Cybersecurity Tips for Small and Medium Businesses

How to Get Started in Securing Your Important Enterprise Assets, Data, and Networks

01. Introduction

If you're reading this, you may have already experienced a cybersecurity breach or, at a minimum, you know an attack on your business is going to happen sooner than later. You probably also know that cybersecurity isn't a quick and easy problem to solve, it can take a lot of time, resources, and regular maintenance.

Most small and medium businesses have substantially less resources than large enterprises to secure their systems, networks, and data. As a result, cost-effective scanners, basic firewalls, and patching systems were historically considered enough to thwart most attacks. With the ever-increasing value of data coupled with the rise in new risks to smaller businesses from attackers leveraging advanced attack techniques with inexpensive toolkits, more sophisticated people, processes, and tools are now required.

As a medium size company who also happens to have decades of experience protecting our Nation from cyber threats, we thought it would be helpful to compile our learnings and provide other small and medium businesses with a starter guide on how to secure your important information. Below are some of the top things to consider as you embark on your cybersecurity journey.

02. How to Get Started

Step 1: Create Your Risk Profile and Assess Your In-House Capabilities

One of your biggest challenges will be deciding whether to invest in the in-house resources (staff and tools) needed to manage and monitor your cybersecurity or to outsource to a trusted 3rd party. To evaluate your needs, start by identifying the unique risks your company faces and how important those risks are to the success of *your* business. For example, list out your mission critical applications, core intellectual property, customer data, and critical assets, then rank how damaging a security breach would be to them.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (http://www.nist.gov/cyberframework/) is a great starting place to wrap your head around the many facets of cybersecurity. Assess your in-house security

capabilities across the five core functions to understand if you're able to properly protect your critical assets on your own or if you need to enlist outside support.

Step 2: Identify and Address Your Top Vulnerabilities

Now that you have your risk profile created, it's time to dig in and identify your existing vulnerabilities. The Center for Internet Security (CIS) creates and maintains a list of *Critical Security Controls (CSCs) for Effective Cyber Defense*. (http://www.cisecurity.org/critical-controls.cfm).

Deploying the top five items on this list can stop 85% of known vulnerabilities! This includes taking an inventory of IT assets, implementing secure configurations, patching vulnerabilities, and restricting unauthorized users. Start by immediately addressing these "low hanging fruits" that attackers find so attractive, then chip away at the rest of them overtime.

Another useful resource to help mitigate identified vulnerabilities is NSA's *Information Assurance Guidance*: https://www.nsa.gov/ia/mitigation_guidance/
It has also become increasingly common for smaller businesses to look to 3rd parties to help assess, deploy, and monitor security. For example, Exact's *Small Business Cloud Barometer 2015* research found that more than 50% of U.S. small businesses are using the cloud to help run their operations today, with security ranking as the top reason for doing so.

Step 3: Invest in Physical Security and Make Your Employees Security-Aware

This may be a given, but your employees are your best 1st line of defense. The more they understand how their actions can affect the company's overall security, the more they can do to prevent problems. For example, hold annual refresher trainings, send company-wide emails warning about the latest phishing scams, and require complex passwords.

Invest in physical security. Badges, surveillance, and alarm systems are now more affordable than ever, they are a critical part to any cybersecurity plan.

Step 4: Create a Cyber-Attack Response Plan

Now you need to decide how to blend reactive and proactive approaches to respond to cyber-attacks. Historically, reactive approaches were the best (and in some cases, the only) line of defense. Attackers now have access to inexpensive tools that allow them to quickly re-purpose more advanced attacks and directly target them, requiring businesses to take a proactive approach to shorten the response time. Both reactive and proactive responses require a mix of security technologies and services such as data leak prevention, endpoint detection mechanisms, malicious traffic security appliances, and threat intelligence.

There is no silver bullet security solution and no one size fits all. These decisions should be based on risks to your identified critical assets and potential damage to the company's revenue stream or reputation. Real-time cyber response is one of the most difficult things for smaller companies to do on their own. We recommend you explore outsourcing this part of your security, not only to have a quicker response time, but to also take advantage of the shared resources security vendors benefit from (multiple threat feeds and a bigger pool of security talent).

Step 5: Get in the Conversation

Now that you have some of the basics out of the way, it's time to get in the nation-wide conversation about cyber threats. Establish a relationship with your local FBI office https://www.fbi.gov/contact-us/field. If you encounter a serious problem, they can help. They also rely on information from companies small and large to identify trends in attacks, to warn when something big might be coming.

Join a regional or national Information Sharing and Analysis Centers (ISAC) http://www.isaccouncil.org/aboutus.html. ISACs are great resources for sharing threat information within your industry.

Step 6: Gut Check – Measure and Regularly Test Your Network Security

Put metrics in place to assess your security effectiveness. It's easy to waste time measuring things that don't matter, so stick to the following:

- Only measure organizationally meaningful things
- Make sure your metrics are reproducible
- Be objective and unbiased
- Measure progression towards a long-term goal

Once you determine what you want to measure, then asses which tools, services and solutions you have or need to get the job done. For example, can you assess how many phishing scams were clicked within your company, do you know the status of your assessed vulnerabilities, how quickly is your IT team updating outdated software, etc. Ask the security questions that are most important to your business and then tailor them to help drive your business decisions.

Conduct periodic 3rd party penetration tests (aka. ethical hacking) to identify vulnerabilities that can often go overlooked. Penetration testing has become increasingly affordable and can be a relatively quick way to get a read on your network security risks. When enlisting the help of a pen tester, see if they can include social-engineering aspects and make sure they help prioritize your vulnerabilities and map out an incremental remediation plan.

03. Conclusion

The above is by no means an all-inclusive “set it and forget it” list of things to do. Good security solutions should meet your industry compliances, but compliance alone may not provide sufficient security to protect your critical assets. This list is just a starting point to help make cybersecurity feel less intimidating. If you’re still overwhelmed and not sure what to do next, feel free to give us a call. We can help answer your questions and quickly get you on the road to a more secure cyber environment.

CONTACT VIASAT

W: www.viasat.com/cyber
E: insidesales@viasat.com
T: 888.842.7281