The Public and Affordable Housing Industry's Guide to

Cyber Risk

HAI Group

January 2017

Why Should I Read the Public and Affordable Housing Industry's Guide to Cyber Risk?

The Internet is a powerful tool that has transformed the way we collect, store, and share data. It also leaves businesses vulnerable to data breaches that could expose them to costly financial and reputational risk. As a housing authority, you store data that are attractive to criminals, making you particularly vulnerable, so preparing for a cyber-attack makes good business sense.

Viruses. Spyware. Ransomware. Even the names sound sinister. As well they should—cybercrime has the potential to cost your housing authority tens of thousands of dollars or more, cripple business activities, and damage an organization's reputation.

Thanks to the ubiquitous use of the Internet and the sheer number of devices used to connect to it today, not to mention the sophistication of cyber criminals and the sneaky ways they trick their way into systems, we're more vulnerable to cyber risks than ever before. It's important to understand those risks and to learn how to protect your organization. Being prepared will help you minimize damage to both your housing authority and the people who trust you with their valuable personal data.

"Cyber liability costs can stack up quickly. The average cost to a public agency that loses records as a result of a data breach is $86 per breached record. So, a public housing authority (PHA) with a thousand records could easily expect to pay approximately $90,000 or more from a data breach."

BILL WAGNER Litigation Partner at Taft Stettinius & Hollister LLP, Commercial, Environmental, and White Collar Litigation

What Is Cyber Risk and Why Is It Important?

HAI Group

According to the Institute of Risk Management, cyber risk is any risk of financial loss, disruption, or damage to the reputation of your organization resulting from a failure of Information Technology (IT) systems. Cyber criminals typically gain control of data through malicious software, or malware, and no organization is immune.

Unfortunately, cybercrime is growing, and cyber criminals are becoming more organized. Meanwhile, their tools are becoming more sophisticated and more readily available, all of which makes it difficult to stay one step ahead of cyber risks.

For example, zero-day vulnerabilities, which are holes in software that are unknown to vendors and are then exploited by cyber criminals before the vendor is aware of the issue, more than doubled from 2014 to 2015, according to global cybersecurity leader Symantec.

Don't make the mistake of thinking that cyber risk affects only target large businesses.

The public and affordable housing industry is not immune. In 2013, nearly 1,000 people on the waiting list for housing at a housing authority in Washington had their social security numbers made public on the Internet.

In August 2015, an e-mail error made by an employee at a housing authority in California exposed the names and social security numbers of an undisclosed number of people. Even the US Department of Housing and Urban Development (HUD) fell prey, when a website error in 2016 exposed the personally identifiable information (PII) of approximately 600,000 people.

Cybersecurity Snapshot:

2012 National Small Business Study

Source: CyberSecurity Alliance, Symantec

87%	87%	59%
SMBs* With 1+ Employee Using the Internet for Daily Operations	SMBs That Do Not Have a Formal Written Internet Security Policy	SMBs That Have No Contingency Plan For Responding to a Breach

*Small- and medium-sized businesses

What Is Cyber Risk and Why Is It Important?

HAI Group

Cybersecurity risks can originate from multiple sources. Risks can come from hackers, rogue contractors, ransomware, and disgruntled employees. They can also come from simple employee mistakes such as lost smartphones, laptops or tablets, or accidental e-mail forwards.

What's more, risks are multiplying as criminals are upping their game by banding together and improving their methods of attack. Indeed, experts now say that even the best computer security can be breached.

The Risks Associated With Cybercrime Are Many and May Include:

- Business interruption from a hacker shutting down a network
- Damage to the housing authority's reputation
- Costs associated with damage to hacked records
- Data liability costs when resident lists or other data are stolen
- Costs to provide credit monitoring services to victims
- Lawsuits

Looking more deeply into the risk, a recent report from the Internet Crime Complaint Center said that, during one 14- month period, US businesses and consumers racked up more than $18 million in losses from a single type of ransomware. Today, even a simple phishing attack can result in stolen trade secrets, sensitive business information, and intellectual property.

If a housing authority views cybersecurity as a questionable and expensive cost center, it is important to change that mindset.

What is Phishing?

Phishing is the fraudulent practice of sending e-mails claiming to be from reputable companies for the purpose of scamming recipients into revealing their personal information such as passwords and credit card numbers.

Federal law now requires vigilance. Indeed, the US Department of Housing and Urban Development Office of Public and Indian Housing issued a notice on April 23, 2015, informing all agencies about their responsibilities for safeguarding PII and preventing breaches of sensitive data. In the document, HUD "expects its third-party business partners, including PHAs who collect, use, maintain, or disseminate HUD information, to protect the privacy of that information in accordance with applicable law."

"HUD's notice provides solid advice on how public housing authorities could protect themselves from a data breach," said Bill Wagner, an attorney and litigation partner at Taft Stettinius & Hollister LLP in Indianapolis, IN. Wagner recommends that PHAs "use readily available guidelines to harden your network, train your employees, create an incident response plan, and practice it."

What Is Cyber Risk and Why Is It Important?

HAI Group

"Most businesses aren't taking cybersecurity seriously enough," says Jonathan Hochman, a senior consultant with ***Hochman Consultants*** (Cheshire, CT). "Anybody dealing in identity information or financial data is especially at risk, because stolen personal information can be used for identify theft and then credit or tax fraud."

If a PHA inadvertently exposes residents' sensitive information, the housing authority could face serious liability. At the very least you may be required to provide free credit monitoring services to those residents, at an average cost of $175 per person.

Major Threats

Hochman says the biggest threats businesses face today are phishing and spyware. "In a phishing attack, the criminal uses social engineering to trick a worker into filling out a form on a fake web page that looks like a legitimate site. For instance, the criminal may send a message saying 'secure file download' and point to a page that looks just like a Google Doc page. The user then enters his Gmail address and password, and the site shows an error. Meanwhile, the user's credentials are now in the hands of the attacker."

Spyware is another common technique that cyber criminals use to access your data illegally. "With spyware, a user may visit an infected web page, where his browser downloads spyware to his computer," said Hochman. "The spyware then sniffs around on the network to determine what sort of environment it is. If it looks like a corporate network, files and data will be gathered, shipped out, and then used to compromise trade secrets, commit extortion, or create opportunistic leaks."

What Is Cyber Risk and Why Is It Important?

While phishing and spyware are the most likely sources of a data breach, a very close second is simple employee negligence, says ***Scott Schleicher***, an underwriting manager in the Cyber and Technology group at XL Caitlin.* An example of negligence that could lead to a data breach is an employee losing his or her laptop.

While damaging, these types of attacks are not the biggest claims Schleicher's company sees. The most expensive cybersecurity attacks come from criminal enterprises. "Phishing and spyware tend to be more contained in their cost than a criminal enterprise cybersecurity attack," Schleicher said.

Regardless of how it comes about, or how sophisticated it is, a data breach can be costly for an organization and devastating for residents or tenants. That's why it's so important to put a plan in place to protect your housing authority.

*HAI Group partners with XL Caitlin to bring our policyholders complimentary cyber liability protection.

Cyber-attack Losses May Include:

- Expense for credit monitoring and identity protection services for victims
- Loss of current and future revenues
- Government fines
- Legal defense fees
- Cost of insurance and implementation of electronic countermeasures to detect future attack attempts
- Damage to an organization's reputation in the market
- Prolonged court cases
- Loss of focus while time is spent cleaning up the aftermath

What Does the Legal Environment Look Like?

Given the number and variety of cyber threats and the rising costs associated with the risk, it's not surprising that lawmakers have attempted to legislate a solution. Here are some of the laws related to cybersecurity:

- PIH Notice 2015-06
- Privacy Act
- Freedom of Information Act
- E-Government Act

The most recent and possibly most comprehensive law is the Cybersecurity Information Sharing Act (CISA), which was signed into law in late 2015. Data Protection Reports show that CISA does three main things:

1. Authorizes the federal government to share unclassified cyber threat indicators and defensive measures among federal agencies
2. Authorizes businesses to monitor their information systems and all information used by their systems, if the monitoring is designed to protect the information
3. Authorizes companies to implement defensive measures on their own IT systems to counter threats

The law also grants businesses full immunity from government and private lawsuits and claims that may arise because of monitoring and information sharing arising from CISA compliance. At the same time, the law requires that PII be protected from unauthorized use or disclosure.

Passage of CISA was controversial, with a number of Silicon Valley companies objecting to potential abuses. Since its passage, federal guidance effectively states that the only information that can be shared under the act is information that is directly related to and necessary to identify or describe a cybersecurity threat.

As mentioned previously, HUD has its own privacy protection guidance for third parties, which outlines responsibilities for safeguarding PII required by HUD. It covers things like protecting sensitive information, training, protecting and transmitting files, records management, incident response, and more. You can find the notice here.

Understanding Your Obligations

There are also a number of state laws that address a housing authority's obligations if their tenants' information is exposed. These rules fall under privacy laws. Ask for an attorney's help in understanding your obligations.

Creating a Culture of Cybersecurity

HAI Group

A housing authority isn't unique in the types of data it stores, but where the information may differ from a larger, enterprise business is the level of protection used to secure that data, along with the amount of training employees receive.

"Commercial enterprises are likely to have better, more up-do-date policies, procedures, equipment, and software [than housing agencies]," Schleicher said. "They may also have better privacy policies and employee training, all of which help reduce risk."

Remarkable as it may seem, many housing agencies lack even basic cyber protections such as policies that outline Internet use for employees. This is a mistake. "Housing agencies need to take the same measures as banks do to protect against cyber risk, because they hold the same kind of high-risk data," said Hochman. "The cost and risk that they should really worry about is what happens if they are compromised. The liability could be substantial."

To create your own plan, get a group of key stakeholders together in your housing authority, then consult an attorney to make sure your team understands your requirements under HUD, state, and any other applicable laws. Next, consult a qualified cybersecurity expert to help craft your plan, which should include instructions on what to do in the event of a data breach at your organization.

"An incident response plan, or IRP, is a valuable tool," said Schleicher.

Be aware, though, that this type of plan is not meant to thwart an attack.

"The IRP outlines who does what," said Schleicher. "Who calls who? Who are the attorneys we use? Do we have a backup computer system we can use? Do we have a method for dealing with communicating to our residents? Our employees?"

Under Attack!

Your housing authority finds its entire system locked because of a ransomware attack. The extortionist demands $1,000 to unlock your system. Rather than fight back, you decide to pay the ransom; after all, what's $1,000 in the grand scheme of things? You also agree to provide credit monitoring to everyone whose data may have been compromised, which is a prudent step with a manageable cost.

You initially feel lucky because, after the ransom is paid, the extortionist does unlock your data. However, weeks later, you detect additional malware in your system. This destructive code was introduced during the original attack and has lain dormant. This code could allow another ransomware attack, so you decide to conduct a meticulous system cleaning, which adds substantial additional expense.

While this is just one possible scenario of a cyber-attack, it demonstrates the lasting impact that can go beyond the initial attack.

Creating a Culture of Cybersecurity

HAI Group

Incident Response Plan (IRP)

An IRP is a very important tool for a housing authority to have. Keep in mind, though, that these plans are only effective if someone commits to reviewing them with your stakeholders and assigning responsibilities. “An integral part of that roadmap is the execution of the IRP at all phases of the breach,” says Schleicher.

Once you have assigned responsibilities, it’s important to conduct a dry run. Businesses have been fined because they failed to test their plan, so make sure to test yours.

Disaster Recovery Plan (DRP)

Beyond having an effective IPR to deal with an ‘incident’ disrupting daily operations, a housing authority needs to have a tested DRP.

A DRP plan maps out specific procedures to follow to recover IT infrastructure during a catastrophic incident that immobilizes a housing authority from operating.

In the last decade, examples of disasters that housing authorities have faced include Hurricane Sandy, the Joplin, Missouri tornados, and the Baton Rouge flooding of 2016. Man-made disasters can also be a threat, such as a server crash, or prolonged power failure.

Once a DRP has been established, it will need to be continuously worked on so that it evolves with changes in your environment; both physical and technological.

Five Questions Executive Directors Should Ask Themselves about Cyber Risk

1. What is the current level and business impact of cyber risks to our organization? What is our plan to address identified risks?
2. How is our executive leadership informed about the current level and business impact of cyber risks to our organization?
3. How does our cybersecurity program apply industry standards and best practices?
4. How many and what types of cyber incidents do we detect in a normal week? What is the threshold for notifying our executive leadership?
5. How comprehensive is our cyber incident response plan? How often is the plan tested?

Adapted from Department of Homeland Security: C3 Voluntary Program: Cyber Risk Management Primer for CEOs

Advanced Security: Keeping up With Hackers

If the basics of cybersecurity—firewalls, secure Wi-Fi, employee Internet use plans and the like—are now crucial, the ever-expanding threat means that additional actions are also becoming increasingly unavoidable. Many leading organizations are already using the following:

Virtual Private Networks (VPNs)

A VPN is technology that creates an encrypted connection over a less secure network. It allows remote computers to perform as if they were part of a secure local network, so off-site employees have comparable access to those onsite. Many quality VPN products are available, making this a comparatively easy and inexpensive cybersecurity tool.

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)

IDS and IPS technologies scan networks for malicious activities such as security threats or inappropriate cyber behavior. These tools start by identifying suspicious activity, then they attempt to block and report it. While IPS is considered more sophisticated than IDS, some experts see value in both technologies, and recommend that they be deployed together to maximize security.

Identity Access Management (IAM) System

An IAM system works to control and monitor user access of information and applications across an entire organization. In addition to safeguarding resources, this system can:

- Generate audit reports and user metrics
- Enforce compliancy with government regulations
- Protect within mobile, cloud, and social media environments

Creating a Culture of Cybersecurity

HAI Group

Despite the growing risk of a data breach, Hochman said that businesses generally use ineffective cybersecurity solutions and protocols. “Forcing users to choose complex passwords and change them all the time does little to nothing to help security,” he said. “Antivirus software is another security measure proven to deliver almost no real value.”

Experts may disagree about the value of certain cybersecurity tools, but the ones HAI Group spoke with all said that creating an incident response plan and having a dedicated response team are important steps.

The ***Software Engineering Institute*** describes a computer security incident response team, or CSIRT, as a focal point for “receiving, reviewing, and responding to computer security incident reports and activity.” These teams have a wide range of security-related responsibilities, including:

- Monitoring systems for security breaches
- Serving as a central communication point
- Documenting and cataloguing security incidents
- Raising security awareness within the organization
- Auditing system and network vulnerability
- Conducting penetration testing
- Staying current on evolving vulnerabilities and cyberattack strategies
- Researching software updates and patches
- Analyzing and developing technologies to minimize security risks
- Providing security consulting services throughout the organization

Interested?

Read more about creating a CSIRT.

Most CSIRTs include a team leader who has ultimate responsibility for cybersecurity, an incident lead to coordinate the response and all communications, and associate members as needed to address compliance issues, public relations, etc. If you run a smaller housing authority and a team of this scope and size doesn’t make sense, ask your attorney to help you develop a structure that does.

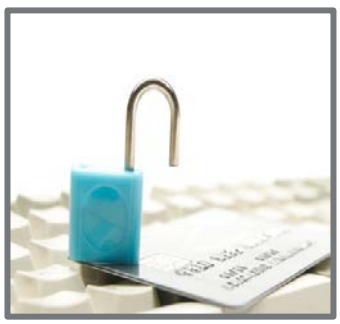
Cyber Liability Insurance

Most businesses are insured against property damage, wrongful termination, and the like. Given the potential damage from cyber threats, it seems logical to purchase insurance coverage for this risk as well. You should know, however, that most standard commercial policies don't cover cyber risks, so more and more organizations are turning to special cyber liability policies.

Cyber risks can be a challenge for insurance underwriters because the field of cybersecurity is so new that actuarial data are limited. Without standard quantitative measures, insurers may rely on creating a qualitative portrait of the applicant's risk management procedures and risk culture. This approach can cause cyber risk policies to be highly customized and costly.

A Cyber Liability Policy May Include One, Several, or All of the Following Types of Coverage:

- Coverage for security or privacy breaches of your tenants' PII
- Forensic investigation costs required to determine the severity and scope of a breach
- Consumer notification and customer support costs, along with the cost of providing credit monitoring services to victims
- The cost of operating a call center to handle inquiries from those affected
- Public relations and crisis management costs
- Legal defense costs and related settlements and indemnity payments
- The cost of restoring, updating, or replacing electronic business assets
- Costs for business interruption and its ramifications
- Liability associated with libel, slander, copyright infringement, product disparagement, or reputational damage when the attack involves a business website, social media or print media
- Expenses related to cyber extortion (e.g. ransom ware) or cyber terrorism



It's important to realize that, whatever the cost of premiums, most cyber insurance policies carry a substantial deductible. In addition, cyber liability policies aren't likely to cover impacts such as IT upgrades and the devaluation of intellectual property. The effects of some of these costs can exceed the insurable loss many times over.

To truly ensure a successful future, maintaining adequate insurance coverage is a key step, but it's only one step. It's also essential to continually attend to the basics and to invest in advanced levels of protection. Most important, an organization should be willing to access technical expertise and outside help when it's needed.

What to do in the Event of an Attack

HAI Group

The organization has developed a cybersecurity plan, installed protective measures, and trained employees. That's a good start. "Plans work against known threats," said Hochman. "The actual attacks can be novel. Employee training helps, but invariably even the best-trained employees will make mistakes and be caught by a sophisticated attacker. Do not rely on your employees' correct actions. The security plan needs to assume that your employees will err."

If a housing authority experiences a data breach, Wagner says to contact an experienced attorney immediately. "The attorney will put your insurers on notice of the incident and analyze their coverage obligations; protect the investigation as much as possible where he or she is able to invoke the attorney/client privilege and other protections; analyze your reporting obligations to your customers, state attorneys general, and other agencies; help you in negotiating with data breach response vendors, and communicate with regulators and defend you in response to regulatory investigations and claims and class-action lawsuits," said Wagner.

It's important to contact an attorney because it can be difficult to know when notification is required. "Statutory notification differs depending on what type of data was breached, how much of it was breached, in what state the breach occurred, and other factors," said Schleicher, adding that there are currently 48 states with notification requirements.

"Many times even if it is not required by state statute we elect to notify anyway, which is referred to as voluntary notification, because by doing so it creates goodwill. PHAs should not try to manage or fix or deal with a breach on their own as the consequences of doing that could be very bad. When they suspect a breach they should call the data breach hotline and report it as soon as possible and we can [take it from there]."

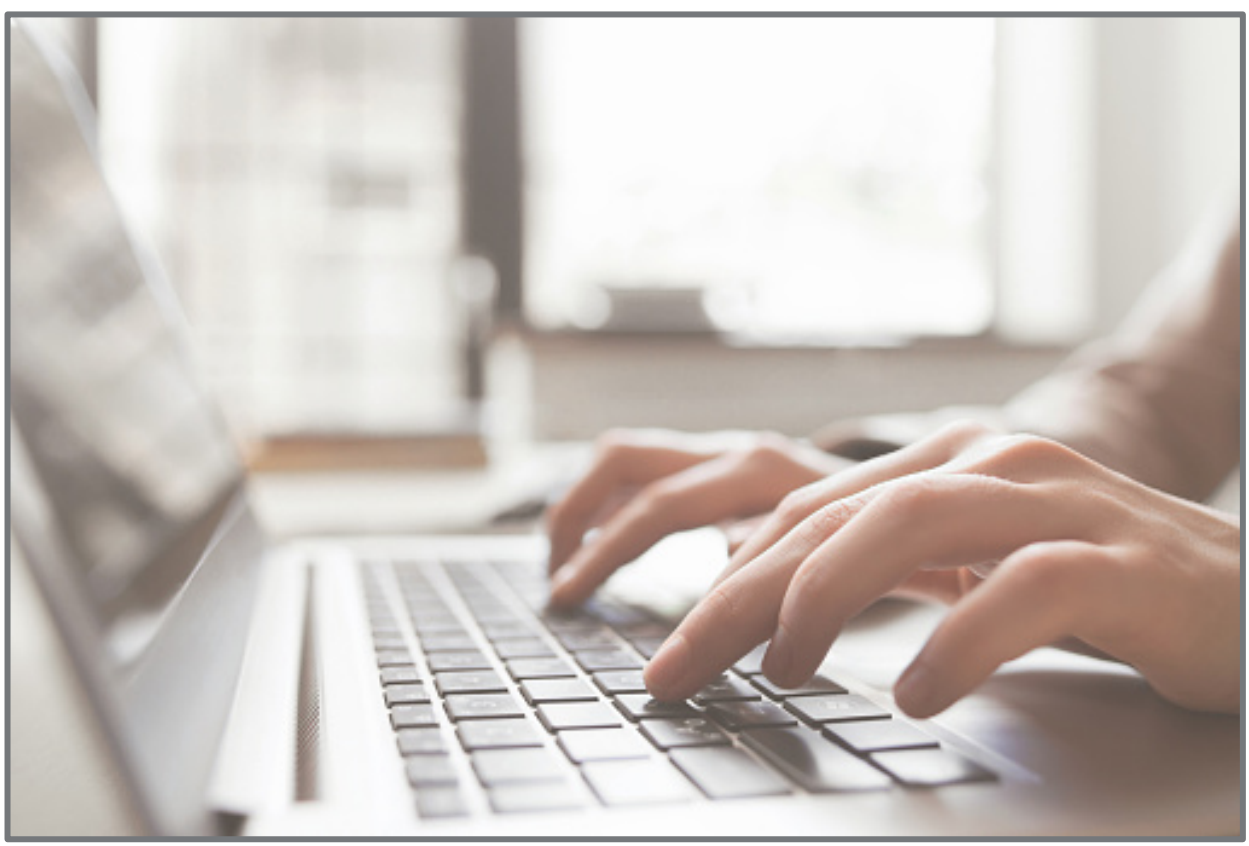
We've Been Hacked?

Making it even harder to combat cybercrime is the fact that many IT departments may not even realize their information has been compromised.

"If [organizations with inadequate protection] were to conduct a security audit, they would find malware on their network," said Hochman. "The first step is to identify the problems and clean them up. Then, train staff to resist phishing attacks and to continue to scan for break-ins. Next, secure sensitive data with secure encryption. Finally, assume that all data will leak. Try to make it hard to use when that happens."

Helpful Resources

- HUD notice: Privacy Protection Guidance for Third Parties
- Free web-based training from the Department of Defense covers a wide range of security topics
- Federal Cybersecurity Information Sharing Act
- Privacy & Data Security Insight blog from Taft Privacy and Data Security Attorneys
- Articles on cybersecurity from Hochman Consultants



HAI Group

About HAI Group

HAI Group serves the public and affordable housing community with special, niche insurance programs as well as other value-added products and services. The Company's continued growth over the past 30 years and diversification into areas where Members have identified needs, demonstrates the Company's commitment to their more than 1,400 stakeholders. HAI Group is dedicated to providing reliable insurance, training, research, and capital solutions in a manner which exceeds expectations. As a Member-owned organization, HAI Group has positioned itself as a recognized leader and expert in the public and affordable housing industry. Headquartered in Cheshire, Connecticut, HAI Group's membership extends across the United States.

Visit www.housingcenter.com to learn more.

For More Information

information@housingcenter.com
www.housingcenter.com
800.873.0242, ext. 291