he recommends hiring external contractors so that the companies can "focus on their core competencies while taking advantage of the scale and skills of those that specialize in information security."[17]

3. Build security awareness. Effective security awareness training is essential. Raising cybersecurity awareness is critical, and every part of the organization should become familiar with cybersecurity best practices. All employees who have access to confidential information, whether they are in sales, marketing, human resources, finance, or senior management — even temporary staff — should receive cybersecurity awareness training.

Companies should encourage behaviors and processes that integrate information security into daily routines, and they should be sure to explain why it's important. Some companies are approaching cybersecurity training in ways that are similar to training for ethics and regulatory compliance. A few, such as Salesforce.com, are attempting to improve security-related behavior with gamification programs. According to Patrick Heim, the company's chief trust officer, employees who participated in its security-related gamification program "were 50% less likely to click on a phishing link and 82% more likely to report a phishing email." [18]

4. Create alliances. Recent data breaches show that skillful hackers can replicate successful attacks. Once hackers identify one security threat and exploit it, oftentimes they reuse the methodology to attack another target. Given this possibility, it's important for IT security staff to coordinate and share information within their organization, within their industry, and even with their competitors. Thus, it's important to create alliances with other companies and with government agencies.

The private and public sectors need to come together to address the cybersecurity challenge. The North Atlantic Treaty Organization (NATO) has called on members to build alliances to combat cybercrime. [19] By joining together, private businesses will be able to develop more comprehensive cybersecurity strategies more economically.

5. Keep abreast of and follow best practices. Many recent data breaches show that security policies are meaningless unless companies have a rigorous, continual way of monitoring compliance. Cybersecurity threats are constantly shifting as new security vulnerabilities are identified and new types of malware are created. Sometimes, even older threats that were thought to be under control rear their heads with a vengeance. The only way to confront modern cybersecurity threats is to keep defensive processes up to date, continually train personnel, stay current on the state of information security, and use control-enabled tools to proactively detect, analyze, and respond to incidents.

Although hackers are always looking for new ways to break in, organizations are also getting better all the time at "knowing their enemies." Some go so far as to invite hackers to identify vulnerabilities. In March 2016, for example, the U.S. Department of Defense launched a four-week bug bounty program in which participants were asked to use their hacking skills to break into selected U.S. Department of Defense public web pages in exchange for prizes and recognition. More than 250 participants submitted at least one vulnerability report, and more than half of the vulnerabilities were "legitimate, unique, and eligible for a bounty," said then-Secretary of Defense Ashton B. Carter. [20] (Mission-facing systems were not included in the program.) Other organizations, including MIT, also use bug bounties [21] along with more traditional approaches to cybersecurity.

New approaches to cybersecurity — and new threats — will undoubtedly continue to evolve. Cybersecurity is a game of cat and mouse in which the cat always makes the first move. But the more you can think like a hacker, the better able you will be to protect your organization.

About the Authors

José Esteves es profesor asociado de sistemas de información e innovación digital en IE Business School en Madrid. Elisabete Ramalho es jefa de estrategia de clientes programáticos para Europa, Oriente Medio y África en Google Inc. Guillermo de Haro es profesor asociado de economía aplicada en la Universidad Rey Juan Carlos en Madrid.

References

1. V. Goel and N. Perlroth, "Yahoo Says 1 billion User Accounts Were Hacked," New York Times, Dec. 14, 2016, www.nytimes.com; S. Fiegerman, "Yahoo Says 500 Million Accounts Stolen," Sept. 23, 2016, http://money.cnn.com; and D. Shepardson, "Verizon Says Hack 'Material,' Could Affect the Deal," Oct. 13, 2016, http://www.reuters.com.
2. H. Kuchler, "Yahoo Data Breach Will Delay $4.8bn Verizon Deal," Financial Times, Jan. 23, 2017, http://www.ft.com; and "Yahoo Says the SEC Is Investigating Its Recent Data Breaches," Fortune.com, Jan. 23, 2017, http://fortune.com.

3. R. Contu, C. Canales, S. Deshpande, and L. Pingree, “Forecast: Information Security, Worldwide, 2014-2020, 2Q16 Update,” Aug. 25, 2016, http://www.gartner.com.

4. N. Dalkey and O. Helmer, “An Experimental Application of the Delphi Method to the Use of Experts,” Management Science 9, no. 3 (April 1963): 458-467.

5. C.S. Dweck, “Mindset: The New Psychology of Success” (New York: Random House, 2006).

6. J. O’Dell, “How 7 Black Hat Hackers Landed Legit Jobs,” June 2, 2011, http://mashable.com.

7. R.J. Anderson, https://en.wikipedia.org/ wiki/Ross_J._Anderson, “Security Engineering: A Guide to Building Dependable Distributed Systems,” 2nd ed. (Indianapolis, Indiana: Wiley, 2008).

8. “Underground Hacker Marketplace Report” http://javascript:rp-2016-underground-hacker-marketplace-report) April 2016, http://www.secureworks.com; V. Goel and N. Perlroth, “Hacked Yahoo Data Is for Sale on Dark Web,” New York Times, Dec. 15, 2016, http://www.nytimes.com; and D.L. Leger, “How Stolen Credit Cards Are Fenced on the Dark Web,” USA Today, Sept. 3, 2014, http://www.usatoday.com.

9. A. Jeng, “Minimizing Damage from J.P. Morgan’s Data Breach,” SANS Institute, March 15, 2015, p. 3; and “Senior Managers Account for Greatest Information Security Risks: Survey,” Jan. 7, 2014, http://www.securityweek.com.

10. T.S. Bernard, “Ways to Protect Yourself After the JPMorgan Hacking,” New York Times, Oct. 3, 2014; D. Rushe, “JP Morgan Chase Reveals Massive Data Breach Affecting 76m Households,” Guardian, Oct. 3, 2014; M. Goldstein, N. Perlroth, and M. Corkery, “Neglected Server Provided Entry for JPMorgan Hackers,” New York Times, Dec. 22, 2014; and E. Glazer, “J.P. Morgan CEO: Cybersecurity Spending to Double,” Wall Street Journal, Oct.10, 2014.

11. “TalkTalk Gets Record £400,000 Fine for Failing to Prevent October 2015 Attack,” Oct. 5, 2016, http://ico.org.uk; and P. Sandle, “TalkTalk Lost More Than 100,000 Customers After Cyber Attack,” Reuters, Feb. 2, 2016, http://www.uk.reuters.com.

12. P. Ziobro, “Target Breach Began with Contractor’s Electronic Billing Link,” Wall Street Journal, Feb. 6, 2014; and B. Krebs, “Non-US Cards Used at Target Fetch Premium,” Dec. 13, 2013, krebsonsecurity.com.

13. “Letter From Anthem President & CEO, Joseph Swedish,” Feb. 6, 2015, http://www.myrha.org; D. Walker, “Exclusive: Mandiant Speaks on Anthem Attack, Custom Backdoors Used,” Feb. 5, 2015, http://www.scmagazine.com; and C. Terhune, “Anthem Data Breach Poses a Big Test for Its CEO,” Los Angeles Times, Feb. 12, 2015, http://www.latimes.com.

14. K. Zetter, “Why Hospitals Are the Perfect Targets for Ransomware,” March 30, 2016, http://www.wired.com; and B. Barrett, “Hack Brief: Hackers Are Holding an LA Hospital’s Computers Hostage,” Feb. 16, 2016, http://www.wired.com.

15. K. Graves, “CEH: Official Certified Ethical Hacker Review Guide: Exam 312-50” (Indianapolis, Indiana: Wiley Publishing, 2007).

16. Based on the military concept of a “kill chain” (a systematic process to target and engage an adversary), Lockheed Martin Corp. developed the “cyber kill chain” model that details each step of a cybercriminal’s operation from reconnaissance to actions on objectives. Many companies have adapted the cyber kill chain model to address their own risks. See E. Hutchins, M. Cloppert, and R. Amin, “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains,” Leading Issues in Information Warfare and Security Research, vol. 1 (Reading, U.K.: Academic Publishing International Limited, 2011), 80-106.

17. S. Somogyi, “Security and Privacy Product Manager at Google Inc.,” http://www.google.com.

18. S. Somogyi, interview with authors, Feb. 2, 2016.

19. L. Wood, “Boost Your Security Training With Gamification – Really!,” July 16, 2014, www.computerworld.com.

20. L. Thompson, “Cyber Alliances: Collective Defense Becomes Central to Securing Networks, Data,” Sept. 19, 2014, www.forbes.com.

21. L. Ferdinando, “Carter Announces, ‘Hack the Pentagon’ Program Results,” June 17, 2016, www.defense.gov.

22. The MIT Security Bug Bounty Program is a student-founded project, run with the school’s Information Systems and Technology department. It can be found at https://bounty.mit.edu.