Cybersecurity Measures You Can Implement To Protect Your Real Estate Business

CERTIFID

Table of Contents

Introduction

It's easy to get lulled into the belief that your company won't be like the other headline-grabbing companies that fall victim to cybercriminals who breach their network security and exploit their data, customers, and brand.

However, as the highly sophisticated ransomware attack on Cloudstar proves, such an attack can happen to any business at any time. Although Cloudstar's situation may be different than others across the real estate industry, such a high-profile breach should serve as a wake-up call for organizations, no matter the size and scope of their business.

So how can your real estate business avoid becoming the victim of a cyberattack?

To accelerate your understanding of core cybersecurity principles and the best practices you should implement to protect your business and customers, CertifID has brought all the essential information together in one place.

An attack can happen to any business at any time.

CHAPTER 1:

Core Cybersecurity Principles

When you talk to a cybersecurity professional, you will gradually learn that all the activities, policies, and systems they focus on fall into one of three categories.

These three categories form the core cybersecurity principles and are often referred to as the CIA triad. These principles include:

Confidentiality:
This principle focuses on protecting private information from unauthorized access. This includes financial records, personally identifiable information (PII), Social Security numbers, and other proprietary information.

Integrity:
This principle centers on the need to protect data's authenticity and accuracy, ensuring that it hasn't been tampered with while stored, in transit, or in use.

Availability:
This principle focuses on ensuring that data, applications, and systems are available to authorized users when needed.

Although security professionals use the above principles to guide and structure their work, they also need to remember they are there to enable the business to operate securely. That means they need to find ways to implement cybersecurity controls without slowing down or hampering regular business operations.

Similarly, it is essential to remember that cybersecurity is an organizational responsibility. This means cybersecurity decisions—including how much money to spend, which systems and assets to protect, what security controls to use, and which risks to mitigate—should be informed by an organization's management, priorities, risk tolerance, and legal and regulatory guidance.

In other words: Although cybersecurity professionals should protect access to systems and data as much as they can, there is a "tipping point" at which too many security controls can either slow down the pace of business or—even worse—encourage employees to find workarounds that bypass the controls altogether.

Find ways to implement cybersecurity controls without slowing down or hampering regular business operations.

CHAPTER 2:

Foundational Cybersecurity Best Practices

So how can real estate organizations protect their customers, data, and brands while also finding a balance between safety and productivity?

Let's break down each security element and discuss the tools and techniques that can be used to find that balance.

Confidentiality

There is more to the concept of confidentiality, which focuses on preventing unauthorized access to sensitive organizational data and systems.

This is because unauthorized access could either be unintentional—like when an employee mistakenly accesses a sensitive file, unknowingly clicks malware in an email, or responds to a spear-phishing scam—or intentional—like when an attacker bypasses security protocols to gain access to sensitive information in a network.

The principle of confidentiality also relates to limiting access to information based on the concept of "least privilege." In this case, least privilege means access to systems, data, and networks should only be granted to users on a "need-to-know" basis. In other words, not only should the number of people with access be limited, but also levels of access should only be as much as is required to fulfill job functions.

Organizations can enforce the confidentiality of their systems and data access in two ways: access control and cryptography.

Access Control

Access control defines limits on when, how, and by whom a system can be used. In practice, access control can come in the form of one or more of the following categories:

Administrative: Access controls founded in policies, job responsibilities (i.e., the separation of duties), or employee training requirements.

Technical: System- or security-based controls that limit certain functions or users based on predefined conditions, such as IP addresses, number of attempted actions outside of permission levels, or even time spent in the system.

Physical: These include environmental security controls such as security cameras, badge-controlled doors, digital or physical locks, and other forms of supervision.

Encryption

The second method to protect a system from accidental and malicious unauthorized access is through encryption. Encryption is enabled via cryptography, including algorithms and key sharing methods to obfuscate data or limit access.

The strength of the cryptographic method can be measured in the number of computer resources required to “break” the key used to unlock, or decrypt, the data.

Integrity

The second pillar of the CIA triad involves integrity, which includes three main elements:

- Protecting data against unauthorized modification.
- Preventing authorized and unauthorized users from modifying data.
- Protecting data consistency, including within the system and in what the data itself is representing.

The primary technique organizations use to protect and monitor the integrity of their systems involves authentication.

The primary technique organizations use to protect and monitor the integrity of their systems involves authentication.

Authentication

User and system authentication determine if a user is who they claim to be when they attempt to gain access or exercise a system privilege.

This authentication process includes two parts: identification and verification.

During identification, the user presents who they claim to be to a verification system (i.e., an identity management system) or a validation feature built into an application. The most common identification is a username, but it can also be a badge or employee number.

During verification, the user must prove their authenticity by providing data that uniquely confirms their identity to the system. This is typically through a password.

Because of growing security concerns and regulatory standards, many organizations have begun to leverage multi-factor authentication, which requires users to present more than one authentication method (i.e., factor) to prove their identity.

In practice, multi-factor authentication can be accomplished using a combination of any of the following types of data:

- Something a user knows (e.g., password or PIN)
- Something a user has (e.g., badge or unique token)
- Something the user "is" (e.g., fingerprint or iris scan)

Availability

The third leg of the CIA triad is availability. Availability focuses on ensuring that the systems used to complete work can perform on demand and provide uninterrupted access. This includes preventing systems from going offline due to misuse, becoming overloaded with malicious traffic or requests, or degrading from malware or misconfiguration.

In practice, organizations can bolster the availability of their systems through three main techniques:

1

Redundancy:
This means having backup (or "fail-over") systems pre-configured, tested, and standing by if the main system goes offline or has a production error. In more advanced cases, this "fail-over process" can be automated, meaning systems can switch from the malfunctioning system to the backup system as soon as a failure is detected.

2

Disaster recovery planning:
As the name suggests, a disaster recovery plan is a proactive exercise that helps organizations prepare the necessary resources, procedures, tools, roles, and responsibilities in case of a natural or man-made disaster. A disaster recovery plan lays out the communications plan, decision tree, and key roles that can make the necessary decisions to restore services and minimize losses.

3

Load balancing:
Also known as distributive allocation, load balancing involves having multiple systems in place to "share the load" of system or network activity so no one specific system is overworked. This also plays into the redundancy technique.

Of course, there are other techniques that organizations can explore and implement to bolster the availability of their business systems, such as outsourcing key functions.

In any case, availability is often measured by the percentage of time that systems are online or "available." For example, a system has "high availability" if its critical services are online and functioning 99.999 percent of the time.

A disaster recovery plan lays out the communications plan, decision tree, and key roles that can make the necessary decisions to restore services and minimize losses.

CHAPTER 3:

Common Cyberthreats

Although every business has a different combination of characteristics, systems, and users, there are common threats that every organization needs to prepare for.

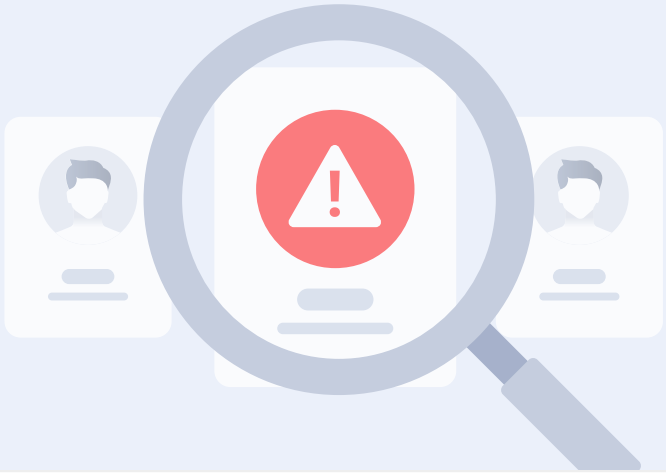
Malware

Any unwanted software installed on your system without your consent is considered malware. Although it can come in different forms and levels of sophistication—including some that can self-propagate—malware can render your systems useless or extract valuable information from your network without your knowledge.

Phishing

A phishing attack involves sending text messages or emails that appear to be from legitimate sources to obtain sensitive information that may be used to gain unauthorized access to a system.

Phishing can involve a cybercriminal using social engineering or technical means. A technical phishing scam could involve a malware-embedded attachment to an email or a link to an illegitimate website to get you to download a virus or pass on personal information.



Social engineering is even more nefarious, as these phishing techniques involve exploiting our natural inclination to trust. For example, a criminal may gain access to your friend, family member, or associate's email account and then request confidential information while posing as your known contact.

An even more likely possibility is that a criminal will create an email account that looks very similar to a trusted account. In doing so, they don't even have to gain access to an account to commit fraud. It's often as simple as changing one letter or number in an email account, like replacing an "I" with a "1". The change is so subtle that most people don't notice it and reply, thinking they are writing to a trusted contact.

Social engineering is a large part of a company's risk exposure and should not be underestimated. Even the best employee or brightest CEO can be coerced into bypassing processes. For example, a criminal posing as a known colleague or business partner could make a convincing case that results in a stakeholder following a different set of wiring instructions or providing sensitive information.

An even more likely possibility is that a criminal will create an email account that looks very similar to a trusted account.

Ransomware

Ransomware is a type of malware that blocks users' access to their data or system or threatens to expose it to outside parties. To regain access, the victim has to pay a ransom to the cybercriminal.

Denial-of-Service Attacks

Either conducted by one attack machine or orchestrated across a large number of machines under the control of malicious software, denial-of-service attacks overwhelm a system's resources and services so that it is unable to respond to legitimate service requests.

Some attackers simply want to take down your systems, whereas others use the system outage to conduct secondary attacks, such as phishing or other advanced hacking techniques.

Business Email Compromise (BEC)

One threat unique to the real estate industry is business email compromise. This type of attack involves a cybercriminal gaining access to or creating a spoof email account and using said email for malicious purposes.

The criminal can often sit on the account for some time, learning more about the stakeholders involved in each transaction and waiting for an opportunity to intervene in a legitimate real estate transaction. When they eventually intervene, they pose as an actual person in the transaction and send an email containing altered bank account information.

Remember, these criminals often act from a fake account that mimics a known and trusted email address. It's always good to double-check sender details and look for anything suspicious before you hit reply.

CHAPTER 4:

Understanding and Mitigating Risk

The above list of potential cyber threats is just a snapshot of what could be a much longer list.

This wide range of potential threats and the number of systems an organization needs to protect can make implementing cybersecurity a complex process. That's why it is essential to understand the role of risk management.

Although cyber-risk management is a domain of knowledge in and of itself, organizational leadership needs to at least be aware of its role in managing information security given the potential for attacks.

Risk management can either be a formalized process in which specific systems, databases, and assets are evaluated for their vulnerabilities or a decentralized process left to individual system owners

It's essential to understand the role of risk management.

In either case, organizations—especially those in the real estate market—need to know how to balance the risks and their associated impacts with the costs of the potential risk mitigation strategies.

For each system, the decisions on which risks to accept, mitigate, or transfer must be documented and reviewed regularly to determine if the assumptions that went into the calculation still apply.

Implementing Cybersecurity Best Practices

Armed with a foundation of cybersecurity principles, an understanding of common cyberthreats, and a framework to make decisions about certain types of risks, businesses can begin to implement cybersecurity best practices.

Get started by considering cybersecurity controls that account for the people, processes, and technologies in your organization. For example, you could leverage a portfolio of cybersecurity tools that:

1. Provide regular security awareness training.

According to one IBM security study, 30 percent of data breaches involve insiders, either unknowingly or maliciously.

This is why comprehensive security awareness training is a key tenant of cybersecurity, especially for those in the real estate industry that have access to a wide range of financial and personal data.

Not only will security awareness training help employees better understand the importance of their role in cybersecurity, but it will also enhance how they handle an incident and prepare them to respond to customers' concerns about privacy.

2. Implement trusted security tools.

As is true of any criminal, a cybercriminal is often looking for the path of least resistance.

When cybercriminals are confronted with security tools that thwart their attacks and frustrate their efforts—such as antivirus and anti-spam tools that block suspicious activity and alert for unusual software or code—it is often enough to scare them off.

There are also more advanced tools designed for businesses in the real estate industry, such as CertifID. CertifID is a user-friendly platform that can confirm the identities of all parties involved in a real estate transaction.

CertifID sends a trusted message to the party, scans the end-user device, confirms their identity, and allows for information to be securely shared. This is especially important when it comes to completing accurate wire transfers.

3. Increase network defenses.

As businesses continue to trend toward remote operations, it is due time to address network defense. Businesses must secure individual computers and the network of devices that enable their web-based services, such as websites, emails, and file servers. If you haven't done this yet, your business is at risk.

First, either take advantage of the built-in security features that come with modern operating systems—such as Windows Defender—or invest in an enterprise antivirus system. Second, utilize network and host-based firewalls to monitor traffic flow and prevent unauthorized access to certain systems, data, or websites. And finally, consider leveraging an enterprise intrusion detection system that monitors network traffic for unusual behavior and flags it for further investigation.

4. Update and patch systems.

Despite their personas, not all cybercriminals conduct sophisticated, multi-stage attacks.

In fact, many cyberattacks leverage known system vulnerabilities that have been reported or patched by software and hardware manufacturers. Cybercriminals keep tabs on updates on patches for critical systems, using them to exploit vulnerable systems that organizations have been slow to update.

It is critical to install the latest software updates recommended by your vendors. This is an easy but essential step to secure the systems you rely on every day.

Cybercriminals keep tabs on updates on patches for critical systems, using them to exploit vulnerable systems that organizations have been slow to update.

5. Implement strong password management.

Passwords are highly sought after by cybercriminals. This is why organizations need to have and enforce strong password management policies.

In addition to changing the default passwords for your network and system devices, organizations should consider implementing multi-factor authentication and setting up password rules that enforce good password hygiene, such as:

- Meeting character size and complexity rules.
- Creating brand new passwords.
- Regularly changing passwords.

And, perhaps most importantly, consider implementing a password manager such as 1Password, Keeper, or LastPass. At this point, it's human nature to use (and re-use) short, simple passwords that are easy to remember. Thankfully, most of these tools can generate random, long, and complex passwords for each of your accounts, but only require one master password.

Password managers come with powerful encryption protocols that ensure your data is secure inside the vault—keeping criminals out and protecting your credentials. Get started with this essential tool today.

CHAPTER 5:

Take the Next Step

As any security professional will tell you, cybersecurity has never been a "set-it-and-forget-it" initiative—it is a moving target that evolves as cybercriminals, their techniques, and the organization's threat landscapes change.

To protect your customers, data, and brand as much as possible, you must make cybersecurity not only a top priority in your business, but also a key part of your organizational culture.

This is precisely where platforms like CertifID fit into the real estate market. CertifID gives you and your customers the peace of mind of knowing that all of the private information needed to complete your transaction is secure and free from manipulation.

Features like these—especially in the real estate industry, in which the consequences of wire fraud are devastating —are essential to your business' success.