CYBERSECURITY SURVIVAL GUIDE

FOR SMALL BUSINESSESS

WHAT SMALL BUSINESS OWNERS CAN DO TO PROTECT THEIR BUSINESS

KEVIN BOBROSKE

PRESIDENT OF LIGHTHOUSE INTEGRATIONS

MBA, CISM

TABLE OF CONTENTS

INTRODUCTION

WHAT IS CYBERSECURITY?

Think of cybersecurity as the lock on the front door to the digital side of your business. It is the practices, technologies, and processes designed to keep your business's online information safe from people who shouldn't have access to it. This includes protecting everything from your emails to customer data, and even access to the software and applications you use every day. Just like you wouldn't want someone breaking into your store, cybersecurity stops the bad guys from getting into your digital systems.

WHY DO SMALL BUSINESSES NEED CYBERSECURITY?

The reality is small businesses are sitting ducks for cybercriminals. Contrary to popular belief, small companies are not too small to be noticed. In fact, they often have weaker security measures if any at all, making them attractive targets.

These are key reasons underscoring the importance of cybersecurity for small businesses like yours:

- Vulnerability to Attacks: Small businesses are often less prepared compared to larger organizations. In their annual Data Breach Investigations Report, Verizon found that more than half of data breach victims were small businesses.
- Cost of Cyber Incidents: Cyberattacks can be financially devastating. The cost of a data breach for small businesses has been seen as high as $2.2M but the average is $15,000 - $25,000.
- Reputation and Trust: A security breach can damage a company's reputation and loss of trust from customers.
- Continuity of Operations: Cyber incidents disrupt business operations, causing downtime that impacts revenue and productivity. The average time it takes to recover from a cyber-attack is 279 days.

This guide will provide you with a foundational understanding of cybersecurity and steps you can take to begin securing your small business against cyber-attacks.

THE FUNDAMENTALS OF CYBERSECURITY

Let's walk through the nuts and bolts of keeping your business safe.

CYBERSECURITY GOALS: THE BIG THREE

The main goals of cybersecurity are summed up as the "CIA". Not the agency but Confidentiality, Integrity, and Availability.

- *Confidentiality*: This refers to making sure only the people who absolutely need to know something can access that information.
- *Integrity*: This is all about making sure the information stays the way it was when you left it, untouched and accurate.
- *Availability*: Ensure that the right information is accessible to the right people whenever they need it.

Now let's get real about some things you can be doing right away to get started.

1. Identify What's Valuable: Asset Inventory
    - Take a detailed inventory of your digital assets. This includes everything from hardware, like computers and smartphones, to software, customer databases, and intellectual property. Knowing what you have is the first step to protecting it.
2. Recognize the Risks: Threat Assessment
    - Understand the threats specific to your business and industry. This could be a virus specific to accounting systems or phishing attacks aimed at healthcare employees. Keep informed about the latest cyber threats and how they could affect your business.
3. Shield Up: Implementing Defenses
    - Invest in robust cybersecurity measures including firewalls, anti-virus software, and intrusion detection systems. I know the free anti-virus and detection software are tempting however, they are easy to get around and are not effective enough for comfort. Don't forget about the human element – ensure physical security of devices as well as cyber awareness training for your employees.
4. Vigilance is Key: Continuous Monitoring
    - Set up systems to monitor your network and devices constantly and notify you when something is off. Look for unusual activity that could indicate a breach. This can be done with security software and by training your staff to report anything out of the ordinary.

5. Quick Response Plan: Incident Management
    - In the case of a security incident, you need to have a detailed response plan in place. It should outline clear steps for containment, eradication, and recover. It's critical you and all employees know who to contact and what to do in the event of a breach.
6. Stay Current: Ongoing Updates and Training
    - Cybersecurity is an ever-changing field. Cyber threats are evolving and becoming more sophisticated every single day. Regularly update your systems, software, and policies to patch vulnerabilities to these threats. Equally important is ongoing training for your employees so they will be able to recognize and respond to new threats.

SETTING A CYBERSECURITY BUDGET FOR SMALL BUSINESSES

Creating a cybersecurity budget is an important step for small businesses. It's about finding the sweet spot between what you can afford and the level of security your business needs. Let's break it down:

WHY NOT JUST USE THE FREE SOFTWARE?

Being a small business means to be on a tight budget. It can be tempting to cut costs by primarily using free cybersecurity tools, but these often lack the comprehensive protection that you truly need.

Why should you be skeptical when it comes to free security tools?

- Limited Features: They typically only offer a baseline of security. They may protect against common viruses and attacks, but they fall short in detecting more sophisticated threats that are constantly changing and becoming the norm.
- Lack of Support: If you run into trouble with a free tool, you're usually on your own. You'd only have minimal if any customer support whereas paid services help you navigate and resolve issues quickly.
- No Customization: Every business is unique with different needs, but free resources are only one-size-fits-all. They may not integrate well with other systems you use or fit in with your day-to-day business operations.
- Compliance Risks: If your industry has regulatory requirements, as most do nowadays, free tools will not provide the level of security or reporting needed to maintain compliance.

- No Assurance: With free resources, there's often no guarantee of reliability or updates. Paid services typically come with a service level agreement (SLA), ensuring a certain standard or performance and reliability.

Investing in cybersecurity means going beyond the basics. While free resources can be a part of your security measures, they need to be complemented with more robust solutions that offer a higher level of security, are scalable, and come with the necessary support to keep your business safe in the long run.

BREAKING DOWN THE BUDGET: WHAT COSTS TO EXPECT

1. Expert Support and Consulting: Hire professionals to set up your security infrastructure. They can pinpoint exactly what you need and how to implement it. Just because you are paying for a tool doesn't mean you are using it correctly or getting the most out of it. The experts will make sure it is set up properly and that you are getting the most bang for your buck. The cost of hiring expert support and consulting can range from a few hundred dollars for basic setups to tens of thousands for more complex systems.
2. Employee Training: Educating your team is non-negotiable. Your employees are your biggest assets but also your biggest liability (when it comes to cybersecurity). Depending on the depth of training, costs can vary from minimal (using existing resources) to significant (for comprehensive, ongoing training programs).
3. Software and Hardware: The right tools can vary widely in cost. Antivirus software might be as low as $30 per device per year, while enterprise-level solutions can run into the hundreds per seat. Hardware like firewalls could set you back anywhere from $100 to $1000+ depending on your needs.
4. Contingency Funds: Always have a buffer. If something goes wrong, you'll need immediate funds to mitigate the damage, which can run into thousands of dollars depending on what happened.
5. Cyber Insurance: Insurance can cover the cost of a breach, from legal fees to customer notification. Premiums can range widely based on coverage levels, from as little as a few hundred to several thousand dollars annually.

FACTORS THAT INFLUENCE YOUR BUDGET

- *Business Size and Complexity*: The bigger and more complex your business, the higher your budget needs to be.
- *Industry Regulations*: Some industries have stringent cybersecurity requirements which can increase costs.
- *Risk Level*: The level of risk you are willing to accept will affect how much you spend.

Cybersecurity spend is an investment in your business's future and resilience. Make sure you're spending wisely on essentials that will protect your business from the ever-growing threat of cyber incidents.

WEB SECURITY

Web security is like the suit of armor that keeps your business's digital presence safe. It's all about protecting the information that defines you and your customers – names, email addresses, phone numbers, physical addresses, banking details, and more. This kind of information has become like currency in the online world; it's valuable and needs to be guarded.

Why is web security a must? Simply put, your business information and customers personal information is constantly under threat from cyber criminals. If this data falls into the wrong hands, it can lead to financial loss, identity theft, and could really damage your business's reputation. It isn't only about protecting data; it's about preserving trust and the integrity of your business.

WAYS YOU CAN KEEP YOUR BUSINESS SAFE ONLINE

- Navigate to Safety: Just as you wouldn't walk into any unknown store and start handing out your personal details, the same goes for online sites. Use legitimate and trusted websites, especially when entering sensitive information. Look for signs of legitimacy such as 'https' (NOT 'http') in the URL or a padlock icon in the address bar, indicating a secure connection.
- Verify Before you Trust: Before providing any personal or business information online, verify the authenticity of the request. If a website or an email asks for sensitive information, double-check by contacting the company of the legitimacy of the request through a trusted channel.

- **Question Information Requests:** If someone is asking for your details, be skeptical. Ask why they need it and how they intend to use it. A legitimate business will have a clear and reasonable explanation.
- **Maintain Your Digital Safeguards:** Never disable security features like firewalls or antivirus software. They act as your first line of defense against online threats. Disabling them, even temporarily can leave you exposed to attacks.
- **Update Religiously:** Keep all your software up to date, including web browsers, plugins, and any scripts running on your website. Updates often include patches for security vulnerabilities that have been discovered since the last version.
- **Strong Passwords Always:** Passwords need to be complex and changed regularly. They should also be unique for each account you have. We recommend using a manager to keep track of your passwords. For added security, implement multi-factor authentication wherever possible.
- **Educate Your Team**: Make sure that all employees are aware of the risks and know how to handle personal and business information correctly. They should be well versed with the signs of phishing attempts and know not to click on suspicious links or share information to unverified sources.
- **Secure Transactions**: If your business involves online transactions, ensure they are secure. Use encrypted transaction processes and ensure that payment gateways comply with industry standards, such as PCI DSS (Payment Card Industry Data Security Standard).

AUTHENTICATION

Authentication is the process of proving your identity to access systems or accounts. Strong authentication practices are essential because they stand between your sensitive data and those who might want to exploit it.

PASSWORD PROTOCOLS

Common password mistakes:

- Using personal information like pet names or birthdays. When hacking passwords, cybercriminals might research their targets, making these passwords low-hanging fruit.
- Recycling passwords across different accounts. One breach can lead to a domino effect, compromising multiple accounts by just accessing one.
- Opting for short, simple passwords. They are the equivalent of using a weak lock on your front door that anyone with a hair pin could pick.

Tips for creating robust passwords:

- Embrace complexity and length. Consider using a passphrase – a sequence of words or a sentence that is easy for you to remember but hard for others to guess, like "BlueCoffeeRain@2498!".
- Avoid common phrases, idioms, or song lyrics. Cybercriminals use sophisticated tools that can guess these combinations.
- Incorporate a mix of uppercase letters, numbers, symbols, and lowercase letters to increase password strength.
- Update your passwords periodically to refresh your security and in case your credentials were leaked in a previous hack without your knowledge.

EMBRACING PASSWORD MANAGERS

Creating and remembering unique passwords for every account you have is pretty much impossible. Cue a password manager. A password manager acts as a digital safe, streamlining the management of multiple passwords. It's a single app that generates, retrieves, and keeps track of complex passwords for each of your accounts, minimizing the risk of a breach.
For business use, it facilitates secure password sharing and ensures that your entire team's login credentials are managed safely and efficiently. Adopting a password manager, such as LastPass, is a smart step towards fortifying your company's data security.

THE ROLE OF MULTI-FACTOR AUTHENTICATION (MFA)

MFA is a multi-lock system where you need more than one key to open the door. It asks for additional proof of identity which falls into three categories:

1. **Something You KNOW:** This could be a password or a personal identification number (PIN).
2. **Something You HAVE:** This includes a mobile device that can receive a text message, a security token, or an authentication app.
3. **Something You ARE:** Biometric authentication such as a fingerprint, retina scan, or facial recognition.

WHY UNIQUE PASSWORDS AND MFA MATTER

Using one password (or similar variations of one password) across all of your accounts is like using one key to get into every room and filing cabinet in your office. By establishing a unique password for each account, you're not just securing a single door; you're fortifying an entire section of your business. It is a simple, yet powerful step that can dramatically reduce your vulnerability.

Now, add Multi-Factor Authentication into the mix, you've elevated your security to a level that would make a cybercriminal think twice. MFA doesn't just ask for a password, it demands proof, something that's uniquely yours, whether it's a fingerprint or a code only you can access. It's the difference between a simple door lock and a bank vault for your accounts. Embracing unique passwords and MFA makes you far less of an easy target for hackers.

ONE-TIME PASSWORDS (OTP): THE EXTRA MILE FOR AUTHENTICATION

OTPs are essentially self-destruct codes for single-use access. They are typically generated through an app or sent to your mobile device, ensuring that even someone with your password cannot access your account without this second code.

TIPS FOR INTEGRATING MFA AND OTP FOR ENHANCED SECURITY

- Educate your employees about the importance of MFA and how OTPs protect their accounts as well as how to use these methods of authentication.
- Implement MFA for all sensitive systems or anywhere that contains private business, customer, or employee information. Ensure that access to this information requires multiple forms of verification.
- Use authentication apps to generate OTPs instead of the less secure method of SMS texts when possible.
- Regularly audit access logs to identify any unusual patterns that might suggest an attempted breach.
- Stay informed about the latest authentication best practices and hacking trends to keep your security up to date.

EMAIL SECURITY: GUARDING YOUR DIGITAL COMMUNICATION CHANNELS

Email serves as the lifeline of business communication, but it's also one of the most common points of vulnerability where sensitive information can be jeopardized. From mistakenly sending confidential information to the wrong person to sophisticated phishing scams, risk is everywhere.

Email is not just a tool for communication, it's a repository of sensitive information and a point of vulnerability for more businesses. A simple error, like sending an email to the wrong person, can lead to a significant data breach.

ENSURING EMAIL CONFIDENTIALITY

Take a moment to double-check recipient details before sending sensitive information. Encrypt sensitive emails to ensure that only the intended recipient can access the contents. Along with encryption, incorporate privacy reminders in your emails and educate your team about the importance of handling information with care.

MAINTAINING AND UPDATING EMAIL SOFTWARE

Your email software is your first line of defense against spam and phishing emails. Regularly update your email client or web service to benefit from the latest security patches. Choose an email provider known for robust security features including an advanced spam filter, as they are more equipped to handle emerging cyber threats.

SPOTTING SPAM AND PHISHING EMAILS

Spam/phishing emails used to be easy to spot but they are growing in sophistication. There might only be an error or two that is hard to catch and sometimes they even contain information that has to do with you or your business operations making them seem more authentic.

Here are some things you should always look for when opening emails and certainly before clicking on any links:

1. Too Good to Be True: If an offer in an email seems too good to be true, it's likely a scam. Whether it's a promise of unexpected money or a threat your account will be closed, use of extreme and emotional language is a red flag.

2. **Check the Sender's Email Address:** Even if it looks like it's from a legitimate source, check the sender's email address carefully. Phishing attempts often come from addresses that are misspelled or have extra characters.
3. **Look for Poor Spelling and Grammar:** Professional companies proofread their communications. If an email is riddled with errors, it's likely not legitimate.
4. **Be Cautious with Links and Attachments:** Never click on links or download attachments from unknown or suspicious emails. They can contain malware that can infect your systems.
5. **Sense of Urgency:** Phishing emails often create a sense of urgency, prompting quick action like 'Click Now' or 'Action Needed by X Date'. Always take the time to verify the authenticity of the email.
6. **Verify Requests for Personal Information:** A legitimate company will never ask for sensitive information via email. If you are ever unsure, contact the company directly through a verified phone number or secure messaging system.

Being on top of your email security is a critical component to your overall cybersecurity strategy. By doing things like double-checking recipients, encrypting sensitive emails, and being weary of every email you receive, you create a robust shield around your business's most frequented digital communication channel. Remember, securing your email is not just a technical task; it's a commitment to maintaining the trust and confidence of your clients, employees, and partners.

DATA BACKUP AND RECOVERY

From customer information to financial records, the data you collect, and store is the backbone of your business operations. However, data can be lost due to a variety of things like cyberattacks, natural disasters, or even human error. This is where backup and recovery come into play.

Data loss can be devastating, particularly for small businesses. It can be time consuming and expensive to get back, if you can get it back at all, unless you have sufficient backup and recovery processes in place. Regular backups ensure that you can recover quickly without major disruptions to your operations. Beyond just the continuity of your operations, many industries have regulations that require data to be backed up securely and failure to comply can result in hefty fines and legal complications.

BACKUP OPTIONS

When it comes to backing up your data, there are several options including:

1. Cloud Backup: Services like Google Drive, Dropbox, or dedicated cloud backup services offer off-site storage of data. They are scalable, generally secure, and protect against physical threats like fires or floods.
2. On-Site Backups: This involves storing data on physical devices at your business location, such as external hard drives or servers. While they offer quick access and control, they can be vulnerable to physical damage and are only as secure as the cybersecurity solutions you decide to implement.
3. Hybrid Solutions: A combination of both cloud and on-site backups, providing both the security of off-site storage and the immediacy of on-site access.

RECOVERY STRATEGIES

- *Regular Backup Schedules*: Establish a routine for how often data is backed up. For critical data, this might be daily or even in real-time.
- *Test Your Backups*: Regularly test your backups to ensure they work correctly and that you can quickly and efficiently restore your data. It's not enough to have backups; you need to know how to and that they can be restore successfully.
- *Clear Recovery Plan*: Have a well-documented recovery plan that outlines the steps to be taken in the event of data loss. Ensure all relevant staff are trained on this plan.
- *Versioning*: Keep multiple versions of your backups and at different locations. In case a recent backup is corrupted, you can revert to an older version or a version from another site.
- *Secure Your Backups*: Protect your backups from cyber threats. If using cloud services, ensure they have strong security measures in place.

Incorporating a robust backup and recovery strategy is not an option but a necessity for modern businesses. It's your safety net, ensuring that no matter what happens, your business's valuable data can be recovered, keeping your operations running smoothly and maintaining the trust of your stakeholders. Remember the goal of backup and recovery is not just to protect data but to ensure the very continuity and resilience of your business.

CLOUD CYBERSECURITY

Cloud computing has become a cornerstone for modern businesses. It offers flexibility, scalability, and efficiency. However, as much as the cloud revolutionizes business operations, it also introduces unique cybersecurity challenges. It is a common misconception that when using applications like Google Drive, Microsoft OneDrive, and Dropbox, cybersecurity is the responsibility of the cloud provider. However, this is far from true. The bottom line is you are responsible for your business's data and its security regardless of where it resides. Understanding and addressing these is crucial for safeguarding your data and ensuring business continuity.

UNDERSTANDING CLOUD CYBERSECURITY

1. Data Protection: Sensitive business and customer data are stored in the cloud and ensuring its safety is paramount to maintain trust and comply with data protection laws.
2. Access Controls: With the cloud, employees can access data from anywhere. This flexibility is great for productivity but also opens up new avenues for potential breaches.
3. Shared Responsibility Model: In cloud computing, security is shared between the cloud provider and the client. Understanding your role and responsibility in this partnership is essential.

KEY ASPECTS OF CLOUD CYBERSECURITY

- Data Encryption: Encrypting data, both at rest and in transit, is crucial. This ensures that even if data is intercepted or accessed, it remains unreadable without the proper decryption keys.
- Access Management: Implement strict access controls and identity verification processes, like multi-factor authentication, to ensure that only authorized personnel can access sensitive data in the cloud.
- Regular Audits and Compliance Checks: Regularly review and audit your cloud security. Stay compliant with industry regulations and standards such as GDPR, HIPAA, or PCI-DSS, depending on your business sector.
- Secure Cloud Services: Choose cloud service providers known for their robust security measures. Look for certifications and compliance with industry security standards.

- **Employee Training and Awareness**: Ensure your staff are educated on cloud security best practices. Human error is a major cause of data breaches, so a well-informed team is a critical line of defence.
- **Incident Response Plan**: Have a clear and tested plan in place for responding to security incidents. Quick and efficient response can minimize the impact of a breach.
- **Regular Updates and Patch Management**: Ensure that all cloud-based applications and services are regularly updated. Outdated software can be a weak link in your security.

Adopting a comprehensive cloud cybersecurity strategy is not just about using the right tools and technologies. It's about cultivating a culture of security awareness within your organization and understanding the shared responsibility model of cloud security. As you harness the power of cloud computing, it's vital to ensure that your journey through the digital clouds is secured against the turbulence of cyber threats.

CONCLUSION: NAVIGATING CYBERSECURITY AS A BUSINESS OWNER

You've made it through this guide, taking an important step towards understanding cybersecurity for your business. Let's discuss the practical steps you can take next as a business owner.

1. **Evaluate Your Needs:** Consider what aspects of cybersecurity are most relevant to your business. Is it protecting customer data, securing online transactions, or ensuring safe email communication?
2. **Seek Professional Help:** Look for IT security companies or consultants specializing in small to medium-sized businesses. They can tailor cybersecurity solutions to meet your specific needs and help you stay within budget.
3. **Cybersecurity Training:** While you might not be handling your cybersecurity measures directly, understanding the basics can help you make informed decisions. Look for beginner-friendly workshops or seminars focused on business owners.
4. **Stay Informed:** Subscribe to newsletters or follow blogs from reputable cybersecurity companies. This will help you stay updated on the latest threats and solutions.

FINDING THE RIGHT CYBERSECURITY PARTNER

- Look for Experience: Choose a company with experience in your industry or with businesses of your size.
- Check Credentials: Ensure the company and its employees have good references, case studies, and industry certifications.
- Understand Their Approach: They should be able to understand your needs to offer a clear plan tailored to your business.

As a business owner, your focus is on running your business efficiently. Understanding cybersecurity at a higher level empowers you to make informed decisions about protecting your business. Remember, investing in cybersecurity is not just a technical decision; it's a business decision that secures your reputation, finances, and future.

FOR ANY QUESTIONS OR FURTHER HELP – CONTACT US

At Lighthouse, our mission is to support small businesses like yours and help you to secure the future of your business.

Contact us to get started on your cybersecurity journey or to improve your current strategy.

Phone: 1(888)–575-7973
Email: info@lighthouseintegrations.com
Website: https://lighthouseintegrations.com/