YOUR CYBERSECURITY NEEDS TO EVOLVE TO KEEP PACE WITH THE BAD GUYS

By Carmine Tiano
Co-Founder and President

www.manawa.ca

Imagine coming into work one day and trying to open your email, but you can't. In fact, you can't do anything because you no longer have access to your own computer network and neither do your employees. Nobody in your office is able to get any work done because the files and systems they need are inaccessible. Your IT team is trying to restore the system from a backup, but that's not working either.

And then your team gives you the bad news: you've been hacked and now the hackers are demanding a huge ransom to give you access to your own network.

It's a nightmare scenario for any company, but it's about to get worse.

Unbeknownst to you or your IT team, the hack didn't just happen that morning. It actually happened six months ago.

HACKER EVOLUTION

Over the last couple of decades, hackers have grown incredibly sophisticated. It is no exaggeration to say that contemporary hackers run their operations like major corporations. In fact, some of these hacking operations are run better than some of the actual companies I have worked with.

The rate of technological evolution and the advancement in hackers' abilities have made it virtually impossible to defend against every threat. Technological giants like Microsoft have gone on record as saying it's not a matter of if you'll be breached, but rather when.

As larger corporations like Microsoft have poured resources into their cybersecurity, hackers have switched their focus to smaller businesses that often have much weaker security measures in place.

The good news is that you can protect your business. You just have to evolve the way you think about cybersecurity.

ASSUME YOU'VE BEEN BREACHED

Small business owners tend to assume their in-house or third-party IT teams have everything under control when it comes to cybersecurity. But, the truth is that if you're a small business owner, it's actually better to assume that you are about to be breached or you've already been breached.

It's known as "Assume Breach Mentality" and it could save your company.

Most people believe that when hackers infiltrate a network, they go for high value targets like computers that handle your finances and immediately make their move and start shutting things down and demanding money.

But, that's not actually the case.

Rather, contemporary hackers will find a way into your network using a low value target like a printer, an old computer in your shipping department that is only used for creating labels, security camera systems, a smart fridge that is hooked up to your network or even an employee's unsecure phone, for example. They do this because these targets usually aren't going to be well protected and they're easier to infiltrate.

Once they've made their way into your network through one of these soft points, they will sit in there for months and gently "probe around" in your network. They will observe the way your business runs and they'll learn as much as they can about the people in your company, your processes, your vendors and generally how you run your operation.

One example of how they gain information is by reading your emails and then sending someone in your organization a fake "spear phishing" email that looks like it comes from a vendor or a supervisor and asks for information. Since the email looks legitimate,

the employee provides the requested information and the hacker is that much closer to their high value target.

Then, once they've got the information they want and have compromised your backups, they drop the bomb by fully activating the malicious software and you are caught.

An "Assumed Breach Mentality" is meant to keep you vigilant about your cybersecurity. Obviously, you hope that you aren't breached and you carry on working as usual, but assuming that you are always on the verge of being breached (or are already harbouring malicious software) will make sure that it is at the forefront of your mind.

Instead of assuming you're safe, you can create a plan, develop the necessary processes, and purchase the required technology that will find out when a breach occurred as early as possible, and then eject the attacker from your network with the goal of limiting the breach as much as possible.

PHYSICAL SECURITY VS. CYBERSECURITY

The reason hackers are able to infiltrate small businesses so easily is because there are so many different ways for them to do it now and those ways continue to multiply as technology gets more sophisticated. Also, many small business owners tend to treat their cybersecurity as an afterthought.

Think about the physical security you have at your business right now.

You have locks on your doors and maybe you also have a fence, bars on your windows, motion sensors, security patrols, a monitored alarm system and cameras.

These can be broken down into three categories:

Prevention

- Locks, fences, bars.

Detection

- Sensors, cameras, alarm system

Monitoring

- Security patrols, alarm system monitoring

Your level of physical security will depend on different factors. If your building is in a fairly remote place on the outskirts of town that doesn't get much traffic, you may feel that locks on the doors are good enough. If you've heard there has been an uptick in crime for industrial neighbourhoods over the past few months, you might also get some

bars on your windows and put a fence around your property. If the next business over had their property broken into and had a bunch of equipment stolen the week before, you might feel the need to get some cameras and security patrols.

It's a process of balancing the cost versus what you believe you need to keep your building safe.

Cybersecurity is similar.

You need to truly know where you are right now in terms of cybersecurity and do some calculating to figure out what level you can afford to be at.

First, let's look at the different levels of cybersecurity in the same way we discussed physical security:

Prevention

- Firewall, anti-virus, multi-factor authentication, up-to-date software security patching, employee security awareness training programs

Detection

- Detection and response platform, Network sensors, Log aggregation

Monitoring

- Security operations centre

Most small businesses are at the Prevention level. This is where you have your basics in place to prevent hackers from getting into your network.

The problem is that many small- and medium-sized companies that are only at the Prevention level actually believe they are at the Monitoring level. They think their in-house or third-party IT teams are detecting and monitoring for hackers, but most do not, or cannot, offer this service.

This leaves small businesses vulnerable.

Let's take a closer look at what each of the items in the Detection and Monitoring levels are:

DETECTION AND RESPONSE PLATFORM

This is software that is meant to detect suspicious activity that has already infiltrated your network and is doing the aforementioned probing to gain access to more valuable information.

NETWORK SENSORS

Network sensors collect data from various points in your network and allow you to determine if you have activity that looks suspicious and should be checked into. They come in a variety of formats.

LOG AGGREGATION

A simplified explanation of log aggregation is when all the various logs in your computer network are collected in one place and are made easily searchable. This means your cybersecurity team can easily view your network logs to see if there is any suspicious activity.

SECURITY OPERATIONS CENTRE

As the name implies, a security operations centre is a monitoring service that analyzes an organization's activity on networks, servers, databases, applications, websites, and other systems for anomalous behaviour that might indicate a breach. The security centre's goal is to detect and analyze cybersecurity threats and respond to them using a combination of technology and strong processes that eradicate any problems.

CHOOSING YOUR LEVEL OF CYBERSECURITY

As previously discussed, you will have to do some calculating to figure out what level of security you can comfortably afford while staying as safe as possible. It would be great if every business could be at the Monitoring level and have the services of a security operations centre, but that may not be possible for smaller operations.

Regardless of how confident you feel in your current cybersecurity situation, if you're running a business you should get a full assessment of your preparedness. You may find that you are completely prepared, but chances are that you are going to find some huge gaps.

Because your own IT team has a vested interest in making you feel like everything is secure already, it is best to hire a third-party cyber security specialist to analyze your setup and identify areas of improvement.

When hiring a specialist company, keep these guidelines in mind:

- They should make everything as clear as possible so you can understand it. It's easy to make things sound impressive when using industry jargon. A reputable cybersecurity company will use everyday language to make sure you fully understand what they are proposing.
- They will have no problem giving you a list of current clients that you can call and talk with. It's easy to put a testimonial on a website, but getting a reference you can have a conversation with is invaluable.
- They should be able to walk you through the procedures they have in place to protect themselves. One of the best ways to ascertain what a cybersecurity company can do for you is to see what they do for themselves.
- They will have no problem giving you the names of the tools they use so you can research them for yourself. Not all cybersecurity companies like to "pull back the curtain" and let customers really see how they do things. A good company will have no problem with transparency.

No matter what level of security you get, it is imperative that businesses of all sizes start evolving their way of approaching cybersecurity. Assume that a breach is inevitable or has happened already. The future of your company may depend on it.