TECHNOLOGY TIMES

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

IN THIS ISSUE

Avenir IT Holiday Party

Inside Threat

3 IT New Year's Resolutions

A Brief BEC Scam Refresher

4 Step Method To Have A Difficult Conversation

Happy New Year!

A message to our clients:

Happy New Year!

Thank you for your continued trust and support during what was another crazy year.

We worked diligently to expand our support & service offerings to you in 2021, and we are so excited to show you what is coming in the New Year!

We appreciate your business and are looking forward to growing with you in 2022.

avenir it

How is it already 2022? I feel like the older we get, the faster time passes by, and I'm not so sure I like it! I remember when 2000 rolled over and our biggest worry was the Y2K bug. Is it just me or has the game of life gotten a lot harder these days?

While 2021 was not without its challenges for a lot of us, we were blessed to have another healthy year at Avenir IT that has allowed us to grow through the pandemic. Like many other businesses, we are trying to navigate the waters of insane vendor inflation rates, new work opportunities and most of all – the continuously evolving world of new cyber threats and attacks geared towards the small businesses we serve. Cyber criminals have become vultures waiting to pounce on any tiny mistake or wrong personal decision we make. While most small

businesses are understanding the importance of cyber security and real time monitoring – some still seem to believe they are invisible.

Our world is changing – and as business owners it is important to recognize these changes and adapt your business accordingly. I know we have, and our service offering of today is so much different than what it was not even 3 years ago! Truth be told – we are extremely excited about what is next for us and where the next 5 years will take us. The IT landscape is changing fast – and it is so critically important that you partner with the right IT vendors to ensure they can take you there.

Throughout 2021, we continued our reign of top 3 best rated IT company in Winnipeg as well as top 50 best managed IT company in Canada which is always very humbling! 2021

Avenir IT 2021 Christmas Party

also saw our team more than double. While Covid prevented us from all getting together often this year – it really felt amazing to host a team of nearly 50 people at our staff Christmas Party. Back in 2019 – we were a whopping 12! We added the following amazing people to our team: Paige Berard - Administrative and Marketing Assistant, Clarissa Chen – Sales Representative, Corey Goslin – Help Desk technician, Derek Rocan – Level 3 technician and team lead, Derrick Wong – NOC Engineer, Eric Kelln – Help Desk technician, James Baldwin – Dedicated technician, Manu Perron – Help Desk technician, MJ Gamolo – Dedicated technician, Rain Anderson – Help Desk technician and Sahib Sekhon – Help Desk Technician.

The best part? They are all truly amazing people and make up the awesome culture and way of being here at Avenir IT. The bad? We outgrew our office once again for the third time in as many years. In fact – our COO, Melissa Ross asked me to forfeit my office space in the Spring and work from home full time.

Covid aside – 2021 was a great year and we have two big goals for 2022:

1. Be the best IT services provider in Manitoba, offering the best user experience and fastest response times ever.
2. Be the best company to work for in Canada.

We have big plans and bigger ideas and as long as we continue to have the right people in the right seats – I don't have a doubt in my mind that 2022 will be the best year ever. We all get the exact same 365 days, the only difference is what we do with them.

On that note – make sure to keep an eye on your inbox as we launch the first phase of a brand new, innovative service in mid-January. Best of all, at no cost to you if you are an existing client of Avenir IT – no matter the level of service. I'm already so excited about this launch and counting down the days until we can invite you for a sneak peak. I'll give you a hint – it's called Avenir IT: Mission Control and I am So. Darn. Excited!!!!!

May 2022 bless you with good health, wealth and most importantly happiness, my friends.

Cheers,

M Manaigre

Mathieu Manaigre

Super Client
of the Month

"Recently, I inadvertently deleted an excel spreadsheet. When I contacted Avenir IT for help, their technician, Corey, managed to set aside other work to correct my mistake right away! After spending about 10 minutes in my computer, he was able to find a version that I had 'deleted' and save it in my client folder. It was amazing service! He, as always, was super helpful. Thank you Avenir IT!"

Terry Betker
President and CEO
Backswath Management

Inside Threat

The threat to a business from outside perpetrators is very real when it comes to cyber-crime. But sometimes the threat comes from within, and it is even harder to detect or prevent in the first place.

Why would someone try to intentionally hurt the very company that provides them with a paycheck? The reasons vary, but there are a few that are repeat offenders. They include stealing proprietary information to take to another job, selling to the competition, or working with cyber-criminals to provide the foundation for an attack.

You may be familiar with companies that provide solution model framework which works to prevent attacks, such as Lockheed Martin's Cyber Kill Chain. These describe the stages of an attack and explain the tactics used, but these programs don't necessarily consider the human element when it comes to cyber-crime. Human behavior can't always be so easily predicted, and a business needs to take the approach of not only training their workforce to fend off cyber-attacks but also looking at each 'human element' as if they are carrying a risk factor for internal inside threat.

Offsetting the Risk

Many times, there are assumptions that leave people believing that someone else is taking care of what needs to be done to keep a business safe, secure, and successful. You should work with your MSP to clearly outline and identify who your internal point persons are when it comes to maintaining your cybersecurity. This outline should not only include all the hardware and software that is in place, but also who internally is keeping your company accountable to engage and use the products that your MSP offers as part of their defense program. The lack of identifying a person is often what leaves a company at greater risk for internal threats, as people just "assume someone else was handling it". Establishing accountability as a factor of your business relationship will provide you with more likelihood of success and lessen the risk of internal dangers.

There are some behaviors that can act as alerts for suspicious behavior.

What to look for:

- An unusual number of files being accessed and opened
- Avoiding or trying to work around security measures that are in place
- Saving files to unusual locations
- Utilizing USB drives to save or move information
- Using tools or software that hides online activity

We know that having hardware and software can protect a business, but don't overlook the human side of cybersecurity, and always make sure that your team knows that safe online habits are integral to maintaining that security.

3 Must-Do IT Resolutions For The New Year

Resolution 1 - Tune up your backup and recovery system. The #1 antidote to a ransomware attack is an up-to-date backup copy of all your data and software. Yet managing backups takes more than just storing a daily copy of your data. For one thing, if your business is at all typical, the amount of data you store grows by 35% or more PER YEAR. If your data management budget doesn't expand likewise, expect trouble.

Resolution 2 - Harness the power of the cloud—but watch your back. Huge productivity gains and reduced costs can be achieved by making full use of the cloud. Yet it's a double-edged sword. Any oversight in security practices can lead to a breach. Here are two things you can do to harness the cloud safely: Prioritize what data must be protected. Trying to protect everything can take focus and resources away from protecting data such as bank account information, customer data and information that must be handled with compliance and regulatory requirements in mind. Select cloud providers carefully. You can't control what happens to your data once it's in the cloud, but you can control who's managing it for you.

Resolution 3 - Set and enforce a strict Mobile Device Policy. As BYOD becomes the norm, mobile devices open gaping holes in your network's defenses. Don't miss any of these three crucial steps: Require that users agree with acceptable-use terms before connecting to your network. Secondly, be sure to install a Mobile Device Management System on all connected devices. A good system creates a virtual wall between personal and company data. And lastly, establish a strong protocol for when a connected device is lost or stolen. Make sure features that allow device owners to locate, lock or wipe (destroy) all data on the phone are preset in advance.

A Brief BEC Scam Refresher

BEC Scams are becoming much more common and can take many different forms. They are primarily used to gain access to financial accounts – however can also be used to gain access to someone's email account or other sensitive information. This type of scam is increasing in popularity and becoming more frequent as the payoff is greater for the cybercriminal.

At its core – a BEC Scam is a form of social engineering. Social Engineering is the ability to manipulate people into giving up confidential information or carrying out deceitful requests. Cybercriminals take advantage of our natural human nature to trust each other - making it easier for them to trick individuals into falling for their scams.

The bottom line is never respond or confirm any requests by email. Even if the email appears to be legitimate and coming from a trusted source, assume that the email account may have been compromised. Always confirm any request for information or financial intent with the sender by phone or in person.

Adapted from "Need to Have a Difficult Conversation? Try This..." by Justin Bariso

Need To Have A Difficult Conversation? Try This 4 Step Method

"We need to talk." In most cases, hearing (or saying) those four words is never fun. But whether you need to give negative feedback or simply speak about an uncomfortable topic, how can you do it with emotional intelligence? It's important to remember that oftentimes how we say something is much more important than what we say. For the future, if you find yourself needing to have a difficult conversation, try this four-step process:

1. Follow the three-question rule.

Before saying something that you think will be difficult for another person to hear, ask yourself:

Does this need to be said? Does this need to be said by me? And lastly, does this need to be said by me, now?

If the answer to all three questions is yes, skip ahead to step three. But if you only make it to the second question, proceed to step two.

2. Consider the time and place.

While calling someone out in front of others may be needed in certain circumstances, it's usually more advantageous to speak privately in a relaxed setting. This shows respect for the other person, and respect begets respect. Additionally, you make it easier to have an actual conversation about what happened.

3. Consider how you want to communicate.

If possible, frame the discussion in a way that relays helpfulness. Asking for permission to share something you've noticed or sharing how you've made a similar mistake in the past, can go a long way in getting the person to listen while minimizing the tendency to get defensive. Additionally, be sure to give the person the chance to express themselves, and how they saw the situation from their perspective. Sometimes this helps expose the other person's blind spots, or it can help you communicate with empathy.

4. Continue learning.

Communication is an art, one that takes time and practice to improve--especially this type of communication, where you are offering criticism or counsel. So, after a conversation like this, take time to analyze and deconstruct. Ask yourself how it went, if you accomplished what you set out to do and how you could improve next time.