GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

Author: Martins, Andrew

Title: "How to Do a Cybersecurity Risk Assessment"

Website: business.com

Organization: Business.com

Date: 09 August 2019

URL: https://www.business.com/articles/cybersecurity-risk-assessment/

Accessed: 15 October 2019

Synopsis: Finding weak points now could protect your small business from costly intrusions later.

- Approximately 43% of cyberattacks target small businesses.
- Experts estimate cybercrime around the world will cost upwards of $6 trillion by 2021.
- According to a study from the University of Maryland, a cyberattack against a computer with internet access happens every 39 seconds.

Data breaches in today's highly connected world have become commonplace. Headlines regularly tell of major retail chains, consumer credit reporting agencies and even government entities falling prey to intrusions from outside attackers.

Do You Need to Conduct a Cybersecurity Risk Assessment?

- Approximately 43% of cyberattacks target small businesses.
- Experts estimate cybercrime around the world will cost upwards of $6 trillion by 2021.
- According to a study from the University of Maryland, a cyberattack against a computer with internet access happens every 39 seconds.

Data breaches in today's highly connected world have become commonplace. Headlines regularly tell of major retail chains, consumer credit reporting agencies and even government entities falling prey to intrusions from outside attackers.

As a small business, it may seem like a daunting task to keep bad actors away from your data and, by extension, your customers' data. Yet by performing a cybersecurity risk assessment, you're taking the first steps to better understanding your network's security flaws and what you need to do to patch them.

Cybersecurity risk assessments are used to identify your most important data and devices, how a hacker could gain access, what risks could crop up if your data fell into the wrong hands and how vulnerable you are as a target. Although you can perform your own comprehensive analysis, there are plenty of companies out there willing to guide you through the entire process and provide a monitoring service for a fee.

It should be noted that depending on your industry, you may already be subjected to mandatory cybersecurity risk assessments from a certified entity. In such cases, you may need to use a third-party system to comply with regulations.

According to the Verizon 2019 Data Breach Investigations Report, 43% of intrusions targeted small businesses. That should come as no surprise since there are nearly 30 million American small businesses, and most of them are soft targets for hackers.

Since the Information Systems Audit and Control Association suggests that a cybersecurity risk assessment should take place at least once every two years, here are some actions and tips you can use today to get started.

1. Gather information

The most important reason for performing a cybersecurity risk assessment is to gather information on your network's cybersecurity framework, its security controls and its vulnerabilities. If you don't know what you're doing or what you're looking for, a poorly conducted assessment could still leave you vulnerable to attack.

"If businesses don't have the experience, the tools or the team to conduct a thorough and accurate risk assessment, and are just trying to save costs by doing it themselves, they can experience increased costs in the future when a hack or data breach that could have otherwise been prevented occurs," said Keri Lindenmuth, marketing manager for Kyle David Group. "Many small businesses don't recover from a data breach because of the financial implications and end up closing their doors forever."

To that end, if your small business has IT professionals on hand with in-depth knowledge of your systems, you should work with them to come up with a plan for your risk assessment.

If you don't employ or contract with IT specialists, but you are familiar with your system and how it operates, you can still conduct your own assessment if you remain objective throughout the entire process.

Often, companies overlook certain aspects of security because changing those things would cause too much of a disruption, or it would cost too much to fix. You need to be willing to make big changes if your results point to major holes in your network.

2. Map out your system

Once you've considered how you're going to go about collecting information, it's time to get started on the actual assessment. To start, you're going to want to determine how your system works, what function it serves and who uses the system, among other things.

Your goal is to determine any risks and vulnerabilities that exist in your network. Once identified, you will need to rate how big a risk those problem areas are, what you're currently doing to mitigate those issues and calculate what your overall risk is.

Consider everything connected to your network. Printers, laptops, cell phones and smart devices are all entry points for malicious code to enter your network. You can find vulnerabilities with the help of some automated programs, such as the paid application Nessus Professional and the free tool OpenVAS, that run vulnerability scans on several aspects of your network to detect risks.

In the office, it's important to make sure your physical devices are secured as well. Attackers often gain access through internet-enabled devices and access your network through unpatched exploits. Devices such as wireless printers, Wi-Fi routers and mobile devices can be exploited to give hackers access to the rest of your network.

An easy way to avoid problems is to make sure your devices' firmware are all up to date. Microsoft has a free tool to help you detect if your Microsoft products on your network are all up to date.

3. Countering the human factor

Human error can also cause network vulnerabilities. One of the biggest causes of data breaches is unintentionally caused by employees who haphazardly click on suspicious links or download attachments from phishing emails. Vulnerability testing on employees' responses and online practices can be useful before initiating specialized cybersecurity training.

You can run a phishing vulnerability test using an online phishing simulator. It allows you to set up emails disguised as those from work colleagues with the goal of convincing employees to download an attachment or submit credentials. Negative results shouldn't result in any punitive action. Instead, you can use that information to set up additional training on cybersecurity best practices and provide your

employees with tips for avoiding phishing attacks. The results can also help you determine if you should implement two-factor authentication on network access.

Along with unintended points of access, your cybersecurity can be put at risk through the use of unencrypted USB flash drives, poor document retention and destruction practices, using unsecured channels to transmit personal information, and unintentionally sending sensitive data to the wrong person.

While accidents may happen, malicious attacks are the most commonly feared cyberattacks. In those instances, malicious software (malware), internal hacking threats or tactics like distributed denial of service (DDoS) attacks can hit your network hard.

Lots of tools exist online to help you determine if attackers can easily strongarm their way into your network through your website. For instance, Pentest Tools is a paid service that scans your websites, web applications and network to determine if vulnerabilities exist. Penetration testing software helps you see where hackers can gain ingress to your data through the web. Common problems with websites are a lack of SSL/TLS certificates and HTTPS, which are factors in securing a domain.

4. Consider the potential risks, their likelihood and impact

Along with considering the technical and human side of cybersecurity, consider which threats may hit your network and how likely that is to happen. During a cybersecurity risk assessment, you're going to want to list every possible point of attack that hackers can exploit to access your network and data, regardless of whether they're malicious or benign in nature.

One way to prepare is to follow the National Institute of Standards and Technology's Guide for Conducting Risk Assessments. This document has sample tables that you can use to assess each potential security risk.

Once the potential threats are identified, you want to determine how they would impact the actual network's infrastructure and defenses.

You're also going to want to determine how likely it is that these threats will actually take place. According to Sage Data Security, you can split this up into "likelihood ratings," such as:

- The threat source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
- The threat source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
- The threat source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

After determining potential threats, how they would impact your network and how likely it is that they'd take place, you're going to need to imagine what would happen if these attacks on your business are successful. I know that can be scary, but if these things did happen, it's important to know how bad things can get and devise a course of action to deal with the fallout. After all, most SMBs have been known to go under

once affected by a data breach.

At the end of the day, your small business's network security is paramount. Your data, as well as your customers' data, are incredibly valuable and important – which, of course, is why hackers want to get it.

If you decide to do your own cybersecurity risk assessment, you may find glaring security problems while familiarizing yourself with the network and how it works. While that's always a good thing, a professional cybersecurity consultant or firm can conduct an even more quantitative risk assessment that can help you avoid massive data breaches caused by some of the newest and most subtle exploits.

Additional reporting by Andreas Rivera