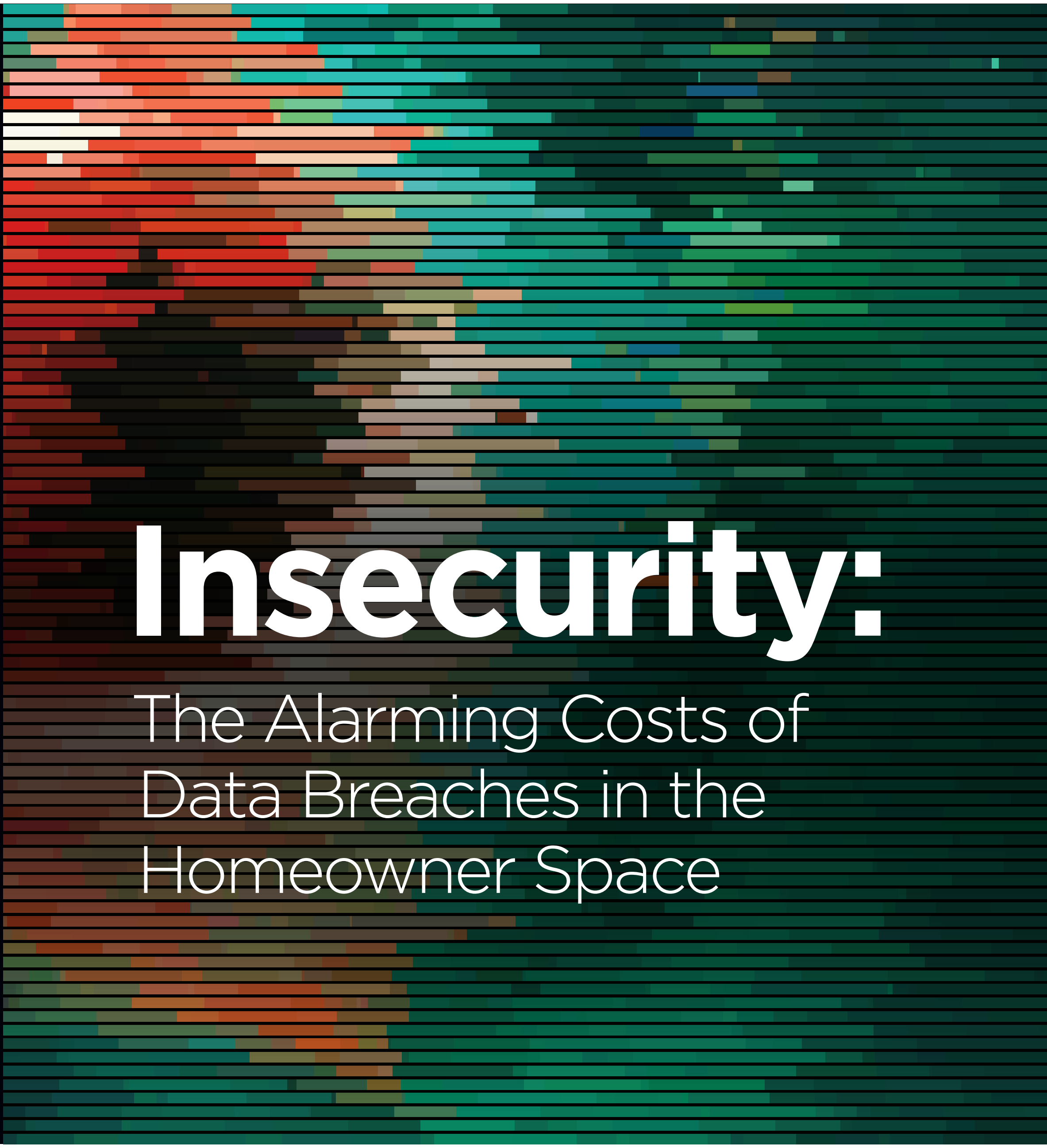
WHITEPAPER

CINC systems



Insecurity:

The Alarming Costs of Data Breaches in the Homeowner Space

Table of Contents

$2.35

million the average cost of a data breach for organizations with < 500 employees in 2020

52%

malicious attacks

25%

system glitches

23%

human error

Introduction

What's the cost of cybercrime? For Mark, the owner of a Seattle real estate company, the price was $50,000.

In 2017, Mark and his partner received an email from someone they thought was a vendor expecting payment. "The cadence and the timing and the email was so normal that it wasn't suspicious at all," he said. "It was just like we were continuing to have a conversation, but I just wasn't having it with the person I thought I was."[1]

Mark's business was victimized by a common cybercrime known as business email compromise (BEC). More than 23,000 BEC cases were reported last year to the FBI.[2] Cybercriminals use phony emails to trick employees to wire money to the wrong accounts.

In Mark's case, the perpetrators hacked into an email conversation with a business partner and started monitoring their discussions. When the disbursement owed was mentioned in a conversation, the attacker sent an email posing as the vendor – but with new wiring instructions.

Mark's situation is increasingly common. The average cost of a data breach for organizations with fewer than 500 employees was $2.35 million in 2020. 52% of the data breaches were caused by malicious attacks, with the remaining data breaches caused by system glitches and human error. The most common reported malicious attacks included compromised credentials, cloud misconfiguration, vulnerability in third-party software and phishing attacks.[3] As an industry that manages the most intimate financial and personal information of more than 139 million[4] U.S. homeowners, awareness of the way homeowner data is managed and protected from cyber attacks is vital to one's bottom line.

"A cybersecurity breach would cause irreparable harm, for both financial and organizational reasons," said Derek Greene, CFM, CMCA, AMS, President/CEO of Community Association Management, Ltd. "Financially, accounts get wiped out and homeowners sue for financial and punitive damages. Organizationally, talented employees grow weary of homeowner complaints and leave."

"Security is not a nice-to-have," said John Yeoh, the Global Vice President of Research at the not-for-profit Cloud Security Alliance. "It's not just a topic that should come up when it's too late. It should drive business."

This comprehensive guide supports efforts of the association management industry to protect homeowner data from a cyber attack. First, it will cover the biggest threats to consider in 2021. Next, it will address how HOAs and homeowners are particularly vulnerable to cyber attacks. It will also provide ways companies can ensure that their data is protected with respects to their company policy and software capabilities. Finally, it will offer a self-assessment for one to complete to determine steps needed to implement greater security within their organization.

"Security is not a nice-to-have. It's not just a topic that should come up when it's too late. It should drive business."

– John Yeoh, the Global Vice President of Research at the not-for-profit Cloud Security Alliance.

On the Lookout:

The Biggest Threats to Consider in 2021

The Threat	What Is It?	2020 Impact	How It Happens	The Result
Phishing Attacks	An attempt to obtain sensitive information by disguising oneself as a trustworthy source	One in eight employees shared information requested in a phishing email in 2020[5]	A cybercriminal will utilize relevant information to the victim – such as email correspondence with a vendor – to receive personal information such as a credit card or banking information	Unauthorized access to accounts (resulting in data breaches) or unauthorized financial transfers
Account Takeover (ATO)	A form of identity theft in which a third party successfully gains access to a user's account credentials	ATO attacks are on the rise, growing by 282% between Q2 2019 and Q2 2020[6]	A cybercriminal poses as a real user to change account details, steal financial information or sensitive data, or use stolen information to access more accounts within the organization	Compromised user account credentials can allow an attacker to gain access to a homeowner's or service provider's account, including their bank account, credit card information, and home address
Compromised Service Providers	A cybercriminal targets the company itself to gain access to personal data	The surge in compromised service providers prompted special attention from the U.S. secret service in June 2020 with aims to prevent major fraud during the holiday season[7]	A cybercriminal takes control of a the company's system, therefore having control of all customer data	Attacks on a service provider's network could allow the cybercriminal to take advantage of employee access to sensitive data and functionality
Malicious Software (Malware)	A virus (otherwise known as malware) is embedded to severely damage a system	There was a 63% increase in never-before-seen malware variants in the first half of 2020[8]	Malware can infiltrate a computer through a number of means, including a hacked website, infected music files, and newly installed programs	Malware infections on computers can result in the breach of sensitive data and can potentially wipe out pertinent data within a company

> **"Cybersecurity is important because it encompasses everything that pertains to protecting our sensitive data, whether that's client information, Homeowner information, financials, banking, or anything in between."**
>
> **– Derek Greene, CFM, CMCA, AMS, President/CEO of Community Association Management, Ltd.**

Facing Insecurity:

Vulnerabilities in the HOA Space

"This industry is a likely target," said Greene. "Because the community association management industry holds sensitive homeowner information of its HOAs and their members,it is one of the riskiest industries for exposure to a cyber attack." Beyond the immediate financial consequence, long-term consequences of a data breach include potential lawsuits from homeowners for punitive damages and lost business from HOAs opting for a more secure management company.

Some major vulnerabilities within the community association management industry include:

Passwords Unprotected. At least 65% of people reuse passwords across multiple sites, and the average person reuses each password 14 times.[9] Many people also use home information, such as their street name and number, for their password. If an attacker were to obtain just one homeowner's password, the attacker could quickly work to gain data from all homeowners within the HOA. Hundreds of homeowners could have their personal data compromised within minutes, causing chaos for the management company.

Outdated Software. Financial institutions have robust security programs and training for their employees. So if a cybercriminal wants to penetrate a bank, the best target is often a third-party vendor of the bank – especially one with outdated software. "We are acutely aware of the detrimental impact a faulty third-party system can have on our data," said Anthony Dister, Senior Vice President of Wintrust Financial Institution. "As a software system transfers finances and homeowner payment data into our system, there is also the potential to transfer a virus into our system." Software solutions that lack sufficient security measures and regular program updates pose a major risk for both the partner bank and the homeowner.

Lack of Policies and Procedures. Many enterprises have adopted a protocol to detect cybercriminal activity and train employees to recognize and report on suspicious activity. Smaller businesses are more vulnerable. As a result, employees within the organization may be more likely to open an attachment from a phishing scam or download a program that contains malware. This can quickly compromise homeowner financial data, and accounts can be wiped clean.

Work-From-Home Attacks. As employees raced from the office to the living room in March 2020, "most organizations implemented a haphazard security policy," Yeoh said. Because of this, cyber attacks increased by 63% since lockdowns were first initiated.[10] Homeowners who use the same login credentials or devices for work and personal relations may pass on malware that intercepts homeowner data from the entire HOA,compromising every homeowner's bank account.

> **"Now that we've made it through 2020, companies need to go back and re-audit the security measures they implemented (or didn't implement) during COVID-19 lockdowns. Something as simple as a family member looking over one's shoulder at their laptop is a data breach. Companies need to make sure they fill in the gaps caused from quickly moving into a work-from-home environment."**
>
> **John Yeoh**
> **Global Vice President, Research, Cloud Security Alliance**

Go Phish!

Email phishing attacks are the number one threat to small businesses. Here are four things one can do to detect a phishing scam:

1. Check the domain
Look at the email address, not just the sender. Does it match? Is it a personal email address coming from a vendor name? Is it from a known colleague or vendor with a slightly different domain? A quick review can save a company millions.

2. Review the content
Since scammers tend to send a phishing email to multiple parties at once, it's common for the content within the email to be poorly written or highly impersonal.

3. Watch out for clickbait
Do not, under any circumstance, open an attachment or click on a link from a personal email that was unexpectedly delivered. One click is all that's needed for the virus to take control.

4. Reach out to the software provider
A company's software provider should be conducting regular training sessions and tests with their employees related to phishing scams, and they can keep one up to speed on the latest trends and 'gotcha' moments within the industry.

A Secure Solution:
How to Keep Homeowner Data Safe

There is hope. A strong partnership between a community association management company and its software provider can stop a cyber attack. Here are some of the most important steps both parties can take to ensure data is protected:

The Company's Responsibilities

Permission settings by user groups:
"Companies should provide super limited privilege to homeowner data," Yeoh said. "Be careful who you provide access to and have a proper plan in place to 'turn off the tap' should an employee leave."

Not everyone requires the same levels of access to data on the system. An accountant may need to see the check number for a homeowner, but a receptionist may not. Built-in group-level permission settings make it easy to define the exact rights that a particular user should have, decreasing the amount of people who have access to sensitive information. A standard process to quickly revoke access also needs to be put in place within an organization for employees should they resign or be terminated.

Employee Training.
Security training should be considered an essential part of employee onboarding and continuing education. Employees should know how to spot a phishing scam, how to tell if a website or program is safe to use, and the latest schemes attackers have been using in an attempt to compromise data.

Strict Policies and Procedures.
Oftentimes, the flexibilities managers allow to ease an employee's day-to-day can make a company far more susceptible to an attack. It's important for every employee - especially those regularly handling sensitive homeowner information – to take the way they handle data very seriously. Policies that should be enforced include:

- Prohibiting shared login credentials
- Prohibiting personal devices, or requiring personal devices to have up-to-date malware protection
- Prohibiting access to homeowner data through a WiFi outside of home or the office

The Software Provider's Responsibilities

Multi-Factor Authentication (MFA):
Multi-factor authentication (MFA) requires users to provide two or more verification factors to gain access into a system. This may include one-time passwords, answers to personal security questions, a phone app verification requirement, and so forth. Since it's unlikely that an attacker would have access to multiple forms of identification at once, MFA makes it more difficult for an attacker to compromise accounts on the system. "MFA should be a must," said Yeoh. "In accessing so much cash flow, it would be foolish to only rely on a password to log into a system."

> **"Multi-factor authentication should be a must. In accessing so much cash flow, it would be foolish to only rely on a password to log into a system."**
>
> **John Yeoh**
> **Global Vice President, Research**
> **Cloud Security Alliance**

Private cloud hosting:
"Not all clouds are alike," Yeoh said. While cloud-based programs are certainly more secure than on-premise solutions, data in public cloud environments have some of the highest rates of data breaches. A private cloud hosting environment helps to reduce the risk of data breaches, and owners should be made aware of the cloud hosting environments that their software companies use. Examples of companies with private cloud environments include Amazon Web Services (AWS), Microsoft, VMware, and Dell.

Endpoint monitoring:
A software provider should incorporate endpoint monitoring and protection. This means that if someone attempts to log into their system in a suspicious location or on a suspicious device, all activity can be tracked. If the suspicious activity is indeed an attacker, access can be immediately revoked.

IT Department Access Limitation:
Access to homeowner data is a privilege, and a software provider should consider it as such. A software company should be able to ensure that the only employees with access to sensitive data is their in-office IT department. These employees should have successfully completed background checks prior to the hiring process, and they should be part of the aforementioned company (meaning that they are not outsourced vendors or freelancers.)

Is Your Homeowner Data Safe?

Now that you've learned about the biggest threats in your industry, it's time to see the next steps you need to take to build a secure organization. Take this quick assessment to see where you stand:

1. What login credentials are needed for your homeowners to log into their portal?

A. A username and password

B. Username, password, and captcha

C. At least two forms of identification, such as a username/password and mobile authentication

Why are we asking this? *Nowadays it's incredibly easy for a cybercriminal to steal a homeowner's password, especially if the password is their child or pet's name. If one homeowner login is compromised, all homeowners within the HOA can be attacked, compromising everyone's bank account. With multi-factor authentication (MFA), users are required to provide two or more verification answers, making it more difficult for an attacker to compromise an account.*

2. How easy is it for an employee in your company to access homeowner payment information?

A. I have strict permission setting guidelines in place between different departments

B. Employees have different permission settings, but I have seen them share logins between each other every now and then

C. Everyone has the same level of access

Why are we asking this? *The fewer the people who have access to sensitive information, the lower the risk of a data breach. It's important to regulate permission settings, only providing access to homeowner data to the employees who need it. Employees should also be highly discouraged from sharing login credentials, as this can present an enormous risk.*

3. Where is your homeowner data stored?

A. A private cloud hosting environment

B. In the cloud, though I'm not sure what type of cloud hosting environment

C. Through an on-premise server (not cloud-based)

Why are we asking this? *While cloud-based programs are certainly more secure than on-premise solutions, data in public cloud environments have some of the highest rates of data breaches. Such data breaches can provide a cybercriminal financial and personal data of all homeowners within an HOA. A private cloud hosting environment (such as Amazon Web Services) helps to reduce the risk of data breaches, and owners should be made aware of the cloud hosting environments that their software companies use.*

4. How do you train employees on phishing alerts in your company?

A. We teach employees how to determine if a message is a phishing scam and have a process in place to report phishing alerts

B. We don't have a formal process in place, but we do tell employees to be on the lookout for emails that look like a scam

C. We don't have a process in place at the moment

Why are we asking this? *Phishing alerts are the number one threat to small businesses when it comes to cybersecurity. It's essential to ensure that your team is properly equipped with a formal policy and procedure to identify and appropriately react to a phishing scam. One click on a wrong link and chaos can ensue.*

5. What is your policy when it comes to working from home?

A. I make sure that my employees are using malware-protected company equipment

B. I'll let my employees use personal devices, but require that they have malware protection

C. I don't have any policy in place for employees working from home

Why are we asking this? *Because of 2020's rapid shift to remote working environments, cybercriminals have taken advantage of haphazard approaches to cybersecurity. It's important to treat an at-home work environment like you would if the equipment were in the office. Encourage the use of company devices if possible, and if using a personal device, require employees to have malware protection in place.*

6. What would your software company do if they were to see a suspicious login from their servers?

A. Their IT department would monitor the activity and cut off access if it's deemed a potential attack

B. I'm sure I would be notified if a suspicious login happened in my system

C. I'm not sure

Why are we asking this? *Any vendor providing software to an association management company should have endpoint monitoring to automatically track suspicious activity and prevent an attack before it's too late. If you're unsure of your software provider's procedures, contact them to learn more.*

7. Has your software company spoken to you about their security measures?

A. Yes – they provide us regular information about what they've done to keep our data and cash flow safe, and they've told us about their future implementations to improve cybersecurity

B. We discussed briefly in the onboarding process

C. No

Why are we asking this? *Security goes beyond the product and the environment – it's about the company's culture, people, and policies as well. A software provider dedicated to keeping data and cash flow safe for their clients and homeowners will ensure that their employees are limiting access to sensitive data, are regularly trained on safe policies, and are communicating the latest threats and enhancements to their clients. Talk to your software provider to see what measures they have taken to ensure your homeowner data is safe.*

MOSTLY A's:

Green – You're Doing Great!

Congratulations! Based on your answers, we can assume that you are very secure within your organization! You are communicating and training your employees on how to recognize and report threats, enforcing secure environments both in and out of the office, and communicating regularly with your software provider about security needs.

What's Next? Continue staying on top of the latest trends and threats in the industry to keep your homeowner data safe, and continue regularly communicating with your employees on how to recognize and report suspicious activity. Your software provider and bank can also support you in understanding the latest threats and upcoming enhancements to their systems. Don't be afraid to ask your software provider what upcoming enhancements they have to further protect your data and cash flow - as you're clearly focused on the safety of your homeowners, your vendors should be, too!

MOSTLY B's:

Yellow – Not So Fast!

Some of the biggest insecurities come from simply not knowing. Based on your answers, it seems that you may be unsure of the security measures your software provider has in place to protect homeowner data. Furthermore, while you are asking your employees to be on the lookout for threats, a more formalized approach may help build alignment within your team that improves your chances of stopping an attack before it's too late.

What's Next? First and foremost, we suggest reaching out to your software provider regarding the questions you were unsure of how to answer. The extra knowledge you'll obtain will make you feel more confident in how homeowner data is handled. Next, we would suggest creating a formalized approach in your organization when it comes to identifying and reporting suspicious activity. Finally, don't shy away from enforcing a policy that can save your company from a cyber attack. While it may feel overwhelming to enforce certain rules with your employees, it will improve alignment in the long run.

MOSTLY C's:

Red – Let's Stop and Review Your Needs

Based on your answers, it seems as though you're lacking a policy to prevent cyberattacks in your organization. You also seem to lack important information from your software provider pertaining to their security policies and protocols, and this could put your homeowners at risk.

What's Next? While it may be alarming to be in this position, there's no reason to fret. Here are some steps you can take right now to improve security in your organization:

1. Start by learning yourself. If you've read through CINC's Whitepaper Insecurity: The Alarming Costs of Data Breaches in the Homeowner Space, you're off to a strong start!

2. Implement a series of training classes and formal policies to your team. Phish alerts, work-from-home protocols, and permission settings are important starting points.

3. Talk to your software provider. Ensure that they are part of your plans to protect your homeowner's data and finances, too. Ask them about their security measures and plans for future enhancements, and communicate these plans with the rest of your team.

About CINC

CINC Systems is the largest provider of SaaS products to the association management space. The company provides transformational technology and services for the community association industry, redefining the way its clients and partners do business. Founded in 2005, CINC Systems became the first Internet-based integrated accounting and property management system for the community association industry. It currently serves nearly 20,000 associations across the country.

Learn more at www.cincsystems.com

Facebook: /CINCSystems

Twitter: @CINCSystems

LinkedIn: /cinc-systems-llc

References

1. Kaste, Martin. "Cybercrime Booms As Scammers Hack Human Nature To Steal Billions." NPR, November 19, 2019. https://www.npr.org/2019/11/18/778894491/cybercrime-booms-as-scammers-hack-human-nature-to-steal-billions.
2. Federal Bureau of Investigation. "Business Email Compromise." Federal Bureau of Investigation. 2021. https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise.
3. U.S. Census Bureau. Population Estimates July 1, 2019.
4. IBM. Cost of a Data Breach I Report 2020. New York: July 2020.
5. "New Report Unveils the Most Vulnerable Sectors and Departments to Phishing Attacks." Corporate Compliance Insights, September 14, 2020. https://www.corporatecomplianceinsights.com/new-report-unveils-the-most-vulnerable-sectors-and-departments-to-phishing-attacks/.
6. Bracken, Becky. "Account Takeover Fraud Losses Total Billions Across Online Retailers." Threatpost English Global, October 2, 2020. https://threatpost.com/account-takeover-fraud-online-retailers/159802/.
7. Cimpanu, Catalin. "US Secret Service reports an increase in hacked managed service providers (MSPs)." ZDNet, July 6, 2020. https://www.zdnet.com/article/us-secret-service-reports-an-increase-in-hacked-managed-service-providers-msps/.
8. Fruhlinger, Josh. "Top cybersecurity facts, figures and statistics." CSO United States, March 9, 2020. https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html.
9. Lancaster, Kevin. "These 10 Password Security Statistics Prove That Your "Password Protected" Data Isn't Safe." ID Agent, July 13, 2020. https://www.idagent.com/blog/10-password-security-statistics-that-you-need-to-see-now/.
10. "Human error poses cybersecurity challenges for 80% of businesses during the COVID-19 pandemic." Security Magazine, November 10, 2020. https://www.securitymagazine.com/articles/93885-human-error-poses-cybersecurity-challenges-for-80-of-businesses-during-the-covid-19-pandemic.