The IT Mill

Like Newsletters Should Be.

Summer 2022

Business

7 Action Items To Safeguard Your Business

By Scott Birmingham, Principal Consultant, C.E.T., C.I.M.

No business owner wants to think about what would happen if their business was hacked. And those who don't want to think about it, usually make themselves an easy target. **A lack of discussion, combined with limiting financial and technical investments, increases their cyber security risk ten-fold.**

An article from TechRepublic, "Report: Many SMBs wouldn't survive a ransomware attack", highlights a new business report from cyber security provider CyberCatch. Information gathered through survey responses collected from 1,200 businesses about their susceptibility and resiliency to a cyber attack revealed key business operational preparedness points that need attention:

30% don't have a written incident response plan to respond to cyberthreats,

20% don't have offline backups of critical data,

34% don't give employees phishing tests to determine their exposure to risk,

75% would only survive three to seven days following a successful ransomware attack.

Businesses and employees are on the front lines when it comes to cyber attacks. Here are seven operational tips to help increase your cyber resilience and preparedness:

1. Ensure that you have a written incident response plan and update it regularly. This is incredibly important as with the ever changing world of technology, threats will continue to evolve.

2. Scan internet-facing assets regularly to prevent hackers from exploiting security vulnerabilities.

3. Keep your employees on guard – send them simulated tests on phishing and social engineering attacks to help them learn what to look for in a suspicious email or link that could contain malware.

4. Segment your network – the idea is to limit the ability of threats spreading.

5. Set up multi-factor authentication – easily one of the best and therefore most recommended methods to prevent attackers from logging in with stolen credentials.

6. Store backups offline – critical files that are stored offline can't be found by attackers.

7. Lastly – TEST your cyber security defences regularly.

BIRMINGHAM CONSULTING
Like IT should be.

21 Mill Street North
Waterdown, ON
L0R 2H0

(289) 895-8948

www.birmingham.ca
info@birmingham.ca

Security Discussion

Why Don't We Drive Cars From The 1920's Everyday?

By Scott Birmingham, Principal Consultant, C.E.T., C.I.M.

We get asked a lot about why we are always adding more layers of cyber security even though clients haven't yet experienced a breach. We call it "**multi-layered cyber defence".**

Traditionally, I've drawn an analogy to the multiple layers of defence of medieval castles (clear visibility lines approaching the castle, moat, drawbridge, high walls, portcullis, etc.). But if a person has never watched Game of Thrones, this analogy might not make any sense.

So, more recently I've started using a car safety analogy. Early cars had little to no safety features: The body and frame provided some protection but it really came down to driver skill and the trust they placed in other drivers not to cause and accident. (Similar to using basic antivirus and hoping nothing bad happens.)

As the automotive industry evolved, so did safety features. Now we have a mix of passive and active features. For example:

- Additional review mirrors
- Seatbelts
- Airbags
- Blindspot detection
- Driver assist
- Heads-up displays
- Automatic lights
- 360° cameras
- Audible warnings

Every one of these features adds an additional level of safety, many of which are now considered must-haves. But why were they initially created? Weren't cars safe without those features? Just like a business without multiple cyber defence strategies in place, the probability of, and effects of, an accident are significantly higher in cars with less safety features.

The world of cyber security is constantly evolving, which means that protection methods are also evolving. We want our clients to be as safe as possible in this ever-changing environment – this is why Birmingham Consulting implements multi-layered defence strategies.

To be as safe as possible in a car, why pick and choose between seatbelts, airbags, mirrors, etc., when really, you need ALL of them?

Shameless Self-Promotion

Newest Team Member Spotlight: Christopher Hamilton

By Christopher Hamilton, Technology Associate

Christopher and his daughter at Waterdown Ribfest 2022

I was drawn to tech from a young age, going back to video games. I started working full time in tech in 2008. My skills have grown throughout the years, working with hotel and bakery chains in Jamaica while getting my degree and certificates. Migrating to Canada in 2021 was another step for me to take my career to another level.

BCI has exceeded my expectations as not only being an IT company that sets itself apart from others, but also being client and community focused. The staff here are great and the *cyber security tools used are cutting edge.* All employees are certified on the tools implemented for clients. I think that this is an understated selling point for the company: their staff are not only trained, they are also qualified.

My favourite BCI core value is **Integrity.** We should always hold ourselves accountable for our mistakes, and by learning from them, we're made stronger. When I'm not focusing on technology, I'm either playing basketball, fishing or spending time with my family. Family is very important to me and BCI has given me the opportunity to enjoy all of that as they strongly believe in work-life balance.

"Thorough, Trustworthy, Quality Service"

PETERS SRD
STEEL RULE

"Birmingham Consulting's quick and quality service and professionalism, even in dire circumstances, is a great asset to the success of our company and keeps our **downtime to a minimum**. Birmingham is great at implementing proactive solutions and recognizing trends that help us stay on our "A-game".

Their **attention to detail**, and **focus on prevention** along with **long-term planning**, are outstanding. Their team's thorough documentation, records and procedures are extremely valuable to us, and we never have to worry about breach of privacy or classified information. We trust Birmingham completely! We have already referred many people to Birmingham with great feedback and we would *recommend them to anyone.*"

Amy Searles - Peters Steele Rule Dies

Technology

Minimizing Your Technical Debt - Why This Practice Could Keep Your Technology Healthy & Secure For Years

By Veronica McMullen, Marketing Manager

There is a general and practical understanding that many things in life need to be regularly reviewed for any required maintainence - e.g. houses (roof, foundation, water), vehicles (brakes, oil, fluids), businesses (policies, budgets, performances), etc. This is because more often than not, **we have all had to manage at least one situation where something needed to be fixed *yesterday*** - that truthfully had been neglected a bit too long.

"Technical Debt" is the collection of items that will need to be updated, fixed, replaced, etc within your technology systems. This includes but is not limited to your computers, cyber security protocols, infrastructure, etc. Reducing your Technical Debt to a minimum should be the goal of your IT department - not just waiting for the next fire.

When computer or technology systems are not maintained properly, let alone securely, **it can lead to substantial unexpected costs.**

Keeping your cyber security and technology infrastructure in the best shape possible year to year is **arguably one of the most effective ways to keep your business secure**, and also elongate the lifespan of your technology investments.

An article from InfoWorld, "How to minimize new technical debt", quotes Ruby Raley, a vice president at Axway, who believes that reducing and addressing Technical Debt is more important today because of skill shortages and financial conditions. She says, **"The need to reduce Technical Debt is going to be front and centre for CIOs.** They will need to find operational efficiencies to fund new projects because of inflation and staffing issues from the Great Resignation and employee burnout. One of these steps will be [technology] consolidation to reduce maintenance spend."

The importance of reducing new Technical Debt with better planning and estimating is stressed by Andrew Amann, CEO of NineTwoThree Digital Ventures: "The first and most important [priority] is proper planning and estimating. The second is to standardize procedures that limit time spent organizing and [allow] more time executing."

IT and cyber security teams must commit and invest in sufficient time to reduce Technical Debt and streamline the introduction of new security and technology measures to your business. Agile organizations should review these proactive practices at least once a quarter.

When upgrades and maintenance are neglected over extended periods of time, your Technical Debt increases. Reduce your debt as much as possible to stave off avoidable challenges later on - as well as improve preparation for other emergencies. The health of your technology will not only save money in the long run, it will also protect your business more effectively.

Kahn's Korner

Our office cat, Kahn, makes our team feel right at home... by rotating his "napping spot" between everyone's desks.

Interactive Infotainment Answers: 1. Cyber 2. Phishing 3. Malware 4. Firewall 5. Uptime

Community

Waterdown Farmers' Market

When: Saturday's until October 15, 2022

Time: 8:00 am - 1:00 pm

Where: Waterdown Royal Canadian Legion, 79 Hamilton Street North, Waterdown

Spend your summer Saturday mornings at the Waterdown Farmers' Market- a much-loved community event drawing more than 900 visitors weekly. Local growers, farmers, small batch producers, VQA vintners and artisans gather to share the fruits of their labour. Featuring fresh-from-the-farm produce, meats, baked goods, VQA Ontario-grown wines and more. There are lots of options to choose from! With safety measures in place to keep customers, vendors, and staff safe. Learn more at www.waterdownfarmersmarket.ca.

Client Spotlight

King Truck Repair

www.kingtruckrepair.com 289-769-9482

Founded in 1987 as a division of KPM Industries, and located in Burlington, Ontario, King Truck opened as an 8-bay shop. More than 30 years later, John Hutter, a shareholder of parent company, purchased the division and now operates it as stand-alone entity King Truck & Equipment Repair.

Over the years, King Truck Repair has expanded both capacity and services. They now operate two shifts across 14 bays and provide heavy equipment repair, truck and trailer repair, welding and fabrication, fleet maintenance, towing, mobile repair, and emergency roadside repair.

They do everything they can to provide you with the best experience and value on your repair needs. From scheduled maintenance to emergency assistance, their team is standing by to support you and your business.

Partner Spotlight

Duo Multi-Factor Authentication

Our Like IT Should Be® Toolbox

Multi-factor authentication (MFA) arguably provides the biggest return on investment when it comes to cyber security and is considered essential as part of a layered cyber defence strategy. Read more: www.getcybersafe.gc.ca/en/blogs/why-multi-factor-authentication-essential-part-cyber-security

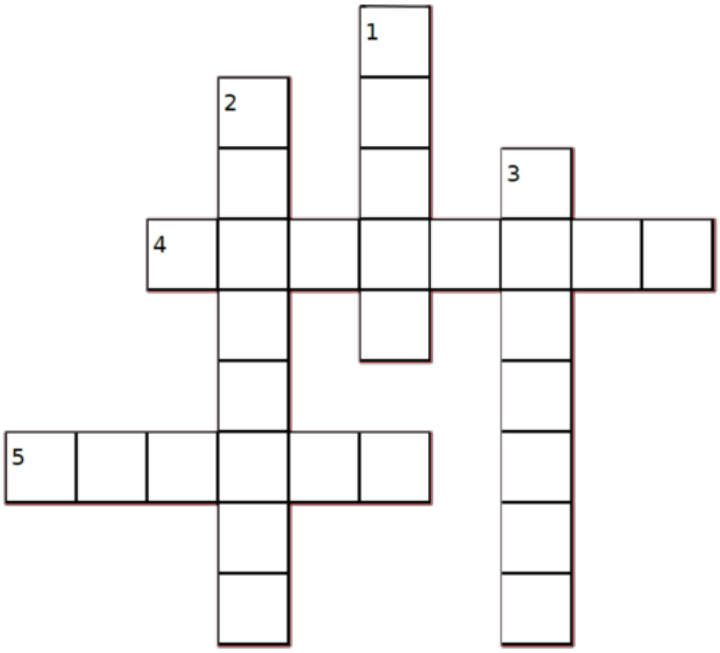
However, one of the challenges with MFA is the vast array of methods and applications that are used to accomplish MFA. It can be confusing and difficult to manage all of them.

Why Duo For Our Clients?

DUO simplifies MFA. We call it "Unified MFA": A single platform for managing MFA for every website, device, or application. Plus, ***DUO not only consolidates MFA, but it also adds MFA protection when logging into computers, laptops, and servers.***

Interactive Infotainment

You've probably heard them a hundred times... but how well do you KNOW these basic technology and security terms? (Answers under Kahn's Korner)



DOWN

1. Prefix *relating to or characteristic of the culture of computers, information technology, and virtual reality (hint: "the _____ age").*

2. Fraudulent practice *of sending entrapment emails to access personal information or company data.*

3. Software *that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.*

ACROSS

4. Network security device *that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies.*

5. Measurement *of how long a business is able to remain "online", increasing productivity (hint: opposite to down____).*

BIRMINGHAM CONSULTING
Like IT should be.®

21 Mill Street North
Waterdown, ON
L0R 2H0

(289) 895-8948

www.birmingham.ca
info@birmingham.ca