IT Security Blueprint

Do you have an effective IT security blueprint for your business? Learn how to strengthen IT security to ensure the safety of your digital assets.

Cybercrime is an ever-present threat to modern businesses. According to estimates by global security software provider McAfee, cybercrime costs nearly $445 billion worldwide each year.[1] Without up-to-date and varied IT security measures, successful hacks can compromise your customers' and employees' sensitive data and harm your systems, resulting in costly downtime, and worse.

Small to medium-sized businesses need to think past the size of their organization and realize that everyone is at risk for cyber-attacks: individuals, government agencies, banks, businesses and more. Without the right guidance, training, and technology to prevent hackers from compromising your data, your business is left vulnerable to a major data breach.

How Can You Tell If Your Business Is Secure?

You can start the process of developing your IT security simply by asking the right questions. Consider the following:

1. **Do you feel that Cyber Security risks could impact your company in the future?**

   The fact is that with your data embedded in more networks, on employee mobile devices, and accessible online, cybersecurity is an undeniable risk of doing business in the modern world. Ubiquitous access to your business data combined with a lack of cybersecurity awareness in your employees represents a clear but hidden danger to your business's very existence!

2. **Do you think proper backups are enough to prevent data loss and avoid business interruption?**

   Despite how valuable data backups are, they are not the be-all and end-all of data loss prevention and business continuity. Conventional data backups only restore raw data, which doesn't account for the integrations and bridges between different aspects of your systems and software. The most dependable solution is a Business Continuity Plan which includes real-world (not simulated) annual disaster recovery

[1] http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2-summary.pdf

testing to ensure the effectiveness of your plan. Trust but verify is always better than trust alone.

3. **Have you performed a formal Risk Assessment of your business and its data?**

   According to a recent article by PayChex[2], 60% of small and medium-sized businesses that suffer a data breach go out of business within six months. A risk assessment can help identify and then mitigate potential risks to your business. It is also helps you spend your finite resources (labor and budget) on the most egregious risks first, ultimately providing the highest return on security investments possible.

4. **Are all your employees following safe password practices and properly protecting all your critical data on company devices?**

   At the center of any IT system is the one key component: the user. You can have the newest, most expensive and technically secure IT on the planet, and a simple human error – a weak password - can undo it all. Without the right password policy, password management tool, and employee training in place, it can be nearly impossible to secure always on and connected everywhere IT environments. Password Management tools provide feedback to employees on how strong a password, establish minimum strength requirements, identify whether a password is used on multiple accounts, and can improves overall computing efficiency by automating login processes. Writing passwords down just doesn't work anymore!

5. **Do you train your employees on emerging Cyber Security Threats such as Phishing, Social Engineering, and how to create strong passwords?**

   As previously stated, the weakest link in any business' cybersecurity is the user. That's why it's so important to ensure your employees are aware of the modern hacking techniques -- such as phishing -- and their role in prevention. An ongoing cybersecurity training program adapts to emerging new attack methods keeping your employees sharp and eagle-eyed for new attacks!

6. **Do you have a robust set of Security governance policies?**

   The foundation of any effective security program is an annually updated and comprehensive set of security policies and procedures. This helps to ensure consistency in security training between old employees and new, prevents repeat

[2] http://www.paychex.com/articles/human-resources/creating-cyber-security-culture Published: Jan 19th, 2016

security incidents, and creates a strong security culture and therefore a more reliable and robust business.

10 Steps To Enhance Your Security

Most business owners cannot confidently claim that their business' IT infrastructure is secure. Can you? There are many steps a small business owner should take to secure its business' IT. Some of the most effective ways to combat security breaches are simple tasks that should be done once and then repeated periodically for an effective security stance at your company. Here are the most important steps to get you started off in the right direction:

1. **Risk Assessments:** A risk assessment is your way of determining where the faults lie in your IT environment. By considering these critical questions, you will better understand your business and how well prepared to detect and hopefully prevent security incidents:

    1. What data do you have, where is it, how does it move throughout your business?
    2. What are my threats? Think of threats as hackers attacking you.
    3. What are my vulnerabilities? Think of vulnerabilities as the weaknesses a hacker exploits, such as missing patches or easily guessed passwords.
    4. How likely is a particular security risk to occur?
    5. What would the impact be?

2. **Vulnerability Scanning:** Regular scans of your IT assets are vital to your security. Any overlooked weakness in your systems could leave you vulnerable to an external threat. By scanning and identifying vulnerabilities you can then apply the right remedies whether it's a software patch, an OS upgrade, or a solution to a coding error in your website. Furthermore, it's important that you never ignore software updates. Software updates don't just improve software functionality; they often eliminate recently identified vulnerabilities being actively exploited by hackers.

3. **Virtual Private Networking (VPN):** Most business users connect to Wi-Fi wherever they find it – whether on an airplane, at a hotel, or in a café. A mobile workforce needs WiFi to get work done! However, it is more important than ever before that you use a VPN to secure your data while using Wi-Fi communications. Otherwise hackers can read your data straight out of the air and break into your email accounts or worse your bank accounts!

4. **Two-Factor Authentication (2FA):** Even the strongest passwords can be stolen (website hack?) and re-used by hackers to break into a business VPN or an individual's bank account. Two-factor authentication is something you know (a

password) combined with something you are (a fingerprint) or something only you have physically (a 6-digit code texted to your smartphone). The combination of any 2 factors is nearly unbreakable authentication. Business are strongly recommended to use 2FA on VPNs. You should require 2FA to access your Bank account(s) – something any bank serious about data security now supports.

5. **Anti-Spam & Anti-Malware:** Utilizing anti-spam and anti-malware technology will help limit the chances of a data breach at your business. Many modern hacking techniques, such as "phishing", require unwitting participation of an employee. Phishing emails trick poorly trained employees into clicking on a malicious link or launching a malicious file attachment, which causes a computer breach, which leads to a major data breach. By blocking spam , malware, and phishing emails from inboxes, your reducing the possibility of an employee accidentally compromising your security.

6. **Web Protection and Content Filtering:** Just like anti-malware and anti-spam, content filtering can help keep potentially dangerous websites from compromising your business. Web and content filters ensure that your employees are kept out of threatening and time-wasting websites, which provides a safe work environment for your employees while reducing the chance of malware entering your IT environment due to employee errors.

7. **Password Managers:** Passwords are the quickest way for a hacker to gain access to your accounts, and it can be easily obtained through social engineering, password cracking, or keyloggers. Keeping track of hundreds of strong unique passwords is nearly impossible for most people, not to mention the need to change them regularly. Password Managers automate password use across websites, applications, and computing systems enabling 14-20 character randomized passwords unique across every single account used! Don't forget to train your employees on your password policy, password complexity requirements, and the password management tools itself! This is one of the single most important steps businesses can take to enhance their security!

8. **Train Your Staff on Cybersecurity Attacks:** Teach employees never to open email attachments from senders they don't know in emails they didn't expect! It is critically important to educate your staff on how to identify Phishing attacks to avoid costly malware damages. Social engineering phone calls soliciting for passwords is another area of concern. The previously mentioned use of Password Managers is another important training topic. Employees and their actions often represent the single largest risk to businesses. Educating and training employees on common attacks goes a long way in preventing costly data breaches.

9. **Cyber Liability:** Responding to a data breach can be a costly and complicated process. Business that suffer a data breach have to deal with a number of issues,

including:

1. Customer notifications
2. Public relations/media communications
3. Regulatory fines
4. And more.

Don't leave yourself unprepared to deal with the fallout of a data breach. Just like the insurance you have for natural disasters, Cyber Liability Insurance Coverage (CLIC) can address the risks of a data breach by covering the many expenses that come with an effective response. From the costs for investigation to threats of extortion from hackers, CLIC is a worthwhile investment that will keep you covered should the worst occur.

10. **Mobile Device Management:** It is no surprise that mobile devices are continuing to become a bigger and bigger part of the business world as companies begin to adopt "Bring Your Own Device" policies for their employees. What's surprising is how unprepared some businesses are for this new step is professional technology. If mobile devices are a part of your business' process, you need to have the ability to provide effective device encryption, strong authentication measures (PINs, thumbprint scanners, etc.). When employees leave your company it is important to be able to remotely “partially” wipe those mobile devices of all company data (email, contacts, calendar) while leaving employees pictures and music intact. Is your business protecting its mobile data appropriately?

Protect your business assets by starting with your IT environment. {company} provides IT services to ensure that your business has a sturdy backbone of digital security measures that you can always rely on. Get in touch with us today at {phone} or {email} to get started.