FEATURE

COULD CYBERATTACKS SHUT DOWN YOUR BUSINESS?

BY MARY LOU JAY

YOU WOULD NOT PUT YOUR VALUABLES AT RISK BY LEAVING YOUR HOME OR YOUR OFFICE UNLOCKED AND UNSECURED. SO WHY WOULD YOU LEAVE YOUR COMPUTER NETWORK, HARDWARE AND SOFTWARE SYSTEMS WIDE OPEN AND UNPROTECTED?

Unfortunately, this is the case for too many contractors. Cybercriminals can take advantage of these vulnerabilities to steal data, prevent companies from accessing their files and disrupt company operations. These activities can impact building contractors of every size, costing them hundreds of thousands of dollars and, in some cases, putting them out of business.

Hackers use a variety of methods to break into their targets' networks and systems.

"The number one problem we have is phishing. People are getting emails that take them to malicious sites, or they go to sites that are fake but look like legitimate logins to systems like Office 365 or Gmail," said Nick Espinosa, an expert in cybersecurity and network infrastructure. Espinosa, the "chief security fanatic" at Security Fanatics, will be a featured speaker at the national 2022 ABC Convention in San Antonio.

Phishing attacks can lead to spoofed emails, where hackers send fake emails that appear to come from employees or managers in a company or from its vendors.

"We had a case in the construction industry where somebody spoofed the financial advisor to the organization, and for about a month and a half they moved over a million dollars out of the company's account to another account," said Espinosa. The hackers included personal and professional details, gathered through their access to the company's email, which made them appear legitimate. The transferred money was long gone by the time the contractor discovered the fraud.

Hackers also send emails posing as vendors requesting payment; they send "updated" banking information along with their invoice. The contractor pays the invoice and may not discover the fraud until the real vendor requests payment.

Malware that triggers ransomware attacks is frequently inserted into a company's email via a phishing attack. Once the ransomware has encrypted a contractor's files, the company must make a payment — often six-figure amounts these days — to get the key to decrypt the data. Some companies go out of business because they cannot pay the ransom or never recover from the incident.

Disgruntled or dismissed employees may sell their company logins and passwords on the dark web, enabling intruders to easily break into the system. An unscrupulous competitor may use a hacker to break into another contractor's network, get bid information, and then use that knowledge to win bids. That can result in major loss of business.

Contractors are favorite targets of cybercriminals because they often do not make the investments in technology and cybersecurity like other industries. "In other industries, they have a lot of vulnerabilities within their environments. Vulnerabilities are most often a result of inconsistent patch management practices and limited knowledge of all devices in the environment," said Philipp Bohren, senior vice president, cybersecurity services, 7 Layer Solutions Inc. In addition, contractors are under time pressure to meet contractual deadlines, so if they suffer a ransomware attack, they tend to pay more quickly and with less negotiation than many other types of businesses.

Some cyberattacks are targeted at certain companies, but many are not. "A lot of these attacks are very opportunistic. [Cyber thieves] have developed bots or programs that crawl the internet and look for open doors, and then they go in and exploit those," said Bohren.

Cybersecurity Risks

Cybercrooks try many different routes to get into contractors' networks.

"Mobile phones are the largest growing threat sector by far," said Espinosa. "People do not really perceive the mobile phone as a computer, but it absolutely is that, and it is on your network a lot of the time."

Remote working has opened new avenues for infiltration. Hackers get into unprotected home networks and enter the company's systems from there, or they may insert malware into shared business files that ultimately infect the company's entire network.

Shared work platforms like project management software could be another avenue for entry. Espinosa said that contractors should be checking third-party vendors' compliance with cybersecurity standards (NIST, SOC2, and ISO 27001, for example) to ensure that their data is protected on these platforms.

Some general contractors are now trying to reduce the threats to their networks by contractual means. "We are seeing many general contractors (GCs), especially on the infrastructure and public side, put very specific cybersecurity-related compliance into their contracts," said Ronnie Kurlander, head of the construction and real estate practice at **Hartman Executive Advisors**. "They are requiring subcontractors to use certain controls or to align with best practices like those from the National Institute of Standards and Technology (NIST)." He added that too many subcontractors are simply signing such contracts without understanding the cybersecurity requirements and obligations they place on their businesses.

Take Action

The first step in creating a good cybersecurity defense is for company leaders to educate themselves about current cybersecurity threats. The next step is to understand what they are risking if their business gets shut down by a cyberattack.

"You have to understand foundationally what your actual operating expenses are," said Espinosa. "If all your computers went down, how much money are you losing per hour?" The calculations would include salaries you are paying to people who cannot work, the lost payments from customers because crews cannot enter their time, the costs for vehicles and for rented tools that cannot be used. Contractors need to look at reputational risk and how the attack would impact its ability to get future work.

Contractors need an assessment of their vulnerabilities and the effectiveness of their current cybersecurity defense systems. While large contractors may employ a full-time cybersecurity professional, that is not always an option for smaller firms. Many small to mid-size businesses rely on third-party IT providers (also known as managed service providers) to handle their cybersecurity, but that is usually not adequate.

CYBERSECURITY STATS

- On average, a company will not detect a cyber intrusion for up to **212 days**, and it will take them another **75 days** to fully resolve the issue. *(IBM)*
- The overall number of data compromises in 2021 was up more than **68 percent** compared to 2020. *(Identity Theft Resource Center - ITRC)*
- Pilfered credentials caused **20 percent** of the data breaches (personal identifiable information, passwords, etc.) *(IBM)*
- In 2020, **36 percent** of all cybersecurity breaches were related to phishing. *(Verizon)*
- Ransomware-related data breaches have **doubled** in each of the past two years. At the current rate, ransomware attacks will surpass phishing as the number one root cause of data compromises in 2022. *(ITRC)*
- In 2020, business email compromise scams were responsible for more than **$1.86 billion** in losses. *(FBI)*

“Managed service providers often utilize low- to mid-range solutions that are not cybersecurity centric; they are data-security-centric,” said Espinosa. Effective cybersecurity solutions cover a much wider range of vulnerabilities. Small companies can employ cybersecurity specialists on a part-time basis to make that expertise more affordable. Ask the companies what certifications they have; their experts should have their own certifications and not rely on the certifications from the third-party providers they are working with.

Espinosa recommends the use of continually updated, enterprise-level security technology, which will proactively protect a company’s entire IT infrastructure. The technology should cover on-premise and cloud-based files, secure any endpoints (other devices connected to the network) and check third-party software on an ongoing basis. While these solutions may be 10 to 20 percent more expensive than mid-level protections, the defense they provide is 1,000 times more effective, he said.

Every contractor also needs a plan for dealing with a cyberattack if it gets hit. “One way that we work with our clients is to establish a security incident response team. Based on data that we have seen from 2021, organizations that have an incident response plan, in place and tested, experienced a 75 percent less cost of recovery, on average, than firms that did not have a tested plan in place,” said Rick Arthur, chief information security officer at Hartman Executive Advisors.

A good backup strategy is integral to an effective recovery plan. Companies should have multiple backups in different locations, including on-site and in the cloud. These backups must be separated from the company’s regular network. To prevent hackers from infecting backup files with ransomware, Espinosa recommends using immutable storage, which does not allow any alterations to the data being stored.

One advantage of cloud storage is that it can store files in multiple locations. If a disaster like a fire or tornado destroys one storage location, the data can be retrieved from other locations.

Kurlander said that companies need to test these backups regularly to ensure that they are working. He has worked with companies that set up their backups years ago, never checked them, and discovered during a cybersecurity review that they have not been working.

Create a Culture of Cybersecurity

People are always the weakest link in cybersecurity protection. Even if a company has all the right protection systems in place, an employee can open the door to cyberthieves by inserting into their company computer a USB stick that contains a file infected with malware. They may share passwords with coworkers, click on a phishing email link that promises free COVID-19 tests or post a written list of their passwords on their computers.

Employees need ongoing education about the methods that cyber attackers are currently using, with an emphasis on the very real financial risks that cyberthieves pose to their company and to their own livelihoods. “This is not a one-point-in-time assessment,” said Bohren. “Cybersecurity is really a journey.”

There are many cybersecurity training programs available today. Some include fake phishing emails, designed to remind employees not to open a file or click on a link. If employees do take the bait, it is an opportunity to remind them of why they need to be more careful.

CYBERSECURITY INSURANCE

With the costs of data breaches growing every year, insurance companies are decreasing coverage and increasing requirements for cybersecurity coverage, according to Remmie Butchko, managing partner, **Georgetown Insurance Service, Inc.**

Social engineering attacks — where employees get tricked into revealing information and/or transferring funds — and ransomware are experiencing the most claim activity. “These are also the areas where insurers are decreasing coverage and increasing deductibles. You are seeing situations where insurance companies used to have $1 million coverage and they are now adding supplements limiting that to $200,000 or even $100,000,” he said.

Not all general liability policies will cover the costs if a contractor is responsible for a customer’s loss of data. That can occur because a contractor hits an electric line and accidentally wipes out data storage systems or because a breach of the contractor’s computer networks leads to its customer losing data. “Contractors need to ask specifically for electronic data coverage in their general liability policies,” Butchko advised.

Insurers are now requiring companies that want cybersecurity coverage to implement security measures such as multifactor identification (MFA) for network access. MFA requires both a password and a code (usually sent to a mobile phone or an email account) to sign in to a company’s network.

To help contractors get the cybersecurity coverage they would like, Georgetown Insurance has partnered with insurance companies that will do a cybersecurity check once the contractor has submitted an application. “By applying to get the insurance, you get a free cybersecurity assessment,” Butchko said.

As with safety programs, it is essential that leadership shows that they are committed to cybersecurity and serious about embedding it into the fabric of their operations. "When you have CEOs or senior leaders who do not follow the policies that have been established, it creates a lackadaisical approach to cybersecurity," said Arthur.

"It really takes a whole organization to move in the right direction, so it is essential that the executive team understands the importance and the necessity of cybersecurity," said Kurlander. "The leadership team needs to drive cybersecurity down into the culture to make sure that everyone feels some obligation and responsibility for securing the organization."

Becoming cybersecure is not something that you do overnight. "It starts with an assessment, an understanding of where you are and where you want to be, and then defining the road map. The road map helps you tackle your priorities to get the projects done," said Arthur.

Protecting your organization against cybersecurity threats may appear an overwhelming task and an expensive one. But, when you wonder whether you can really afford a good cybersecurity program, consider how much more it will cost you, in the long term, if cybercriminals successfully target you. ■

RANSOMWARE THREAT CONTINUES TO GROW

Nick Espinosa, from Security Fanatics, spends a lot of time these days working with companies that have been hit by a ransomware attack. While he can assist many businesses, he also has seen cases where a third-generation family business leader must tell the company's founder that a cyberattack has forced them to close.

Ransomware is on track to surpass phishing as the number one cause of data compromise in 2022, according to the Identity Theft Resource Center (ITRC). Even if you pay the ransom, it does not mean you will be back in business just like before. On average, companies recover only 65 percent of their data even after they pay a ransom.

Security company Sophos reports that in 2021, the average ransom paid by mid-sized organizations was $170,404. But the real cost for a company is much higher — running around $1.85 million. That includes downtime, people time, device cost, network cost and lost opportunities.

CYBERCROOKS NOW USE RANSOMWARE IN FOUR DIFFERENT WAYS:

- They encrypt your data, and you pay a ransom to get the key to unlock it.
- They copy your data and threaten to make information public or sell it to other companies unless you pay. (This threat increased significantly in 2021.)
- They use your information to go after the data of companies that you are doing business with, then try to extort them by threatening to reveal their data.
- They will harass you by knocking out your website and/or using denial-of-service attacks to take down the internet in your office.

Following good file-backup procedures can help companies continue their business if cybercriminals encrypt their data. To prevent hackers from revealing your data publicly, Espinosa recommends using digital rights management (DRM) solutions to protect your data. With DRM, only authorized users can get into the data; hackers will not have that authorization.