CW technology

LEARN HOW IT WORKS

TIPS FOR CYBER SECURITY & BEST PRACTICES

Jeremy Caine
Chief Technical Officer

CW technology

TABLE OF CONTENTS

AUTHOR'S NOTE

Jeremy Caine is a partner and the Director of Technology at CW Technology.

With over 20 years of experience in providing IT solutions and exceptional customer service, he understands that technology is an aid to help businesses achieve their goals.

Jeremy's passion for technology dives deeper than just on the surface level... He focuses on learning how technology positively affects the day-to-day business operations , ensuring that all clients obtain their optimal, customiazed solutions.

At CW Technology, Jeremy's role is demonstrating to clients how simple technology and its implementation is.

According to his expertise, technologic success is all about strategic positioningto provide secure, reliable, and easy solutions that align with business processes. When not at work, Jeremy enjoys relaxing up at the family cabin in north Minnesota with his wife and two daughters.

INTRODUCTION

Cyber threats are an ever increasing concern for small and midsize businesses (SMBs). Today, more sophisticated and managed attacks are happening at an ever increasing rate. To think your business is too small or too isolated to be affected by a cyber attack can be a devastating miscalculation...

WHY IT MATTERS

Recent studies show that 71% of data breaches happen to companies with less than 100 employees. This is a startling number - one all SMBs must be aware of and plan for, especially since they tend to invest significantly less into cybersecurity than their large company counterparts.

Cybercriminals often target SMBs because they collect personally identifiable information that can be used for identity theft, tax fraud, and other financial crimes. This includes customer, employee, and vendor information such as:

- Name, address, and date of birth.
- Social security, driver’s license, and insurance.

This is all a criminal needs to commit a cyber attack, or data breach, on SMB's. Once hit, they are immediately and excessively hurt, including countless expenses, a damaged reputation, and diminished brand equity. Approximately 60% of small businesses go out of business after a data breach!

Legal, IT, breach notification, and identity monitoring expenses add up quickly, leaving owners and employees stressed and anxious after data breaches. Following a data breach, lack of trust causes current customers to leave a business, while the negative publicity keeps new customers at bay.

CHAPTER 1

RANSOMWARE IS A THREAT TO ALL BUSINESSES

Ransomware is a method of holding data hostage until a ransom or payment has been made to release the data; it is usually associated with fake emails, or phishing emails, that contain malicious attachments such as Microsoft Word documents or PDF files.

Once these attachments are opened, a program locks or encrypts all the data, spreading to workstations and servers on the network.

6,192

Businesses fall victim to a ransomware attack each day.

20 BILLION

Estimated cost of ransomware attacks by 2021.

104%

Average increase in ransomware payments since 2019.

Criminals target healthcare organizations, law firms, financial service organizations, and any businesses that have valuable data which they cannot afford to lose.

As a result, hospitals, law firms and many other organizations shut down for weeks... This is due to the successful ransomware attacks that have encrypted the entire network and made access to company data and systems impossible.

CHAPTER 2

EMPLOYEES ARE YOUR WEAKEST SECURITY LINK

A recent IBM study stated that 95% of data breaches are caused by employee mistakes such as falling victim to a phishing or ransomware attack, losing a laptop or smartphone, or sending sensitive information to the wrong recipient.

To prevent such mistakes, employees must be consistently trained in security awareness and have basic knowledge on how to avoid such attacks.

BEST PRACTICES

Although criminals target SMBs as a whole, employing best practices can help protect yourself and any company against cyberattacks and data breaches on any level. The following are best practices that you should take to minimize your risk:

SECURE PASSWORDS

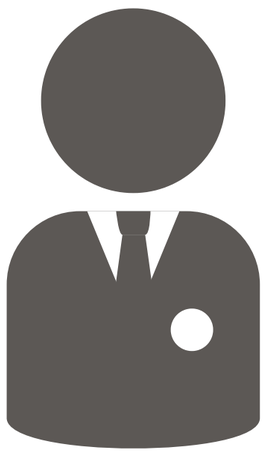
Passwords are the key to networks, customer information, online banking and social media. Password best practices include:

- **Use strong passwords.**
- **Consider using a password manager.**
- **Consider using multi-factor authentication.**

ENCRYPT DATA

Many businesses don’t realize how much sensitive information is on mobile devices, emails, spreadsheets, documents, PDF files and scanned images. The best way to protect sensitive information is to use encryption. This means if a mobile device is lost or stolen and the data is encrypted, then the incident would not result in a report-able breach.

EMPLOYEE SECURITY TRAINING



95% of data breaches are caused by employee mistakes. It is critical to ensure that employees understand the risks to sensitive information and the threat of data breaches. Phishing and ransomware are leading methods of attacks.

Employees need to know how to spot phishing emails, phishing websites, and the dangers of email attachments. Training needs to take into account the dangers of hacking, stolen mobile devices, posting sensitive information on social media, among other causes of data breaches.

A good training program continuously reminds employees about the dangers of data breaches, how to avoid becoming a victim, and being prepared for any new scams and attacks.

DATA BACKUP AND RECOVERY

Backing up data will always protect your business from data loss, whether its from damaged servers, natural disasters (i.e. flood, fire), explosion, or malicious codes (i.e. ransomware).

Having up-to-date data backups and a disaster recovery plan will help recover and restore valuable information. Without having access to customer information, business process documents, financials, and any other necessary information, many businesses fail after a data breach....

Data backups ensure that all valuable data is recoverable, and should be periodically tested for such validity

SECURITY RISK ASSESSMENT

Many SMBs don't know where their critical data is, how it is being protected, or what the associated risks are. For this reason, it is critical to go through a security risk assessment - SRA. An SRA is a crucial step in understanding the risk(s) your business and its sensitive information faces.

An SRA does the following:

- Completes inventory of customer, employee, vendor, and any other sensitive data.
- Identifies how your data is currently being protected - risks of phishing scams and ransomware, dangers of lost mobile devices, insider threats, and preparation for disaster..
- Makes recommendations on how to lower the risk(s) to the data.

Cybersecurity is a business blind spot risk, and needs to be evaluated and mitigated just like other business risks, making an SRA that much more of a best practice.

CYBER LIABILITY INSURANCE

Cyber liability is an evolving area of insurance provides financial protection in the event of a cyber attacks and data loss. Any business that stores sensitive data in the cloud, or on an electronic device, must have cyber liability insurance. It covers the costs and legal claims for a business to recover from a data breach, virus, and other cyberattacks.

Typically, it does not cover items such as bodily injury or property damage claims, property loss, criminal activity, and social engineering. For this reason, it is very important to work with a qualified insurance professional to find the right coverage levels and limits for your business.

CONCLUSION

While the risks are many, the ability to protect your business and your customers is more than achievable.

CW Technology has a process-driven plan that provides the necessary protection through a combination of disaster recovery planning, employee engagement training, and toolset monitoring and management.

If you are worried about cyber security threats to your business, then contact us today to discuss how we can implement the optimal security processes and tools for you!

Duluth, Minnesota

5614 Grand Avenue, Duluth MN 55807
(218) 728 - 6000

Plymouth, Minnesota

2415 Annapolis Lane N, Suite 100, Plymouth MN 55441
(952) 544- 5400

Grand Rapids, Minnesota

212 N Pokegama Ave., Grand Rapids MN 55744
(218) 728 - 6000