MESSENGER

August 2024

Digital Dangers

Safeguarding And Navigating Cybersecurity

BY BRIAN AMIDEO

PAGE 14

Powerful Partnership

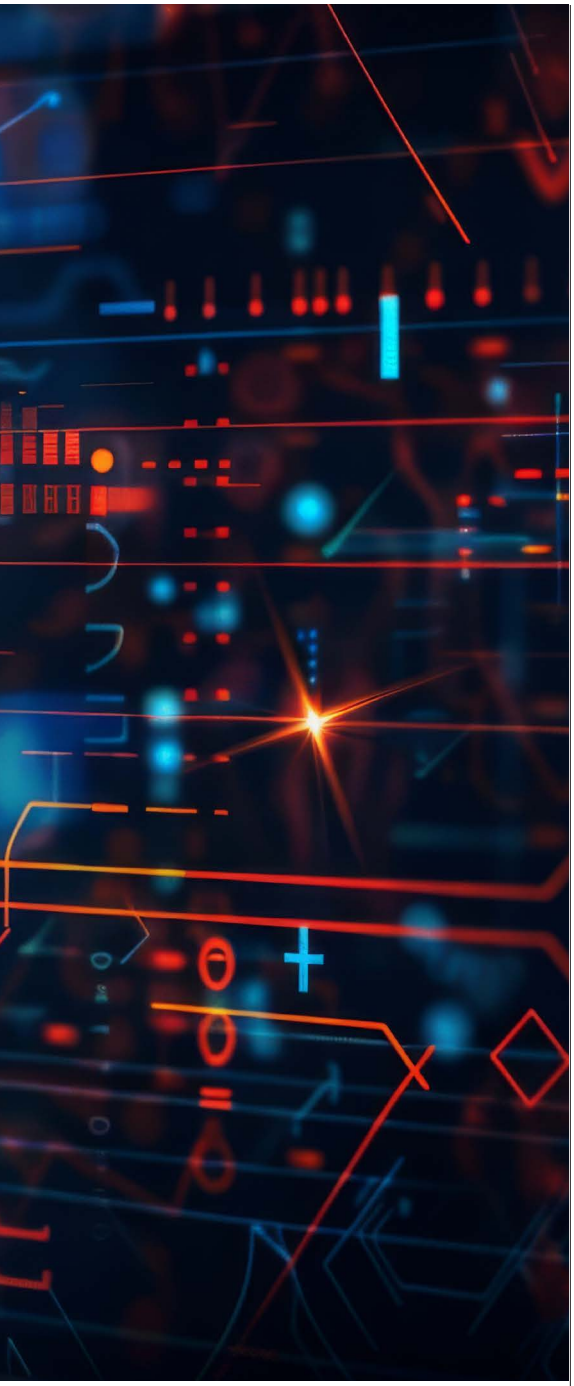
Digital Dangers

Safeguarding And Navigating Cybersecurity

BY BRIAN AMIDEO

In an age where digitization permeates nearly every aspect of our lives, the self-storage industry is not exempt from digital transformation. With the convenience of online reservations, payments, and management systems, self-storage facilities have become reliant on technology to streamline operations and enhance customer experience. However, this reliance also exposes the industry to cybersecurity threats that can compromise sensitive data and erode trust.

I come from the physical security world of gates, alarms, cameras, and keypads—things to manage access or prevent it. Without them, you risk unauthorized entry to common and personal space and property. We must apply this theology to the technology side. These layers play a role together, as not one of them can do the job alone. Physical security devices need to be protected from the bad actors who are working to gain access to your information, just like the gate and door locks help prevent someone from wandering on your property. If your facility was across the street from one with those basic safeguards and you had none, would you be competitive? How do you protect your business and your renters' digital and physical property? How much personal information are you responsible for? This is cybersecurity and what cybersecurity insurance does to mitigate in the unfortunate situation when that scenario happens.



Understanding The Risks

The self-storage industry deals with vast amounts of personal and financial data, including customer information, payment details, and access records. This wealth of data makes self-storage facilities prime targets for cyberattacks. Malicious actors may attempt to breach security systems to steal valuable data for identity theft, financial fraud, or ransomware attacks.

One of the primary challenges facing the self-storage industry is the diverse nature of its clientele. While some customers may rent storage units for short periods, others may require long-term storage solutions. This diversity creates complexities in data management and cybersecurity, as facilities must secure data for both transient and extended periods while ensuring compliance with privacy regulations.

The common misconception is believing that you are too small to be a target. Small and medium-sized businesses are attacked more than large organizations. We just don't hear about those on the news. It's just not as interesting or sexy. It's hard to report on $50,000 when you can sensationalize $50 million. A large, more mature organization will have continuity plans in place and the funds to survive the process. How many SMBs can handle the downtime, remediation costs, or the reputational damage? The answer is almost none! The real cost is not the ransom price but the cost to fix the problem.

Mitigating Cybersecurity Threats

To mitigate cybersecurity threats effectively, self-storage facilities must adopt a multi-layered approach that encompasses technological solutions, employee training, and regulatory compliance.

ROBUST IT INFRASTRUCTURE

Investing in robust IT infrastructure is essential for safeguarding sensitive data. This includes implementing firewalls, encryption protocols, intrusion detection systems, and regular security updates. Additionally, facilities should consider cloud-based data storage solutions that offer advanced security features and redundancy to prevent data loss in the event of a breach.

EMPLOYEE TRAINING AND AWARENESS

Human error remains one of the leading causes of cybersecurity breaches. Therefore, comprehensive employee training programs are crucial for raising awareness about cybersecurity best practices and potential threats. Employees should be educated on password hygiene, phishing scams, and protocols for handling sensitive information. Regular training sessions and simulated phishing exercises can help reinforce security awareness among staff members.

PRIVILEGED ACCESS MANAGEMENT AND MONITORING

Implementing stringent access management measures is vital for preventing unauthorized access to a company's and its clients' sensitive data. Privileged Access Management (PAM) protects against credential theft and privilege misuse by assigning higher permission levels to accounts with access to critical resources and administrative-level controls. PAM is based on the principle of least privilege, which ensures that users are only granted the minimum access levels required to perform their job functions.

COMPLIANCE WITH REGULATIONS

The self-storage industry is subject to various data protection regulations, such as the California Consumer Privacy Act (CCPA). Compliance with regulations is not only a legal requirement but also essential for maintaining customer trust. Payment Card Industry (PCI) compliance is a set of 12 security standards that businesses must follow when accepting, processing, storing, and transmitting credit card data. Facilities must ensure that their data handling practices adhere to relevant regulations, including data encryption, anonymization, and secure data disposal procedures.

Looking Ahead

As technology continues to evolve, the self-storage industry must remain vigilant against emerging cybersecurity threats. The rise of Internet of Things (IoT) devices, mobile applications, and remote management systems introduces new vulnerabilities that require proactive measures to address.

Furthermore, the increasing digitization of customer interactions presents opportunities for innovation and enhanced service delivery. Mobile apps that enable customers to access their storage units remotely or receive real-time updates on security alerts can improve convenience and customer

satisfaction. However, these innovations must be accompanied by robust cybersecurity measures to safeguard against exploitation by malicious actors.

In conclusion, cybersecurity is a critical concern for the self-storage industry in an increasingly digital world. By implementing comprehensive security measures, investing in employee training, and staying abreast of regulatory requirements, self-storage facilities can protect sensitive data, preserve customer trust, and maintain a competitive edge in the market. As custodians of valuable possessions and information, safeguarding storage goes beyond physical locks; it requires a steadfast commitment to cybersecurity.

Shielding Storage

Continuing where digital threats loom large, the self-storage industry finds itself increasingly reliant on digital systems to manage operations efficiently and cater to customer needs. While this digitalization brings many benefits, it also exposes self-storage facilities to many cyber risks. In this landscape, cyber liability insurance emerges as a crucial safeguard, offering protection against the financial and reputational fallout of cyber incidents.

Cyber Liability Insurance

Cyber liability insurance is a specialized form of coverage designed to protect businesses from the financial consequences of cyberattacks and data breaches. It provides coverage for various expenses incurred in the aftermath of a cyber incident, including legal fees, notification costs, forensic investigations, and even extortion payments in the case of ransomware attacks.

For self-storage facilities, cyber liability insurance is particularly vital due to the sensitive nature of the data they handle. From customer personal information to payment details, self-storage facilities possess a treasure trove of data that cybercriminals target for theft or exploitation. In the event of a data breach, the costs can quickly escalate, encompassing not only financial losses but also damage to reputation and customer trust.

Cyber liability insurance policies typically offer coverage across several key areas:

- **Data Breach Response -** This covers the expenses associated with responding to a data breach, including forensic investigations to determine the cause of the breach, notification costs to inform affected individuals, and credit monitoring services to mitigate potential identity theft.
- **Third-Party Liability -** If a data breach results in third-party claims or lawsuits, cyber liability insurance can cover legal defense costs, settlements, or judgments. This includes claims of negligence, breach of privacy, or failure to protect sensitive information.
- **Regulatory Compliance -** In the wake of a data breach, self-storage facilities may face regulatory investigations and fines for non-compliance with data protection laws. Cyber liability insurance can help cover the costs of regulatory defense and any resulting fines or penalties.
- **Cyber Extortion -** In the event of a ransomware attack, where cybercriminals encrypt data and demand payment for its release, cyber liability insurance can cover ransom payments as well as the expenses associated with negotiating with extortionists.

Choosing The Right Coverage

When selecting cyber liability insurance for their self-storage facilities, owners and operators should consider several factors:

COVERAGE LIMITS

Ensure the policy provides adequate coverage limits to mitigate potential financial losses in a cyber incident. Assess the potential costs of data breach response, legal defense, regulatory fines, and other expenses to determine appropriate coverage levels. The most common portion underinsured is the aggregate relative to the company revenue. It needs to be at a point where the insurance can float the business during the downtime.

POLICY EXCLUSIONS

Pay close attention to policy exclusions to understand what is not covered under the insurance policy. Common exclusions may include acts of war, intentional acts, or certain types of cyber incidents.

ADDITIONAL SERVICES

Some cyber liability insurance policies require additional controls in place, such as risk assessments, employee training, and breach response planning. IT Managed Service Providers (MSPs) services can help self-storage facilities strengthen their cybersecurity posture and mitigate risks proactively while managing the technology on the day to day.

Invest In Coverage

In an increasingly digitized world, cyber threats pose significant challenges to the self-storage industry. Cyber liability insurance provides a crucial safety net, offering financial protection and peace of mind in the face of evolving cyber risks. By investing in comprehensive cyber liability coverage, self-storage facilities can fortify their defenses, safeguard sensitive data, and preserve customer trust in an era fraught with digital peril.

We can no longer do it ourselves or have a guy. We can no longer hope it doesn't happen to us or wish for the best. Self-storage needs dedicated, hands-on IT services and insurance, whether internal or external. Now add the high-level experts to guide those in the trenches. It requires specialized expertise in key areas that the proverbial Swiss Army knife individual can no longer do at a level we need things done. We are at the beginning of a new frontier, and we must embrace and trust those that dedicate their time to understanding to help protect our business and our clients. ■

Brian Amideo is the business solutions advisor for FullScope IT. He has been a technology enthusiast and professional for over 30 years.