**The Ideal Security Setup for a Small Business**

Josh Barber

Department of Physics and Computer Science, Wilfrid Laurier University

CP-601: Seminar in Technology Entrepreneurship

Nur Kurak

October 6, 2021

**The Ideal Security Setup for a Small Business**

Technology has grown to be an important fabric of everyday life, especially for small business enterprises. In fact, in 2018, the Chamber of Commerce conducted a study showing that 84% of small enterprises are using at least one major digital platform to provide information to customers and 75% are using a tech platform for sales (Laura, 2018). It would be silly to not take advantage of the lucrative online market, but doing so can cause risks. One of the main risks of taking advantage of the online market is that it exposes the business to the outside world. Exposing the business will only make the business vulnerable to cyber-attacks. Cyber-attacks according to IBM, are unwelcomed attempts to steal, expose, alter, disable or destroy information through unauthorized access to computer systems. Some of the more common types of cyber-attacks include backdoor trojans, cross-site scripting, denial of service, DNS tunneling, malware, phishing, ransomware, SQL injection, and/or zero-day exploits (ibm.com, 2018). Cyber-attacks have been a noticeable threat for the last coming of years and a small sized tech enterprise cannot defend itself being unprepared. In 2017, 61% of small businesses have experienced some form of cyber-attack, leaving on average $2,235,000 of damages (Laura, 2018). Also, the number of small-sized businesses that go out of business within six months of a cyber-attack is as much as 60%, according to the national Cyber Security Alliance of Canada (futurpreneur.ca, 2019). To prevent such damages, having a clear-cut plan to prevent cyber-attacks may be worth it, even though it may be financially draining. Here are some good practices to make sure a small enterprise can remain operational and/or prevent valuable information from being stolen.

Cyber security is based on three fundamental goals: confidentiality, integrity, and availability (getcybersafe.gc.ca, 2013). Within the goal of confidentiality, information must only be given to those that have permission to access it. Examples of keeping valuable information secure would be to use general passwords, two-step authentication, data encryption, security tokens, and/or biometric verification. Integrity is to maintain that all information is intact, complete, and uncorrupted. Checksums of data can be performed to help verify the data upholds integrity. Database backups or any other type of redundancies should be used to provide the information in case the data does become corrupt, deleted, or incomplete. Availability is to maintain the uptime of services so information can be acquired by the business or clients. Within having the hardware consistently reliable to maintain availability, may require frequent maintenance. Perhaps having servers that are waterproof and/or fireproof so it can still be operational during natural disasters. Within these three fundamental goals, necessary provisions can be created and maintained to uphold them in numerous ways. According to Canada’s Get Cyber Safe to determine the type of provisions necessary for cyber security, the business may need to look at:

* 1. Determining what assets are needed to secure.
  2. Identifying the threats and risks that could affect those assets or your business overall
  3. Identifying what safeguards you should put in place to deal with threats and secure assets.
  4. Monitoring your safeguards and assets to prevent or manage security breaches.
  5. Responding to cyber security issues as they occur
  6. Updating and adjusting to safeguards as needed

After auditing your business for cyber security, it is then best to create an organized plan and act. Typically, roles and responsibilities would be handed out to at least one member within the business to handle cyber security. From here, planning, acquiring and implementing safeguards would be necessary. Also learning about current threats, new threats, trends, and security options so the cyber security implemented is sound and futureproofed. It is also important in making sure the ones responsible for cyber security are still given guidance and encouragement through creating and planning future cyber security projects as cyber attackers are always looking for exploits.

It is one thing to have technological cyber security measures put into place, but cyber security awareness from the employees may be of one of the more important measures. Enforcing work policies and standards, such as using designated security software to access important work assets, never using personal information such as accessing personal online banking and only browsing secure or work-related websites through the work station may be necessary. Using a VPN can also help keep a connection secure and safe. This way, important personal information cannot be limited from being tracked and expose vulnerabilities. Being aware of social engineering techniques would also show to be useful, so critical information cannot be easily handed over. Employees should follow protocols when faced with questionable phone calls or emails to always be suspicious and reach out and ask for help if the information requested may jeopardize the company's safety in any way.

A backup plan is essential for any business. In case all data is lost due to a natural disaster or any other reason, it is imperative to make sure there is a way to retrieve and restore all data assets. If the business is small, using a portable drive to store all the valuable assets may be an option. However, there is the option of storing things securely online or within a local server that will have constant backups and versioning. Redundancy of the storage of the valuable data assets can also help protect against the data assets from becoming corrupted, so having a RAID configuration may be worth it as well, as this provides secure uptime and availability for clients and the business. Also, adding a rate limiter to the business’ designated servers in case of any DDoS attack could shore-up network bandwidth securing uptime as the perpetrator’s IP address or addresses can be blocked.

The implementation and maintenance of cyber security can be costly, but chances are cyber security is well worth it. As previously stated, the ramifications of being attacked could result in dire consequences of lawsuits, downtime, loss of reputation, and/or valuable information stolen. So, it is always important to make sure as a business owner to stay ahead of the cyber-attack game and invest the time and money. For sure programmatically using security tokens and enforced secured passwords is necessary for logins to access crucial information. Personally, would recommend online storage, such as using Google’s Cloud, where information is guaranteed to be secured with frequent backups. Google’s Cloud can eliminate public facing files within its storage and allow specific files to be acquired by using secured tokens. The secured tokens can also be customizable, which can limit certain users from accessing certain files. This would be the least expensive option compared to building your own server network and trying to determine security flaws within, whereas Google can handle it with just a monthly fee. However, if local servers are used, using an internal intranet to access data assets would be best. A secured VPN would be necessary to connect to the work servers for those working remotely, while also informing employees of specific work policies and standards, to limit any type of exposure to the public. For sure having any servers public facing should be prepared for any type of cyber-attacks. Within using Kubernetes, additional pods can be configured for your service to lighten the load of any DDoS attack. Implement a rate limiter to the service, to block or limit specific IP addresses from access your servers. Having a firewall to stop unauthorized access to the internal and external networks is inexpensive and necessary. The firewall can also be configured to filter out any type of phishing emails or limit unwanted traffic so things can be much more secure. Having secure software on work computers or laptops such as an antivirus, would also be recommended. ESET PROTECT offers an antivirus for businesses, and has been in the industry for 30 years, being exceptionally reliable in keeping things secure and safe. Overall, this would be a great start to any business’ cyber secure architecture.

**References**

Government of Canada / Gouvernement du Canada. (2013, September 20). *Get cyber safe guide for small and medium businesses*. Get Cyber Safe. Retrieved October 5, 2021, from <https://www.getcybersafe.gc.ca/en/resources/get-cyber-safe-guide-small-and-medium-businesses#defn-update>.

Laura, A. (2018, June 28). *What is the impact of technology on small business?* Thrive Global. Retrieved October 5, 2021, from <https://thriveglobal.com/stories/what-is-the-impact-of-technology-on-small-business/>.

*Protect your small business from cyber attacks*. Futurpreneur Canada. (2018, May 30). Retrieved October 5, 2021, from <https://www.futurpreneur.ca/en/2018/protect-your-small-business-from-cyber-attacks/>.

*What is a cyber attack?* IBM. (2018). Retrieved October 5, 2021, from <https://www.ibm.com/topics/cyber-attack>.