Startups, Think about Cybersecurity on Day 1
March 2015

Cybersecurity has become a growing concern in the boardrooms of America's largest companies. *But it's not just big businesses that are vulnerable*. Startups, entrepreneurs, and small businesses are not immune from cyber threats. In fact, according to Symantec, from 2012 to 2013 there was a *300% increase in cyber attacks on small businesses*. It's true that small businesses, startups, and entrepreneurs are all in different stages of maturity—but that does not mean they do not all have extremely valuable data.

Cyber criminals target vulnerable computer systems regardless of whether the systems belong to a Fortune 500 company, a small business, or a home user. In fact, cyber criminals tend to target the weakest link in any system, whether that link is a person vulnerable to exploitation or an "as a service" platform developed by a startup. Cyber criminals are aware that small businesses and startups typically have fewer security systems to detect and prevent attacks. For that reason, they are prime targets. In addition, startups are more likely to use cloud-based services to store sensitive data, which might not have strong encryption technology or may succumb to vulnerabilities in third party infrastructure.

When faced with a cybersecurity breach, larger corporations tend to have contingency plans and staff that enable them to continue with business as normal. The reality is that startups do not have always have dedicated IT staff, a comprehensive understanding of cybersecurity risks, or the resources to purchase enterprise-level security tools. If a small business or startup has a breach, it can shut them down for days or weeks. That can be financially devastating. More importantly, it can destroy the reputation of the company and trust in the product. This can translate into a loss of customers, lack of faith from advisors, and concern from investors in an increasingly competitive venture market.

Regardless of how many resources you have to dedicate to cyber security, here are some simple steps to take to get started:

- **Use sound strategies to protect your business from day 1.** Establish a cybersecurity plan early that can grow with your business to protect your most critical assets. Develop a continuity of operations (COOP) plan so you can bounce back if you experience a cyber security incident.

- **Educate employees.** Identify industry and government created resources that may be beneficial to share with your employees and to start speaking the same language on cybersecurity threats, vulnerabilities, and steps to prevent breaches and/or attacks. As your company matures, consider developing your own set of resources and policies that are created from industry best practices.

- **Back up critical information.** Back up critical data according to a set schedule to ensure that critical data is not lost in the event of a cyber attack or natural disaster. Store backups either on an external hard drive, at an offsite premises, or in the cloud.

- **Secure your connections.** Use and regularly update antivirus and antispyware software on all computers. Automate patch deployments across your organization, use a firewall, encrypt data in transit, use digital certificates on email, and hide your Wi-Fi network. Protect all pages on your public-facing websites using HTTPS.

- **Be aware of attacks.** Social engineering attacks are highly effective and require little technical expertise. Exercise caution when opening e-mail, clicking on URLs, and downloading attachments.

- **Not Safe for Work (NSFW) applies to startups, too.** As many entrepreneurs use their personal computers for work, it is very important to use caution when browsing the Web. Drive-by attacks are an increasingly common and highly effective way for attackers to deliver exploits. Use malware and virus detection software to mitigate these attacks but realize that NSFW content applies outside of the co-working space, as well.

- **Monitor and defend your network.** Ensure, either by person, electronically, or both, the Internet and network's activities. Since many startups leverage a variety of technologies, it is important to monitor and defend your network not only on computers, but on mobile devices and apps as well. Adequate steps to defend your network to include: firewalls, intrusion detection systems, Internet content filtering, anti-virus software and log management. Update operating systems of mobile and network devices and install applicable as soon as possible. There are many open-source tools readily available that can be used to do this.

- **Check third parties' security reputation.** Before contracting with a third party firm, whether for cloud hosting or software development, find out who you are dealing with. Check the service level agreement for clauses regarding security breaches and downtime. Ensure the organization has an information security team – and get their contact information. To the greatest extent possible, ensure that code used in your systems and applications meets independent code review standards.

To help small businesses, startups, and entrepreneurs get started, the Department of Homeland Security (DHS) has identified a variety of resources available to help these entities manage risk and increase their cybersecurity resiliency:

- **Stop.Think.Connect. Campaign:** a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. On the Stop.Think.Connect. website is a Toolkit that businesses or entrepreneurs can access the following resources to help improve their cybersecurity including:

- **The Critical Infrastructure Cyber Community (C-Cubed) Voluntary Program:** a program to help businesses use the National Institute of Standards and Technology (NIST) Cybersecurity Framework, which helps organizations mitigate cyber risk. Examples of resources that can be found on the C-Cubed Voluntary Program's website include:

- **Cyber Information Sharing and Collaboration Program (CISCP):** a no-cost information sharing partnership between for businesses to share awareness about cybersecurity risks and needs. The program provides participants with a range of timely and actionable products including threat and vulnerability information, early warnings and alerts focused and recommended practices. CISCP can also be leveraged to help develop **Information Sharing and Analysis Organizations (ISAO)**, which were announced as part of President Obama's February 2015 Executive Order - Promoting Private Sector Cybersecurity Information Sharing. ISAOs can give startups the opportunity to collaborate with others not necessarily in the same sector or sharing the same maturity level, but motivated by a common idea of information sharing to increase cyber resilience.

- **Cybersecurity for Small Business training course**: offered by the U.S. Small Business Administration, covers the basics of cybersecurity and information security, including the kind of information that needs to be protected, common cyber threats, and cybersecurity best practices.

- **Federal Small Biz Cyber Planner:** a tool for businesses to create custom cybersecurity plans. Developed in partnership between the Federal Communications Commission, DHS, the National Cyber Security Alliance, and private sector partners, the Small Biz Cyber Planner includes information on cyber insurance, advanced spyware, and how to install protective software.

For additional information, e-mail CCubedVP@hq.dhs.gov or visit www.us-cert.gov/CCubedVP or www.dhs.gov/stopthinkconnect.