APRIL 2022

TECHNOLOGY TIMES

Insider Tips To Help You Run Your Business **Better, Faster, Easier** And More **Profitably**

IN THIS ISSUE

WHAT'S NEW?

There are plenty of big things that happened this past month at Avenir IT and we are thrilled to say that they will be continuing into April!

Between Mathieu announcing our new initiative to secure 1,000 Manitoba Businesses at a conference of his business peers in Orlando, and its official launch - it is safe to say we have been busy bees.

We will continue to be buzzing about as we prepare for our appearance at the upcoming 2021 IBAM Broker Con on April 19th. Be sure to come a to visit our table!

Avenir IT Commits $2.5 Million of Services to Help Protect 1,000 Manitoba Businesses

Considering growing cyber security threats – increased by recent global events, there is now a bigger need for proactive cyber security measures to match these threats in all spheres. Not only have we seen in uptick in cyber crime on the world stage, but we have also seen a concerning increase in reported attacks to Manitoba businesses. In 2020, Manitoba saw 1,973 reports of cyber crime, which is up from just 565 in 2016. From seeing these numbers double and continue to grow from there in the past few years, our mission to protect Manitobans from hard-hitting cyber blows has been solidified. This is exactly why we have recently teamed up with leading partners in cyber security to help secure 1,000 Manitoba businesses of all sizes at no cost throughout 2022 and 2023.

As of this month, we are starting a new initiative by offering a complimentary cyber security scan with a 30-minute session to review our findings and action plan so that organizations can clean up the issues discovered during our analysis, with the goal of educating Manitoba organizations to ensure

I just wanted to send you a quick note to say thank you to the Avenir IT team. We are so glad to be partnered with them! Everyone at Avenir IT has been a pleasure to work with, and their work is always so helpful to us.

Janet Campbell
President and CEO,
Joy Smith Foundation

they don't become victim to, or receive a devastating financial blow caused by cybercrime.

Our proposed security scan is extremely easy to complete, requires very little time and is non-disruptive to your team. In fact, it's as simple as sending a link to your staff and asking them to download and run a small application. The reasoning behind this process is to educate you and your staff what type of information or access would be available to a cyber criminal **when** *your staff clicks on a malicious link within a website, email or attachment*.

Once the scans are completed, we require a couple of days for the analysis of the information and preparing the presentation of findings as well as an action plan.

Once the reports are ready - we will schedule a follow-up meeting to review these findings and action plan to resolve any cyber security issues found and what is required to resolve them.

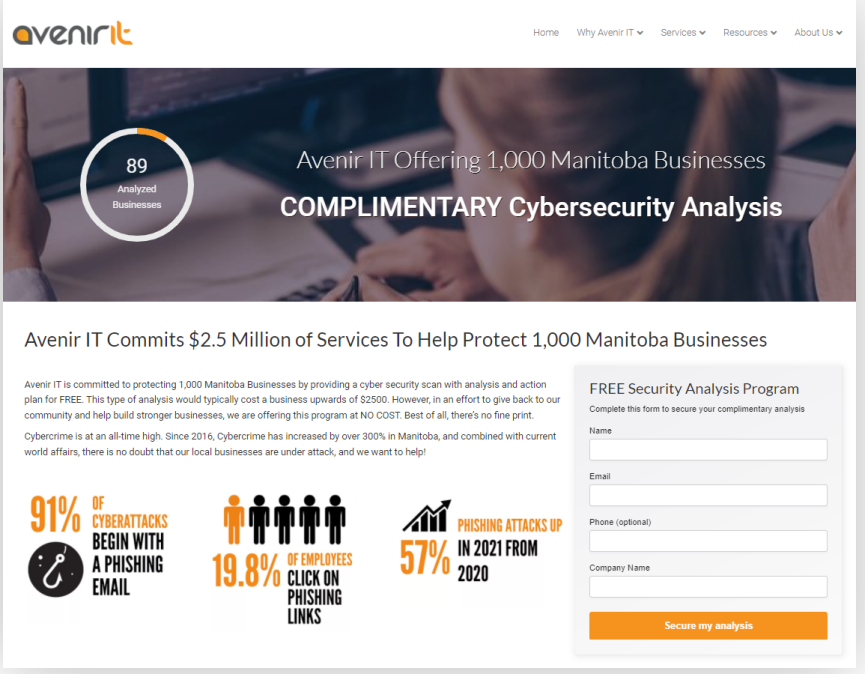
Our vision to help secure fellow businesses was inspired by our own roots as a proud, successful local business. Now more than ever, we are in a great place to do what we aspire to do most of all: to give back to our wonderful, perseverant community.

If you are a client of Avenir IT - then rest assured that you have either already been contacted or will soon be contacted with more information and a scheduled scan. If you are not a client of Avenir IT, then please head over to https://avenirit.com/protect-manitoba to secure your complimentary security scan with an actionable plan.

No matter the size of your business, the state of your IT, or wether you have internal IT, outsourced IT or no IT, we hope to garner your support in our upcoming endeavour, and to work together toward our common goal of helping Manitoban businesses thrive.

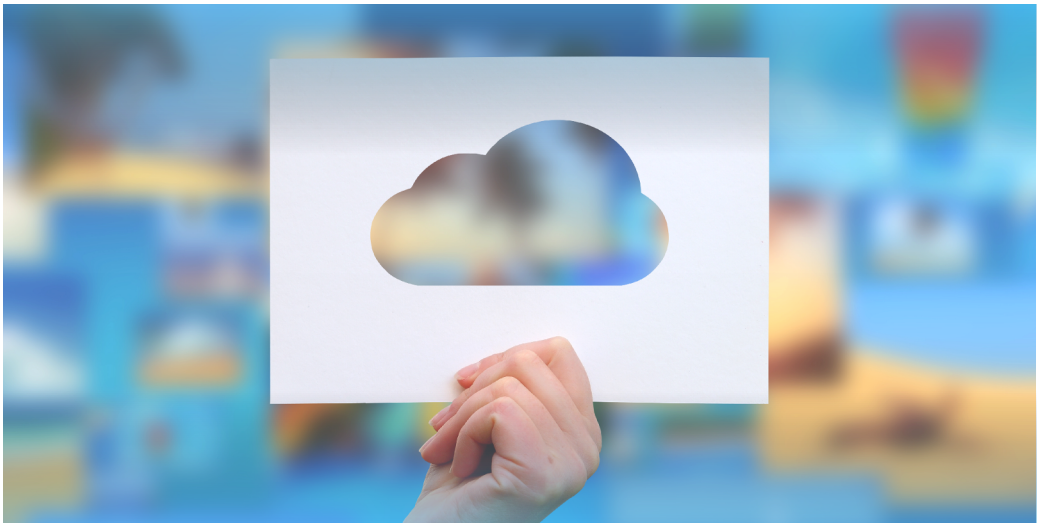
So please, to secure your complimentary scan and action plan, please sign up at https://avenirit.com/protect-manitoba.You can also reach out to our team at (204) 289-4384.

WE ♥ MANITOBA BUSINESSES



The scan and analysis will give you insight into:

- What information hackers can access if they get into your network
- An analysis of your backup and disaster recovery strategy
- Inspect your network security settings to ensure they are up to date and working properly
- Check your computers and/or servers' security updates and patches
- Review accessibility to confidential information on Microsoft 365
- Audit your virus definitions and protection.
- Assess your staff education strategy to prevent future attacks
- And more...



Traditionally, general cybersecurity concerns, as well as data loss and leakage issues, have acted as barriers to adopting cloud-hosted solutions. More workloads moving to the cloud indicates that enterprises are overcoming their fear of cloud security threats—enough, at least, to allow some of their data and applications to reside in the cloud.Nevertheless, security threats and other risks of cloud computing still exist, and companies should take steps to avoid (or at least mitigate) them.

So, Who Exactly is Responsible for Cloud Security?

To understand the risk that cloud security threats pose, it's important to delineate responsibilities for securing different aspects of cloud computing. The split of responsibilities among the public cloud provider and the customer organization varies greatly depending on the computing model: SaaS, PaaS, or IaaS. To that end, let's briefly explore the differences in cloud computing models…

Infrastructure-as-a-Service (IaaS) Cloud Computing

In the Infrastructure-as-a-Service (IaaS) model, the cloud service provider agrees to manage and secure the facilities, datacenters, network interfaces, processing, and hypervisors. The customer must manage and secure the virtual network, virtual machines, operating systems, middleware, applications, interfaces, and data.

Platform-as-a-Service (PaaS) Cloud Computing

That split of responsibilities changes a bit for the Platform-as-a-Service (PaaS) model. The cloud provider has the same duties as the IaaS provider, but also adds responsibility for the virtual network, virtual machines, operating systems, and middleware. The customer organization is left with responsibility for securing and managing applications, interfaces, and data.

Software-as-a-Service (SaaS) Cloud Computing

With Software-as-a-Service (SaaS) the cloud provider is responsible for the security of everything from the infrastructure to the application. The customer organization must ensure the security of its data as well as access to the application.

At the end of the day, however, the cloud provider and the enterprise customer must work under a shared responsibility model with the ultimate goal of keeping the enterprise's data safe and secure. To summarize, generally, your cloud service provider is responsible for monitoring the infrastructure and services provided to your enterprise, but is not responsible for monitoring the systems and application your enterprise creates using the provided services, or the data you place in the cloud. The cloud provider may give your organization monitoring information related to your use of the cloud's services. This information should be used to augment data from your own monitoring tools.

With it being every trickster's favourite holiday again this month, we are in for a good laugh - but those who have forgotten about April Fools may be in a for shock!

Between jump scare zoom meeting backgrounds, plastic wrapped doorways, and soy sauce in the coffee pot, the office prank possibilities are endless - so make sure to keep your eyes peeled for any funny business!

The same goes for the any potential security threats that may pop up! To quote William Shakespeare, "A fool thinks himself to be wise, but a wise man knows himself to be a fool". Failing to be on your guard, not only this April 1st, but at all time could end getting you fooled into falling victim to a devastating cyber attack.

Although there doesn't seem to be a link between April Fool's day and rises in cyber attacks, April Fool's Day attacks have happened. Notably, in 2009, the once dormant Conficker C virus activated on April 1st and caused all kinds of IT havoc for organizations and individuals alike.

7 Tips To Make Big Decisions With More Confidence

1. Pinpoint your goals. Unless you identify your personal goals, you'll feel like you're making decisions without a map. A vague idea of where you want to end up is better than nothing, but goals are better road maps when they're specific and measurable

2. Define your values, too. Similarly, your values — much like a compass — should guide your decisions, mostly because you won't feel confident or rewarded if your choices don't align with them.

3. Take stock of previous decisions. Make a habit of reflecting on decisions you've made in the past, especially when you have another decision ahead of you. Ask yourself: In the last week, month, or year, what decisions worked out well, and why? What didn't end up working out, and why?

4. Weed out irrelevant thoughts and feelings. Your feelings aren't always reliable indicators of what's right and what's not. But you also shouldn't totally ignore them — they just may not be super helpful in this specific decision. Before you act, notice the thoughts and emotions that automatically rise to the surface. Ask yourself which ones are actually relevant to your decision, and which ones are just getting in the way?

5. Be choosy about sources of advice. The constant influx of information we all face daily can make decision-making extra complicated. Identifying ahead of time who you want to involve in decision-making processes so you don't feel overwhelmed when a big decision comes.

6. Lower the risk. If you're excited about the potential of a decision but you're worried about a factor you can't control getting in the way of your success. Identifying simple ways to lower the risk can increase your confidence — and the odds your decision will work out the way you want.

7. Don't be afraid of messing up. Lastly, remember you're allowed to make mistakes. If you find yourself anxious about a decision, ask yourself, "What is the worst that could happen?" Answer yourself honestly. You may find that the level of worry you're experiencing is unwarranted, and sometimes, you'll realize that in fact you were considering a risk not worth taking.

The Best Ways You Can Improve Cloud Security

1. Deploy multi-factor authentication (MFA). Mandating the use of multi factor authentication on your cloud applications can ensure that only authorized personnel can log in to your apps and access sensitive data in your on- or off- premises environment.

2. Manage your user access to improve cloud computing security. Most of your employees don't need access to every application, or every file in your cloud infrastructure. Assigning proper access control not only helps prevent an employee from accidentally editing information that they shouldn't have access to, it also protects you from cyber criminals who have stolen an employee's credentials.

3. Monitor end user activities with automated solutions to detect intruders. Real-time monitoring and analysis of end user activities can help you spot irregularities from your team's normal usage patterns, such as a log in from an unknown IP or devices. These unusual activities could indicate a breach in your system, so catching them early on can allow you to fix security issues before cyber criminals cause mayhem.

4. Provide anti-phishing training for employees on a regular basis. Cyber-criminals can steal employees' login credentials through social engineering techniques like phishing. Offering ongoing training is the best bet in preventing employees from compromising your company's sensitive data. Keep in mind we said "ongoing" - phishing training is not one and done, it's a continual process that needs be managed by someone within the organization in order to make it effective!

5. Consider cloud-to-cloud back up solutions. Should your data be accidentally deleted or breached and wiped, there is nothing your provider can do past a certain time period. Most cloud providers do store deleted data in their data centers for a short period of time, so be sure to check with your cloud provider to determine what this time frame is, and if there are fees to restore your data.

Adapted from "The Key to Making Big Decisions With More Confidence" by Asheley Abramson