WHY DOES MY BUSINESS NEED REGULAR SECURITY ASSESSMENTS?

With so much mission-critical data and sensitive information out there today, there's a lot at stake for organizations of all sizes, and risks are present every day. Even one small gap in your layered security approach can leave you vulnerable to malicious attacks.

Standard anti-virus protection, encryption methods, and firewalls can only get you so far. Without adequately identifying and analysing the risks to your business, you can never manage them well enough to protect against potential threats.

Performing a comprehensive security assessment regularly is one of the most important things you can do to protect your business in the long-term and help to reduce risks effectively. An in-depth security risk assessment is proven to reduce the negative impact and losses of a data breach, as well as strengthen security measures to prevent future attacks, helping to keep your organization from ending up in the mainstream news cycle.

COMMON SECURITY THREATS TO PROTECT AGAINST

Cyber attacks and data breaches are a regular occurrence around the world; in the new reality that we live in, this is now happening daily. For every new security measure innovation put into place, hackers can move quickly to find vulnerabilities and code-gaps that will let them enter your networks and systems freely.

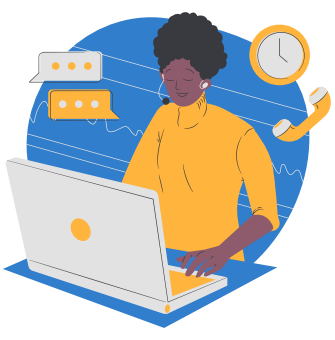
There have been a staggering number of large-scale data breaches in this century alone that have accounted for an incredible amount of confidential information being leaked online or otherwise used maliciously. While large enterprise companies account for most of the media coverage, small businesses are the most vulnerable to cyber threats and have the most to lose in comparison.

Some common security threats to be aware of:

1 USING OLD AND OUT-OF-DATE SECURITY SOFTWARE

It can be easy to get into the habit of using your same software applications. Unfortunately, this is one of the worst things you can do for your cybersecurity. Without frequent updates, license renewals, and other system checks, your networks are vulnerable to a variety of issues. Ask yourself: When was the last time you updated all of the apps in your Microsoft Office Suite?

2 FREELY GRANTING EMPLOYEE ACCESS



When hiring and firing employees, access to critical accounts can become a serious problem. By merely defaulting to making everyone an administrator or forgetting to remove key players when they leave the company, your business can't effectively manage who is accessing your systems and networks - or when.

3 GENERATING UNSECURED PASSWORDS

Even today when security breaches are so prevalent, people use passwords that are basic enough to hack right into. And, if that's not the case, it's surprisingly common for most people to leave their passwords out for the world to see, steal, and use to gain access to your systems. Consider the regular UPS delivery person bringing your business mail - will they see the password on the note taped to your display? In most cases, a data breach can cost much more than a risk analysis.

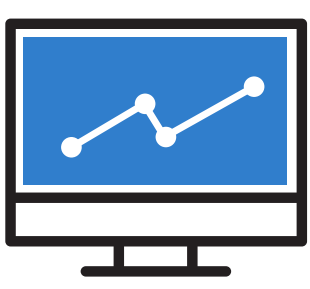
In most cases, a data breach can cost much more than a risk analysis.

Performing a security assessment will help your business to identify and flag these issues as risks to your organization, so you can better prepare and protect.

Step 1 IDENTIFY SYSTEM WEAKNESSES AND POTENTIAL THREATS

Before offering advice and tactics on how to improve, we first have to take a look at your current system setup. By forming a deep understanding of your weaknesses and potential cyber security threats, we're better able to provide strategic recommendations.

Step 2 ANALYSE AND IMPROVE YOUR NETWORK STRENGTHS



Doing a full evaluation of your current IT or tech department is also incredibly important. Having a complete, holistic view of your business' security strengths allows us to come up with the best solutions for enhancing them and making them stronger than ever.

Step 3 DEVELOP A THOROUGH IT SECURITY ROADMAP

No security assessment can be finalized without a robust security roadmap in place. We work with you to develop security goals that are in sync with your ongoing objectives as an organization, so you'll be set up for cybersecurity success every step of the way.

With a full security assessment completed, your organization will be much more informed and effective when it comes to the vulnerabilities of cybersecurity, including how to mitigate risks. While our network security risk assessments are created in a customized way to fit the needs of each business.

Davichi