4 TIPS FOR CYBERSECURITY

Your Business Cybersecurity Guide

Centaris
248-284-7100
www.Centaris.com

CENTARIS™

71% of data breaches happen to businesses with less than 100 employees.

Smaller Businesses are Easy Targets

Small and midsize businesses (SMBs) spend less on cybersecurity than larger organizations. Cybercriminals will take addresses, social security numbers, dates of birth, driver's license numbers, bank account numbers, and more. They target SMBs because of the amount of information they hold. Hackers can use this identifiable information for identity theft, tax fraud, and other financial crimes.

"Data breaches don't just happen to large companies; they happen to businesses of all sizes."

60% of Small Businesses go out of Business After a Data Breach

Data breaches can be costly and harm a company's brand. Expenses for identity monitoring, IT, breach notification, and legal counsel can add up quickly. Following a data breach, clients frequently stop doing business with a company because they no longer feel trusted, and bad press discourages potential clients from using the company's services. Data breaches create psychological stress and anxiety in business owners and staff.

Ransomware is a Real Threat to All Businesses

Ransomware is a form of cyber-attack that involves encrypting data and demanding a ransom or payment for decrypting and releasing the data. Ransomware is commonly linked to deceptive emails known as phishing emails, which typically include harmful attachments like Microsoft Word documents or PDF files. Upon opening these attachments, a program will lock or encrypt all the data stored on the workstation.

Ransomware can spread to other workstations and servers on the network. Criminals target healthcare organizations, law firms, financial service organizations, and businesses with valuable data. These hackers are aware that it is more convenient to seize a company's data as a ransom rather than stealing it for personal use. The odds of being apprehended for dispersing ransomware are significantly lower compared to conventional hacking or cybercriminal activities. Hospitals, law firms, and many other organizations have closed for weeks because of successful ransomware attacks that have encrypted the entire network and made access to company data and systems impossible.

"A single employee falling for a phishing scam is all it takes to destroy your business."

Employees are Your Weakest Security Link

According to one study, employee error is to blame for 95% of data breaches. These errors include sending private information to the wrong person, losing a laptop or smartphone, and being a victim of ransomware or phishing attacks. Security awareness training is necessary for staff members to help avoid errors that result in data breaches. Even though SMBs are a target for criminal activity, by following best practices, you can shield your business from data breaches and cyberattacks.

"The following are 4 best practices that you can take to minimize the chance of data breaches."

1. Secure Passwords

Passwords are the access codes for networks, consumer data, online banking, and social media platforms.

Password best practices include:

Use Strong Passwords.

- Make the password at least 8 characters long. The longer the better. Longer passwords are more difficult for hackers to figure out. Use upper- and lower-case letters, as well as numbers and symbols.
- Passphrases are something to think about employing when you're creating passwords. If feasible, use a personal sentence like "I attended Lawson Middle School in 2002" so your password would look like this: "I@LMS#2002."
- Don't use dictionary words. If it's in the dictionary, there is a chance someone will guess it. Criminals regularly use software that can guess terms and words found in dictionaries.

Change Passwords.

For safety reasons, change your passwords every 60 to 90 days.

Don't Post it in Plain Sight.

Even though this may appear to be self-evident, research has shown that too many employees stick a note with their password on their computer monitor.

Consider Using a Password Manager.

You can create very strong passwords for each of your accounts using programs or Web services because you only need to remember one password to access the program or secure website that stores your credentials.

Consider Using Multi-Factor Authentication.

Set up two-factor authentication, which requires you to enter a random code that appears on your phone. This way, hackers cannot access an account without having physical access to your phone.

2. Encrypt Data

There are many USB drives, smartphones, and lost laptops that lead to data breaches.

The amount of identifiable data stored on mobile devices is something that many businesses are unaware of. Emails, spreadsheets, project papers, PDF files, and scanned photos may contain sensitive information.

Encrypting sensitive data is the best approach to keeping it safe. Encryption is considered a "safe harbor" under multiple federal and state regulations. This implies that if a mobile device is lost or stolen and the information on it is encrypted, there would be no breach that needs to be reported. Notifying customers or those who may be impacted would not be necessary.

Types of Encryption

Mobile Device Encryption.

Encryption is possible for USB drives, laptops, and cell phones. Encryption will protect any data that is on these devices.

Email encryption.

Emails could contain sensitive information and should be encrypted. An encrypted email will protect the data that is sent.

Workstation encryption.

Desktops and workstations can be encrypted in the same way as we can secure laptops to safeguard any data that is stored on them. If workstations are broken into or stolen, it is critical to have encryption installed on each individual workstation. It is possible for a data breach to occur if businesses do not implement encryption on a stolen workstation.

3. Employee Security Training

Employee errors are to blame for 95% of data breaches. Making sure staff members are aware of the dangers of private data and the possibility of data breaches is essential. Ransomware and phishing are the two most popular attack techniques. Employees must be aware of the risks associated with email attachments and how to recognize phishing emails and websites. The risks of hacking, lost or stolen mobile devices, sharing private information on social media, and other factors leading to data breaches must all be considered during training.

In a successful training program, your staff will be reminded about the risks associated with data breaches and the steps they may take to avoid becoming victims. Every day, cybercriminals come up with new schemes and attacks, and it is your responsibility to make sure your staff are aware of these schemes.

"Employee errors cause 95% of data breaches."

4. Perform a Security Risk Assessment

A security risk assessment (SRA) is a critical step to understanding the risk to your business and sensitive information.

An SRA will inventory customer, employee, vendor, and sensitive data, identify how you are currently protecting the data and make recommendations on how to lower the risk to the data.

Understanding your risk of phishing scams and ransomware, the risks of lost mobile devices, the risk of insider threats, and how well prepared you are for a crisis are all things that may be accomplished with the assistance of a security risk assessment (SRA).

Without a thorough understanding of risk, it is difficult to implement the safeguards needed to protect your business. Like any other company risk, cybersecurity must be assessed and managed.

"Many small and medium-sized businesses are unaware of potential hazards to their vital data."

www.Centaris.com | 248-284-7100