November 11, 2019 by Ilija Stankovski

FILED UNDER : DATA & SECURITY

Cyber Security Threat Assessment: How to Manage Risk

Many business owners and IT professionals struggle with understanding and addressing cybersecurity risks. What follows is a process for how you can discover your own level of cyber risk and a framework of guidelines to start doing something about it.

Who is at Risk?

The unique problem with cybersecurity is that it applies across every industry segment and size of company. It doesn't matter if you are a small insurance brokerage in Saskatchewan or Manitoba, a large Oil and Gas company in Alberta, or a provincial Crown corporation in British Columbia–all organizations are impacted by potential threats.

- If you use email, you are at risk.
- If you have a website, you are at risk.
- If you go online to conduct your business, you are at risk.

In today's world, it is obvious that the likelihood and impact of cyberattacks are increasing. However, some people and companies just do a better job of being prepared, and they formulate a security posture that encourages the "hooded villain" to go search elsewhere. That's why it's critical to start your risk assessment process immediately, and that you consider cybercrime as serious as any other threat to your business.

> *In a recent CIRA survey of Canadian businesses, "71 per cent of organizations reported experiencing at least one cyber-attack that impacted the organization in some way, including time and resources, out of pocket expenses, and paying ransom."*
>
> *2019 CIRA Cybersecurity Survey*

The big question is: what can you do by yourself, right now, to manage the security hazards posed by cybercriminals and cyberattacks?

What Can You Do?

What we do in the cybersecurity industry is mitigate the risks of your vulnerabilities being exploited by threats. While that sounds like a mouthful, and make no mistake it is a complex and nuanced field, there are some straightforward principles that can guide you in assessing your level of risk and in the basic steps you can take to protect your organization.

First, let's arm you with some fundamental information:

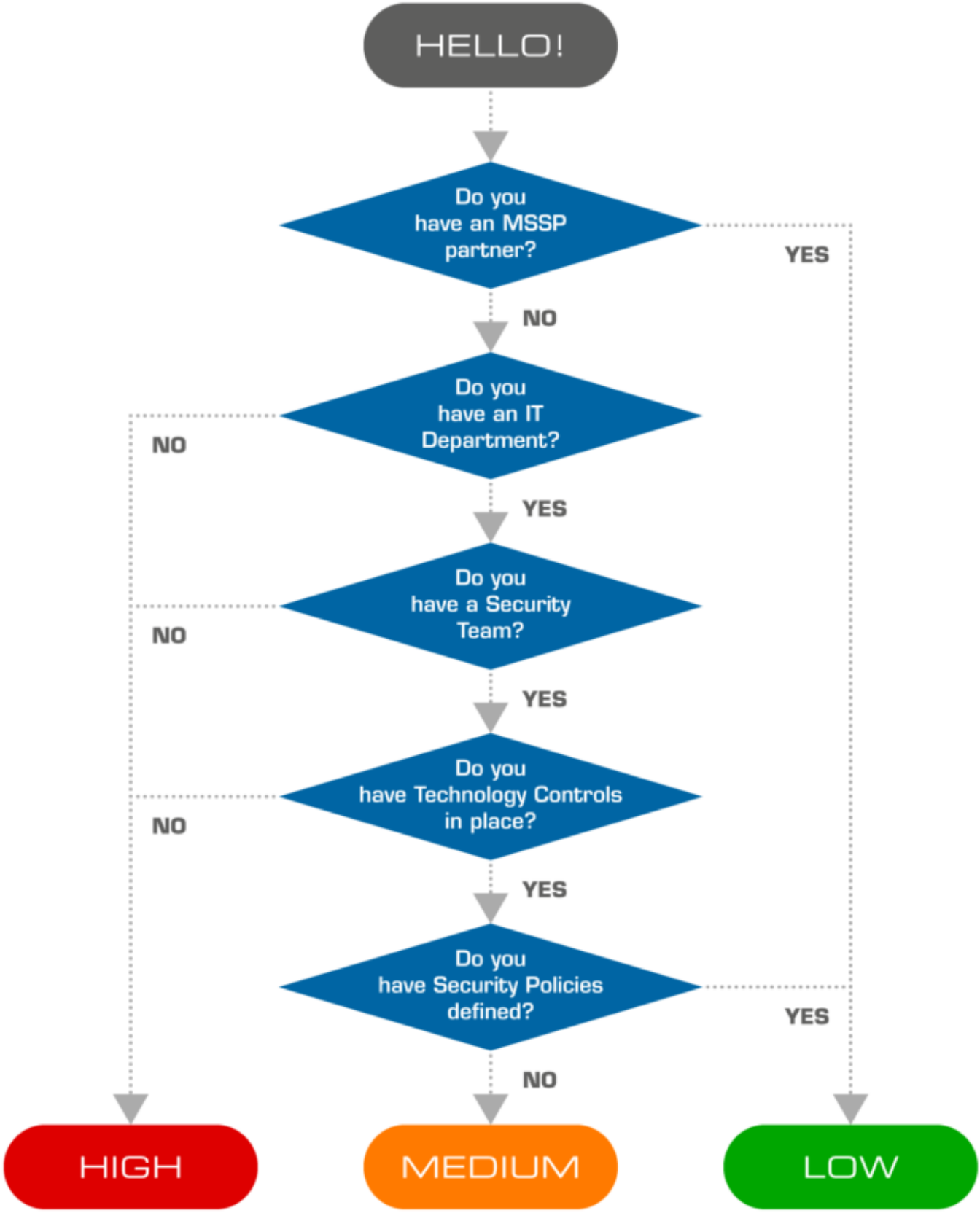
Cybersecurity risk increases due to vulnerabilities and threats in software, hardware and 'wetware' (otherwise known as humans). **Risk** can be reduced by applying security **controls** which are solidified by using industry **standards**.

Now repeat those bold words: risk, controls, standards … risk, controls, standards … risk, controls, standards.

Good, now let's begin! Follow this flowchart to find your current level of risk:

WHAT IS YOUR LEVEL OF RISK?

Cyber Security Threat Assessment



While this is a very simplified analysis, what we are trying to determine is if there are adequate people, technology and policy controls in place that will mitigate cyber risk for your organization. If no controls are in place, then your risk is high. Remember? Risk, controls, standards. Obviously, your Managed Security Service Provider (MSSP will conduct a much more thorough and in-depth evaluation when completing a real security assessment, but essentially, they will be looking for these same things—risk, controls, and standards.

Side note – *It not guaranteed that if you establish a partnership with an MSSP that your risk will be completely eliminated or become low; however, it is fair to say that this step will significantly lower your current level of risk!*

Now that we've identified your level of risk, the next step is to utilize a framework from which we can begin lessening that risk. At WBM, we look at three guiding principles when implementing a security blueprint – people controls, technology controls, and policy controls.

People Controls

The first fundamental in mitigating cybersecurity risk is ensuring that there are clear people controls in place. Most companies believe that cybersecurity is merely a technology play (i.e.: the belief that installing and running one "magical machine" can thwart all the dangers imposed by cybercriminals. Well, that's just not the case. The people controls of your cyber threat preparedness plan are just as important as the technology and policy controls involved.

Ultimately, people controls are about awareness, buy-in, training, and championing the cybersecurity cause within your organization.

Technology Controls

Although technology is not solely the only answer, it is obviously an important component of any risk management strategy. In fact, there are multiple pieces of hardware and software that should be installed and actively managed to ensure the right equipment is deployed at the right endpoints. From next generation firewalls to breach detection systems to backups to advanced email security protection to patching, and more… the right-fit technology stack will form an important line of defense.

Policy Controls

Lastly, policy controls are the backbone of what will keep your cybersecurity posture vigilant. From a documented incident response process that can be implemented immediately in a time of crisis, to insurance and employment policies that address cybersecurity protection, policy controls round out a holistic and pragmatic risk management strategy.

There you have it–you understand your basic level of risk and have some simple guidelines to help inform what you can do about it. Ultimately, if you've gleaned anything from this post, it should be that you can and should get started today. There is no reason to delay this decision and the dangers are very real. Find your internal champions, gain executive buy-in, and start adopting a security posture that gets you protected and keeps you there! With this in place, you can start focusing on innovation for your business, not just protection, and you can introduce new waves of value into your organization.

Ilija Stankovski

With over 20 years of protecting companies and their data, Ilija Stankovski has emerged as a respected industry leader in cybersecurity in Canada. With deep understanding of the hacker's mindset, coupled with experience and training in leading cybersecurity technologies, Ilija

shares some important insight on getting started with protection against cyberattacks.

Connect on LinkedIn