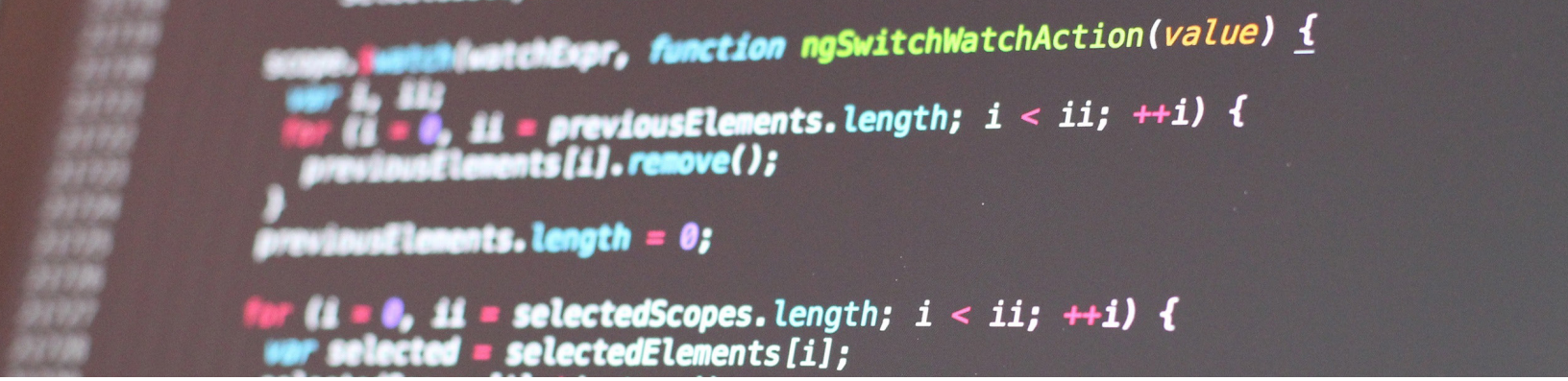


Cyber Attacks

By David Wasson
Vice President, Cyber Liability Practice Leader

Cybercrime. Hardly a new phenomenon, but the rising number of attacks against mid-sized businesses and the sophistication with which they are deployed make this a dangerous time. According to Cybersecurity Ventures, a cyberattack occurs every 40 seconds, with hackers illegally accessing sensitive employee data, using a company's servers for criminal activity or simply shutting an organization down.[1]

These attacks are common and often costly. According to Cisco Systems, more than half of mid-sized companies have experienced a hack. Of these, 20 percent of the organizations estimated the cost of the breach between $1 to $2.5 million. These costs include ransom demands, legal services and IT consultants.

Even if a breach does not result in actual monetary loss, the loss of consumer trust and subsequent public relations nightmares (Marriott International, Yahoo!, and Equifax are just a few that come to mind) are equally onerous. According to Worldplay, 46 percent of businesses said they experienced a loss of reputation and erosion of brand value after they were hacked.

Furthermore, businesses may be liable if sensitive information obtained during an attack is exploited, opening the door to lawsuits from customers and employees alike.

A combination of cybersecurity and insurance is necessary to modern commerce. Without it, your organization runs the risk of severe disruption and loss of income.

WHAT CYBER CRIMINALS WANT

Ransomware is still the most popular form of hacking. Criminals use social engineering (a method of hacking which involves an employee opening a suspicious email and clicking a link or attachment) to install malicious code (malware), which allows hackers to infiltrate firewalls and company servers, leaving business information inaccessible. To regain access to their data, the only option that many businesses have is to pay hackers. Ransom payments are expensive, a cost that is compounded by the loss of productivity during the lockout.

Beyond ransomware, new motivations such as "cryptojacking" are on the rise. Cryptojacking uses malware installed on a company's server to mine cryptocurrency (i.e., Bitcoin), resulting in server slowdown (or destruction) and levying massive power bills. This fast growing form of hacking affected 25 percent of companies in 2018.[2]

However, money is not the motivation for all hackers. Cybercriminals can include nation-states and hacktivists, all motivated by political agendas. One example is the recent allegations against the Chinese government, who allegedly infiltrated giant tech companies such as Amazon and Apple to steal information on American citizens.

WHO IS AT RISK AND WHO IS PREPARED?

While all companies are in danger of an attack, not all industries carry equal risk. Some sectors experience more attempted hacks than others. As a result, organizations in these industries tend to be more prepared for cybercrime. Conversely, the fewer hacks an industry experiences on aggregate, the more vulnerable they are.

Take, for instance, the entertainment industry. According to Verizon's Data Breach Investigation Report, entertainment companies had 7,188 attempted cybercrime incidents in 2017. Of those, only 33 attacks successfully infiltrated firewalls. When you consider the 2014 Sony Pictures attack executed by the North Korean government, these strong security protocols make sense. Nobody wanted to be the next Sony, which led to entertainment organizations of all sizes implementing proper protection measures.

Conversely, other industries experience fewer attacks. However, the attacks that do happen are more devastating. That is because industries that are not targeted as often have fewer security defenses. Simply put, many organizations become complacent and skimp on cyber protection. Construction companies, for example, see fewer incidents, but almost all of them become breaches. The same holds true for the healthcare, financial and retail sectors.

This suggests that many companies only address cybersecurity after a major attack occurs or they themselves are targeted. For these companies, it is often too late.

METHODS OF HACKING

How do criminals infiltrate companies and install malware?

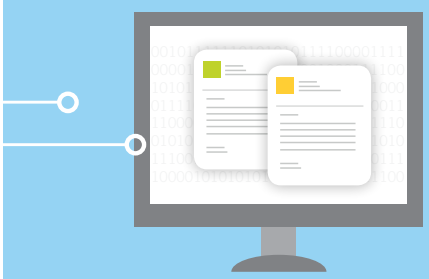
> Phishing

The common term for email-based social engineering is "phishing," with the attachment or link acting as bait. More than 70 percent of cyber attackers used emails designed to look trustworthy to deliver malware.[3]

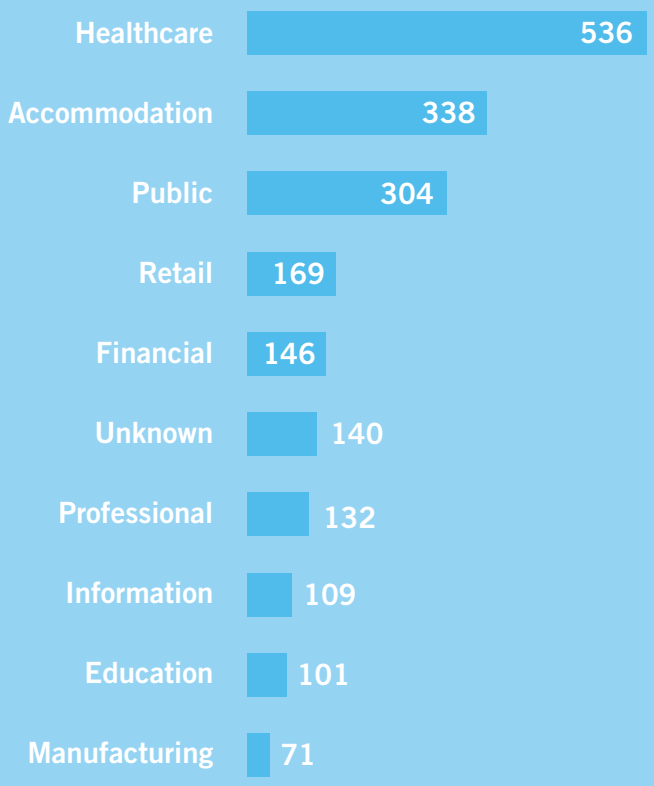
For every email received from a clearly fake account offering a free cruise, there is a more sophisticated criminal sending an email from what looks like an official company letterhead, from what appears

70%

of cyber attackers used **emails designed to look trustworthy to deliver malware.**



2018 Breaches by Industry



Verizon, *2018 Data Breach Investigations Report*

to be a real person. While there may be typos or strange text atypical of an official communication, the emails look real enough. In these scenarios, it is easy for someone in a rush or not paying attention to assume what they are opening is from a legitimate source.

> Pretexting

Like phishing, pretexting involves emails from suspicious accounts. Where the two diverge is in the desired interaction. Instead of asking the recipient to click on a link, the goal is for them to engage in a series of emails. This back and forth builds trust between criminal and target, especially when the target believes they are speaking with an executive or CEO of their company.

Malware is rarely the goal of pretexting. Instead, bad actors focus on convincing an unwitting employee to give up passwords or sensitive company data/information. In this sense, pretexting is like the notorious "Nigerian Prince" scams. Criminals promise royal riches beyond your wildest dreams, but the mark needs to send the bad actor money first to a bank account they control.

Like phishing, though, pretexting is far more sophisticated. Consider the following example: Employee John received an email from CEO Jennifer at the company where he works. A big conference was on the horizon, and Jennifer needed help. John asked what he could do, and Jennifer emailed back requesting that John buy gift cards for every attendee. Jennifer advised John that he should put the gift cards on his personal credit card, and once John emailed the passcodes, Jennifer would reimburse the expense.

Unfortunately, John did not know the emails from Jennifer were coming from a criminal posing as the CEO. While there were giveaways like blurry photos, small typos and an email URL that was different from the company's official address, John trusted the emailer because of the exchanges between the two.

> Malware

Social engineering often paves the way for the first domino to fall in a cyber attack. As soon as one computer or mobile phone is infected, bad actors can easily install malware, giving them access to a company's servers and network.

Criminals are especially interested in employee W2s, which are readily accessible once a breach has occurred. W2s are valuable because they provide all the information criminals need to commit tax fraud—social security number, date of birth and salary information.

PREPARING FOR AN ATTACK

Criminals send thousands of emails every day, hoping one person will click on a bad link. Modern cybersecurity techniques are necessary to protect business operations, but even the most robust security will not protect from every attack. That is why organizations must prepare their staff, educating on how to spot suspicious emails and where to report them.

CREATING A SECURE CULTURE

Security starts with company culture. From a knowledgeable workforce to IT solutions, executives should focus on a top-down approach to cybersecurity, which requires buy-in from board members and executives. While many executives may understand the risks cybercriminals pose, the potential of an attack is an abstract concept, one that is difficult to place a monetary value on until a hack occurs.

However, the cost of cyber protection—both security infrastructure and insurance—pales in comparison to what a company under attack could experience. According to a study by Malwarebytes, around 33 percent of businesses across the world are infected with ransomware, and one in five shut down operations immediately after criminals encrypt company data.

RISK ASSESSMENT AND CYBER LIABILITY INSURANCE

When considering cyber security, insurance brokers will complete a risk assessment, helping a company better understand their cyber vulnerabilities. Knowing where your deficiencies lie is the first step to creating and managing strong cyber security steps.

Of course, truly effective cyber security starts with an open, transparent culture. Companies should encourage reporting of both opened and unopened phishing emails. Too often phishing attacks go unnoticed because of concerns about the repercussions from management. A prosecutorial environment could leave an organization vulnerable to attack because it disincentives open communication.

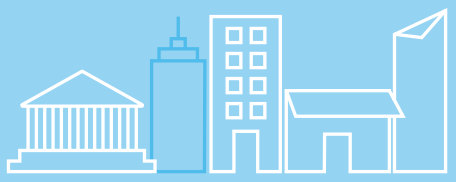
Very few people are likely to open a phishing email, but those who do may click on a link or attachment more than once. Criminals only need one opening and they can often rely on the four percent of people who frequently open malicious emails.

PHISH YOUR EMPLOYEES

A culture of open communication can reduce the risk of cyber attacks, but preemptive training measures should be implemented as well. A two-pronged approach to identifying vulnerable employees and cyber education can stop hacks before they start.

1 in 5

businesses shut down operations immediately after criminals encrypt company data.



According to a Malwarebytes study

Many companies run phishing campaigns on their employees. Through a third-party vendor, emails are sent company-wide that resemble phishing attacks. The emails look official, but usually come from a strange address and exhibit the markers of a bad actor's attempt to attack a company—typos, suspect links and strong language.

You will receive a detailed account of everyone's interaction with the email—if it was deleted, reported to IT or a link was clicked. Instead of shaming those who failed the phishing test, think of it as an opportunity to train those employees that need it. It is possible many do not know what phishing is, or they are not aware of the harm that could come from opening the wrong attachment.

WHEN ALL ELSE FAILS

Businesses can and should implement simple security features like two-factor identification and hiring a cyber expert. Since criminals exploit older technology, all operating and security systems need to remain up to date.

But even the best-laid security plans can not cover every contingency. Criminals are developing new ways to break through firewalls, and there is no way of knowing how successful they will be in the future. That is where cyber insurance comes in, to help mitigate disaster should a breach occur.

Companies must address cybersecurity with the assumption that an attack will happen to them. Whether criminals are out to steal money or sensitive information, companies that are not prepared could face millions in damages.

Interested in learning more about cyber insurance? Contact your Hays Representative today or email us at info@hayscompanies.com.

Hays Expert: David Wasson

David Wasson is a Vice President and leads the Cyber Liability Practice at Hays Companies. He has over a decade of experience in Technology and Cyber Liability, including five years underwriting the coverage. In addition to a BS in Finance from Saint Louis University, David also holds CIPP/US and CIPM designations from the International Association of Privacy Professionals and was an inaugural recipient of the CCIC designation through Chubb and Carnegie Mellon University.

www.hayscompanies.com

1. Cybersecurity Ventures, *Cybercrime Damages $6 Trillion By 2021*
2. Secure Channels, *25% of Companies Affected by Cloud Cryptojacking*
3. Verizon, *2018 Data Breach Investigations Report*