Cybersecurity and Privacy Risks

Information for Self-Storage Businesses

MINICO
A JENCAP® COMPANY

Cyberattacks on small and medium-sized businesses in 2018 increased at a rate of nearly 425% over the previous year.[1]

Like most small and medium-sized businesses, self-storage operations are not immune to a cyberattack. In fact, the personal customer data and payment information your self-storage facility collects and stores makes your business as much of a prime target for hackers as a large corporation.

Unfortunately, independently owned self-storage facilities or small self-storage operations that aren't as vigilant about safeguarding their facility's management software systems and customer data are unwittingly putting their business and the customers they serve at risk for a breach. Staying educated on the latest scams, understanding how your business can fall victim to cybercrime and applying risk management best practices can help make you less vulnerable.

In this white paper, we'll look at the cybersecurity risks faced by self-storage operations and the impact a breach can have on your business, as well as trends in cybersecurity threats and best practices to help mitigate and reduce your exposure.

Small Business Cybersecurity Data

43% of all cybersecurity attacks are aimed at small businesses, and that number is expected to increase.

54% of SMBs believe their businesses are "too small" to be targeted by cybercriminals.

83% of SMBs say they lack the money they would need to recover from a cyberattack or data breach.

Is Your Self-Storage Business at Risk?

Imagine business as usual at your self-storage facility...and then it happens. You or an employee clicks on a malicious link from a bad email or unsecured website that freezes your system's data. Or an employee receives an email that appears to be from you, a manager, or a vendor that asks for a reply for the purpose of gaining access to your management system. Once inside your system, cybercriminals install malicious software or create a portal for hackers to steal sensitive customer data and payment information.

"When you consider the different types of personal customer information stored in a facility's system and that a standard self-storage facility can transact between 10 and 20 payments per day, owners must be proactive when it comes to cybersecurity," says James Appleton, Director of Sales, Special Risks, for MiniCo Insurance Agency. "Facilities that continue to operate with outdated software, store information on a local platform and don't keep up with anti-virus and ransomware protection are prime targets for a breach."

One reason self-storage facilities are at greater risk for a cyberattack is that many continue to store customer and security information locally on a software program/database or on the system's physical hard drive.

[1] 4iQ Identify Breach Report 2018, *Identities in the Wild: The Long Tail of Small Breaches.*

For customers making payments, having their financial information stored on a local platform versus a web-based facility management software program makes their information a lot easier for hackers to access. On the security side, additional risk factors of storing data locally include the risk of tenant security gate codes and alarm systems being transmitted or hijacked as nonencrypted data makes it easier for cybercriminals to locate and steal information.

The Financial Impact of a Breach

If your self-storage business is the victim of a data breach, the financial costs incurred to resolve and recover from the event can be staggering. According to the Ponemon Institute**,** the average price for a small business to clean up after a breach is approximately $690,000, and this figure doesn't take into account the loss of revenue.

Some of the more direct costs associated with a data breach include:

- Notifying your storage customers that a breach has occurred. This can include having to hire a third-party consultant to manage recovery efforts as well as mail and email communication procedures that include communicating with data-protection regulators and other related parties.
- Conducting a forensic investigation to determine the source and extent of the breach.
- Fines and penalties imposed by the Payment Card Industry Security Standards Council, payment card associations, and your facility's own financial institution.
- Ongoing customer credit report monitoring and identity theft repair and, in some cases, costs associated with reissuing credit and debit cards to customers whose personal data was compromised.
- Upgrading or having to replace your compromised computer system, payment software and hardware, and server.
- The often-required implementation of additional security monitoring services to ensure ongoing compliance with the Payment Card Industry Data Security Standards (PCI DSS).

Financial Costs of Cybercrime

A cyberattack caused by a weak or stolen employee password costs a small business an average of $383,363 per incident.

Source: Microsoft

Lost Revenue and Reputational Costs

In addition to the more direct costs associated with a breach are the loss of customers and the good reputation of your storage business. According to IBM, a data breach can cost a small business up to 5% of its annual revenue in lost business**.** In fact, approximately 60% of small businesses end up closing their doors within six months of a data breach because they are unable to fully recover from the financial or reputational impact.

For the 40% that do survive, data breach costs can follow them for years. The IBM report found that just 67% of the total cost of a breach happens in the first year, with 22% occurring in the second year after the breach and 11% of those costs accruing past the second year.

But perhaps the biggest long-term consequence of a data breach is the loss of customer trust. In a competitive market, a business must work tirelessly to build and maintain the integrity of its brand. Unfortunately, a single compromising data breach can harm even the best of reputations, making it difficult for a small business to fully recover.

Consumers today are willing to share their sensitive information with businesses because they assume that the proper security measures are in place to protect them. When renting a storage space from your facility, your customers trust you to keep their personal data and payment information safe and secure.

Don't Let Your Self-Storage Facility Become an Easy Target

As small business operations, self-storage facilities can be prime targets for cybercriminals who can use customer information to rob bank accounts via wire transfers, steal customers' personal identity information, and commit other fraudulent activities. Unfortunately, no matter how prepared you may be, data breaches can still occur.
In general, many small businesses are vulnerable to data breaches for three key reasons:

- They don't believe they are at risk.
- They often lack the time, resources, and technology know-how to implement safeguards to protect their businesses.
- It typically takes a smaller business longer to detect a breach once it happens.

The Top Five Cybersecurity Threats For Self-Storage Facilities

Password Attacks. A password attack often uses an automated system in which different password combinations are used to try to gain entry to a network. A hacker would target an easily accessible site within your system and use a password to gain access to personal customer information for identity theft purposes as well as confidential payment data.

Malware. Short for "malicious software," malware works by infecting a computer to disable a system, prevent user access, or steal sensitive or valuable data. Malware is typically hidden in an email attachment, link, popup, or webpage. It works by breaching a network through a vulnerability such as when a user downloads an email attachment or clicks on a dangerous link that installs risky software.

On average, cyber attackers spend 146 days (20+ weeks) on a business network before being detected.

Source: Microsoft

Phishing

Today, phishing remains the top method of cyber-criminals, accounting for 93% of all breaches, which are conducted predominantly over email.

Source: Verizon Data Breach Investigations Report (2018)

Ransomware

Nearly 70% of ransomware attacks in 2018 targeted small businesses, with an average ransom demand of $116,000.

Source: Beazley Breach Response Services

MITM Attacks

The primary goals of an MITM attack are to:

- Steal personal information for identity theft.
- Gain login credentials from a user.
- Get a credit card number or other payment information.

Phishing. In a phishing attack, someone masquerades as a trustworthy source in an attempt to bait a user to surrender sensitive information, such as a username, password, or credit card number. Another way to look at phishing is as a door where a hacker picks the lock and a phisher convinces the user to let them in. The three most common types of phishing attacks on small businesses are:

- **Deceptive phishing.** A user receives an email that claims to come from a recognized source and asks a user to reenter sensitive information or make a payment.
- **Spear phishing.** A user receives an email that looks legitimate and may have information such as a name, position, company, or work phone number to trick them into believing the sender is authentic.
- **Pharming.** Criminals send users to a fraudulent website that looks legitimate. Unlike a typical phishing attack, victims don't have to click a link. Instead, hackers use a computer to redirect the user to a fake URL.

Ransomware. Ransomware is a type of malicious software designed to block access to a computer system or computer files until a sum of money is paid. It freezes a computer and encrypts files on the system to make data inaccessible. A warning pops up and demands that you pay a ransom within a certain time frame in order to receive a private key to decrypt and restore access to your files. Once encrypted, there is no technical way to fix your system other than wiping it clean and restoring it with backup data.

Man-in-the-Middle Attack (MITM). Also known as an eavesdropping attack, an MITM attack lets hackers secretly put themselves between users and a web service they're trying to access, allowing the attackers to filter and steal personal customer data. The strategy gives the perpetrator the ability to insert their own cryptocurrency wallet to steal funds, redirect a browser to a malicious website, or passively steal information to be used in later cybercrimes. An attack can come from an email, social media, or simply by browsing the internet.

Cybersecurity Best Practices

Cybersecurity best practices should encompass a multilayered protection strategy that includes:

- **Conducting password management policy/training at your facility for all employees.** Cybersecurity training should include password management that covers best practices in how to create strong passwords using a combination of numbers, letters and symbols.

- **Using a web-based PCI-compliant software system.** A web-based facility management system is a superior method of safeguarding your data versus storing information on a local platform where it is an easier target for hackers.
- **Protecting your wireless network.** Safeguard routers by changing the default name and password, disabling remote management, and logging out as the administrator once the router has been set up. Be sure that routers use WPA2 or WPA3 encryption (a certified Wi-Fi hardware technology) to ensure outsiders can't read information sent over the network.
- **Prohibiting the connection of personal or untrusted storage devices or hardware to computers, mobile devices, or networks.** Remind employees and management that USB drives and external hard drives should not be shared between personal and business computers or devices, and no unknown or untrusted hardware should be connected to the facility's system or network.
- **Backing up and encrypting data in the cloud.** A cloud-based data backup program allows you to automatically and safely store your system data independent of your facility management software system. The encryption process transforms data into ciphertext, which is nearly impossible to use without decryption. In the event of a cybersecurity event, having your data safely stored off premises allows you to quickly retrieve and restore your system's information.
- **Implementing multifactor authentication.** Consider a rotating PIN in addition to a password to verify a user's identity when accessing the company email or network. This provides an additional level of protection even if a user's password has been compromised.
- **Controlling access to your facility's network.** Establish procedures that limit employee access to only what is needed to perform their jobs. Create a process for immediately revoking user access and changing passwords when an employee leaves your business or is let go.
- **Establishing a recovery plan.** After a cybersecurity incident, it is important to begin recovery efforts as soon as possible in order to resume normal business operations. A recovery plan helps expedite the process by making it easier for your facility to restore and resume services more quickly.
- **Securing cyber insurance.** Cyber insurance is a critical component of cybersecurity management for self-storage facilities, covering both first- and third-party costs as well as business interruption expenses if a cybersecurity breach forces your business to shut down. Examples of specific coverages available under a cyber insurance policy include notification expense,

crisis management, regulatory investigation expense, data breach liability, content liability, data loss and system damage (data restoration), data extortion, and business interruption.

Conclusion

A cyberattack can have a serious financial and reputational impact on your self-storage business. Staying informed on key issues, regulatory changes, and laws as well as implementing proper risk management best practices and safeguards that include cyber insurance can make it much easier to prevent and detect a security issue and help facilitate recovery.

MiniCo Insurance Agency's Cyber Insurance Program

MiniCo Insurance Agency launched the first insurance product designed specifically for self-storage facilities in 1974 and remains the nation's leading provider of specialty coverage for self-storage risks. To address the growing issue of cybersecurity risks for self-storage businesses, we offer a monoline cyber insurance program that provides critical coverage for costs resulting from a data breach and related expenses associated with the loss of data.

MiniCo Cyber Insurance Program: Coverage Highlights

- **Security and Privacy Liability.** Includes liability to employees and customers in the event of data theft.
- **Data Recovery and Loss of Business Income**. Includes denial-of-service attacks and system malfunction.
- **Privacy Regulatory Defense and Penalties.** Includes costs to comply with any regulatory action following a data breach.
- **Crisis Management Costs**. Includes costs of customer notification, support, and credit-monitoring expenses.
- **Data Extortion.** Includes payment of "ransom monies" to secure the return of data. Coverage available nationwide with limits up to $1 million.

For more information on MiniCo's cyber insurance program for small and medium-sized businesses, visit **www.minico.com/cyber** or call **800-528-1056**.