**The Definitive Guide to Cybersecurity for Startups**

Starting a business requires a great deal of planning and collaboration right from the start. Often in process of setting up a startup, businesses focus on the noticeable business functions such as sales and operations only, overlooking other less obvious but very important functions such as handling its cybersecurity infrastructure. Just as technology is a vital part of every business today, it is important to protect your organization from cyber threats. It is often perceived that small businesses or startups need not worry much about cybersecurity, since they are not under the radar of cybercriminals. But the fact is that small startups are easier to infiltrate into, and hence easier targets for hackers. A cyber-attack can bring a large business to its knees, and make a small company go completely out of business. This is why it is vital for startups to learn and understand the importance of cybersecurity for their business. Here is a guide to how startups can keep their company secure from the very beginning.

**Step One: Conduct a Business Risk Analysis**

Your resources as a startup will be limited during the period of infancy. Hence, it will be difficult to keep your business protected from all potential threats. The best way is to conduct a research and identify threats relevant to your industry with the potential to bring the most damage to your business. When such threats are identified, your startup can allocate all necessary resources and time to combat those threats.

Some of the most common threats startups are facing are as follows:

**Stolen Business Information**

It can be damaging for a business if its competitors have access to their contract bids, sales strategies and pipelines, product plans and financial statements.

**Data Breach**

In case of a data breach, you have to bear all the costs including their data recovery, regulatory fines and lawsuits. This threat is most relevant to financial services and security companies. Most of the times the targets of data breach attacks are online support or ecommerce websites that store customer information such as debit or credit card data. Startup business cannot afford to lose their customers since they have limited resources to relaunch after a tarnished reputation.

As in many other cases, data breaches are often a result of employee negligence. To prevent your business from potential data breaches, you need to limit access to your valuable data. When you put a limit to who can view customer’s financial information, you narrow down the number of employees who may accidentally click on a phishing link. You may be sure about your employees taking all the measures, but you cannot say the same for your third-party vendor employees. Hence, businesses need to ensure to limit the type of documents their third-party vendors can view. Also create a risk mitigation or breach response plan for a proactive response in case of an actual breach.

**DDoS Attacks**

DDoS attacks are especially damaging for ecommerce businesses, taking down your website, mobile application and APIs. As a result, you will not only lose revenue for the timeframe of the attack but also lose potential and existing customers. Most businesses know that even only a few minutes of downtime causes severe damage to the company’s reputation and results in decreased customer confidence.

**Insider Threats**

It is often said that employees are the weakest link in jeopardizing the information security. Even loyal employees cannot guarantee to keep your network protected as sometimes a lack of judgement on their part could give away access to hackers. Cyber criminals use social engineering and phishing links to trick employees and leak their sensitive information without them even knowing.

Teach your employees about password best practices and also train them to recognize phishing and social engineering attacks. They should know to check the sender’s email address, format and name, especially in case of an unexpected request. Before clicking any link in an email, make sure that it came from a trustworthy source or otherwise don’t open it. If an email asks for an information, make a phone call to the sender first to cross check its authenticity.

**Malware and Ransomware**

In a ransomware attack, hackers infect systems by encrypting their critical files and then asking them to pay a ransom for getting access back to those files. For startups today, ransomware is considered as one of the top threats. Contrary to popular belief that only established businesses face ransomware attacks, startups are equally at risk because of being an easy prey. This is because new businesses spend lesser on employee training and security software and are easy targets. Many of them don’t have the right technology to detect ransomware and once infected, they don’t have a complete system backup. This causes them to typically pay for the ransom to recover the data. In fact, it is this willingness of paying which makes startups an attractive target. While hackers may not demand the same large ransom amounts as they do from large organizations, they can still get a large payoff by attacking multiple startup businesses.

**Step 2: Invest in the Right Security Software**

Choosing the right platforms for your business is crucial for your success. If you choose a platform that lacks security, you are inviting potential security issues for your startup. If a platform’s security is cracked, it can mean a downfall of your organization from there. For this reason, it is important to invest in a secure platform and an [internet provider](http://www.planetdish.com) that is known to be reliable and successful.

Consider, if you don’t invest in a software service, your business may suffer from data loss, compromised credentials, hacked APIs, Denial of Service Attacks, violation of regulatory compliance, Advanced persistent threats, hijacked traffic and many other threats. With security as a service, you can overcome these without paying hefty amounts or exhausting your IT resources as most of these services integrate with your existing infrastructure.

**Step 3: Adopt a Security-centric Culture**

A startup’s culture will set a tone within the organization for years to come. It is important to embrace a security-centric culture right from the start. If we take an example of Facebook or Google, both companies adopted security in their culture early on, and today they have strong cyber teams. In order to make security work in an organization, every employee needs to not only comply with policies but also actively and vigilantly stay alert for any suspicious activity.

Here are few ways that can help reinforce security culture in a startup.

* Share your risk analysis with all employees to keep them aware of potential threats to your business
* Conduct periodic information security awareness sessions and ensure that everyone attends.
* Create a reporting mechanism for employees to report a suspicious activity.
* Schedule vulnerability assessments and security audits at least once a year.

**Step 4: Secure Your Website**

For startups that depend actively on a website, such as ecommerce businesses, it’s important to secure it by installing SSL certificates. SSL or Secure Sockets Layer is a security technology of global standard which allows encrypted communication between a web server and browser. It greatly decreases the risk of leakage of sensitive information such as passwords and credit card information. In essence, it allows a private conversation between two parties by authenticating the website and encrypting the data being transmitted. This helps to keep the customer data secure and safeguard the site from hacking attempts.

**Step 5: Network Security**

Your network of servers and clients is the primary target for cybercriminals. As a startup, you need to keep a network oversight to maintain control and visibility right from your early days. Hire a security engineer who ensures the prevention, detection and remediation of all your network devices. Run weekly vulnerability scans from a reliable service and dedicate an account to the scanner for accessing your servers. If vulnerability scans detect any required patches that were not automatically deployed, install the patches manually.

**Step 6: Physical Security**

Physical Security of your work premises is as important as network security for many reasons. It avoids the threats associated with social engineering, data and equipment theft, and targeted credit card thefts due to its proximity to [electromagnetic field of the card readers](cardzgroup.com). To ensure physical security, keep all your entry points locked and keep a log of all guests coming to your office. Also hand over visitor badges to guests for wearing. Install surveillance cameras at all entry and exit points, along with frequented office areas.

**Step 7: Be Prepared for Failure**

Quite often, businesses deploy plans for preventing and detecting cyber threats, but fail to create a risk mitigation plan for remediating actual cyber-attacks. Just like other operations, your cyber security plan can also fail sometimes, even for threats that were anticipated and accounted for. Anticipating failure and preparing for risk mitigation is just as important as preventing threats. The longer it takes for an incident to remediate, the more damage you will incur and give more time to hackers to steal your information assets.

For instance, what is your backup plan if a DDoS attack takes your API, mobile app or website down? How will that impact your business operations and customer retention? What can be done during that time to communicate with customers and mitigate the impact of the attack on them? Have you arranged backup servers or have a secondary DDoS protection service in place?

**Final Thoughts**

Even with all the measures in place, it’s not possible to anticipate all potential threats and attacks coming your way. The only effective way is to stay well informed about all emerging threats and follow the basics of cybersecurity. With all these steps in place, you will have the insight into your network, understand your weaknesses, know why and where you need to spend, and have a workforce that supports and practices your business need of cybersecurity.