Cyberattacks and Ransomware and Hacks – Oh My!

Best practices to mitigate risk for companies and communities in this age of ever-increasing cyber threats

By Julianne B. Goodfellow / *National Multifamily Housing Council* and Valerie M. Sargent / *Broadband Communities*

Increasingly, the news about cyberattacks is that they disrupt not just single companies but also the organizations with which those companies do business. One of the most notorious cyberattacks of 2020 was the hack on SolarWinds, an information technology firm in the U.S. Foreign hackers went undetected for several months, allowing the attack to spread to SolarWinds' client list, which included private companies (80 percent of the cyberattacks) and the U.S. Department of Homeland Security, the Department of the Treasury and other government agencies.

In June 2021, a ransomware attack brought Colonial Pipeline Company, an East Coast–based fuel pipeline, to a halt. The event disrupted the economy – the company reportedly controls nearly half of the East Coast's gasoline, diesel and jet fuel flows – and showcased how slow and costly getting back up and running was. How did this happen?

Both attacks underscore that even companies with strong cyber defenses are vulnerable to cyberattacks. Multifamily owners, property management companies and apartment communities are finding themselves asking not just "Are we vulnerable?" but also "What can we do to better protect our broadband networks and business continuity if we are the victim of a cyberattack?"

RECOGNIZE THE WEAK LINKS

In early 2020, hackers believed to be directed by the Russian intelligence service accessed SolarWinds' software system and covertly added malicious code. A company that manages IT resources, SolarWinds regularly sent out routine software updates to customers' systems in March 2020. Unbeknownst to the company, that update contained malicious code that created a backdoor into customers' systems. From there, the hackers were able to install malware that allowed them to spy on the entities affected by the hack. It took nine months for a private company that was the victim of the hack to realize something was happening.

In the case of Colonial Pipeline, that ransomware attack was enabled by a compromised password. Companies that have employees who access the company network remotely should note that this breach was conducted via a virtual private network. According to a Bloomberg report, "The account was no longer in use at the time of the attack but could still be used to access Colonial's network … The account's password has since been discovered inside a batch of leaked passwords on the dark web. That means a Colonial employee may have used the same password on another account that was previously hacked."

These examples demonstrate that hacking can easily happen through a third party or may be the result of a security gap within the broadband network, including something as simple as a compromised password. Anyone who exists on the internet, does work within the cloud, or is connected online in any way is vulnerable. If it can happen at a governmental level or the most sophisticated tech companies, trust that it can happen to anyone, any company or any community.

REDUCE RISK WITH THESE TIPS

People often think of cyberattacks stemming from a suspicious-looking hacker hunched over a computer in a dark room somewhere, typing away to access the dark web and conduct clandestine operations. But there are many ways an organization can fall victim to a cyberattack, and many times vulnerabilities are created through day-to-day user or system errors. This may be because protections are weak or because

someone found extra security steps onerous, or even because an asset, such as a smart-home product or broadband network, lacked proper security. All vulnerabilities create potential entry points for rogue activity by cyber actors.

What steps should companies take to protect their technology assets? Here are 10 ways to mitigate cybersecurity risk and ensure systems and tools are in place to protect systems.

Segment information technology (IT) and operational technology (OT) networks. Organizations can face great vulnerability if networks aren't segmented. Segmentation limits an adversary's access beyond the initial entry point and protects other areas of the network. It also means that any access points provided to third parties or employees will be limited to what they need to access, reducing risk to the overall network. Keep common-area Wi-Fi traffic network separate from the office business network to help eliminate any vulnerabilities.

Back up data offline, and test it regularly. Too often, people using cloud technology think they are "safe" with everything backed up to the cloud. However, if technology malfunctions or malware is installed, files may not be backed up properly. Don't learn this the hard way and suddenly find that nearly 60 days of new files were lost because someone thought they were backed up to the cloud. When a computer ultimately crashes, it's too late for the reminder to supplement digital cloud storage with a physical backup.

Thoroughly vet the cybersecurity practices of supplier partners and third-party providers and understand liability and security responsibilities. When considering new technology, it's important to know all the assets to track, make sure firmware and software are updated, and have a third-party management program. Building a plan that ensures technology is supported for the full life cycle and that products no longer supported are removed from the network is important. Don't let a Colonial Pipeline incident happen by keeping old access points and information out there.

Use multifactor authentication for remote access to IT and OT networks. In the case of Colonial Pipeline, the combination of a compromised password and a lack of multifactor authentication likely led to the massive breach. Multifactor authentication provides an added layer of protection through a cybersecurity tool, creating an extra step to sign into an account. It could be something as simple as having the system text or email an access code. Users receive such requests on their phones or in their email, alerting them to attempted access if someone is trying to get into the system with their credentials.

Use strong spam filters to prevent phishing emails from reaching users. One of the most common cyberattack vectors is phishing emails. The malicious actor sends an email that is designed to dupe a user to click on a link or download an executable file. When a victim engages with the email, the malicious actor may be able to access a user's credentials, computer or organizational network. Some phishing emails are clearly from scammers, but phishing emails are increasingly sophisticated and include messages tailored to recipients. One frequent approach is to spoof the email address of a senior executive and request that the receiver sign a document or transfer money. But other phishing emails use simple techniques, such as offers for tickets to popular shows or events, and end up providing cybercriminals access.

Conduct an employee phishing prevention training program, including regular employee testing. Employee education is one of the most important ways to mitigate cyber threats. Training and education, along with testing, will help assess risks and determine whether there are vulnerabilities resulting from poor decision-making on the part of employees. Catching mistakes in a training exercise that allows retraining in any instances in which hackers might target employees is much better.

Filter network traffic, and block new malicious IP addresses. Companies that filter inbound and outbound network traffic can put security rules in place to filter that traffic utilizing IP address, port and protocol. This blocks any malicious IP addresses that are known threats or possible risks.

Have a program in place for software updates and patch management. With so many on-site employees, is management confident that communities regularly update all their computers on a timely basis and ensure that security patches can correct any errors in code? Humans often put things off to do later, so companies need regular programs to track updates with all employees. Employees often think that equipment is updating on its own. Some systems may have automatic updates in place, but others require manual updates. Established plans and processes help ensure systems are up to date and protected from new threats.

Install and maintain anti-virus and anti-malware programs. This is especially important so that security patch updates are installed and rolled out to users before there can be a threat to customers. Anti-virus and anti-malware programs also can catch potential intrusions and eliminate risk. If a credit card is expired or there is no regular plan for the renewal of these programs, they can lapse and create vulnerabilities for users and systems.

Consider cyber insurance. It can be extremely helpful to reduce financial impact and as a way to take a complete inventory of policies and practices. Cyber insurers have established checklists to respond to areas in need of attention. Checklists can guide companies in doing what they need to do. Many have found out how to improve their practices through their cyber insurance requirements. Be certain to look at what a policy covers regarding liability. For instance, if a third-party supplier has an event, who has liability within that situation? Where does liability fall, and what protects a company?

REMEMBER IT'S A CRIME

It's always better to be prepared and have plans in place before facing a cyber intrusion. Remember that law enforcement views cyberattacks as criminal activity and that a successful attack leaves a company as the victim of a crime.

Companies are strongly encouraged to build relationships with law enforcement in advance of an event or a cyberattack. Doing so provides excellent opportunities to find out what's happening, what threats exist, and how to work with peers when facing common threats. The sooner cyber-crime victims contact law enforcement after realizing funds are missing, the sooner they can use forensics to find out what happened and sometimes retrieve lost funds.

HELPFUL RESOURCES

Firms must stay up to date on developing, ever-evolving threats and emerging prevention and response measures. Here's a shortlist of useful resources to learn about threats and best practices.

For U.S. government resources to monitor current threats:

- **Stop Ransomware**
  www.cisa.gov/stopransomware
  U.S. Cybersecurity and Infrastructure Security Agency (CISA) alerts, current activity reports, analysis reports and joint statements from the nation's risk adviser
- **CISA Resource Hub**
  www.cisa.gov/cyber-resource-hub
  Professional, no-cost assessments that evaluate operational resilience, cybersecurity practices, organizational management of external dependencies, and other key elements of a strong cyber framework
- **US-CERT Current Activity & Vulnerabilities**
  https://us-cert.cisa.gov
  Regularly updated summary of the most frequent, high-impact types of security incidents and vulnerabilities

For building relationships with federal law enforcement and cyber professionals and participating in cyber threat information sharing/best practices:

- **InfraGard**
  www.infragard.org
  A public-private partnership between the FBI and U.S. businesses to provide education, information sharing, networking, and workshops on emerging technologies and threats
- **Commercial Facilities Cyber Working Group**
  www.infragardncr.org/commercialfacilitiescyberworkinggro
  The partnership between the real estate industry companies, InfraGard, and the Real Estate Information Sharing and Analysis Center (RE-ISAC) ❖

Julianne B. Goodfellow is vice president, government affairs for the National Multifamily Housing Council, and can be reached at jgoodfellow@nmhc.org. Valerie M. Sargent is a multifamily speaker, trainer and executive consultant and the multifamily news correspondent for ***Broadband Communities****. Contact her at valerie@bbcmag.com. For more information, visit www.nmhc.org, www.bbcmag.com or www.valeriemsargent.com.*