PHOTO CREDIT: ©Max Taylor Photography Inc.

Defending Your Data:

Shielding Sensitive Info from Cybercriminals

Strategies and tactics for thwarting cyberattacks, such as hacking, phishing, identity theft and more

By Mark Battersby

The recent headlines about internet hacking and security breaches have focused on large retailers and big banks. Unfortunately, fraud and financial data losses are not limited to retailers or any one industry. Linen, uniform and facility services businesses are increasingly vulnerable to cybercrimes and fraud.

Cybercrime and cyberattacks are among the fastest-growing crimes today, with 43%-45% affecting small businesses, according to *SQ Magazine* and other sources. Prevention is the best approach, even though cybercrimes and cyberfraud may qualify as casualty or theft losses for tax purposes and may be covered by insurance.

The Threats

Today, with almost every business involved in some form of internet commerce or data storage, such as customer lists, employee information, books, records, receipts, tax documents and credit cards, a significant number of businesses have minimal contingency planning capabilities for dealing with a cyberattack. A 2026 report in *SQ Magazine* found that 19% of businesses hit by cybercriminals still had little or no plan to address future data breaches or losses.

The Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3) received 859,532 complaints in 2024, with reported losses exceeding $16 billion, representing about a 33% increase from 2023. The top three categories by complaint volume in 2024 were phishing/spoofing, extortion and personal data breaches—a key reminder that the "front door" is often an inbox, not a firewall—(**bleepingcomputer.com**) (**fbi.gov**).

Using the internet to conduct business or retain records heightens cybersecurity risks for linen, uniform and facility services operations, as cybercriminals can strike from within or outside the business. Hackers can steal customer lists or credit card information, and viruses can infect the organization's files, causing significant damage.

Cybercrime: A Growth Industry

Cyberthieves are constantly coming up with new ways to steal passwords, hack files and download sensitive data that can be sold—or used to steal from a linen, uniform and facility services business or its customers. The incidence of cyberthefts and fraud is increasing. Cybercrooks may steal your operation's customer list or credit information. Viruses can infect files, causing costly havoc. Cybercrime is a fast-growing category, with U.S. cybercrime losses in 2024-'25 at $16 billion, according to the FBI's IC3.

It's important to create security measures that not only keep cybercrooks at bay, but also prevent the operation's employees from snooping where they shouldn't and ex-employees from accessing the system after they leave the company.

The Internet continues to make electronic banking more convenient. But it also creates new risks. With electronic banking, every linen, uniform and facility services business assumes greater liability for online fraud.

In essence, every business using electronic banking must take careful stock of its account-reconciliation process. A lax approach to cybersecurity could leave the operation with few options in the event of cyber fraud.

Surprisingly, a large number of small business owners and managers reportedly aren't concerned about cyber threats—either external or internal. External threats include a hacker or cyber-criminal stealing data, while internal threats usually involve an employee, ex-employee or contractor/consultant stealing data.

Unfortunately, data breaches or hacking incidents can harm any business and can undermine trust among consumers, partners and suppliers. Every business, especially those transacting sales online, should have a cybersecurity plan that includes keeping computers "clean," protecting information, frequently changing passwords and using effective antivirus software.

Managing Risks

No business is immune to cyber threats. Taking the necessary precautions is critical. A data breach or hacking incident can not only harm a commercial or institutional laundry but also damage your reputation among customers, partners and suppliers. All businesses must take steps to protect their operations from cyber threats and help employees stay safe online. In fact, it's a laundry operator's obligation to protect the data and the financial information of its customers, suppliers and employees.

While cyber threats pose risks to any business, a strong cybersecurity strategy can give it a competitive edge. Stopping information theft means protecting sensitive data, including operational, customer and supplier financial records.

Tips that can help secure a laundry operator's data, reduce its liability and—in many cases—lower the cost of insuring against potential losses, include:

- Isolating from the rest of the operation's network any computers that are used for sensitive applications, such as making electronic bank deposits.
- Controlling access to data by limiting to secure channels the delivery and exchange of customer-, supplier- or employee-related documents and information.
- Requiring employees to enable multi-factor authentication (MFA), which is resistant to phishing on all accounts that offer it. Phishing is a type of scam in which criminals pose as a trusted company or individual (such as the company's bank) via email, text or call to trick the business into revealing sensitive information, such as passwords or bank details. It's often as simple as clicking on a false link to a fake website that looks legitimate.
- Requiring strong passwords and considering utilizing a password manager.

- Getting a firewall. There are affordable, easy-to-use hardware and software approaches.
- Backing up all data regularly. This should include establishing measures both to protect and test all backups.
- Getting anti-virus software and using it. There are several popular packages, most of which are relatively inexpensive.

When an employee or contractor who has had access to the system leaves the business, the employer should ensure that their passwords are disabled at the end of their tenure to lock them out of the system.

Everyone needs to learn the basics of protecting the business from phishing. Action steps include:

- Creating—and implementing—a data-security plan that includes immediate notification of all affected parties.
- Educating all employees on the dangers of phishing and account takeovers. It only takes one employee to click a link, giving cybercriminals access to the operation's entire system.
- Sharing liability by demanding similar protocols with suppliers and checking for compliance.

Keeping cybercriminals away from laundry operations is essential to preventing data theft. That means keeping all security-related and antivirus software up to date and monitoring employees with access to sensitive information. This includes "hard" assets, such as documents. Managers should oversee the shredding of these documents.

Insurance Aid

Today's insurance policies typically don't cover a business's data, although some of a business's insurance policies may offer general liability protection. For example, commercial crime insurance policies may cover funds lost to cyber fraud, such as phishing or so-called "business email compromise," but only if the loss directly follows a computer attack.

Under most commercial coverage, data breaches are generally not considered physical damage. This can lead to disputes over whether standard general liability policies cover them. Conversely, dedicated cyber insurance policies are designed to cover system damage, data replacement and extortion.

Cyber-liability policies were created to cover identity theft, business interruptions caused by network shutdowns, damage to a business's reputation, and the costs associated with data breaches. Policies can also cover the theft of digital assets, malicious attacks via computer code, human errors that disclose sensitive information, credit monitoring services and lawsuits. Many operators are beginning to recognize the importance of cyber insurance in today's complex and high-risk digital landscape.

Adoption varies widely by company size, but a 2024 Huntress survey found 22% of companies still don't have cyber insurance (meaning about 78% do). Separately, NAIC market reporting shows the U.S. cyber insurance market includes millions of policies in force and billions in premiums, reflecting broad growth and participation. (**huntress.com**) (**content.naic.org**).

Cyber liability insurance can cover attacks by hackers, viruses and "worms" that steal or destroy a business's data. Worms are a type of malicious software (malware) that can self-replicate and spread across networks without human intervention. That means they don't require a user to click, install, or open anything.

Other policies, such as Employment Practices Liability, can cover e-mail or social-networking harassment and discrimination claims, while Media Liability Insurance can cover trademark/copyright infringement.

Tax Considerations

As noted, cybercrimes may qualify as casualty or theft losses, although their deductibility is often limited. And remember, personal losses, except those incurred in a trade or business or in a transaction entered into for profit (e.g., investment-account fraud), are not tax-deductible.

Losses from any sudden or unexpected event, such as a fire, flood, vandalism or theft, usually qualify as business-loss deductions. Losses are deducted in the year they occurred or, in the case of a theft loss, when discovered. Naturally, documentation is required, and any deduction must be reduced by any insurance or other compensation received or for which there is not a "reasonable" prospect of recovery. If an incident occurs, preserve documentation (bank records, incident reports, insurer correspondence), and consult a tax professional early (**irs.gov**), (**law.cornell.edu**).

Win the War

A growing number of cyberthreats increasingly target businesses of all sizes. They need to defend their data using every available protection strategy—including cybersecurity—to shield sensitive information from cybercriminals. Cybersecurity is—or should be—an ongoing process. Because technologies, regulations/laws and cybersecurity threats continue to evolve, every linen, uniform and facility services professional should strive for continuous improvement of their operation's cybersecurity risk management. **TS**

MARK BATTERSBY is a freelance writer based in Ardmore, PA.