Fall 2022

The Mill

Like Newsletters Should Be.

Business

Top Cyber Insurance Terms Explained

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

When working with clients to submit applications for Cyber Insurance, they often tell us that they don't understand the terminology on the application form. **We have had so many questions on this that we now offer FREE Cyber Insurance Readiness Checks at birmingham.ca/CIRC**. Here are top insurance terms with simplified explanations:

"IT Security Audit" (AKA Cyber Security Assessment)

Explanation: The underwriter needs to know some kind of review of your cyber security has been conducted. This could be done by internal staff or by an external 3rd-party. This may not necessarily be a department or company that provides IT services, as IT and cyber security are NOT the same thing. That would be like saying a window & door company does the same work as a company that installs and monitors alarms for windows and doors.

"Penetration Test"

Explanation: Sometimes referred to as an "external penetration test", this is an experiment to determine if an unauthorized person can access your network, computers, servers, email, etc. "Unauthorized" means someone who does not have permission to access your files, emails & data.

"Vulnerability Assessment"

Definition: Vulnerability assessments are a systematic review of security weaknesses.

Explanation: Vulnerability assessments and penetration tests often get confused. The key difference is that you can pass a penetration test but still have vulnerabilities. Vulnerabilities include anything from out-of-date software and hardware to lack of antivirus protection to inability of your staff to identify fraudulent emails.

"Personally Identifiable Records/Information (PII)"

Explanation: According to the Canadian federal government, "personal information includes any factual or subjective information, recorded or not, about an identifiable individual. This includes information in any form, such as age, name, ID numbers, income, ethnic origin, or blood type and more." A common question on insurance applications is some form of "How many PII records does your company store, including present and previous employees?" Higher numbers of PII records generally translates to higher risk for the underwriter.

***Was this helpful?** Birmingham Consulting has a FULL and comprehensive "cheat sheet" of Cyber Insurance Terms with explanations that aren't techno-babble - learn more at birmingham.ca/cyber-insurance-terms.*

Security Discussion

What Is The Difference Between Cyber Security & IT Services?

By Veronica McMullen, Marketing Manager

Although the fields are related and share some common goals, cyber security professionals and IT professionals **focus on two different areas** when it comes to technology.

> *"Information technology focuses on the systems that store and transmit digital information. Cybersecurity, in contrast, focuses on protecting electronic information stored within those systems."*
>
> *2021 article from ZDNet - https://zd.net/3S5CY8S*

It is for this reason that organizations have separate roles for Chief Information Officer (CIO) and Chief Information Security Officer (CISO or CSO).

The main focus of CIOs and IT is organizational productivity by ensuring that the information and technology people need to do their jobs are working as expected.

The focus of CISOs and cyber security professionals is to protect that information and technology from unauthorized access.

> *"In most cases, cybersecurity is considered an IT job. However, cybersecurity jobs usually focus on protecting digital information. Some organizations may give these individuals the job title of cybersecurity specialist or cybersecurity manager. Related cybersecurity job titles include cybersecurity engineer or cybersecurity administrator."*
>
> *2021 article from ZDNet - https://zd.net/3S5CY8S*

To build an analogy, think of your family doctor (a "general practitioner" or "GP"). A GP has a broad spectrum of knowledge but because it's so broad, it's impossible to have deep knowledge in every area of healthcare, which is why specialists exist (pediatricians, dermatologists, cardiologists, ophthalmologists, etc.).

Using this analogy, a CIO would be akin to your family doctor and a CISO could be likened to an immunologist.

Shameless Self-Promotion

Newest Team Member Spotlight: Brody Atto

Brody, 2022 Fall Season in Hamilton

By Brody Atto, Technology Associate

I have been working in tech to some degree for over 10 years. I started working part time at my family's business under their IT manager while studying. There, I quickly grew to love the complexity of managing a business IT environment and the joy of helping end users. Earlier this year, I decided to move on to grow my skills in a more demanding environment. Moving from a family business, I had worried that I would not fit in well with the corporate environment that is common within the IT industry. I came to be pleasantly surprised when meeting the BCI team, to learn that **they value people and relationships more than just being another IT company**.

BCI doesn't sit back and wait for businesses to ask for help, but are always looking to go the extra distance to proactively help people in need. Not only when someone is having a technology issue, but as well as in the community and charity organizations.

When I started at BCI, one of the first things I learned about the company is how they improve their services - this continues to stand out every day through one of their core values, "Always Exploring." **It's not enough that we have a good solution today, we are always exploring new ways to improve.** Better security, better processes, better products.

"Of All The Things I Think About, IT Isn't One Of Them"

MOFFATT
SCRAP IRON & METAL INC.
METAL RECYCLING SOLUTIONS

" Our industry is regulated by multiple government agencies and depends on technology for compliance tracking in addition to daily operations. So when technology disruptions occur, we need them fixed fast. **We dealt with technology issues for years until referred to Birmingham Consulting.** Now our IT just works. We are worry free and know we have back up data if needed.

And for the odd time, when we experience a disruption, Birmingham deals with it right away. **They treat our business like it's their own.** Of all the things I think about, IT isn't one of them. "

Steve Moffatt - Moffatt Scrap Iron & Metal

Technology

The 6 Levels Of A Truly Proactive Managed Service Provider

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

Every managed cyber security provider and managed IT service provider (MSP) describes themselves as proactive when it comes to managing your infrastructure. But, how can a business understand what it means when a security or IT organization describes themselves as "proactive" – and what kind of value will it actually bring to your operations? Here are the 6 levels of proactivity a cyber security or IT team might ACTUALLY be referring to when they describe themselves as proactive:

LEVEL 1: CAPTAIN OBVIOUS

Consider when someone informs you a piece of equipment is old and needs to be replaced to pre-empt problems. Is that being proactive or just common sense? Simply pointing out the obvious and **calling it proactive is doing you a disservice**.

LEVEL 2: UPDATES, PATCHING AND MAINTENANCE

Many cyber and IT teams regularly perform these necessary activities - however, some teams use this level to describe themselves as being proactive. Having worked in manufacturing for many years, I look at these activities at a higher standard - which is that updates, patching and maintentance are preventative measures, not proactive. Similar to how **changing the oil in your car is universally understood to be preventative, not proactive**.

LEVEL 3: MONITORING AND ALERTS

The majority of MSP's function at this level as a matter of course: Monitor systems and if something is abnormal, receive an alert about it. Here's where proactivity comes in - upon triaging the alert, go ahead and resolve the condition that caused the alert. **Logical. But is it truly proactive?**

LEVEL 4: TECHNICAL ALIGNMENT REVIEWS

Technical alignment checkpoint (TAC) reviews are an effective proactive strategy - they continuously assess the technical environment or cyber security measures to identify and resolve potential issues BEFORE they happen. Major points scored for any MSP that does these reviews - but unfortunately, they remain a rarity.

LEVEL 5: THE TIDE RISES ALL BOATS

This is the practice of **applying lessons learned and improvements** gleaned through TAC from one organization to all organizations managed by that MSP, without compromising confidentiality. This is a **truly proactive** practice, but is often unnoticed and therefore undervalued.

LEVEL 6: GUIDANCE & RISK MANAGEMENT

This level of proactivity combines key knowledge and skills of understanding business objectives, appreciating future threats from the ever-changing cyber security landscape, **discerning between technology trends and fads** and more. These skills help MSP's make key recommendations that provide deliverable value, as well as build resilience against potential future threats / risks.

BOTTOM LINE: Being **truly** proactive is not easy and requires an investment of time, energy, and of course, money. However, the return on that investment will make you wonder why you didn't do it sooner.

Kahn's Korner

Our office cat, Kahn, supervises our internal printing needs - not very effectively, but he tries.

Interactive Infotainment: 1. Sender's email typo,
2. Suspicious attachment file type AND stating it's urgent,
3. Subtle grammar errors in body of the email.

Community

Flamborough Women's Resource Centre

Call: (289) 895-8580

24/7 Crisis Line: (905) 387-8881

Website: intervalhousehamilton.org

The Flamborough Women's Resource Centre is a rural chapter of Interval House of Hamilton, providing services to women with or without children who are experiencing family violence, abuse and/or human trafficking. They provide a starting point for women living within the rural areas of Flamborough and Hamilton. Interval House offers a wide variety of programs and services, including counselling, peer-support and legal advocacy. Counselling services are provided through a trauma-informed lens and designed to build on self-efficacy and resiliency.

Client Spotlight

D'Orazio Infrastructure Group

www.doraziogroup.com ☎ (905) 829-8777

D'Orazio Infrastructure Group delivers complete turnkey solutions for core infrastructure projects. Founded in 1966, they have a long history completing traditional and design-build projects in the municipal and private sectors of the water, wastewater and earth-moving – "core infrastructure" – sectors of the construction industry. **Their philosophy is and always will be to deliver quality projects, on schedule, on budget** with minimal community disruption, while meeting or exceeding the needs and expectations of our clients, the public, and any other stakeholder.

Each day brings with it new challenges that require a dynamic company supported by dynamic individuals – and D'Orazio is **ready to be put to the challenge.** They have worked throughout Southern Ontario on numerous, successfully completed private and public sector core infrastructure projects with values up to $30,000,000. With a wealth of knowledge on projects large and small, simple to complex, they have the proven track record and experience their clients expect.

Partner Spotlight

ThreatLocker®

As part of its overall protection strategy, ThreatLocker doesn't permit any application to run if it's not part of a pre-approved list. ThreatLocker also has the ability to isolate approved applications so that they don't access information they're not supposed to. For example, CAD software is safe; but it shouldn't be accessing financial information – if this happens, there is a strong possibility that the CAD software has been compromised and ThreatLocker would block it.

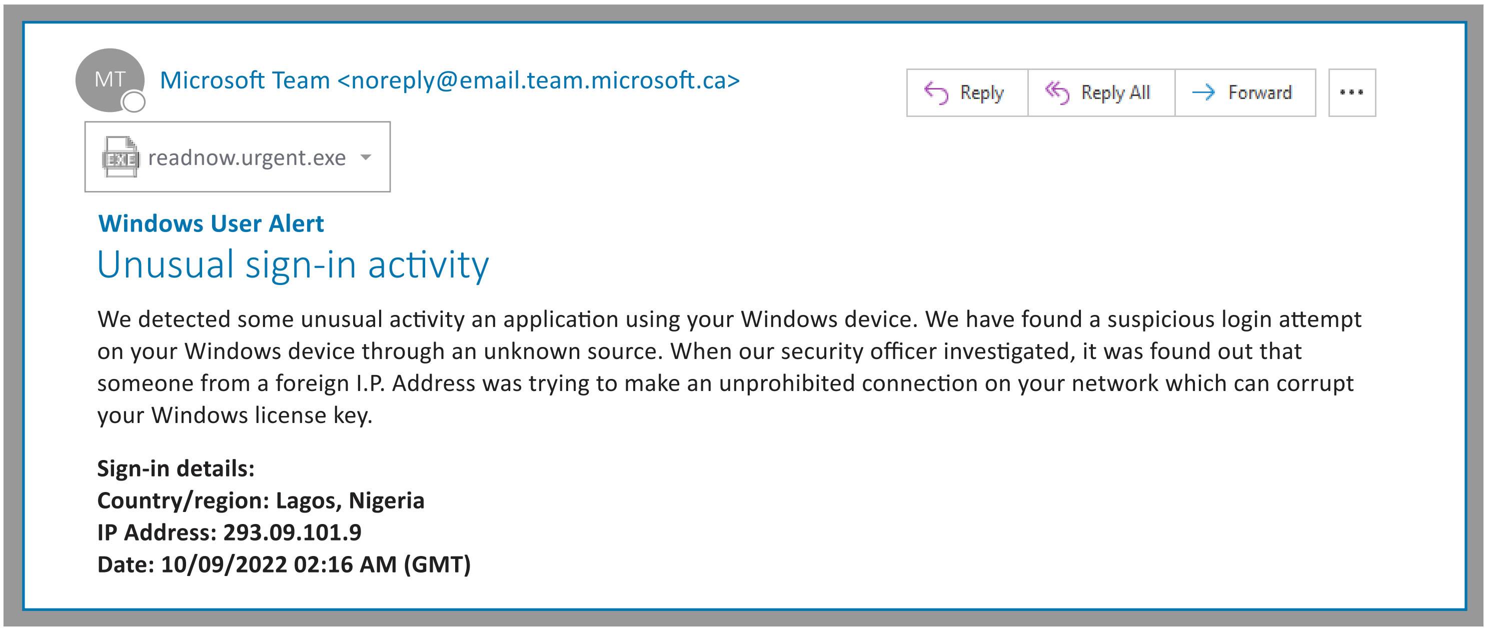
The technology behind ThreatLocker is called "zero trust". In other words, by default, don't trust any application that hasn't been vetted.

Why ThreatLocker For Our Clients?

ThreatLocker is one of the security layers we implement for clients. Other examples of security layers include multifactor authentication, security awareness training, next-gen antivirus – to name a few. It's important to create layers of defense for a few reasons - this includes making it more difficult for attackers to compromise a system, and ensuring clients are still protected in the event of a security supply-chain compromise.

Interactive Infotainment

Not every sign of a phishing email is in plain sight - How many RED FLAGS can you catch in the email below? Answers under Kahn's Korner.



Microsoft Team <noreply@email.team.microsoft.ca>

readnow.urgent.exe

Windows User Alert

Unusual sign-in activity

We detected some unusual activity an application using your Windows device. We have found a suspicious login attempt on your Windows device through an unknown source. When our security officer investigated, it was found out that someone from a foreign I.P. Address was trying to make an unprohibited connection on your network which can corrupt your Windows license key.

Sign-in details:
Country/region: Lagos, Nigeria
IP Address: 293.09.101.9
Date: 10/09/2022 02:16 AM (GMT)