Five-Step Checkup for Your Cyber Protection

NPC Safe Computing Webinar Series

April 19, 2022

Larry Keating, President
Darren Mar, National Sales Manager

NPC DataGuard™

Presenters

Larry Keating
President

30 years' experience with information technology, remote communications and data security.

Darren Mar
National Sales Manager

More than 10 years in SMB technology products and services, with emphasis on financial services small office security.

Thank You!

ALIGNED
capital partners inc.

MFDA
Mutual Fund Dealers Association of Canada
Association canadienne des courtiers de fonds mutuels

PPI Solutions

Manulife Securities

Advocis
The Financial Advisors
Association of Canada

MANDEVILLE
PRIVATE CLIENT INC.

FaithLife
FINANCIAL

AON

Investment
Planning Counsel
IPC VALEURS MOBILIÈRES

GROVE POINT
FINANCIAL

HollisWealth

IDC
WORLDSOURCE
INSURANCE NETWORK INC.

Advisor Research
Group Inc.

CI FINANCIAL

IIAC ACCVM
INVESTMENT INDUSTRY ASSOCIATION OF CANADA
ASSOCIATION CANADIENNE DU COMMERCE DES VALEURS MOBILIÈRES

FINANCIAL LITERACY
COUNSEL INC.

GLOBAL
MAXFIN INVESTMENTS INC.

EQUITY
Associates Inc.

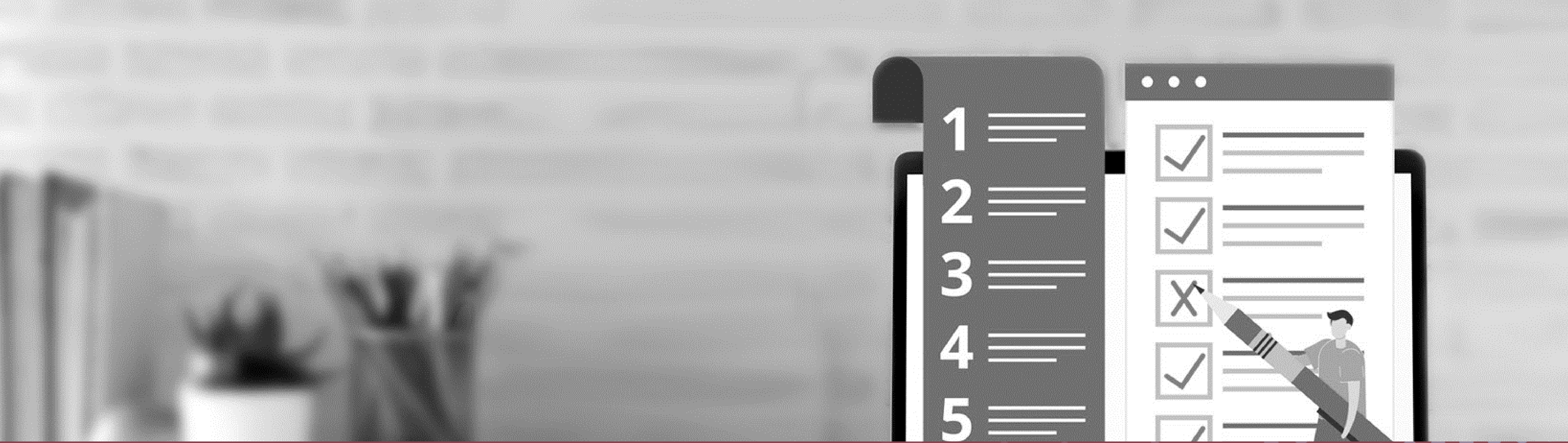
NPC Solutions

Secure managed computers and Microsoft 365 for the professional and SMB office.

- NPC Secure Managed Computers
  - Hardware, encryption, backup, system software, security, technical support, managed and monitored for you
- NPC Managed Microsoft 365
  - SharePoint, Exchange Email, Teams, and a host of productivity tools
- Dedicated Account Manager
  - A custom and consultative approach

Agenda

- The Importance of Routine Cybersecurity Checkups
- Five-Step Cybersecurity Checkup
- Maintaining Good Cyber Hygiene
- Q&A



The Importance of Routine Cybersecurity Checkups

Attack Methods

Threats are up

300%

since the pandemic started

Source: FBI IC3 (Internet Crime Complaint Centre)

Email and web browsing

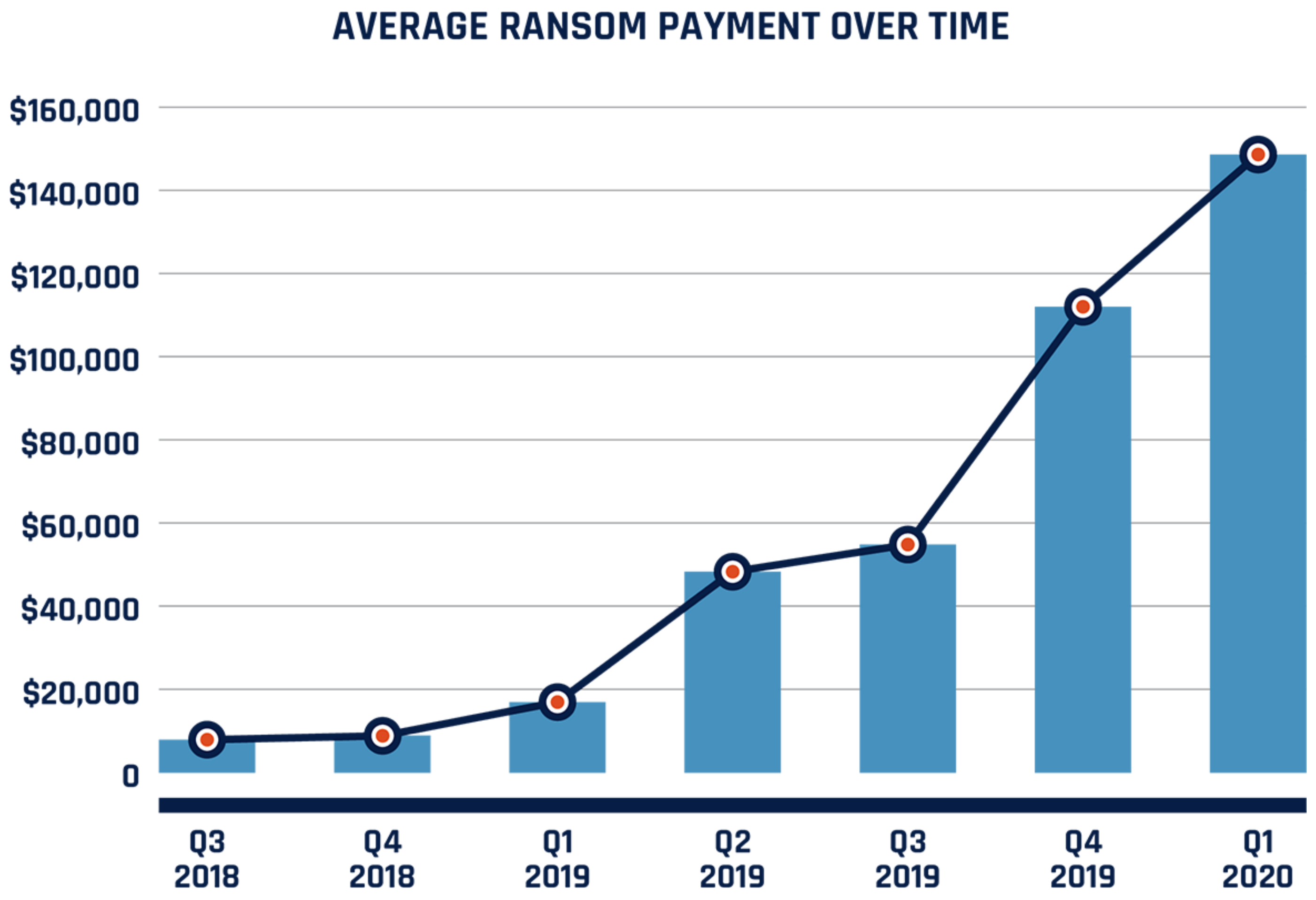
Remote desktop

Improperly Protected Networks

IoT devices

Supply Chain Attacks

Ransom Payments Increase



Source: Canadian Centre for Cyber Security: November 2020 Threats to Canadian Financial and Economic Health - Canadian Centre for Cyber Security

Increase in Tactics to Coerce Payment

Doxing:

- Steal and leak data if ransom to unlock not paid
- May cause violation of contract terms, non-disclosure agreements, privacy laws, securities laws, loss of intellectual property, or intellectual property protection

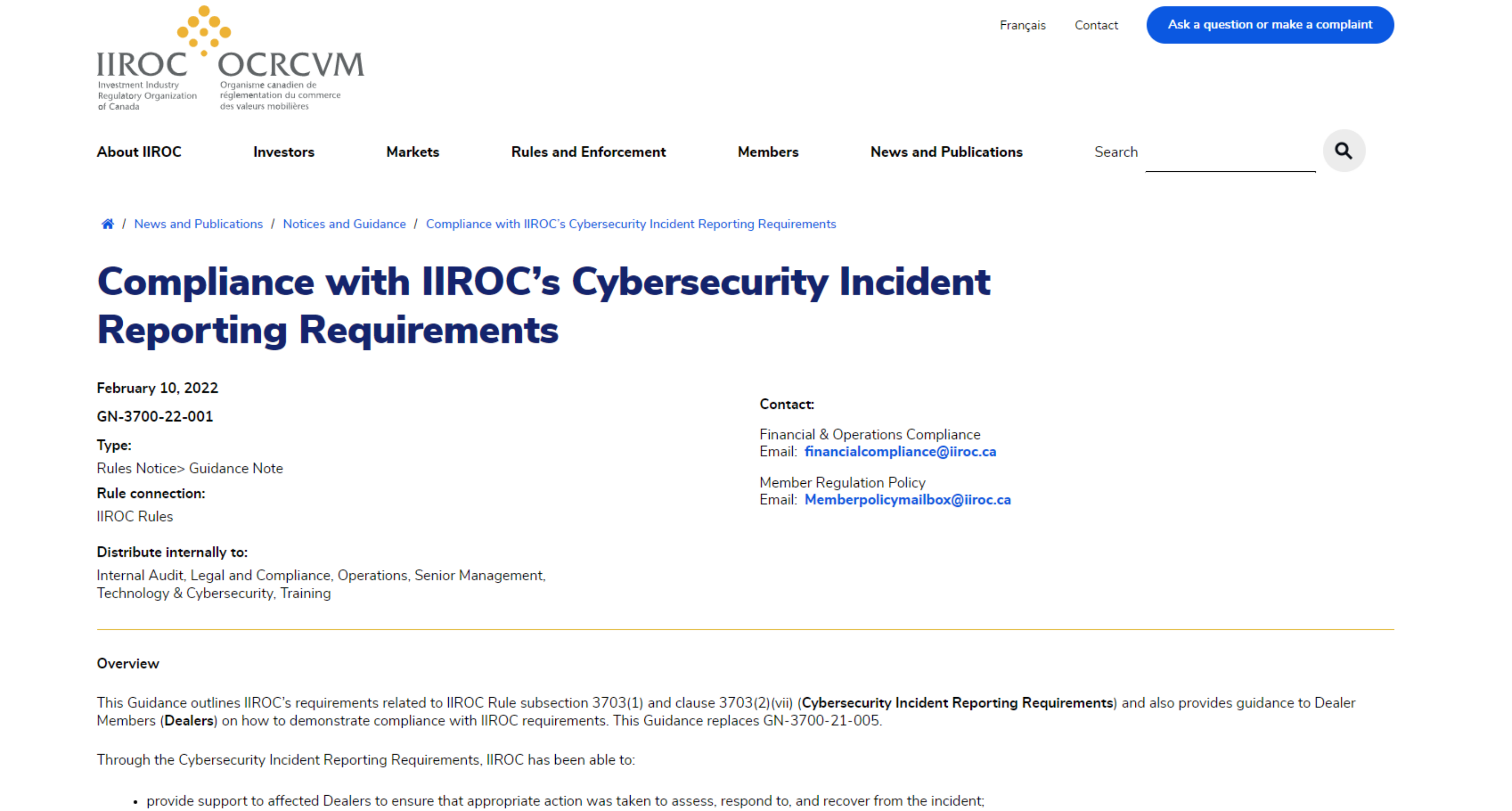
Shaming:

- If ransom still not paid, advise victim’s clients, suppliers, partners, etc., of the breach via victim’s social media and stolen email lists

Double-Encrypting:

- A second layer of encryption requiring a different key, or two or more segments of data have different keys

IIROC – Mandatory Breach Reporting



IIROC OCRCVM
Investment Industry Regulatory Organization of Canada
Organisme canadien de réglementation du commerce des valeurs mobilières
Français
Contact
Ask a question or make a complaint
About IIROC
Investors
Markets
Rules and Enforcement
Members
News and Publications
Search
News and Publications / Notices and Guidance / Compliance with IIROC's Cybersecurity Incident Reporting Requirements

Compliance with IIROC's Cybersecurity Incident Reporting Requirements

February 10, 2022

GN-3700-22-001

Type:
Rules Notice> Guidance Note

Rule connection:
IIROC Rules

Distribute internally to:
Internal Audit, Legal and Compliance, Operations, Senior Management, Technology & Cybersecurity, Training

Contact:

Financial & Operations Compliance
Email: **financialcompliance@iiroc.ca**

Member Regulation Policy
Email: **Memberpolicymailbox@iiroc.ca**

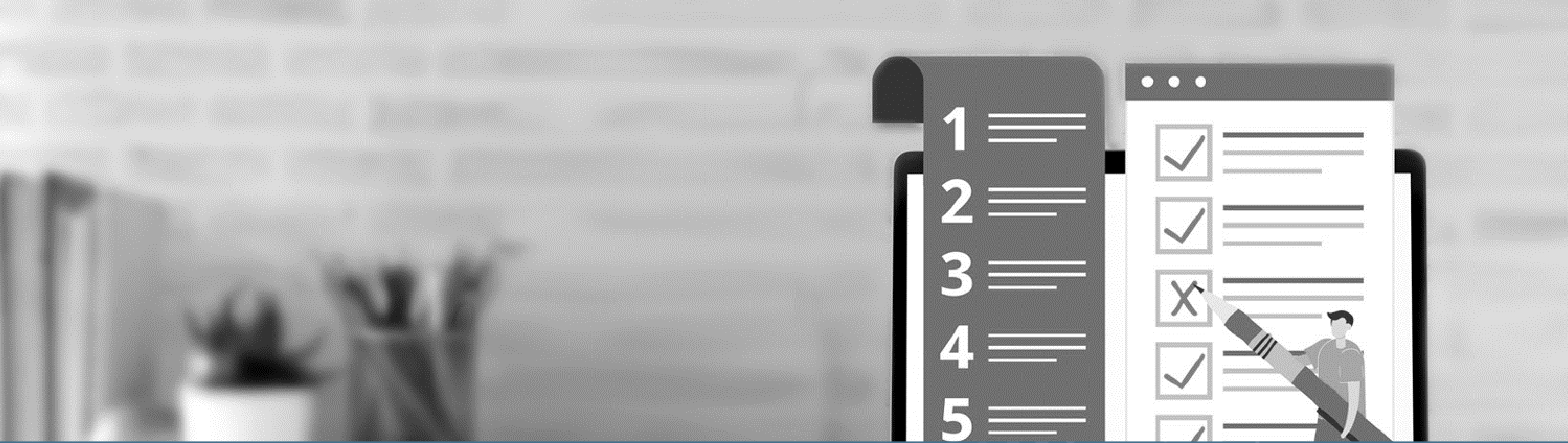
Overview

This Guidance outlines IIROC's requirements related to IIROC Rule subsection 3703(1) and clause 3703(2)(vii) (**Cybersecurity Incident Reporting Requirements**) and also provides guidance to Dealer Members (**Dealers**) on how to demonstrate compliance with IIROC requirements. This Guidance replaces GN-3700-21-005.

Through the Cybersecurity Incident Reporting Requirements, IIROC has been able to:

- provide support to affected Dealers to ensure that appropriate action was taken to assess, respond to, and recover from the incident;

Source: Compliance with IIROC's Cybersecurity Incident Reporting Requirements | IIROC



Cybersecurity Checkup

STEP 1: Passwords and MFA

Password and MFA Checkup

Save this **checklist** for later.

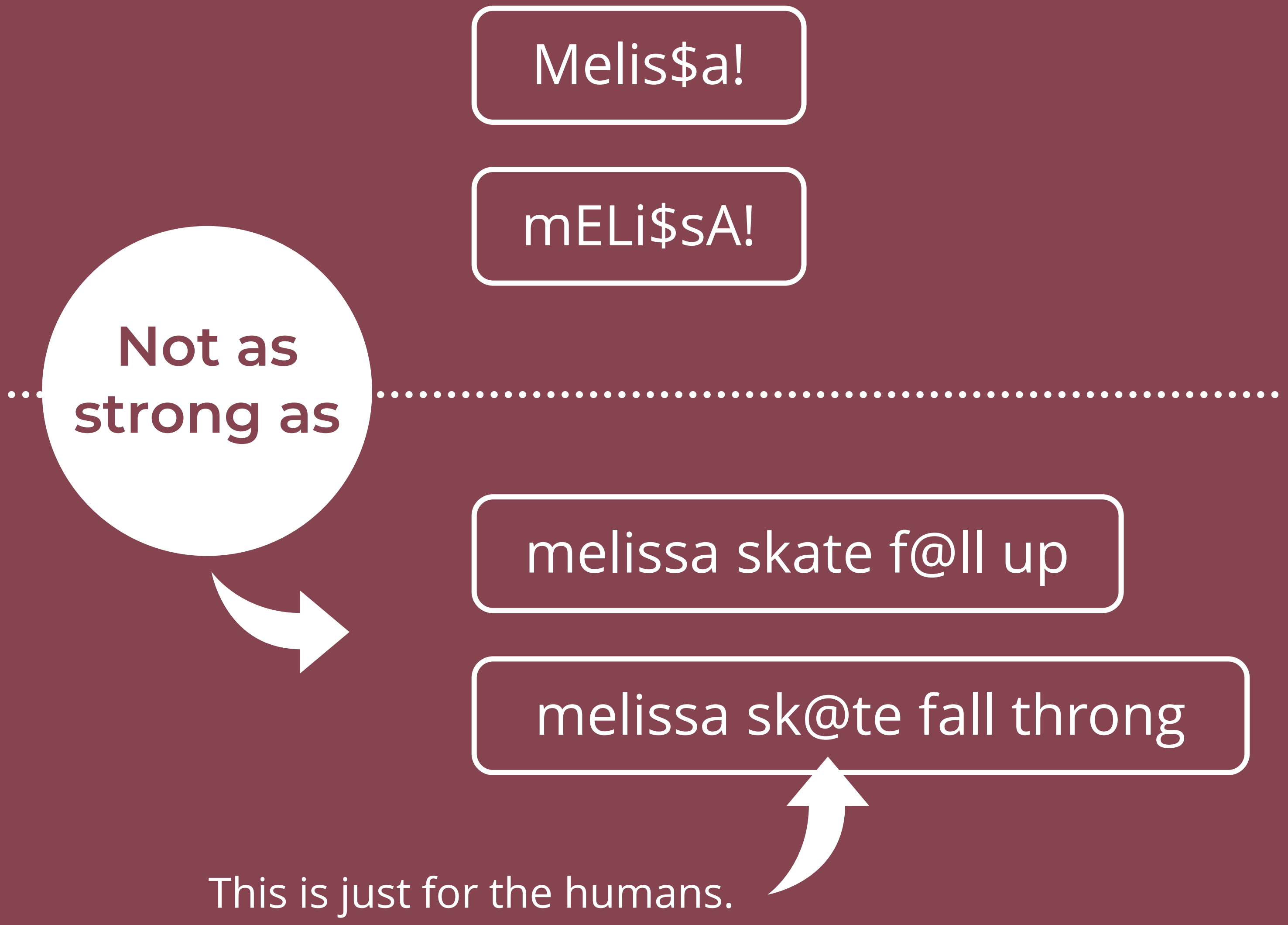
- ❑ Review (or establish) your password and authentication policy
  - ❑ Minimum password lengths
  - ❑ Change requirements
  - ❑ Requirements for 2FA or MFA
  - ❑ Etc.
- ❑ Inventory what systems and devices require passwords, commenting on length and complexity requirements, risk factors of key systems
  - ❑ Check on staff meeting those requirements
  - ❑ Consider the use of password management tools, and SSO (Single-Sign On) solutions, fingerprint readers

Passwords and Passphrases

Favour length over complexity.

Create a passphrase that is a memorable mental image for you.

Try to use on uncommon word.



Melis$a!

mELi$sA!

Not as strong as

melissa skate f@ll up

melissa sk@te fall throng

This is just for the humans.

Passwords and Passphrases Best Practices

Save this **checklist** for later.

- ❑ Use passphrases, favour length over complexity
- ❑ Change your passwords regularly – every 90 - 120 days
- ❑ Never text or email a password with the login name
- ❑ Never use the same password twice, or in more than one place:
  - Have I Been Pawned https://haveibeenpwned.com/
- ❑ Never use easy to guess security confirmation questions, especially if you have published that detail on social media
- ❑ Never confirm a password online through a link you are uncertain of, never give it up over the phone or in a text
- ❑ Never embed personal info in your browser
- ❑ Use fingerprint readers
  - Allows longer passwords and passphrases, without the inconvenience of having to frequently type them

Writing Passwords Down

Save this **checklist** for later.

Follow these practices:

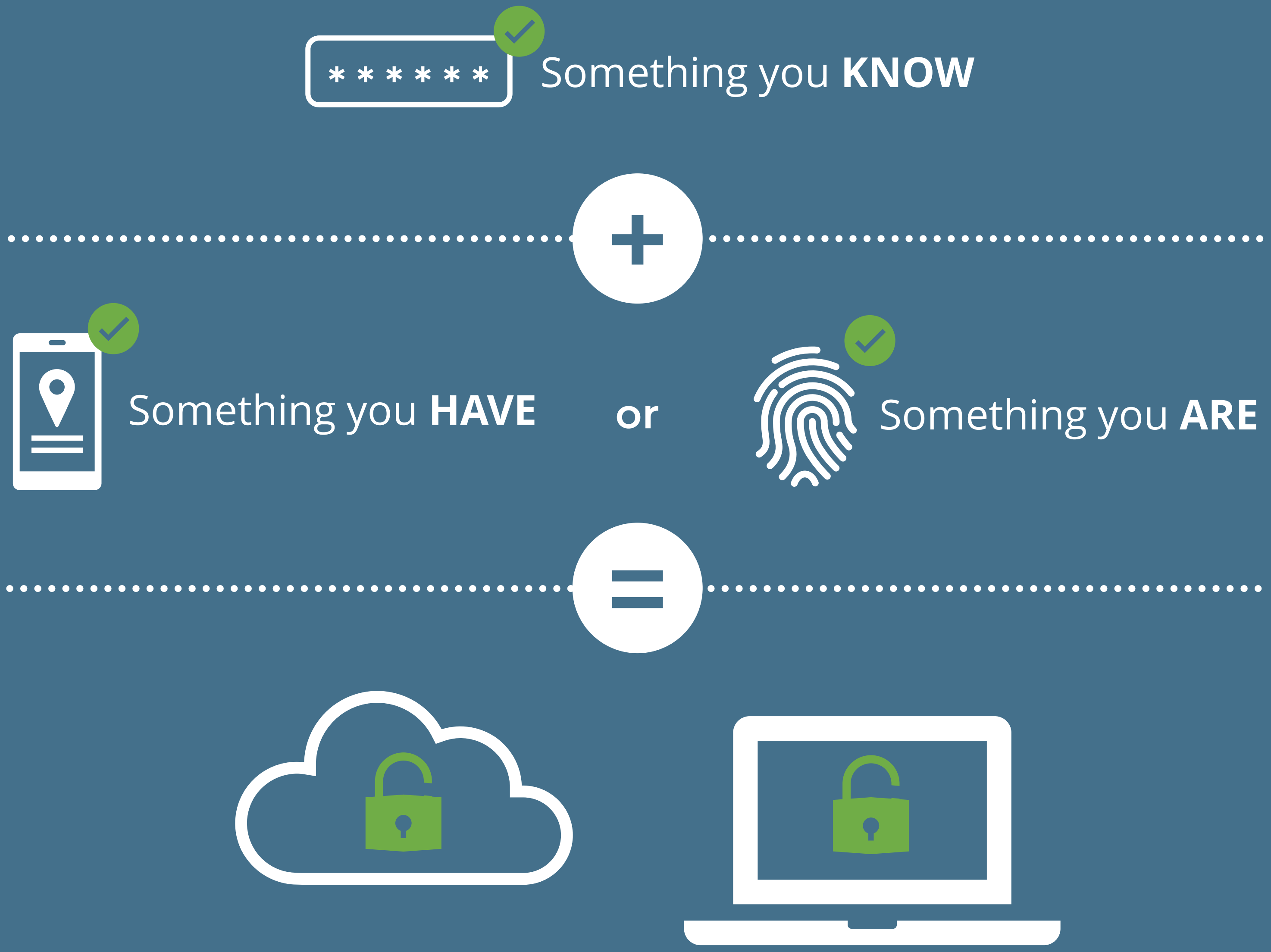
- ❑ Be absolutely certain you store and manage a list securely
- ❑ Do not write down the associated usernames or site/services they are for. But know that for most of your logins it is your email address, and that is known
- ❑ Change them slightly in the list, but do not make the change uniform

Consider and investigate carefully online password managers.

Multi-Factor Authentication

<u>Definition:</u>

A method of allowing access to applications, websites, systems or devices, only after the user presents two or more pieces of authentication evidence.



****** Something you **KNOW**

+

Something you **HAVE** or Something you **ARE**

=

Forms of Attack MFA Prevents

Stops "brute force attacks", or account compromise from lost or stolen passwords/credentials, or poorly constructed primary authentication systems:

Man-in-the-Middle (MITM) Attacks

Credential Stuffing

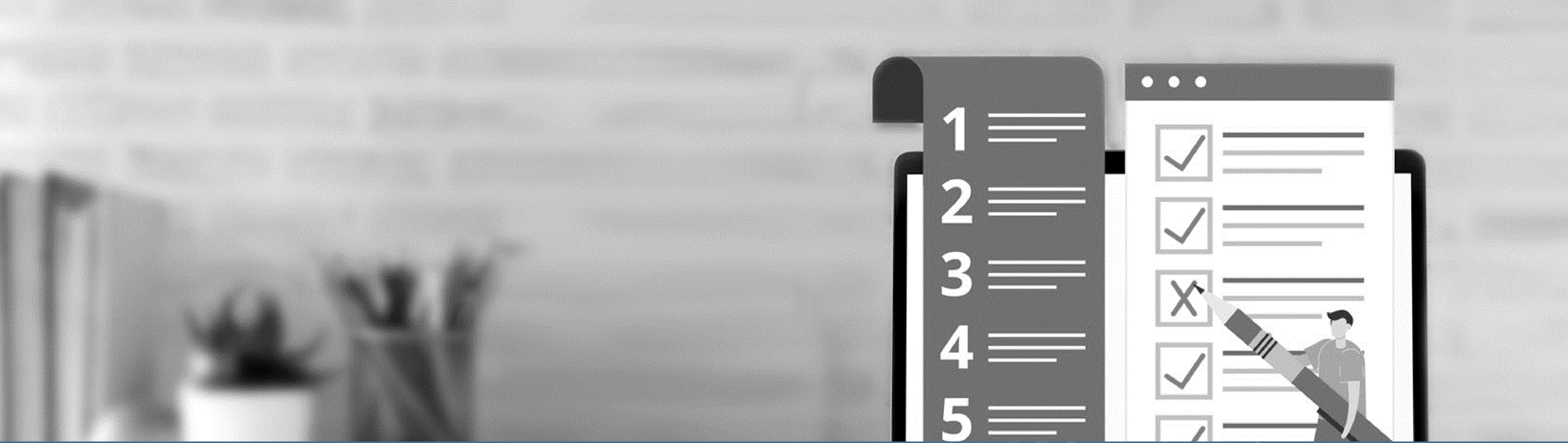
Phishing

Spear Phishing

Reverse Brute-Force Attacks

Brute-Force Attacks

Keyloggers



Cybersecurity Checkup

STEP 2: Computers and Systems Security

Protect Your Endpoint Devices

☐ Save this **checklist** for later.

- ❑ Ensure you have up-to-date and fully patched:
  - ❑ Computer BIOS, operating system, Office suite
  - ❑ System apps like Java and Adobe
  - ❑ Web browser
  - ❑ Anti-malware suite
- ❑ Enable encryption, and manage it carefully
- ❑ Enable personal firewall on endpoint computers
- ❑ Change default passwords on all IoT devices
- ❑ Only do your work on a secured device

Protect Your Systems

- ❑ Apply principles of least privilege for user access, lock admin accounts
- ❑ Employ adequate spam email filtering and content scanning, provided by your ISP, email service, or optionally on your firewall
- ❑ Ensure all your web connections are https
- ❑ Use a VPN if you are still accessing a private server or using public Wi-Fi
- ❑ Ensure you have a professional look at your remote desktop setup

Save this **checklist** for later.

Backup Your Files

Save this **checklist** for later.

The ultimate failsafe against loss, theft, fire, mechanical failure, human error, viruses, Trojans, malware, etc.

Sometimes necessary for regulatory compliance.

- ❑ Make sure your backup will restore
- ❑ Do not keep your backup in the same place as the computer(s) you are backing up
- ❑ Ensure you have a backup multiple versions deep, and it connects to your computers only when backing up
- ❑ Distinguish between file sharing, primary storage vs. backup

Secure Your Wi-Fi

- ❑ Ensure that your home Wi-Fi:
  - ❑ Has a strong, long password that has been changed from the default
  - ❑ WPA2 level security is enabled
  - ❑ Disable UPnP - Universals Plug and Play
  - ❑ Disable WPS – Wi-Fi Protected Set-Up
  - ❑ Ensure your home router is patched and up-to-date
  - ❑ The router's firewall, if present, is enabled
  - ❑ Has an obscure SSID, or disable SSID broadcast
- ❑ Change default passwords on all IoT devices

Save this **checklist** for later.

Secure Work From Home Checklist

- ❑ Browsing:
  - ❑ Decline data sharing, restrict cookies
    - A more "personalized" browsing experience is a poor trade-off for your identity
  - ❑ Resist saving credit card information and auto-fill information in your browser
  - ❑ Don’t play, casually browse, or shop on your work computer
- ❑ Ensure your smartphone is secured, consider an anti-malware app for it
- ❑ Don’t forget about physical workspace security:
  - ❑ A separate, low-traffic area
  - ❑ Ensure home bandwidth is adequate

Save this **checklist** for later.

Train Your Staff

- ❑ Have clear policies in place for computer use, passwords, information handling, etc.
- ❑ Don’t click what you don’t know:
  - ❑ Links or attachments in unexpected emails
  - ❑ Websites you are uncertain of
- ❑ Observe error and warning messages from your computer
- ❑ Observe email addresses
- ❑ Establish email source and address verification process

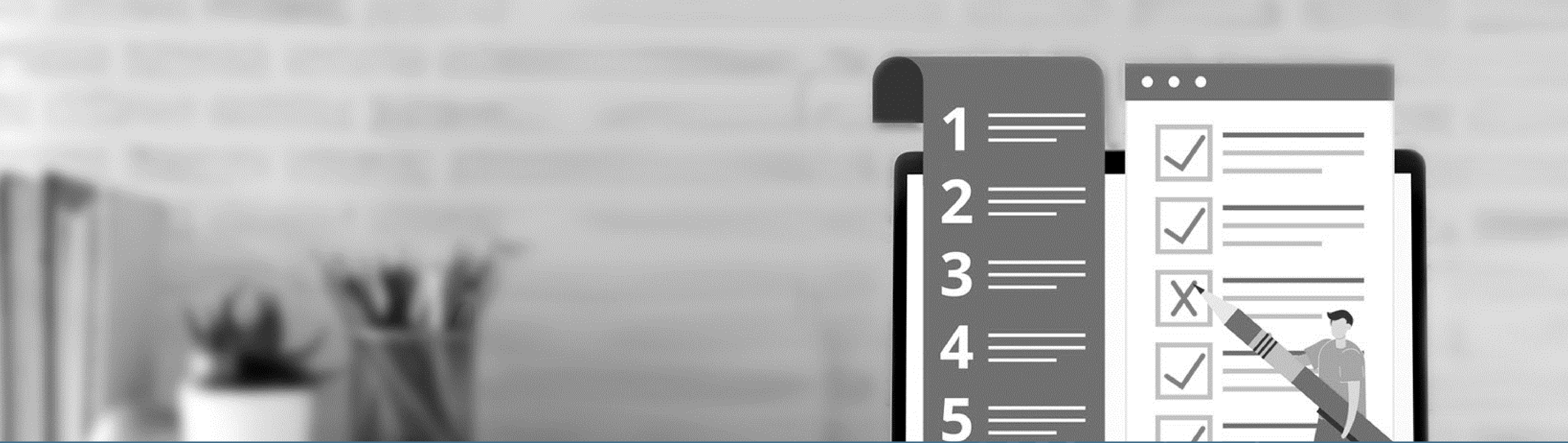
Save this **checklist** for later.

Protect Your Company

❑ Conduct a risk assessment, preferably using a security professional

❑ Acquire a specific cyber package, in addition to your E&O or general liability package

Save this **checklist** for later.



Cybersecurity Checkup

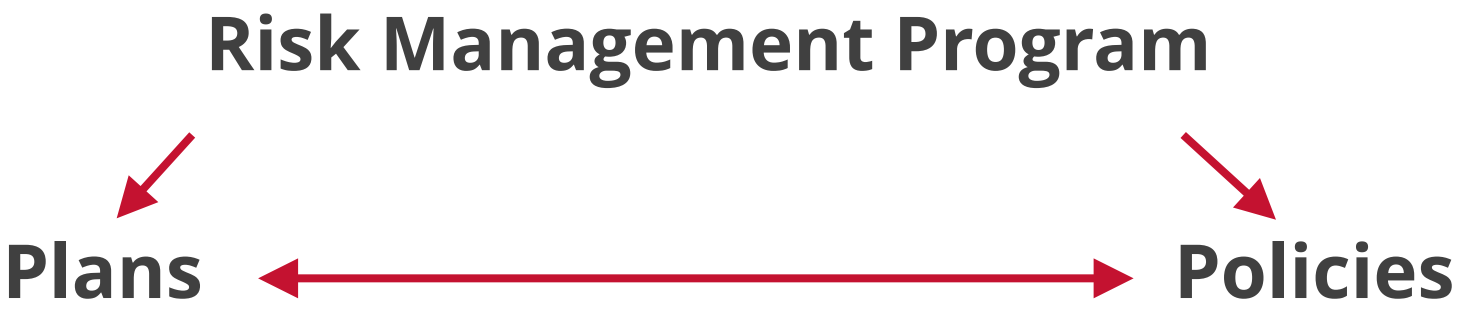
STEP 3: Policies and Plans

Review your Computing and Information Security Policies and Plans

Save this **checklist** for later.

- ❑ Check to ensure you have appropriate cyber protection and information security policies and plans in place
- ❑ Check to ensure the plans you have are up to date
- ❑ Ensure staff are revisiting the plans at least biennially
- ❑ Keep plans and policies as simple as they can be, but meet effectiveness requirements

Policies and Plans: Top 5 Picks



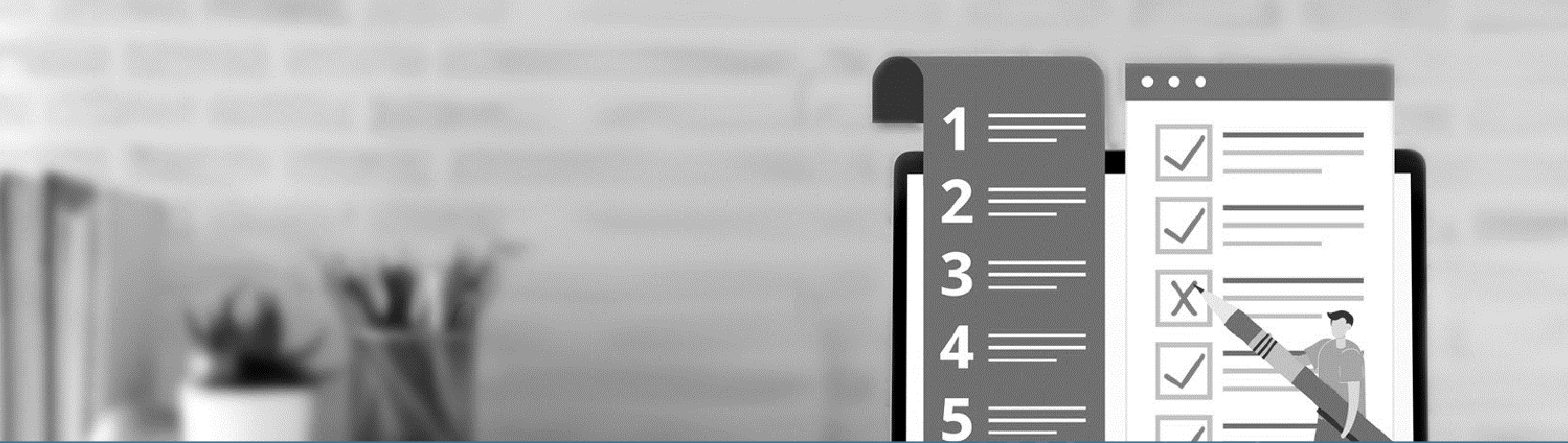
Risk Management Program

Plans

Policies

1. Incident Response Plan (IRP)
2. Business Continuity Plan (BCP)
3. Information Security Plan
4. Asset Management Plan
5. Vendor Risk Assessment

1. Privacy Policy
2. Computer, Mobile, and USB Device Policy
3. Password Policy
4. Data Encryption and Backup
5. Email Use / Social Engineering Awareness



Cybersecurity Checkup
STEP 4: Incident Response Plan

Plan 1: Incident Response Plan

The plan I would do first if I had no other plan or policy in place:

- ❑ What are your particular risks, what type of incident would have the most impact
- ❑ Have an Incident Response Team organized and at the ready
- ❑ Ensure a lawyer, your insurance agency, and your compliance professional are part of the team, and are immediately contacted in the plan
- ❑ Map out how you will communicate within the team
- ❑ Know your regulator or professional association reporting requirements and timelines
- ❑ If you do business internationally or extra-provincially, know your responsibilities in those territories
- ❑ Map out how you will mitigate damage, quell the attack
- ❑ Ensure you are using professional technical services immediately to minimize damage, preserve evidence
- ❑ Perform a post-mortem, and extensive post-event technical testing
- ❑ Test and revisit the plan at least annually

What’s an Incident?

Any event that causes the loss or theft of data, breach of your systems, attack on your operations, attack on your clients –it could be both an internal or external attack:

- Ransomware
- Business Email Compromise (BEC)
- Loss of login credentials, unauthorized access to systems
- Loss of a device – laptop, desktop, smartphone, USB storage device
- Physical break-in or insider theft of paper records

What Your Plan Will Look Like

Keep it simple

- Your plan may be two pages, or twenty:
  - For professionals handling sensitive data, even a company of one needs a plan
  - Make it commensurate with the size and complexity of your operation
- You share it with key team members, internal and external, and will access it to lead you in an emergency
- It is better to have some kind of a plan, than no plan at all (…this from a hardcore perfectionist ☹)

NPC IRP Template

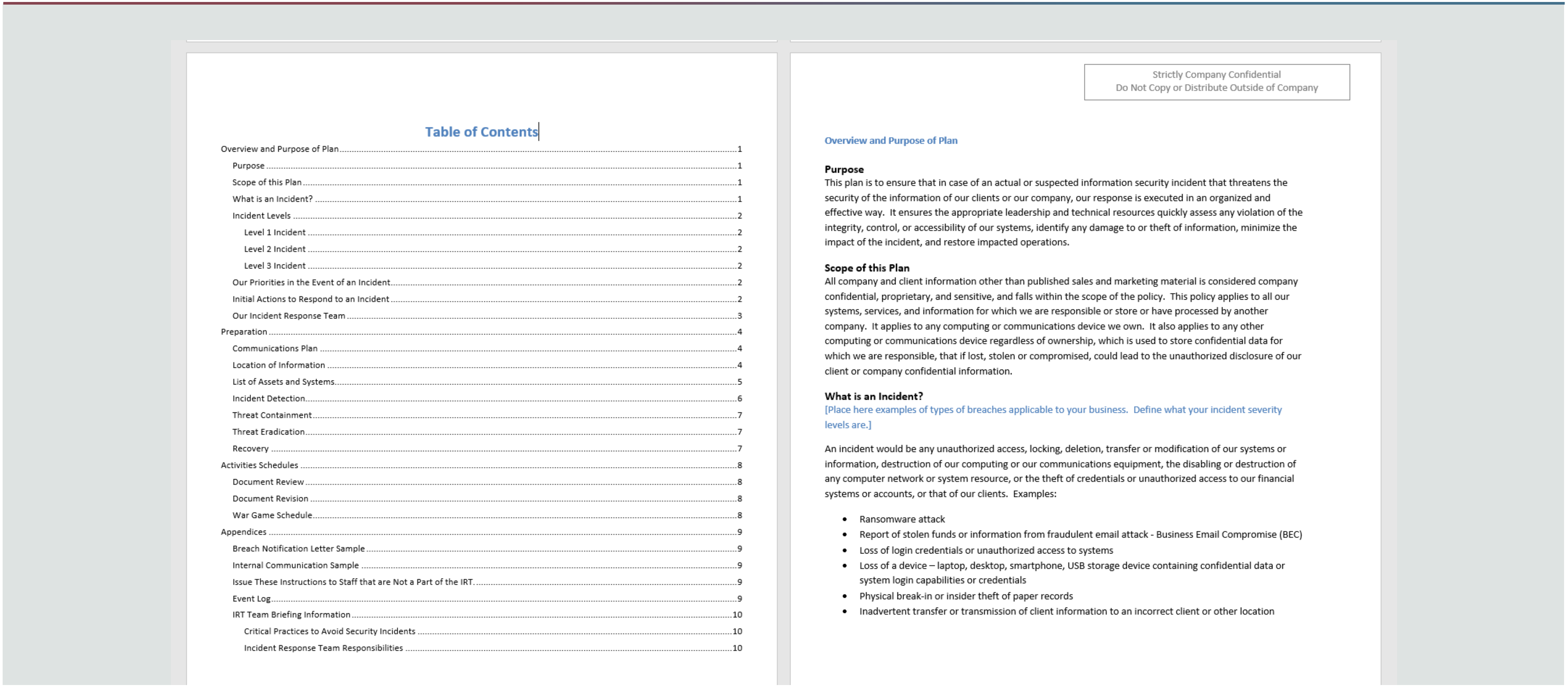


Table of Contents

Strictly Company Confidential
Do Not Copy or Distribute Outside of Company

Overview and Purpose of Plan

Purpose

This plan is to ensure that in case of an actual or suspected information security incident that threatens the security of the information of our clients or our company, our response is executed in an organized and effective way. It ensures the appropriate leadership and technical resources quickly assess any violation of the integrity, control, or accessibility of our systems, identify any damage to or theft of information, minimize the impact of the incident, and restore impacted operations.

Scope of this Plan

All company and client information other than published sales and marketing material is considered company confidential, proprietary, and sensitive, and falls within the scope of the policy. This policy applies to all our systems, services, and information for which we are responsible or store or have processed by another company. It applies to any computing or communications device we own. It also applies to any other computing or communications device regardless of ownership, which is used to store confidential data for which we are responsible, that if lost, stolen or compromised, could lead to the unauthorized disclosure of our client or company confidential information.

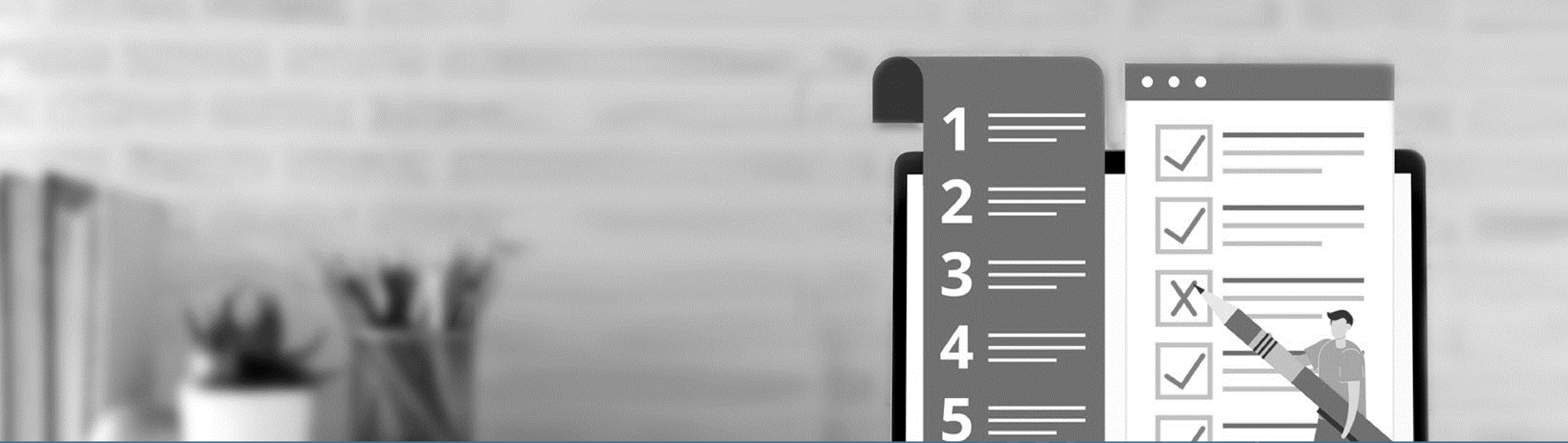
What is an Incident?

[Place here examples of types of breaches applicable to your business. Define what your incident severity levels are.]

An incident would be any unauthorized access, locking, deletion, transfer or modification of our systems or information, destruction of our computing or our communications equipment, the disabling or destruction of any computer network or system resource, or the theft of credentials or unauthorized access to our financial systems or accounts, or that of our clients. Examples:

- Ransomware attack
- Report of stolen funds or information from fraudulent email attack - Business Email Compromise (BEC)
- Loss of login credentials or unauthorized access to systems
- Loss of a device – laptop, desktop, smartphone, USB storage device containing confidential data or system login capabilities or credentials
- Physical break-in or insider theft of paper records
- Inadvertent transfer or transmission of client information to an incorrect client or other location

https://go.npcdataguard.com/incident-response-template-download



Cybersecurity Checkup

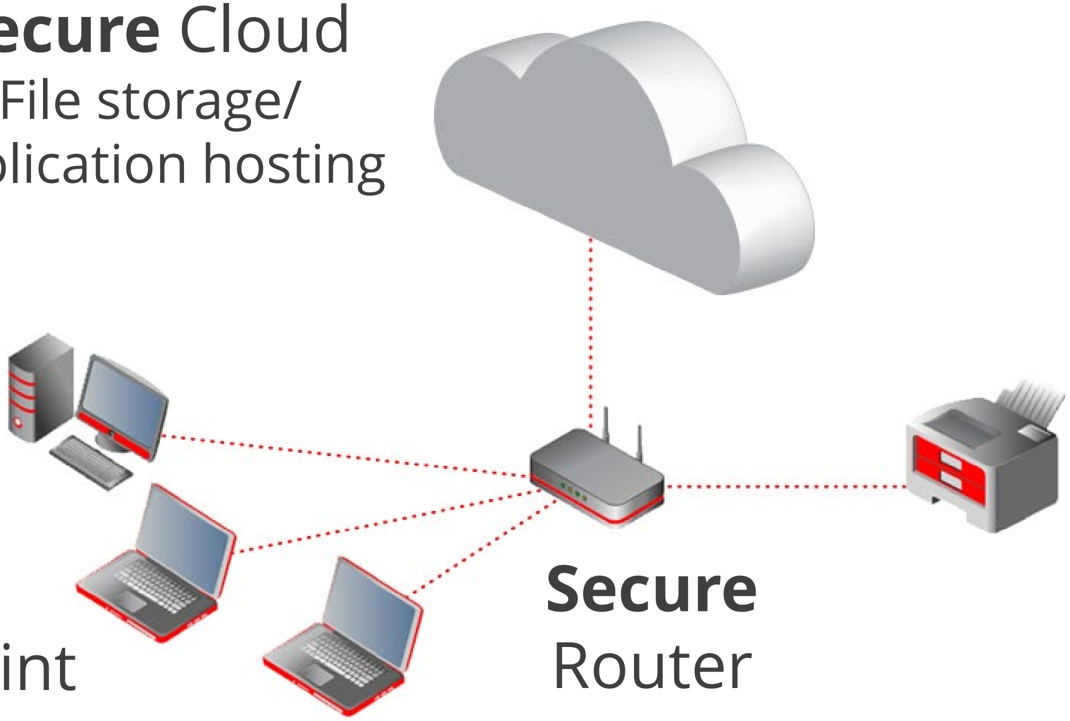
STEP 5: As-a-Service and Cloud Technologies

Review your use and adoption of "as-a-service" and cloud computing technologies

Save this **checklist** for later.

- ❑ Check to ensure you have identified any use of online services in your company, and they are within policy and regulatory standards
- ❑ Review the security level, policies and contract terms of any third-party provider
- ❑ Identify opportunities to replace traditional "break/fix" technology supply models
- ❑ Review business processes, methods and tools frequently with your team to identify simplification advantages, given new technology developments and as-a-service capabilities

Office of the Future



Secure Cloud
File storage/
application hosting

Secure Printer,
Copier, Scanner

Secure
Router

Secure Endpoint
Devices

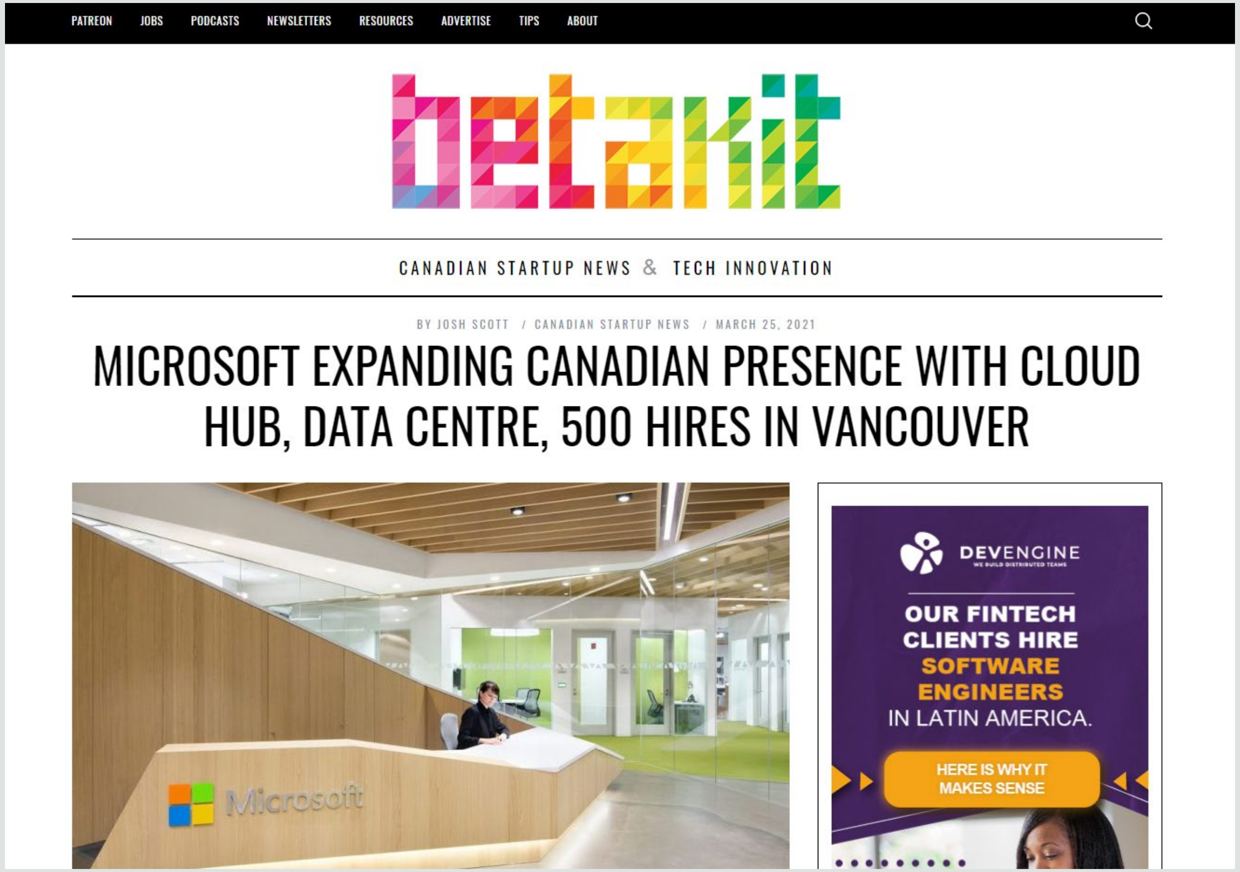
What’s the Benefit?

- As-a-service models remove the cost of custom-building common application, network, server, security, and services needs
- Specialization by the provider allows more features for less cost, improved performance, security, and reliability
- Allows for more economical “scaling up” or “scaling down”

It is difficult to compete with the security, speed, reliability and economics of specialization

Microsoft Security…

- Microsoft employs nearly 4,000 professionals in Canada, more than 100,000 in the U.S.
- Data centres adhere to ISO 27001, ISO 27018, SSAE 16 SOC1 Type II audit and controls standards
- The data centres are built from the ground up for external and internal security
- Massive internal analysis systems employing AI and using advanced signals intelligence protect your data
- Advanced content control and multi-engine malware scanning



CANADIAN STARTUP NEWS & TECH INNOVATION

BY JOSH SCOTT / CANADIAN STARTUP NEWS / MARCH 25, 2021

MICROSOFT EXPANDING CANADIAN PRESENCE WITH CLOUD HUB, DATA CENTRE, 500 HIRES IN VANCOUVER

Source: Betakit, March 25, 2021

Five-step Cyber Protection Checkup Recap

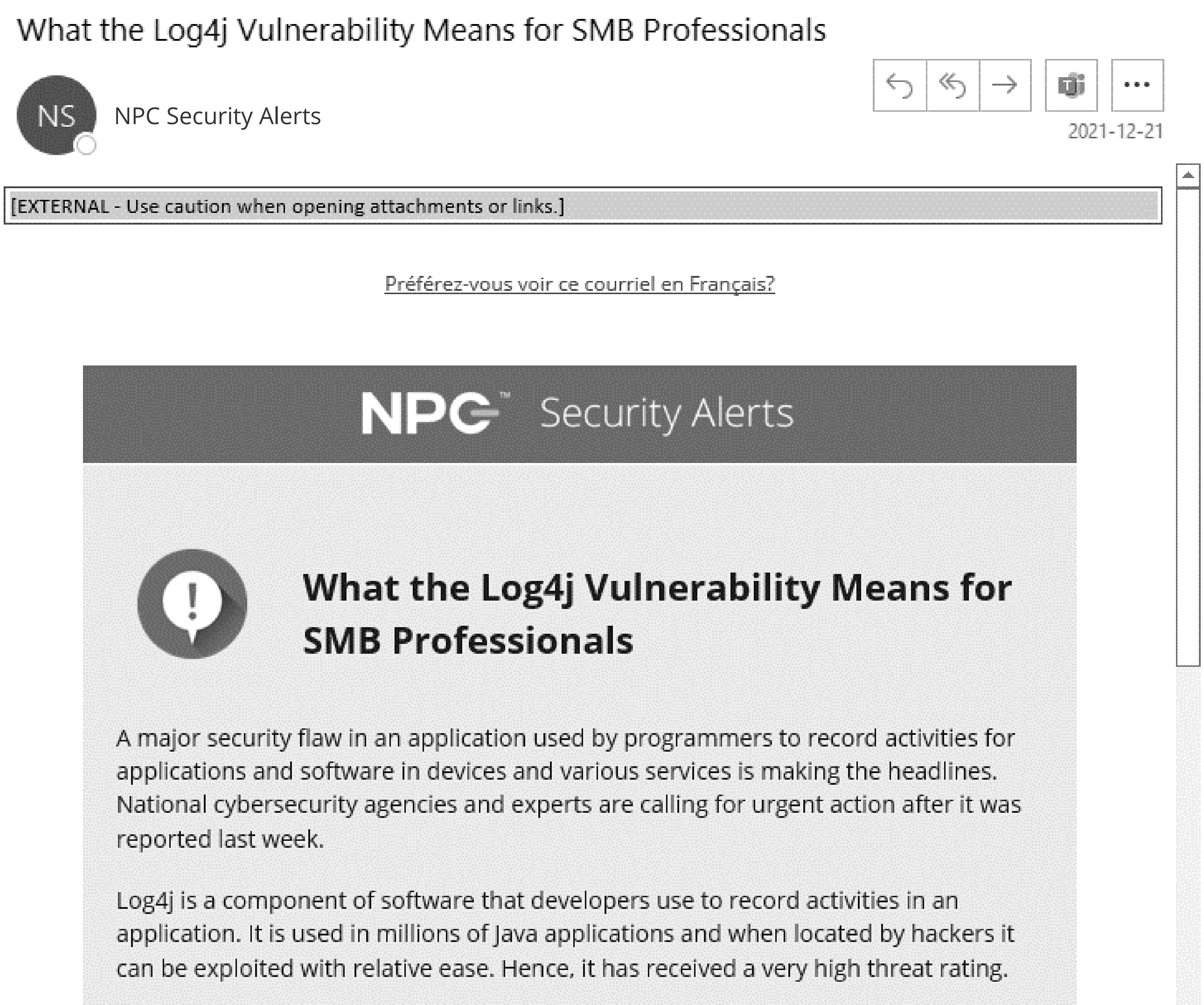
Review:

1. Passwords and Multi-Factor Authentication
2. Computers and Systems Security
3. Policies and Plans
4. Incident Response Plan
5. As-a-Service and Cloud Technologies

Additional Resources

NPC Security Alerts

npcdataguard.com/alerts



What the Log4j Vulnerability Means for SMB Professionals

NS NPC Security Alerts

2021-12-21

[EXTERNAL - Use caution when opening attachments or links.]

Préférez-vous voir ce courriel en Français?

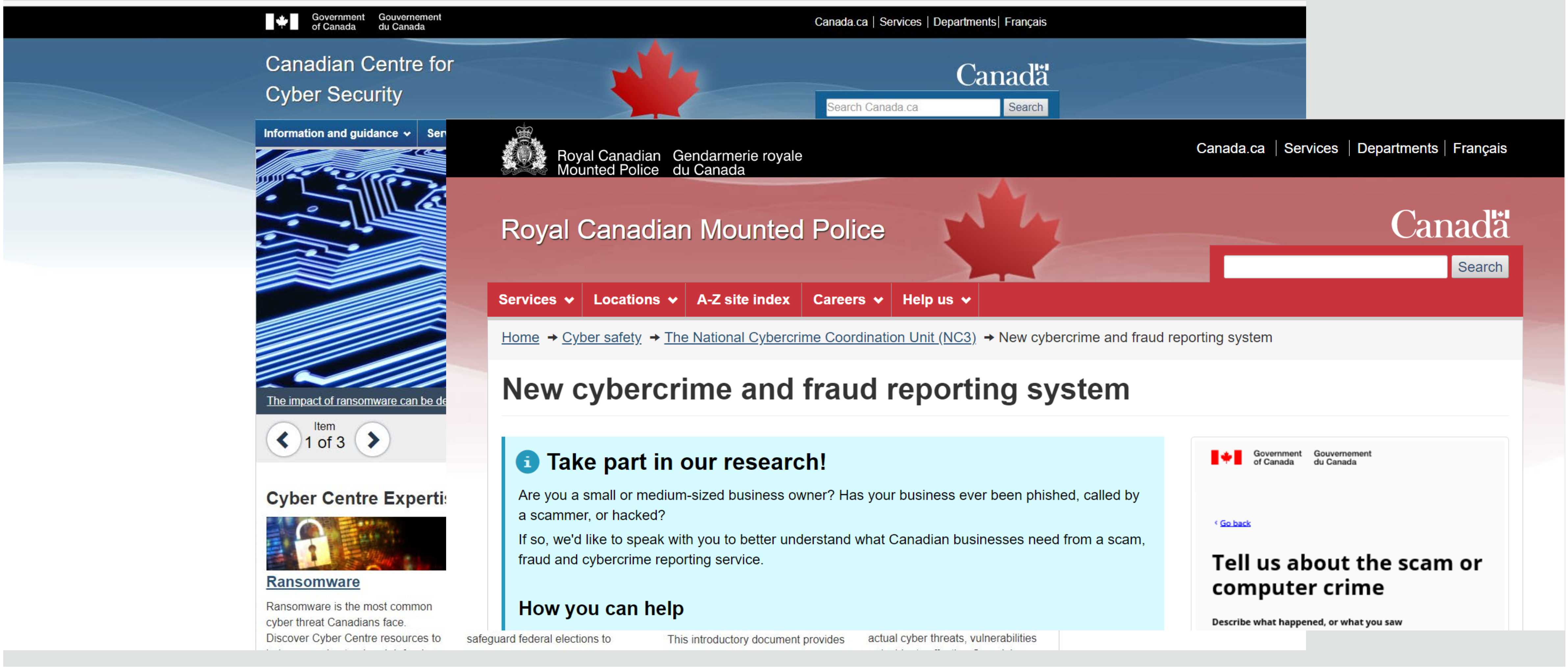
NPC™ Security Alerts

What the Log4j Vulnerability Means for SMB Professionals

A major security flaw in an application used by programmers to record activities for applications and software in devices and various services is making the headlines. National cybersecurity agencies and experts are calling for urgent action after it was reported last week.

Log4j is a component of software that developers use to record activities in an application. It is used in millions of Java applications and when located by hackers it can be exploited with relative ease. Hence, it has received a very high threat rating.

CCCS, RCMP



Government of Canada | Gouvernement du Canada

Canada.ca | Services | Departments | Français

Canadian Centre for Cyber Security

Canada

Search Canada.ca | Search

Information and guidance | Ser

The impact of ransomware can be de

Item 1 of 3

Cyber Centre Experti

Ransomware

Ransomware is the most common cyber threat Canadians face. Discover Cyber Centre resources to

safeguard federal elections to

This introductory document provides

actual cyber threats, vulnerabilities

Royal Canadian Mounted Police | Gendarmerie royale du Canada

Canada.ca | Services | Departments | Français

Royal Canadian Mounted Police

Canada

Search

Services | Locations | A-Z site index | Careers | Help us

Home → Cyber safety → The National Cybercrime Coordination Unit (NC3) → New cybercrime and fraud reporting system

New cybercrime and fraud reporting system

Take part in our research!

Are you a small or medium-sized business owner? Has your business ever been phished, called by a scammer, or hacked?

If so, we'd like to speak with you to better understand what Canadian businesses need from a scam, fraud and cybercrime reporting service.

How you can help

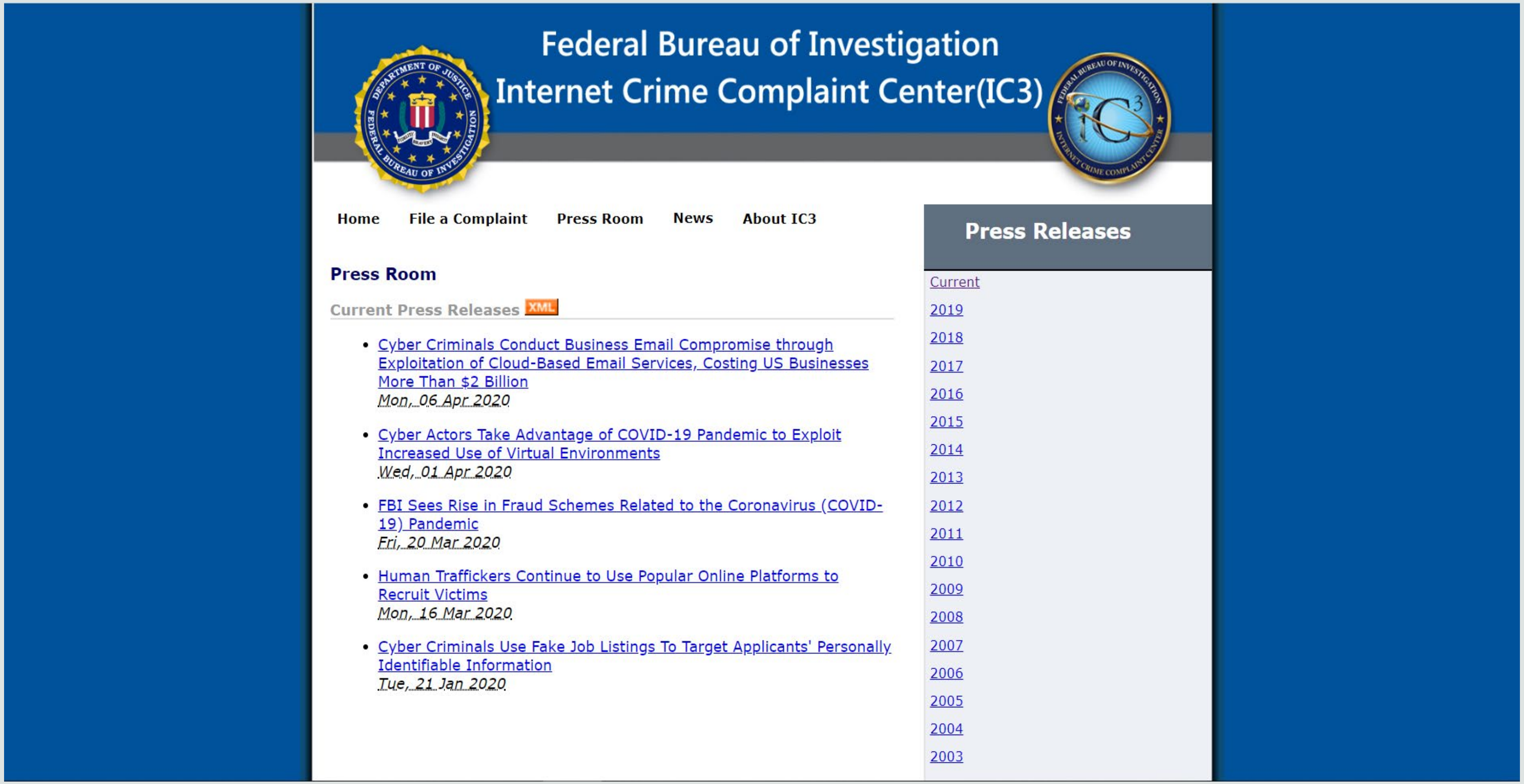
Government of Canada | Gouvernement du Canada

‹ Go back

Tell us about the scam or computer crime

Describe what happened, or what you saw

FBI IC3



Federal Bureau of Investigation
Internet Crime Complaint Center(IC3)

Home File a Complaint Press Room News About IC3

Press Room

Current Press Releases XML

- Cyber Criminals Conduct Business Email Compromise through Exploitation of Cloud-Based Email Services, Costing US Businesses More Than $2 Billion
  Mon, 06 Apr 2020
- Cyber Actors Take Advantage of COVID-19 Pandemic to Exploit Increased Use of Virtual Environments
  Wed, 01 Apr 2020
- FBI Sees Rise in Fraud Schemes Related to the Coronavirus (COVID-19) Pandemic
  Fri, 20 Mar 2020
- Human Traffickers Continue to Use Popular Online Platforms to Recruit Victims
  Mon, 16 Mar 2020
- Cyber Criminals Use Fake Job Listings To Target Applicants' Personally Identifiable Information
  Tue, 21 Jan 2020

Press Releases

Current
2019
2018
2017
2016
2015
2014
2013
2012
2011
2010
2009
2008
2007
2006
2005
2004
2003

Upcoming NPC Webinars

npcdataguard.com/webinars

April 21st 1pm ET (30-minute)	NPC DataGuard Solutions Overview
May 10th 1pm ET (60-minute)	Protecting Your Identity Online
May 12th 11:00 MT (60-minute)	Advocis Calgary A Preventive Strategy to Protect From Ransomware Attacks

NPC Webinars Recordings

→ npcdataguard.com/webinars

Enhancing Password Security and the Power of MFA

Building an Incident Response Plan for the SMB

Increase Revenue and Lower Cost Through As-a-Service Technologies

Business Email Compromise Attacks and How to Prevent Them

+ 12 more, and new topics will be added

Q&A

Larry Keating
lkeating@npcdataguard.com
905-305-6501

Darren Mar
dmar@npcdataguard.com
905-305-6513

Thank You

Please Be Safe & Stay Healthy

NPC™

Smarter Computing