HAI Group®

Cybersecurity Playbook

Navigating Cybersecurity in Housing

Developed for housing leaders determined to thwart cybercriminals and protect their organization

HAI GROUP CYBER SECURITY RESOURCES

Contents

Cybersecurity doesn't have to be technical and overwhelming.

We're here to break it down.

Even the best-prepared housing organizations are vulnerable to cybercriminals seeking to hold data and systems hostage in exchange for payment. Since 2016, the U.S. has experienced around 4,000 ransomware attacks daily. Cybercriminals don't just focus on larger companies with deep pockets—70% of ransomware attacks affect businesses with fewer than 1,000 employees.

"Everyone is a target, and I cannot stress that enough," said Scott Stevens, chief information security officer of cybersecurity firm Integrity Technology Solutions. "Malicious actors are going to find ways to exploit whomever they can. When you look at housing organizations, they often don't have the resources to protect themselves."

Even if you train employees to recognize the signs of common cybersecurity attacks, keep systems patched, manage access to vital assets, and use the most sophisticated antivirus detection system, the risk of a cybersecurity breach remains. That's where your organization's cyber insurance coverage—or lack thereof—comes into play.

There are costs to insuring risks and funding cybersecurity enhancements. Still, those costs should be considered an investment, said Jonathan Hochman, founder of Hochman Consultants, an internet security and website development firm.

"If you're not proactive, you will inevitably be hit, and you will have major expenses responding to a data breach," Hochman said. "You have a loss of reputation. You have all kinds of problems. You have to pay for good security because it's the cheapest way to get along."

This playbook will help you identify your organization's cyber risks, understand the benefits of cyber insurance, and develop a cyber defense plan that will help prevent your organization from being caught off guard.

Ransomware Attacks on the Rise

Ransomware isn't new, but the threat it poses is becoming more common for businesses and government organizations alike. According to the FBI, "ransomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return."

Ransomware is a way for hackers to monetize their activities," said Scott Stevens, chief information security officer of cybersecurity firm Integrity Technology Solutions. "They take control of all of your data, all of your systems, everything that you have. Once they control it, they're going to pop up and offer to give you your information back—if you pay the ransom."

Housing organizations store sensitive resident data, or personally identifiable information (PII), making them targets for cybercriminals. Beyond encrypting this PPI so you can't access it, cybercriminals may threaten to leak this data unless you pay the ransom.

The FBI and most cybersecurity experts agree that ransomware victims should not pay.

"[Cybercriminals] are going to use every method that they can to put pressure on you to pay the ransom," Stevens said. "It's a challenging position to be in."

Stevens, who has over 30 years of cybersecurity experience, said he was involved in a situation where a business he was assisting decided to pay a ransom demand. A few minutes after the payment was sent, the hacker responded and demanded that the organization pay an additional ransom. The situation was resolved after the company agreed to a second, smaller ransom payment, but the situation also caused the business a week of downtime, Stevens said.

The surge in ransomware attacks can be partially attributed to the COVID-19 pandemic, said Richard Moore, CEO and founder of cybersecurity firm CyberSix. In 2020, ransomware attacks in the U.S. were up 600%.

"In the pre-COVID work environment, you could simply walk over to a co-worker's desk and ask them if they actually sent you an email you suspect of being a phishing attack," Moore said. "Working remotely doesn't provide that same defense."

Real-Life Ransomware Scenarios

The examples below show the impacts of ransomware attacks on housing organizations and the public sector:

- *An attack on a housing organization left 700 employees and some 55,000 residents temporarily without access to the organization's web portal. The hacker also leaked information about dozens of employees online.*
- *A cyberattack infected an entire county, taking the county's systems offline, according to the FBI. The county had backup servers, but the servers were also hacked because they weren't isolated from the county's main network. The county paid a $132,000 ransom, the FBI noted.*
- *Hackers infected a city's systems and demanded a $76,000 ransom. While the ransom wasn't paid, according to the FBI, it cost the city an estimated $9 million to remediate the attack and restore services.*
- *A housing organization had its financial data held hostage at a time when the data was necessary for reporting. The housing authority decided not to pay the ransom. The hack still cost the housing authority "both time and stress."*
- *A county's computer systems were infected after a user allegedly opened a malicious email link or attachment, according to the FBI. County officials decided to rebuild their systems rather than pay the $1.2 million ransom. The county spent $1 million on new equipment and technical assistance, the FBI said.*
- *A housing organization experienced two successive ransomware attacks, which the organization's leader described as "a nightmare." The attacks forced the organization's employees to retype and scan documents to recoup encrypted files.*

The Science of Social Engineering

From phishing to vishing to physical tailgating, social engineering attacks are on the rise—probably because they're so effective.

"Social engineers use the scientific method to analyze and understand social systems so they can design the appropriate methods to achieve the desired results in human subjects," said Richard Moore, CEO and founder of cybersecurity firm CyberSix.

Malware (a catchall term for malicious software) attacks such as ransomware are facilitated through social engineering, often using phishing schemes. Here's a brief scenario from the FBI:

> *In a phishing scam, you might receive an email that appears to be from a legitimate business and is asking you to update or verify your personal information by replying to the email or visiting a website. The web address might look similar to one you've used before. The email may be convincing enough to get you to take the action requested.*

Phishing is just one of several techniques used by social engineers, but it is common in business settings. This hacking technique is more than just a trick that people fall for, Moore said. “It’s actually based in science.”

Popular Social Engineering Techniques

- Phishing
- Spear Phishing
- Water-Holing
- Pretexting
- Diversion Theft
- Baiting
- Quid Pro Quo
- Tailgating
- Honeytrap
- Rogue

“A social engineering attack can deliver a significant payload,” Moore said. “In [ransomware] attacks, criminals use the scientific methods of influence to get someone in your organization to click on a link, visit a webpage, or open a PDF so they can access your systems and do physical and economic damage to the housing organization.”

Emails appearing to be from colleagues, associates, popular social media sites, banks, or IT administrators are commonly used to lure unsuspecting targets.

Spear phishing is similar to phishing, but it is a more targeted email attack with the goal of penetrating an organization’s defenses. There’s a personalized component to spear phishing.

Hackers conduct research to find out whom the target regularly communicates with, and use this knowledge to convince the target to click on a malicious link or attachment.

Once that link or attachment is opened, ransomware is automatically installed on the organization’s system.

Malicious social engineering can be prevented with employee training, Moore said. There are several security awareness training platforms that can provide virtual training on the newest social engineering tricks being deployed against companies.

“We’ve found that by mandating 2–3 minutes of training per quarter and 45 minutes of training annually, we have significantly reduced the threat of social engineering,” Moore said. =

Why Buy Cyber Liability Insurance?

It's common to assume your general liability insurance policy includes cyber liability. The reality is that these policies are separate but equally important in today's landscape. General liability coverage protects housing organizations from a wide range of exposures, including injuries and property damage, but isn't designed to handle the nuance of cyber risk.

For example, a cybercriminal might obtain and leak an organization's personally identifiable information (PII), including names, addresses, and Social Security numbers of residents or employees. A cyber liability policy can assist in notifying victims about the data breach—required by law in each state—by either providing the organization with a breach notification vendor or covering notification costs.

Any housing organization that waits until after it has experienced a cyber breach to shop for cyber liability coverage may have difficulty finding an insurance carrier willing to take on the risk.

A cyber liability policy can also help cover risk mitigation efforts and remediation and recovery costs, including legal, public relations, and IT expenses. Most general liability policies don't cover these aspects of a cyber breach or explicitly exclude them.

Without the proper cyber liability coverage, your organization could be left picking up the bill for a majority of breach-related expenses, if not all. Any housing organization that waits until after it has experienced a cyber breach to shop for cyber liability coverage may have difficulty finding an insurance carrier willing to take on the risk. If so, the carrier is likely to charge a higher premium.

Consider your organization's cyber risk

Before securing cyber liability coverage, organizations must identify potential risk factors, said Scott Stevens, chief information security officer of cybersecurity firm Integrity Technology Solutions.

"These do not have to be drawn-out projects," Stevens said of risk assessments. "This is something that you can legitimately do in a couple of days if you focus on what technology risks are out there."

Housing organizations should perform assessments at least annually, leveraging in-house expertise or a third-party service to examine operational, privacy, and security risks, he said.

The process can include steps like determining what kind of sensitive data the organization stores, how many employees have access to such data, and what type of data-protection measures are in place to mitigate risk.

Once risks are identified, organizations should mitigate them and ensure they're covered under a cyber liability policy.

A sampling of cyber liability coverages

While they differ by insurance carrier, the following coverages are some of the critical components of a cyber liability policy, according to Angel Fear, senior account executive at HAI Group:

Privacy and Network Security Liability

- As noted earlier, a cyber breach can lead to the disclosure of sensitive data. This coverage helps handle claims arising from such disclosures, Fear said.

Regulatory Proceeding

- If a data breach results in the violation of privacy law(s), state and federal regulatory agencies may have questions for your organization. This coverage helps cover costs related to investigations and proceedings brought against your organization, Fear explained.

Breach Event Costs

- According to Fear, this coverage assists with costs related to initial cyber breach consultations, call center services, credit monitoring, identification theft assistance, and credit/identity restoration services. She said this coverage could also help cover breach notification, IT forensics, and PR/crisis management expenses.

Business Interruption

- Downtime is not a good time for any business, especially housing organizations. Business interruption coverage helps with expenses and loss of income due to a network interruption, Fear said.

Cyber Extortion/Ransomware

- Ransomware is on the rise, Fear noted. Cyber extortion coverage provides resources to respond to ransomware cyber incidents (when your organization's data is held hostage and cybercriminals demand a ransom payment).

Cybercrime Enhancements

- Beyond the above coverages, there are enhancements your organization can include in its cyber liability policy, providing nuanced coverage for specific incidents such as:
    - social engineering;
    - phishing;
    - invoice manipulation; and
    - cryptojacking.

Enhancements aren't always available, and if so, they tend to be sublimited, notes Dan Burke of insurance brokerage Woodruff Sawyer. A sublimit places a maximum on the amount available to pay that type of loss. For example, if your organization has a $1 million cyber liability policy with a 25% sublimit on social engineering coverage, your organization would be limited to a $250,000 payout for that claim.

Assessing Your IT Needs

As cybersecurity attacks become more common in the affordable housing industry, it's critical that you assess your organization's information technology (IT) needs.

Your IT team serves as one of your frontline defenses against cybercriminals by:

- maintaining your computer network;
- training employees on various systems;
- providing technical support;
- assessing potential threats; and
- ensuring things run smoothly.

If a cybercriminal breaches your organization, chances are your IT team will be the first to notice, setting off a chain of time-sensitive events to pinpoint and remediate the incident.

Not all housing organizations are alike. Some prefer an in-house IT team, while others rely on consultants, or a hybrid model.

No matter the approach, it's essential that your organization properly vet your IT team's qualifications. If you're not an IT expert, it can be difficult to find the right questions to ask, said Richard Moore, CEO of cybersecurity firm CyberSix.

"These five questions are a good place to start," he said.

1. What certifications do the people who will work on my account hold?

In terms of cybersecurity certifications, Moore said, organizations should seek firms with CISSP (Certified Information Systems Security Professional) certified staff.

Certifications should also align with the platform and network tools your organization uses.

For example, if your organization uses Microsoft Office 365, the firm you select should ideally have someone on staff with MS 500 or AZ 500 Microsoft certifications, Moore said.

New certifications and those new to the industry should raise questions, Moore noted.

2. Has the firm ever had a security breach or been subject to a contractual breach?

Ask who has access to your organization's systems and their qualifications. Check if the firm is ISO 27000 certified (or equivalent). This certification covers information security management systems.

Request a copy of the firm's most recent SSAE 16 SOC II audit. This voluntary audit evaluates a firm's security, availability, processing, integrity, and privacy operations. A firm with no recent audits or a recent "unclean" audit should raise red flags.

The firm should also provide a copy of its information security policy, which outlines how an organization manages, protects, and distributes information.

3. Does the firm have direct knowledge of the housing industry?

An IT firm with experience in the housing industry is a plus, but not necessarily a requirement, Moore said. General IT and cybersecurity certifications are sufficient.

A firm with an understanding of the specific privacy concerns within the affordable housing industry is ideal. Government experience is also helpful, Moore added, especially for housing authorities.

4. Does the firm's contract include basic cybersecurity measures?

The firm should provide a security audit immediately to identify any critical vulnerabilities, Moore said.

"Ask questions about the security tools the firm is providing," he added. "Ask about monitoring for security events and how they correlate that information into data that the organization can use to make better cybersecurity decisions."

The firm should patch your system whenever software updates become available, actively monitor your network environment, and provide quarterly reports on the status of threats and security updates.

If the IT firm can provide training to employees to help avoid social engineering attacks, that's a bonus.

"Most IT firms do not have the right training expertise," Moore said. "Having a subject matter expert or platform that can support education is what all companies should be doing to educate their employees."

Developing Your Cyber Incident Response Plan

Despite your organization's best efforts to boost cybersecurity, not all incidents can be prevented. To prepare for and respond to these breakthrough attacks, your organization should develop a cyber incident response plan outlining steps to minimize losses, fix weaknesses, and restore services.

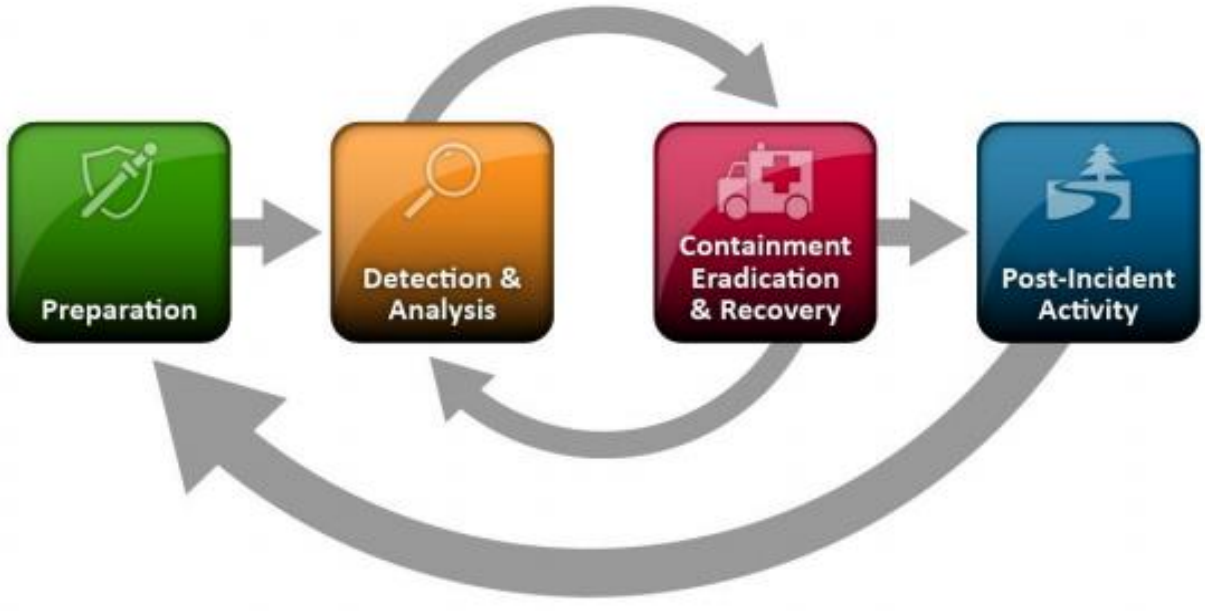
At a high level, this might not sound dissimilar to a business continuity plan. Your cyber incident response plan and business continuity process should be in sync. Responding to a cyberattack is a "complex undertaking" that requires "substantial planning and resources," according to the National Institute of Standards and Technology (NIST) Computer Security Incident Handling Guide.

The NIST guide lays out a four-phase approach for handling cybersecurity incidents:

- Preparation
- Detection and analysis
- Containment, eradication, and recovery
- Post-incident activity

Richard Moore, CEO of cybersecurity firm CyberSix, explains how housing professionals should approach each phase in developing their cyber incident response plan.

"Having a plan is one of the first steps in addressing cybersecurity, and it costs only time and effort," Moore said.



Preparation

During the preparation phase, develop a policy that defines what your organization considers a cybersecurity incident. Include any internal and external reporting requirements, including your insurance carrier's claim filing details. This policy should be used to inform the details of your cyber incident response plan, including the structure of your cyber incident response team and how often the group meets.

If possible, the plan should include different "playbooks" for different types of cybersecurity incidents.

"You should create playbooks for different cyber threats and one executive playbook to allow for smoother and less stressful approaches to incidents," Moore said.

Your incident response team should include employees or vendors with technical, legal, human resources, and communications expertise. Management should be represented, as should an employee from the department that was compromised.

Cyber incident response team members can be part- or full-time depending on the size of your organization and the frequency of cybersecurity incidents. You can also rotate members in and out of your incident response team and allow members to perform other tasks.

"Incident response teams should meet semi-annually at a minimum if no actual incidents have occurred to walk through and test out the playbooks," Moore said.

Prepare to prevent

A crucial part of the preparation process is ensuring mitigation efforts are in place to prevent successful cyberattacks in the first place. Moore suggests employee training through an in-house subject matter expert or your cybersecurity training vendor.

"Having a subject matter expert or platform that can support education is what all companies should be doing to educate their employees," he said.

Your in-house IT team or consultant should also:

- conduct periodic risk assessments of your system;
- patch your system whenever software updates become available;
- maintain network security and monitoring; and
- provide quarterly reports on the status of threats and security updates.

Moore suggests moving any on-premise equipment such as servers to a cloud computing service like Azure or AWS, because if your organization has limited in-house expertise, "no one is really taking care of your physical equipment, including updates and security."

Multifactor authentication (MFA), also called two-factor authentication (2FA), is a must-have for housing organizations, because it adds a layer of protection that makes it more difficult for cybercriminals to access your systems.

"MFA is a security enhancement that requires you to present two pieces of evidence—your credentials—when logging into an account," Moore said. "You probably used MFA in some form already: at the ATM, for example, when you put your bank card into the machine and it asks for your PIN."

Your credentials can fall into any of three categories:

1. Something you know (e.g., password or PIN)
2. Something you have (e.g., mobile phone)
3. Something you are (e.g., fingerprint)

To enhance security, your credentials must come from two different categories.

"Entering two different passwords would not be considered multifactor," Moore said.

Investigatory resources

Consider having a cyber forensics firm on retainer. Most organizations don't have the resources or expertise to diagnose a cybersecurity threat alone.

A forensics firm's primary objectives are to:

- investigate the source of the breach and contain potential threats;
- identify the extent of sensitive data accessed by cybercriminals; and
- fix vulnerabilities to prevent a similar breach from happening again.

External legal counsel should also develop a detailed timeline of events and communications, including crucial forensics details.

Consult with your internal legal counsel before entering into any agreement with an external service.

Media relations

Be prepared to handle media inquiries about any potential cybersecurity incident. Your cyber incident response plan should include procedures that comply with your organization's media interaction and information disclosure policies.

For example, many organizations find it helpful to designate a single point of contact and at least one backup. Consider conducting media training sessions for your entire incident response team that include mock interviews and press conferences.

During a cybersecurity breach, your incident response team should also maintain an incident narrative, preferably with oversight from external counsel to ensure any sensitive internal communications are shielded by privilege.

At a high level, the narrative should describe the initial point of entry, breach tactics, and crucial instances of data compromise. This narrative is a starting point for all external communications, including media, to ensure consistent and accurate messaging.

Detection and analysis

There's no shortage of cyberattack vectors that can affect your organization. Ransomware is a common attack, particularly in the housing industry, due to the personally identifiable information (PII) you collect and store. Determining if and how an attack occurred is often the most challenging part of the incident response process.

As noted in the previous section, your in-house IT team or consultant should monitor your network for signs of a breach. Employees trained in identifying common attack methods (e.g., social engineering tactics like phishing) should also report any unusual activity outlined by your cybersecurity policy.

If you identify a potential threat early enough, your organization may have an opportunity to avoid a breach by updating network settings/software, warning staff, and monitoring the situation closely.

If all signs point to a potential breach, your organization should contact a cyber forensics firm (ideally, this firm is already on retainer) to investigate. Your cyber incident response team should also notify internal and external stakeholders designated by your cyber incident response policy.

Law enforcement coordination

After a breach, notify law enforcement if it aligns with your organization's cybersecurity stance, Moore noted.

"When sharing information with law enforcement, I would recommend sending only the information necessary to conduct a criminal investigation," he said. "This should align with the organization's position on 'pursue and prosecute' or 'defend and contain.'"

Most law enforcement agencies that deal with cybercrime have anonymous submission platforms to share sensitive information without any repercussion to the organization. The NIST Computer Security Incident Handling Guide recommends contacting only a single law enforcement agency to avoid jurisdictional conflict.

Containment, eradication, and recovery

In this stage, your cyber forensics firm should work closely with your cyber incident response team to develop a containment strategy before an incident overwhelms resources or increases damage.

For example, NIST lists "sandboxing" as a form of containment in which cybersecurity experts monitor the attacker's activity in a contained environment to gather additional evidence. Before implementing a containment strategy, discuss the pros and cons with your organization's legal counsel and cyber incident response team.

Your forensics firm should also gather evidence, if possible, to help resolve the incident and assist with any potential legal proceedings. If necessary, the firm may eradicate components affected by the incident, such as breached user accounts.

Once your forensics firm remediates any outstanding threats, your IT team can restore your system to normal operations. In some cases, your organization may need to restore the system from a backup or rebuild it from scratch, which can be costly.

Post-incident activity

After the immediate threat is neutralized, housing organizations should perform "a postmortem analysis of what and who is impacted by the breach," Moore said.

Learning and improving

Your organization's postmortem analysis should also focus on learning and improving.

"Ensure that you have followed your playbooks, updated them based on any changes, and communicated clearly and with facts about what happened and how the organization responded," Moore said. "This is a defensive move to protect your reputation." Your organization should also ensure all processes are understood and well documented.

"For example, if you have a process for transactions and payments, you should never fall for the CEO sending you an email to transfer funds," Moore said. "That should alert you that someone is trying to surveil your environment."

Work with your IT team and forensic firm to repair gaps and vulnerabilities as soon as possible.

"The biggest mistake I see organizations making after the attack is actually doing nothing and thinking that the containment was all that was needed," Moore said.

Reporting

It's essential that your forensics firm attempt to determine whether cybercriminals accessed any personally identifiable information (PII), and if so, whom the organization may need to notify based on state regulations.

Every state has a law requiring notification of security breaches involving PII, such as Social Security numbers (refer to your state-specific breach notification law for details).

Notify your insurance carrier(s) and prepare to file claim information within the contractually required timeline. This should be a formal notification, by either ticket system or email, with the email added to the meeting minutes for your board of directors.

Moore noted that it takes most organizations about six months or longer to fully recover from a significant data breach.

"A formal written report should always be issued at the end of the investigation that concludes legally what happened and what the facts were," he said. "These reports should be non-opinionated and simply stated. Executive management and your legal counsel can determine what should be included in the overall final report, but facts are important to have while building a remediation plan."

Bolstering Your Cyber Defenses with Data Backups

Cybercriminals would like nothing more than to hold your housing organization's system and sensitive data hostage.

Their goal is to force you to pay a ransom to regain access and prevent data leaks. Even if you train employees on the signs of common cybersecurity attacks, keep your systems patched, manage access to vital assets, and use the most sophisticated antivirus detection system, the risk of a cybersecurity breach remains.

If cybercriminals breach your system, all isn't necessarily lost, as long as you have the right backup system in place, said Jonathan Hochman, founder of Hochman Consultants, a firm specializing in website development and internet security.

Three "big risks" neutralized by backups

A backup service provides the ability to recover data you need in the state you need it in. Backups are essential to your organization for more reasons than you might think.

"You have at least three big risks that you can take out by having a good backup for each computer," Hochman said.

1. *Ransomware/Cyber Breach*: If you get ransomware or malware in your system, you can wipe the system and restore everything from backup. While you should never rely on backups alone for cybersecurity, they're a must-have. Here's a fictional yet feasible scenario:

> *A housing authority employee receives what appears to be an email from the housing authority's executive director asking the employee to download and review a file. There's a warning that the email came from someone outside of the organization, and the executive director's email is slightly different. Still, the employee isn't paying attention and clicks the link.*
>
> *Unfortunately, the link includes ransomware. A cybercriminal encrypts the housing authority's system, rendering it useless unless the ransom is paid. The housing authority is prepared for such an attack. Instead of paying the ransom, which doesn't guarantee the breach will be resolved, the housing authority reverts to a backup stored on a cloud service. The organization regains access to its system and can continue operations.*

2. *User Error*: An employee might accidentally delete an important file or forget to save a file before closing it. If your organization has a backup process in place, the file can be quickly restored. While this scenario isn't as devastating as a cybersecurity breach, it can save valuable time and effort.

3. *Failure Point:* If your hardware experiences any failure, you can rest assured that your files are safe in the cloud and can be restored to new hardware.

In addition to the above, backups can be helpful during litigation. If you need to prove what data you did or didn't have at any given time, you can use your backup to re-create your system as of that date.

"It could actually be evidence that's useful to you," Hochman said.

Choosing the best backup service for your organization

There's no shortage of backup vendors available to your organization, but not all services are created equal.

There are several attributes of backup services that housing organizations should be on the lookout for, Hochman said.

Automatic

"A good backup is done automatically without human intervention," Hochman said. "Any system that depends on discipline is inevitably going to break down."

For example, if an IT employee or consultant who manages the backup process leaves, responsibility may not transfer smoothly.

"Then, you suddenly discover when you have a ransomware attack that your system hasn't been backed up in nine months," Hochman said.

> A good backup is done automatically without human intervention. Any system that depends on human discipline is inevitably going to break down.

Cloud-based

Your backed-up data should be stored offsite and completely disconnected from your system, so it's not exposed to the same risks as your network. In other words, your backup should be in the cloud (i.e., an internet-based data center).

"That way, if your network is overrun with malware, your backup is not affected," Hochman said.

Cloud services such as Azure and AWS allow you to store data without any common network dependencies. Different people should manage your onsite system and offsite backup.
"One risk you're backing up against is a disgruntled employee or an employee with malicious intent," Hochman said. "You have to assume that your head of IT might go rogue and decide to erase every server, and you need to protect yourself against that."

Preferably, the backup is remote and run by a reliable and responsive vendor.

"You want to make sure they're doing regular backups," Hochman said of backup vendors. "Make it part of their contract. You want to have a service-level agreement that says that in the event of a catastrophic failure, the vendor guarantees to restore your data from backup within a designated timeframe. If you can get that assurance, that's ideal."

At the very least, he added, the vendor should commit to responding to issues within a specific time frame.

Version history

If your backup vendor doesn't store older versions of your organization's system long enough, you could find yourself in a predicament. Cybercriminals don't always make it obvious when they've breached a system.

"Your data could be infected, and you may not know about it for some time," Hochman said. "You want to have at least 90 days' worth of backups, and maybe more."

If a breach occurred 31 days ago and your backup service only stores 30 days of your system's version history, your backup won't revert to a clean, breach-free state.

He noted that you don't necessarily need to back up your system every day during those 90 days.

Restore time

After a cyberattack, you want to restore your system from backup as quickly as possible. How long will that take? That's precisely what you should ask your backup vendor, Hochman said.

Your backup vendor should be able to provide a restoration estimate based on the amount of data they're storing. You only need to back up data and settings, Hochman noted. You don't need to back up operating systems and application files (e.g., Microsoft Windows, Microsoft Office, etc.), as your IT team can reinstall those.

"You need to have the actual step-by-step process in place to do a full restore," Hochman said. "In that moment of panic, you don't want to be starting your planning. You want to have it all written down."

If you know ahead of time how long it takes to restore your system, you can plan around that downtime and any potential negative impacts.

"In that moment of panic, you don't want to be starting your planning. You want to have it all written down."

Testing

A backup of your system isn't much help if it fails when you need it most. Backup testing isn't something your organization necessarily needs to worry about, but it's something to discuss with your backup vendor.

"You don't need to test your backups if you have a good vendor who specializes in backups because they test their system all the time," Hochman said.

Self-service

A backup service with self-service capability is ideal. It's common to rely on your backup to recover a mistakenly deleted Word document or Excel spreadsheet.

"There are many times you'll use it just to grab a single file," Hochman said.

Your IT team should be able to manage this process for your organization.

Backup tools at your disposal

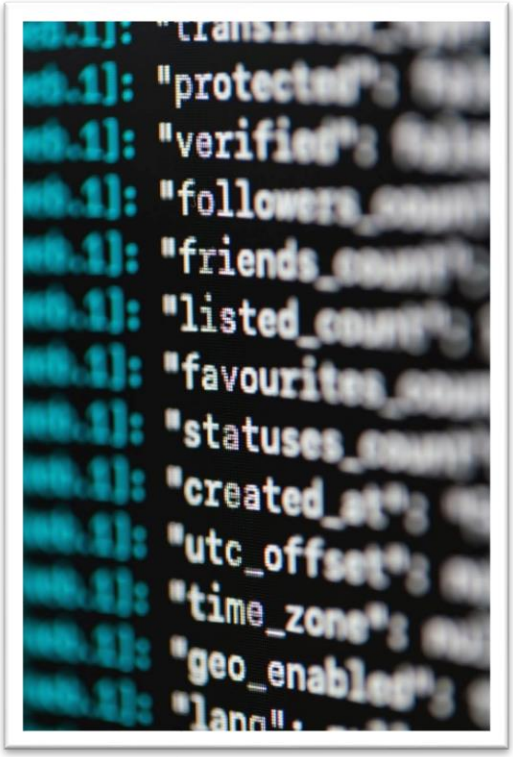
Whether your organization uses Windows or Mac software on its workstations, you have readily available cloud-based backup solutions at your disposal.

On the Windows side, take advantage of Microsoft OneDrive, said Hochman. For Mac workstations, iCloud (which you're probably familiar with if you have an iPhone) is a great backup option.

"Every computer eventually gets replaced," Hochman said. "When you replace your computer, you can erase it and restore the files and data from your backup on the new computer. It makes your migration from an old computer to a new computer very simple."

For backing up web applications such as your organization's website, Hochman designed a system called CodeGuard.

"It's designed for doing automatic backups of web server data, websites, and web applications," he said. "It can back up the code and the database."



Backups: Not the only answer to ransomware

Given the growth in cybercrime, there's a sense of peace of mind in having a backed-up system.

"When you get attacked by some malware scumbags, and they send you the ransom demand, you may think you can say 'go to hell, I've got backups—I'm going to restore everything, and I don't need you,'" Hochman said.

But it's not that simple, unfortunately.

"You don't want to rely on backups as your only defense against ransomware," Hochman said. "You should be doing everything you can because cybercriminals will not only lock up your data, but also leak your data. The backup is half the problem solved."

Often, attacks occur when software isn't patched or updated to protect against the latest vulnerabilities.

"If you pair your backing-up with only one other process that will keep you safe, it should be automatic application of patches and updates," Hochman said. "You want to be aggressive about applying updates and patches as soon as they come out. Backing up allows you to do that. If the patch somehow goes wrong and causes problems with your data, you have your backup."

Regular penetration tests should be conducted on your website, especially if the website is public-facing, accepts login and payment info, and stores any sensitive information. Your in-house IT team or consultant should facilitate these tests.

> "You don't want to rely on backups as your only defense against ransomware…. Just because you have backups doesn't mean you don't have to worry about other types of network security."

"As a general rule, if a website hasn't been tested before, and it's the first test, the website has vulnerabilities," Hochman said.

Organizations should be proactive in their approach to cybersecurity. There are costs to hiring vendors and funding security enhancements, but those costs should be considered an investment.

The Benefits of a Cyber Forensics Retainer

Among your priorities after a cyberattack is finding the root cause of the attack and then preventing further harm. Most organizations don't have the resources or expertise to diagnose a cybersecurity threat alone.

That's where a third-party cyber forensics firm comes in. Forensics firms specialize in collecting digital and physical evidence to uncover what happened during a cybersecurity breach.

A retainer is a fee you pay for services that span a specific period rather than a specific project. You're paying up front to have an important service available to you on short notice.

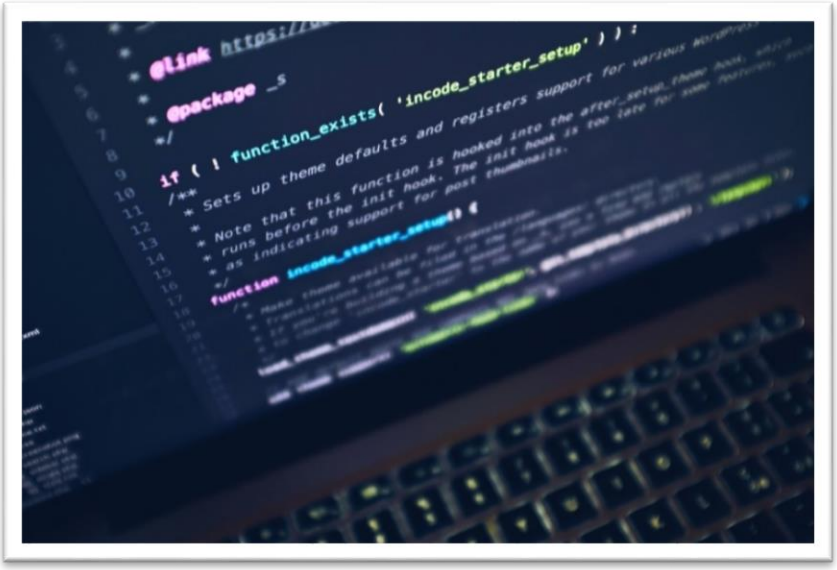
You might feel this is an unnecessary expense, but if your organization is affected by a cybersecurity breach, having a firm on retainer can result in better decisions and long-term savings, according to Richard Moore, CEO of cybersecurity firm CyberSix.

"Having a forensics retainer in place before an incident ensures the housing organization is prepared and is not making decisions during an incident," Moore said. "Making decisions under pressure leads to poor decisions."

Moore suggests engaging a forensics firm through external legal counsel to help maintain legal privilege over any internal written communications.

Time is of the essence after a cybersecurity breach. Having a firm on retainer allows the investigation and remediation to begin earlier.

If you wait too long to engage a forensics firm after a potential breach is identified, the evidence could be gone already, and your organization (and its data) will remain at risk.



Every state has a law requiring notification of security breaches involving personally identifiable information (PII), such as Social Security numbers. Refer to your state-specific breach notification law for details.

A forensics firm will attempt to determine if cybercriminals accessed any PII, and if so, whom the organization may need to notify based on state regulations.

Keeping a forensics firm on retainer can also alleviate concerns from internal IT staff that a breach investigation by a third party will be slower than one conducted by in-house teams. Having a relationship with a forensics firm before an incident allows the firm to build trust and familiarity. This familiarity can help streamline the investigation process.

The firm also serves as an independent investigator, giving all parties involved confidence in an objective review of the breach.

What does a forensics retainer typically cover?

A retainer can cover different aspects and time frames depending on whether you're dealing with the forensics firm directly or engaging a firm through external legal counsel (the next section covers why external legal counsel is recommended).

The typical retainer should cover at least 48 hours of investigation time, Moore said.

The scope of the investigation generally includes determining the source and severity of the breach, identifying what information was accessed, preserving evidence, and containing threats.

Depending on your organization's needs, the retainer can cover a lengthier investigation with training, exercises, and other benefits, Moore noted. Consult with your internal legal counsel before entering into any agreement with an external service.

Selecting and managing your cyber forensics firm (with legal privilege in mind)

When selecting a forensics firm, Moore suggests managing the process through external legal counsel for three reasons:

- External counsel usually has experience hiring and working with qualified forensics firms.
- Managing the process through external legal counsel helps maintain legal privilege.
- External counsel can prepare and maintain the investigation timeline to help answer detailed questions with consistency and accuracy.

In the event of a cybersecurity breach, your organization may face various legal risks. If a lawsuit is filed, plaintiffs may request that your organization turn over all written materials related to a forensics investigation as part of the discovery process.

Written communications between internal counsel and a forensics firm are considered part of the ordinary course of business and typically can't be withheld. Precedent has established internal legal counsel as part of the organization, negating attorney-client privilege.

Meanwhile, any written communications with external legal counsel (and the consultants they refer, such as forensics experts) enjoy attorney-client privilege because the law firm was retained for legal advice or in anticipation of litigation.

"Having external counsel helps protect the organization from litigation and ensures that privileged and confidential emails remain that way," Moore said.

A detailed timeline of events and communications, including crucial forensics details, should preferably be maintained and managed by external legal counsel.

"Just like any litigation activity, computer forensics activity must follow the same evidentiary handling process," Moore said.

For More Information

Visit housingcenter.com
Find out why affordable housing agents and brokers work with HAI Group

Subscribe for More Insights

✉ **Sign up to receive the latest news and events from HAI Group.**