WHITE PAPER

EXECUTIVE RISK

Protecting Your Organization from Cybercrime

SANDRA K. CARROLL, ESQ.
Vice President
Strategic Risk Advisor – Executive Risk
Hylant

HYLANT

hylant.com

EXECUTIVE RISK

Protecting Your Organization from Cybercrime

The major breach that's about to cripple your company's operations didn't start in the executive suite at your headquarters. It didn't slip in through one of your call centers or sneak past a sales rep using an insecure airport Wi-Fi node between flights. Nor was it triggered by carelessness on the part of a supervisor in your North Alabama production facility.

It began in Jarrod Carver's off-campus apartment. You never met Jarrod, but the marketing team in your Schenectady office says he was the best intern they've ever had. In fact, they were so impressed with his ability to craft amusing social media posts they gave him a company email account. That was two summers ago, and this morning, when Jarrod decided to see if that account was still live, he opened his inbox. He glanced at an old email about updating passwords and clicked on the link it contained, giving a pair of hackers in Bratislava the opportunity to plunge your company into a chaotic event.

A COMMON MISCONCEPTION IS THAT ... DATA IN THE CLOUD CANNOT BE AFFECTED BY CYBERCRIMES. HOWEVER, THE CLOUD IS NOTHING MORE THAN A COLLECTION OF NETWORKED COMPUTERS IN MULTIPLE PHYSICAL LOCATIONS THAT ARE POTENTIALLY VULNERABLE.

Cybercrime encompasses a bewildering, fast-growing array of criminal activity involving computers, computer networks and the increasing number of network-enabled devices often referred to as the "internet of things" (IoT).

The many types of cybercrimes are carried out by a broad mix of individuals and organizations. Besides hackers who prowl for vulnerabilities in companies' computer systems, there are thieves who seek personal information they can resell to other criminals, spies seeking intellectual property on behalf of foreign governments, terrorists who hope to create major disruptions and even some companies conducting shady "intelligence" activities to better understand their competitors. All these bad actors use creativity and innovation to try to stay a step ahead of security experts.

Financial and Reputation Damage

While corporate IT teams wage a constant and generally effective effort to stop and deter cybercriminals, successful high-profile attacks capture headlines and public attention. The Insurance Information Institute reported 1,108 data breaches in 2020, affecting over 300 million people. Large breaches during 2021 included more than 280 million customer records left accessible by Microsoft and the ransomware attack that put Colonial Pipeline out of business for six days, with severe impacts on the East Coast's gas supply. Volkswagen of America and Facebook also experienced breaches during the year. And in late 2020, the SolarWinds breach may have given criminals access to more than 18,000 government agencies.[1]

Beyond the financial cost to the affected organizations and their customers, these incidents often cause significant damage to the reputations they have worked so diligently to create in the marketplace. Although the organizations may not be culpable for the attacks, the perception among customers and the public is that they failed to adequately protect the information that had been entrusted to them.

Cybercrime's Many Types

Those who commit cybercrimes generally either target devices and networks directly, or they try to use devices and approaches such as phishing to facilitate crimes. Major examples of cybercrimes affecting organizations include:

- DDoS Attacks. A distributed denial of service attack involves overwhelming a network or site to shut it down.
- Botnets. Criminals use malware to infect large numbers of devices and then use networks of the infected devices to perform malicious activities.
- Phishing. Emails containing attachments or URLs are sent to unwary users. When users click on them, they may be prompted to provide confidential information such as passwords or unknowingly download malware.
- Exploits. Hackers develop and sell "kits" that can be used to gain control of a computer by exploiting vulnerabilities in popular software.
- Ransomware. By using malware, hackers access and encrypt files, demanding a ransom be paid in exchange for a decryption key.[2]

As criminals gain experience with these techniques, they adapt and refine them. For example, in the early days of ransomware, hackers would encrypt only a handful of current files, so organizations with robust backup plans could escape unscathed. Today's more sophisticated ransomware users will study an organization's network at length and encrypt more files, including the backups.

Today's more sophisticated ransomware users will study an organization's network at length and encrypt more files, including the backups.

In the first half of 2021, the average ransomware payment reached $570,000, an 82 percent increase over the prior year. The highest demand was for $50 million and the largest confirmed payment was $11 million. Besides encrypting data, the actors behind ransomware are also starting to publicly release sensitive information, launch DDoS attacks on victim's website, and even contact the victim's customers if they fail to make the ransom payment.[3]

The Federal Bureau of Investigation does not advocate paying ransom, noting that some organizations do not receive the promised decryption key and that successful ransomware attempts encourage criminals to make more attacks or allow those criminals to fund other illicit activities.[4]

The Safe Cloud?

A common misconception is that an organization storing its data in the cloud cannot be affected by cybercrimes such as breaches and ransomware. However, what we refer to as the cloud is nothing more than a collection of networked

computers in multiple physical locations. While cloud operators may claim superior security and might have highly sophisticated defenses, their systems are potentially vulnerable.

Biggest Vulnerability

We opened this paper with a scenario in which an incident resulted from a former intern unwittingly clicking on a link in a phishing email. It's a scary concept, but it's no scare tactic. Verizon regularly issues a technical analysis of data breaches, and their 2021 report concluded that more than 85% of breaches involved a human element.[5]

In other words, your organization can implement an entire suite of security solutions, backup programs and other strategies to keep criminals out of your systems, and all those efforts can be foiled by a single employee (or ex-employee who hasn't been removed from your network) clicking on a link in a phony email.

Developing a Response Plan

Given the sheer number of attempted cyberattacks, it's not a matter of whether your organization is likely to face cybercrime, but when it will happen. Given that perceived inevitability, it's critically important to prepare for how you will respond to a breach or other crime. The most practical way to do that is to create an incident response plan.

Just as your company has a safety plan that includes steps to take if a fire breaks out in one of your facilities or what you'll do in the event of an active shooter in your office, you need a formal plan detailing how you'll react if the company is disrupted by a cyber event. In fact, because such a disruption is far more likely than a fire or a violent act, that incident response plan is even more critical to your organization's continued health and operations.

Your response plan should consider the most likely types of cyberattacks and detail the worst-case impacts they would have on your operations and data. It may be useful to conduct a tabletop exercise in which everyone who would be involved in the defense and recovery effort is presented with different scenarios and talks through the process step by step. Such exercises may call attention to gaps in procedures, conflicts in responsibilities, and duplicated efforts. As the ideal response to each scenario is determined, save it in writing so others will know what to do when faced with the situation.

INCIDENT RESPONSE PLAN

Just as your company has a safety plan that includes steps to take if a fire breaks out in one of your facilities or what you'll do in the event of an active shooter in your office, you need a formal plan detailing how you'll react if the company is disrupted by a cyber event.

What Not to Do

When organizations want to get back to business as quickly as possible, they may be tempted to immediately wipe their networks and restore from the most recent backup. That's a bad idea for a couple reasons. First, as discussed earlier, hackers are becoming more sophisticated and more likely to infect backup systems as part of ransomware attempts. Second, wiping the networks eliminates all the tracks and traces forensic experts might be able to use to identify the source of the attack and the specific methods the hackers used to gain access. It's like cleaning a room in which a murder occurred before the crime scene technicians arrive.

Another common mistake is not using off-site backups frequently enough. Backing up your organization's data to a nonconnected site is a wise move, but if you only do that monthly, an attack may mean losing up to 30 days' worth of data. Any additional cost or hassle involved in more frequent off-site backups is probably well below what recovering from a single incident would involve.

Critical Component: Training

Because employees and their actions may be the greatest vulnerability for cyber events, training them about the risks and the importance of their own role is vital. Even the most attentive employee can be fooled by a well-crafted phishing email, especially when wading through a deep stack of emails or under high levels of stress.

Strategies such as sending fake phishing emails and following up with employees who click on the links can help. Two training strategies that have worked well for some organizations are sending smaller amounts of training materials more frequently and developing an incentive program that recognizes and rewards people for doing the right things. For example, instead of scolding the handful of employees who fall for the phony phishing email, complimenting those who weren't taken in (and giving them rewards such as credit for the company store) reinforces the correct behavior.

The Executive's Role

Data breaches and cyber events create significant direct costs, but that's just the beginning. In today's litigious environment, they also generate significant financial risk for executives and directors, as aggrieved customers and shareholders seek compensation for what they perceive as a lack of oversight and/or failure to meet SEC disclosure standards. For example, Yahoo was forced to pay nearly $145 million in liability claims and regulatory matters related to its data breach, and CEOs at Target and Equifax resigned after their organizations encountered cyber issues. Global data breaches in 2020 reportedly cost companies an average of $3.86 million per breach.[6]

Cyber risks carry significant legal and regulatory implications, so boards and leadership teams need to devote regular attention to discussing how those risks will be avoided, managed, mitigated, or insured. The National Association of

CYBER RISKS CARRY SIGNIFICANT LEGAL AND REGULATORY IMPLICATIONS, SO BOARDS AND LEADERSHIP TEAMS NEED TO DEVOTE REGULAR ATTENTION TO DISCUSSING HOW THOSE RISKS WILL BE AVOIDED, MANAGED, MITIGATED OR INSURED.

Corporate Directors (NACD) published a handbook on oversight related to cyber risks, urging leaders to think of cybercrime as a risk management issue involving the entire enterprise, instead of seeing it solely as the responsibility of the IT operation. NACD points to the National Institute of Standards and Technology (NIST) Cybersecurity Framework as an excellent starting point for developing an enterprise-wide program.[7] Most state cybersecurity laws, like Ohio's 2018 legislation, provide for safe harbors against claims in data breach litigation where companies conform to cybersecurity frameworks such as NIST.

A Never-Ending Effort

The inherent problem with most controls related to cybercrime is that they are reactive, based on crimes that have already been committed. Organization leaders can't be expected to outguess what the next brilliant cybercriminal is planning, nor can they anticipate all the potential vulnerabilities in the technologies their companies increasingly depend on. The only solution is to maintain vigilance about cyber risks, remain informed about developments in cybercrime, and ensure that these issues are a regular part of agendas and planning.

SOURCES

[1] Insurance Information Institute
https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime

[2] "Types of Cybercrime," pandasecurity.com
https://www.pandasecurity.com/mediacenter/panda-security/types-of-cybercrime/

[3] Palo Alto Networks, Inc.
https://www.paloaltonetworks.com/blog/2021/08/ransomware-crisis/

[4] Federal Bureau of Investigation
https://www.fbi.gov/investigate/cyber

[5] Verizon 2021 Data Breach Investigations Report
https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf?

[6] Insurance Information Institute, op. cit.

[7] Tyler Cybersecurity
https://www.tylercybersecurity.com/blog/cybersecurity-roles-and-responsibilities-for-the-board-of-directors

September | 2021