Building an Incident Response Plan for the SMB

NPC Safe Computing Webinar Series

June 21st, 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

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

HUB

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

IDC WORLDSOURCE INSURANCE NETWORK INC.

Advisor Research Group Inc.

CI FINANCIAL

EQUITY Associates Inc.

FINANCIAL LITERACY COUNSEL INC.

GLOBAL MAXFIN INVESTMENTS INC.

GROVE POINT FINANCIAL

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
- Cyber Assessments and Pen Testing

Agenda

- The Incident Response Plan
- Building Blocks
- Q&A

NPC IRP Template

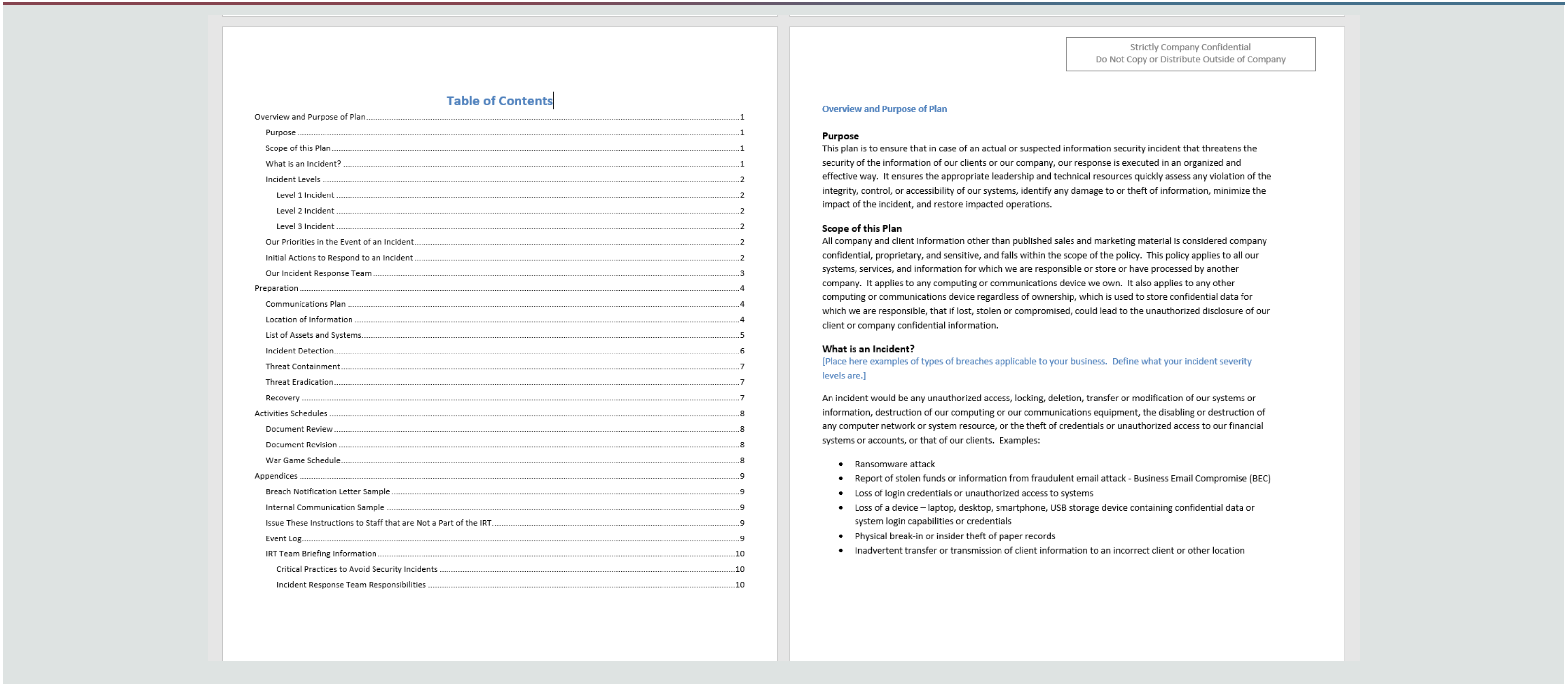


Table of Contents

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

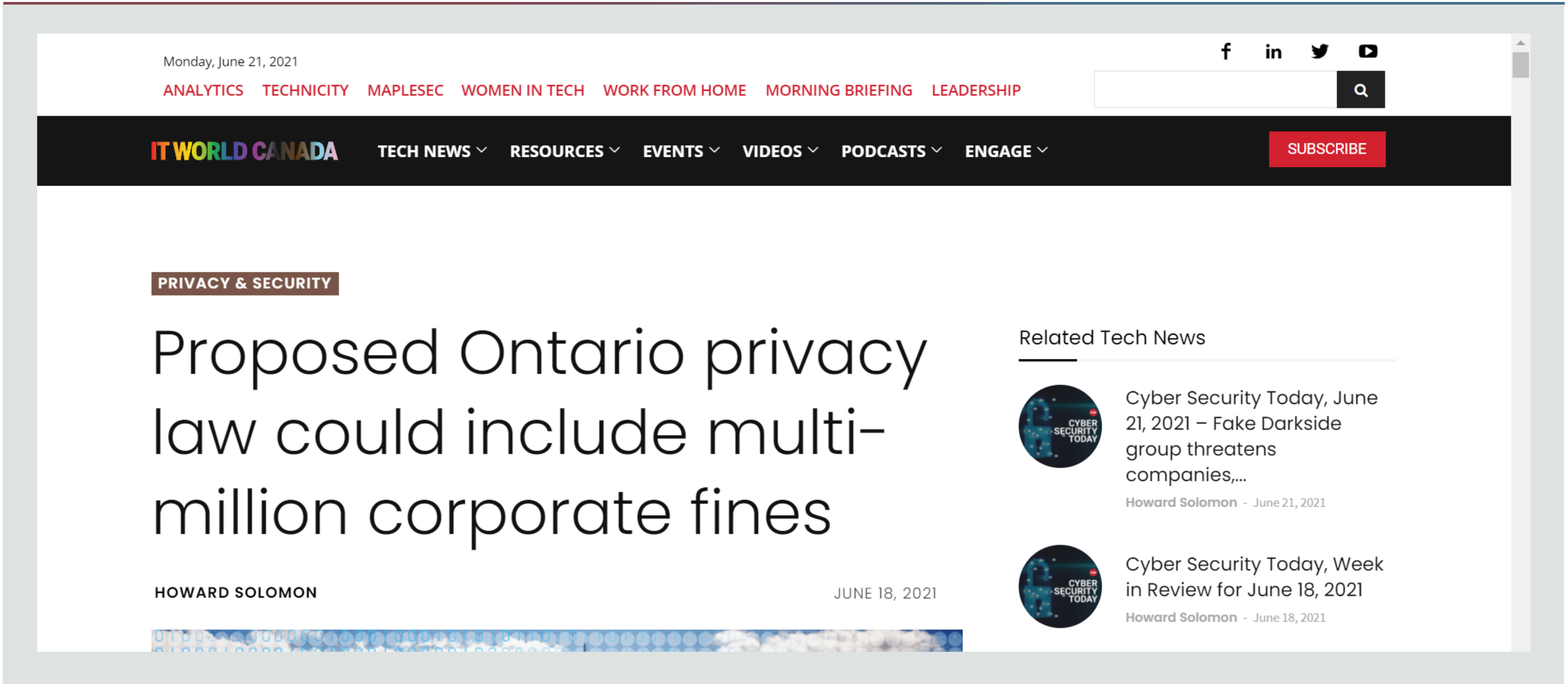
Attack Methods

Threats up 300% since pandemic started:

- Email and web browsing
- Remote desktop
- IoT devices
- Improperly Protected Networks
- Supply Chain Attacks

Source: FBI IC3 (Internet Crime Complaint Centre)

Governmental Regulation



Monday, June 21, 2021

PRIVACY & SECURITY

Proposed Ontario privacy law could include multi-million corporate fines

HOWARD SOLOMON

JUNE 18, 2021

Related Tech News

Cyber Security Today, June 21, 2021 – Fake Darkside group threatens companies,...

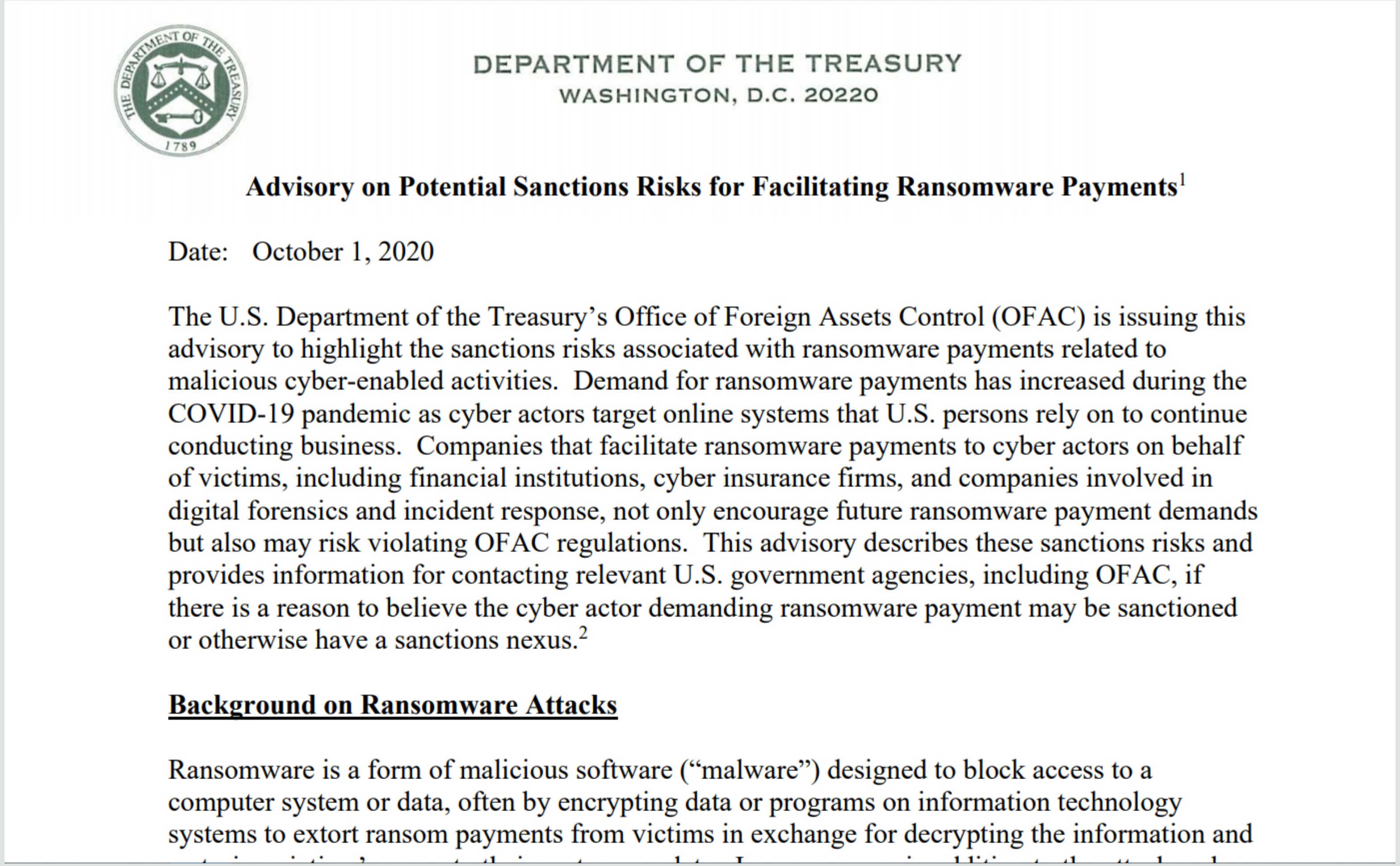
Howard Solomon - June 21, 2021

Cyber Security Today, Week in Review for June 18, 2021

Howard Solomon - June 18, 2021

Source: Cybereason Global Study June 2021 – Ransomware: The True Cost to Business

Increasing Legal Risk for Paying Ransoms



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments[1]

Date: October 1, 2020

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is issuing this advisory to highlight the sanctions risks associated with ransomware payments related to malicious cyber-enabled activities. Demand for ransomware payments has increased during the COVID-19 pandemic as cyber actors target online systems that U.S. persons rely on to continue conducting business. Companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response, not only encourage future ransomware payment demands but also may risk violating OFAC regulations. This advisory describes these sanctions risks and provides information for contacting relevant U.S. government agencies, including OFAC, if there is a reason to believe the cyber actor demanding ransomware payment may be sanctioned or otherwise have a sanctions nexus.[2]

<u>Background on Ransomware Attacks</u>

Ransomware is a form of malicious software ("malware") designed to block access to a computer system or data, often by encrypting data or programs on information technology systems to extort ransom payments from victims in exchange for decrypting the information and

Source: [U.S. Department of Treasury]()

Myriad Policies and Plans

Risk Governance Program

Programs and Plans

- Information Security Program
- Data Collecting, Handling and Retention Program
- Vendor Risk Management Program
- Asset Management Program
- Human Resources Training Program
- Physical Security Program
- Regulatory Compliance Program
- Business Continuity Plan (BCP)
- Incident Response Plan (IRP)

Policies

- Privacy Policy
- Acceptable Use Policy
- Password Policy
- Computer, Phone and USB Device Policy
- BYOD Policy
- Email Use Policy
- Removable Media Policy
- Remote Access Policy
- …

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 in the plan are immediately contacted
- ❑ 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

Which Plan is Which

- An Incident Response Plan is a set of guidelines and information resources to respond to a specific incident in the moment
- A Business Continuity Plan is a post-incident business recovery action plan

What is 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

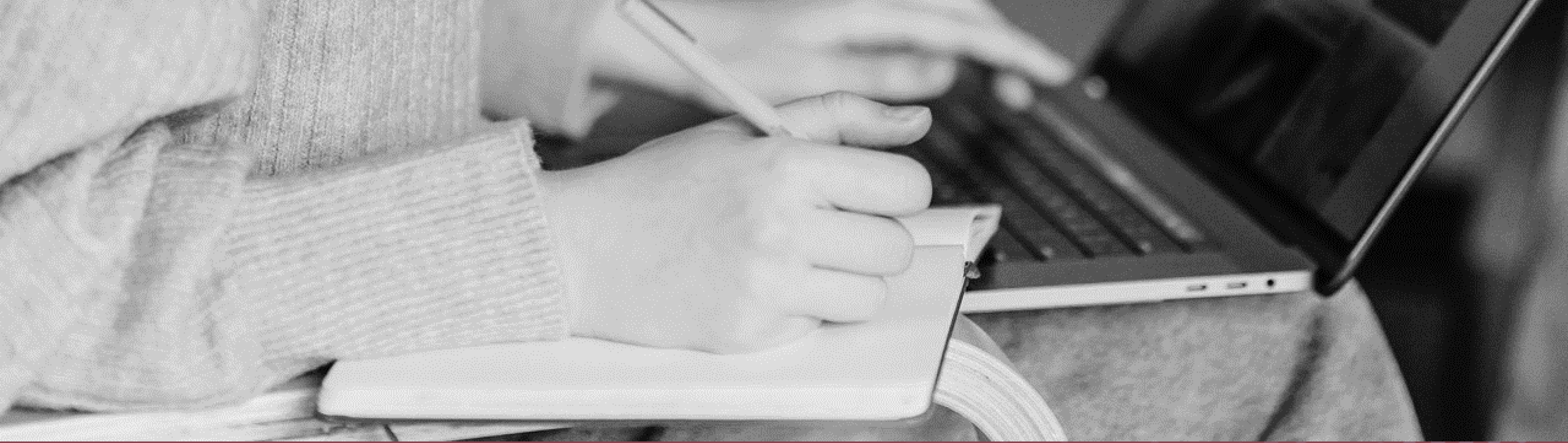
Keep it simple

- 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 ☹)

What Your Plan Will Look Like

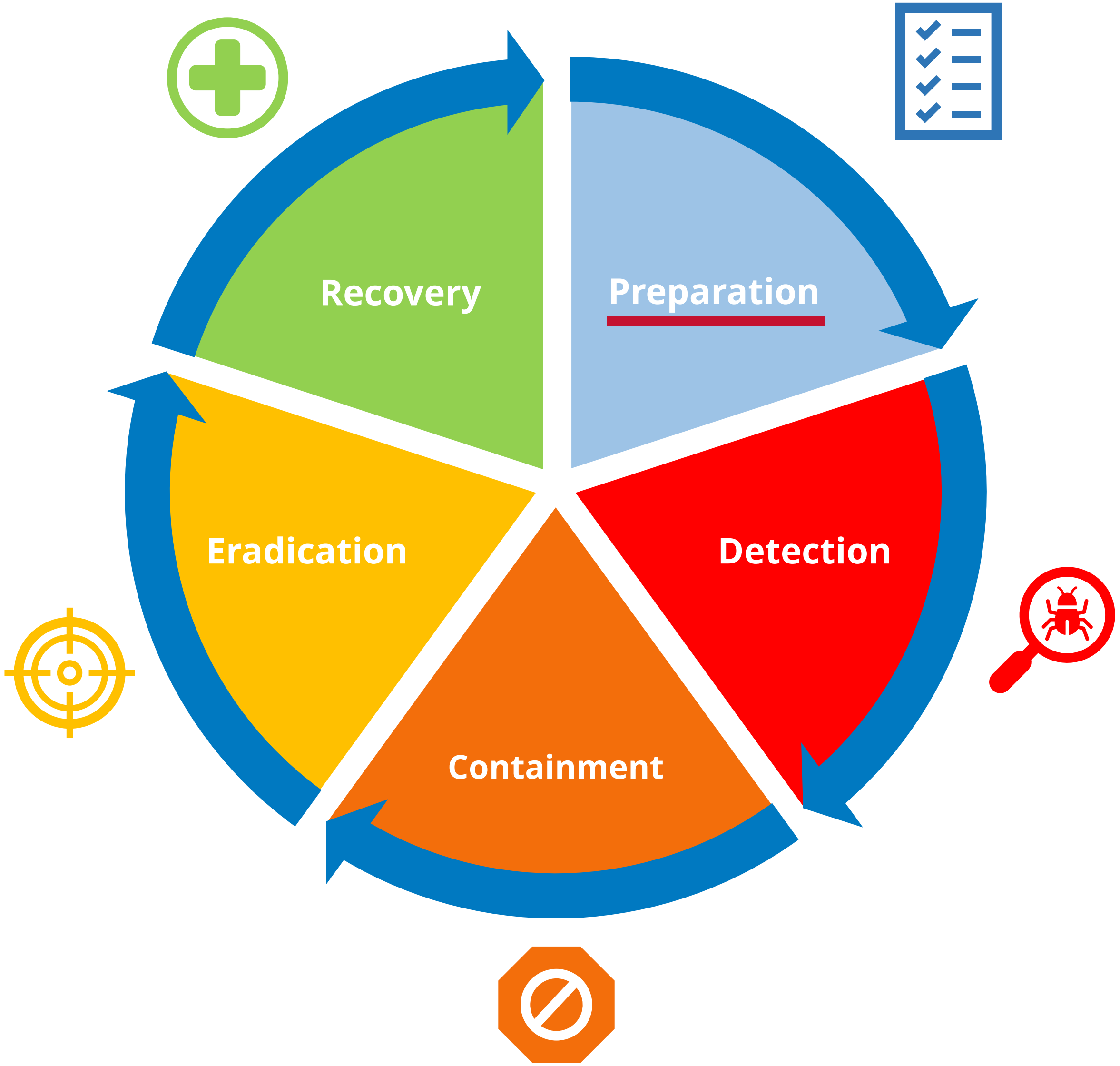
Be simple, but accurate and clear in your steps

- Use checklists, use simple flowcharts
- Detail roles, responsibilities, accountabilities – who is in charge?
- Technical and non-technical people must work together
- Decide in advance your priorities – what matters most - protecting client data? protecting corporate data? restoring operations?
- Identify risks specific to your business, and grade them

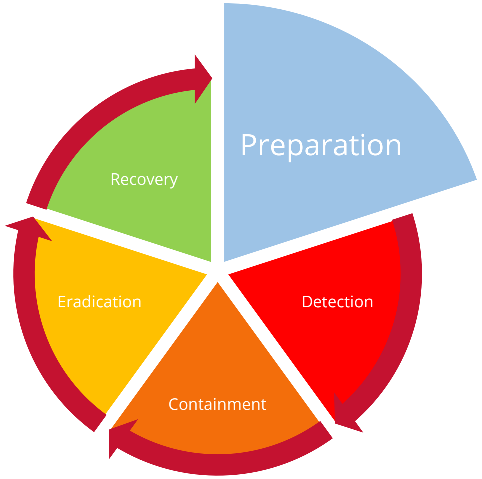


Creating Your IRP | Building Blocks

IRP Building Blocks



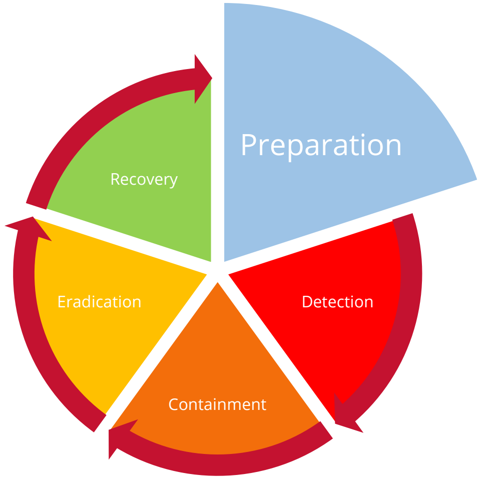
Preparation



Identify and document

- ❑ Where your information is:
  - Computers – server and endpoint (laptop, desktop, tablet)
  - Smartphones, USB devices
  - Cloud services
  - All files at home and office
- ❑ What are your computing, communication and system assets:
  - Devices, types, models, serial numbers

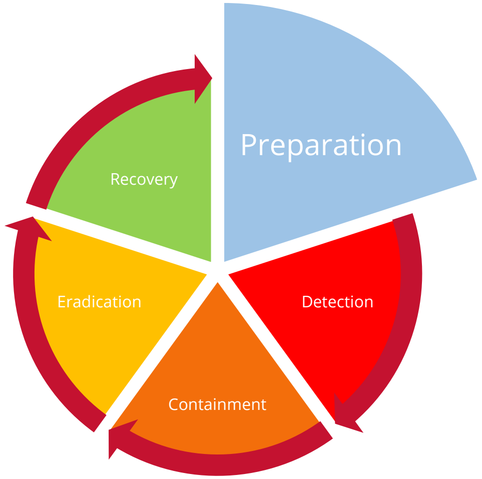
Preparation



Record at what point an event becomes reportable, and to whom

- ❑ Identify your legal obligations and recommended practices:
  - Government regulators – federal, provincial, state, foreign
  - Industry regulators
  - Professional associations
  - Contractual obligations
- ❑ Understand the concept of “Real Risk of Significant Harm”

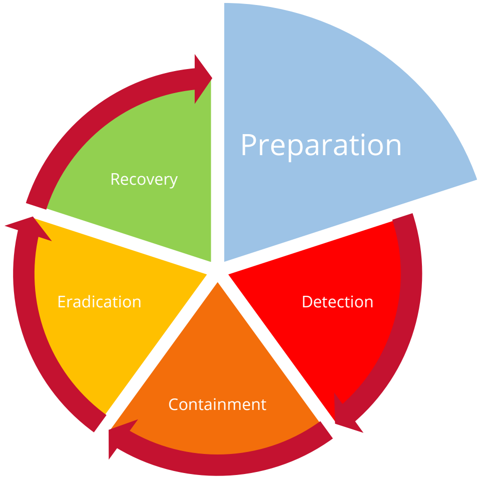
Preparation



Create your Incident Response Team

- ❑ Key members of your organization
- ❑ Your IT support or MSP
- ❑ Identify or have on retainer a professional cyber security incident response company
- ❑ Your insurance company
- ❑ Your lawyer

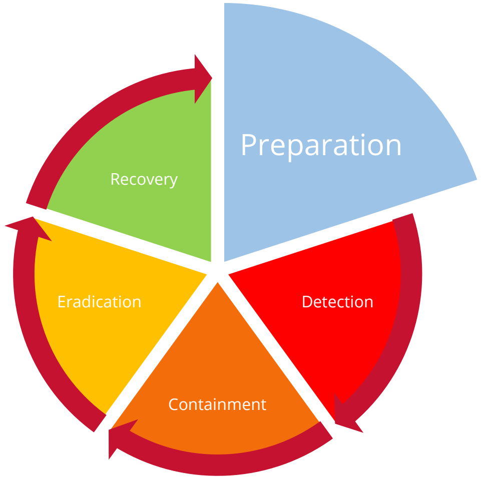
Preparation



Create your Incident Response Team

- ❑ Who has what role, establish accountability
- ❑ Indicate who has top level access to what systems:
  - Ensure IR Team members with access to systems are aware they must know or have their passwords to those systems, without the benefit of stored auto-logins!

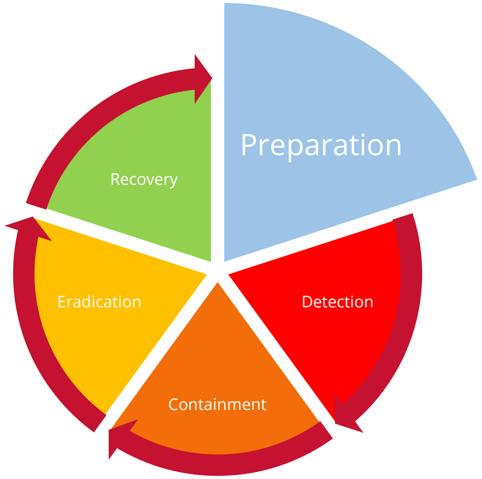
Preparation



Create a Communications Plan

- ❑ Document in your plan who will contact whom on the IR Team, in what order, and what to do if a party is unavailable or unresponsive
- ❑ Who decides how much is said and when
- ❑ Document who is in charge of external messaging:
  - Be careful not to say too much, too soon. This is a time you can overdo transparency and increase the damage to you or your stakeholders – assume the threat actors are listening!
- ❑ Decide now what to do if parts of your communication methods are down – no email, no VoIP phones

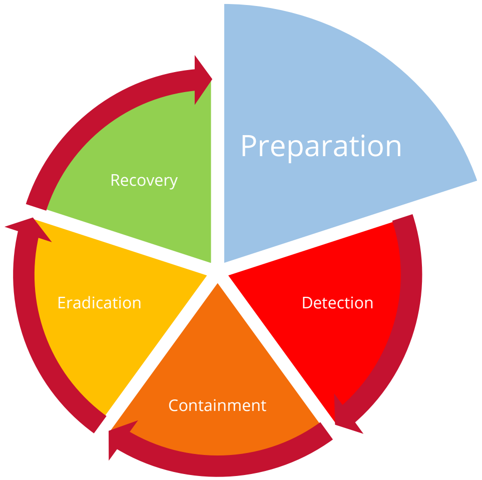
Preparation



Assess what tools you have to detect a threat, and your ability to use them

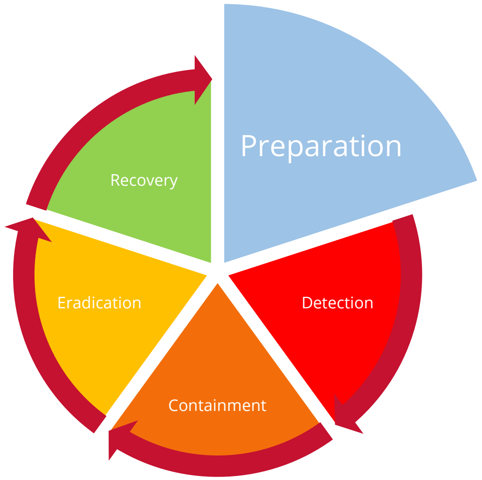
- ❑ Identify what logs are created by your connectivity devices, servers, anti-malware software, computer operating systems, etc. If logs are not being kept, activate them or upgrade to systems that do so
- ❑ Does your MSP or IT provider monitor your devices and logs?
- ❑ Do your back-end and service providers have an IDS (Incident Detection System)? A SIEM (Security Incident Event Management) system?
- ❑ Ensure you know what a cloud provider will do if they have a breach, or detect one related to your account. Must they tell you? How soon?

Preparation



- Create Quick Response Guidelines to insert in your plan for most likely scenarios, or areas that would be of most concern
- Hold a mock incident response event (War Gaming) annually. Walk through your plan to see if it will work in practice, particularly your communication plan
- Prepare a breach notification letter, just the framework, in advance
- While taking great care to protect your Incident Response Plan’s confidentiality, store multiple forms of your plan and IR Team contact information on and offline

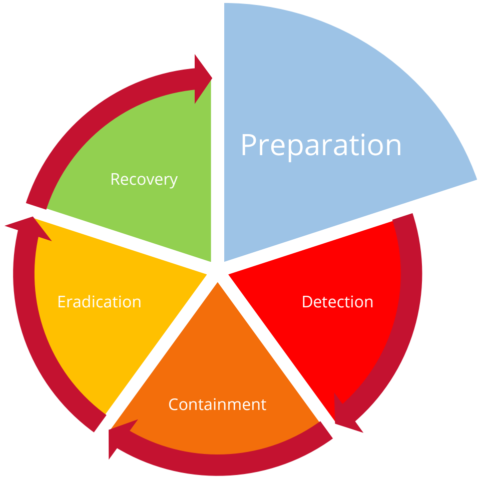
Preparation



DON'Ts to be listed in your plan

- ❑ Don't panic – you have a plan, stay calm, follow the plan
- ❑ Don't immediately shut systems down – shut downs and restarts can trigger additional behaviour in malicious software, destroy forensic information, and cause the loss of other data
- ❑ Don't start using data cleaning and wiping tools unless you know what you are doing and have collected the proper forensic data beforehand
- ❑ Don't immediately use domain administrator credentials. Threat actors may have launched a small attack and are in a system watching for those to do greater damage

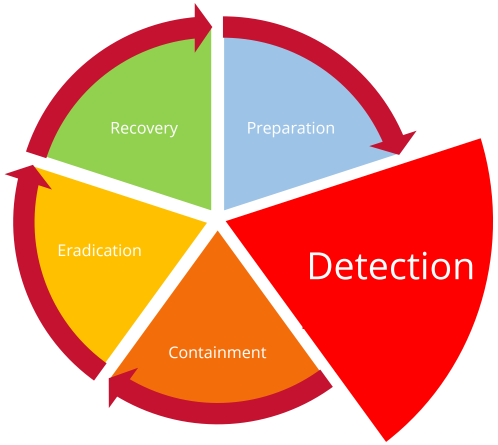
Preparation



DO's to be listed in your plan

- ❑ Do consult your IR Team or IT Support for immediate instruction on specific actions related to deleting files, shutting off systems, changing access, etc.
- ❑ Do disconnect devices from the Internet
- ❑ Do make notes and record carefully the name of any malicious files if found, and any observable system effects; new file extensions, what appeared to happen, device behaviour, system performance
- ❑ Do have all systems and devices backed up
- ❑ Do have ample cyber insurance

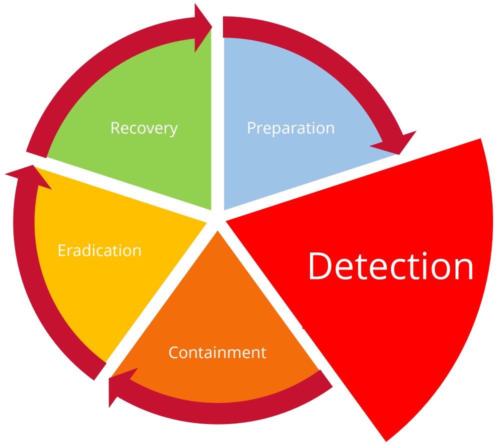
Detection



Event detection

- ❑ Watch for unusual transactions – identify in your plan a few examples of what they might look like
- ❑ Conduct periodic cyber assessments, reviews of IT systems
- ❑ Watch for abnormal device or system behaviour, slow network performance
- ❑ Take comments from external contacts, clients, suppliers, etc., seriously if they have received spoof emails, odd requests or transactions that seem to be related to you or your business with them

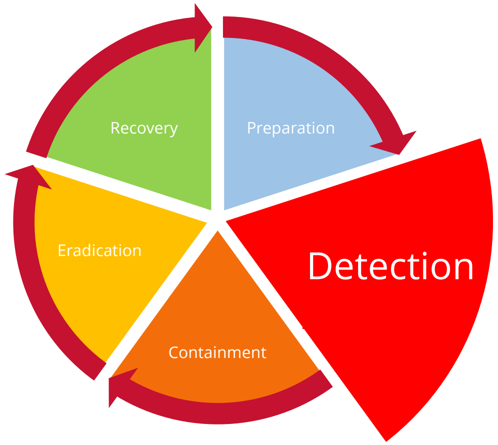
Detection



Event detection

- ❑ Check occasionally with your MSP, IT, Cloud or back-end providers any activity in their logs, IDS (Incident Detection System) or SEIM (Security Event Incident Management) system, or require them to provide periodic reports
- ❑ Monitor Internet usage
- ❑ Know that some incidents can happen over weeks, even months

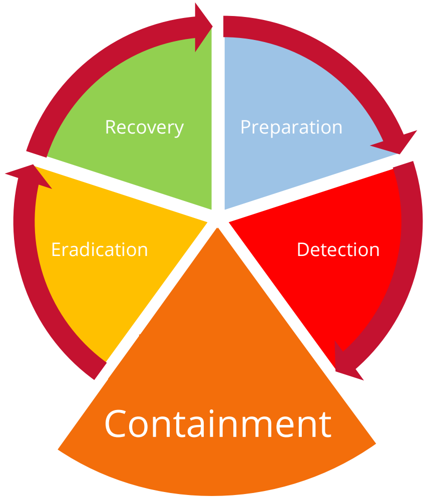
Detection



Incident detected!

- ❑ Activate your IR Team and IR Plan
- ❑ *Communications Checkpoint* - decide where/when/how much to communicate, both internally and externally
  - (You will likely trigger only the internal communications plan at this stage)

Containment

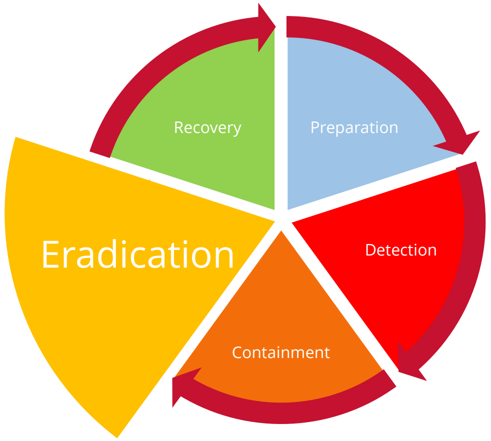


Stop the damage

- ❑ Define in your plan the steps you would take to identify what system or device has been attacked or lost, what information is missing*, what systems need to be taken off-line, what passwords need to be changed
- ❑ Look for cause - determine as quickly as possible the source of the infection, method of accessing the system, how a device was lost or stolen, etc.
- ❑ Ensure copies of information, damaged computers or affected storage drives are retained for later analysis if they are being replaced

* Go to your backups to help determine data losses

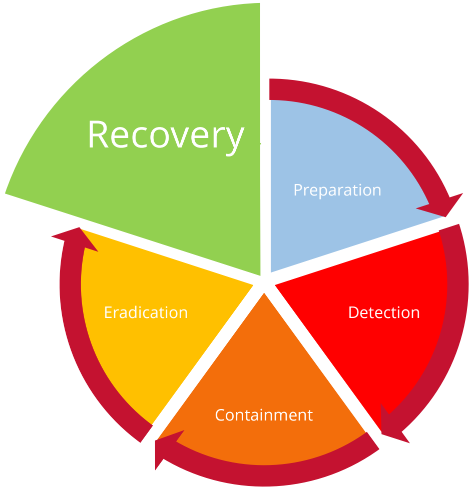
Eradication



Eliminate the source of the problem

- ❑ Document how you will remove the threat, who will do it, to what length can you shut down systems and delete information safely, close off the systems and for how long
- ❑ For lost or stolen devices trigger remote destruction, making note of device GPS or IP location data if available
- ❑ Determine who decides on the “all clear and clean” to commence recovery
- ❑ *Communications Checkpoint* - decide where/when/how much to communicate, both internally and externally

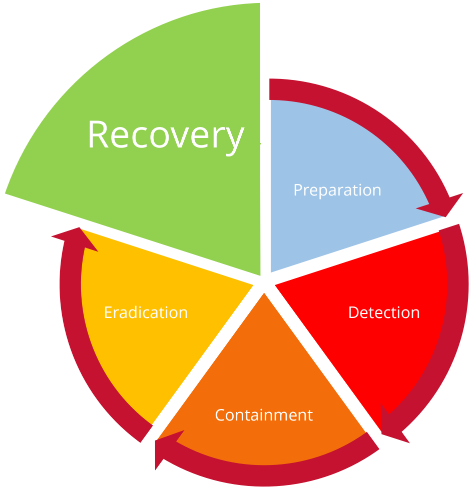
Recovery



Getting back to work

- ❑ Document now how will you restore your information and bring systems back online once the threat has been neutralized
- ❑ If required, begin the notification process:
    - ❑ Regulators, clients, suppliers, business partners, etc.
- ❑ Hold post-mortem meetings
    - ❑ Upgrade your security posture or training
    - ❑ Update your IRP

Recovery



Keep a detailed event log of all details. Required in Canada under PIPEDA for loss of PII (Personally Identifiable Information)

- ❑ Date, time, location of event
- ❑ Describe incident and its discovery
- ❑ Communications details (who, what, and when)
- ❑ Any relevant data from your security reporting software and event logs
- ❑ Remediation taken

Building an IRP

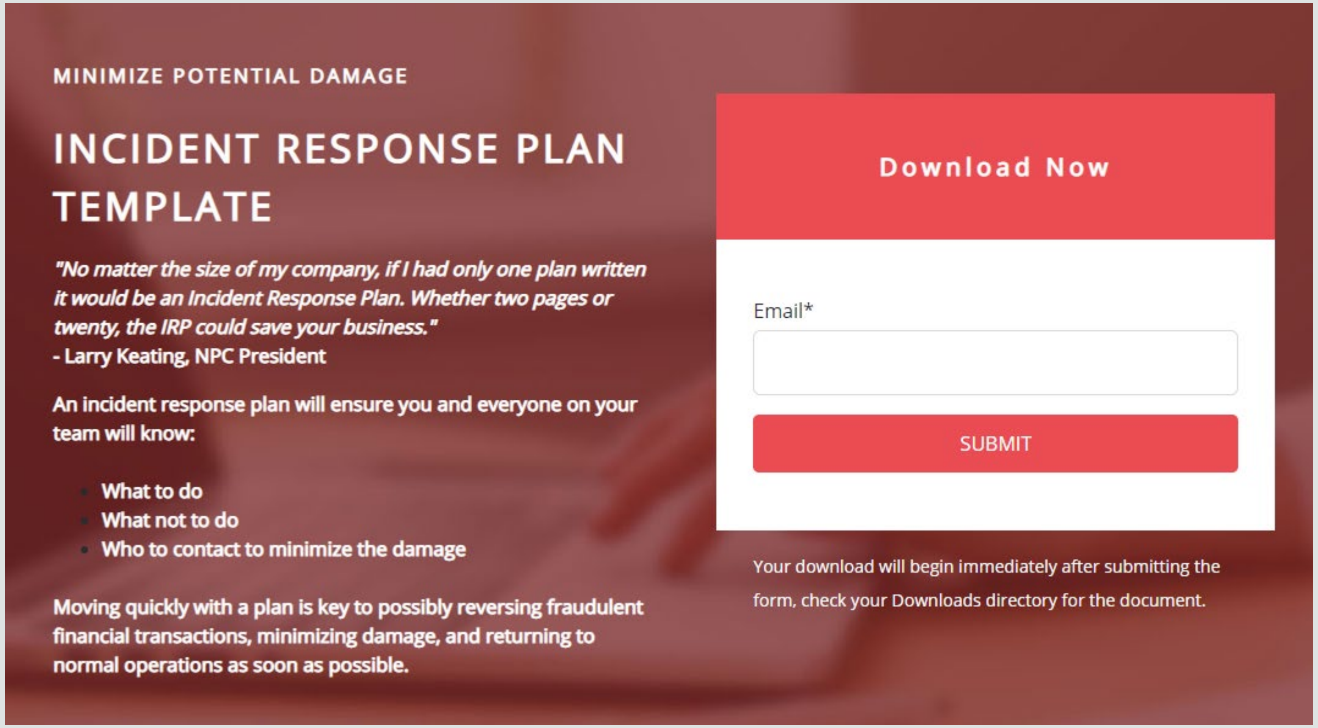
Recap

- ❑ Understand and communicate to your team the importance of the IRP to your organization
- ❑ Research your risks, technology, location of data, and regulatory/professional requirements
- ❑ Identify key IR Team members, and especially outside resources – identify who is in charge
- ❑ Know what to say and when during an incident
- ❑ Keep detailed records of every event, reportable or not
- ❑ Keep it simple and accurate

Security is Essential to Success

Data protection is a business issue, not just a compliance or IT issue. Think early, think strategically, and transform the challenge into a productivity, cost containment and business advantage.

NPC IRP Template



MINIMIZE POTENTIAL DAMAGE

INCIDENT RESPONSE PLAN TEMPLATE

"No matter the size of my company, if I had only one plan written it would be an Incident Response Plan. Whether two pages or twenty, the IRP could save your business."
- Larry Keating, NPC President

An incident response plan will ensure you and everyone on your team will know:

- What to do
- What not to do
- Who to contact to minimize the damage

Moving quickly with a plan is key to possibly reversing fraudulent financial transactions, minimizing damage, and returning to normal operations as soon as possible.

Download Now

Email*

SUBMIT

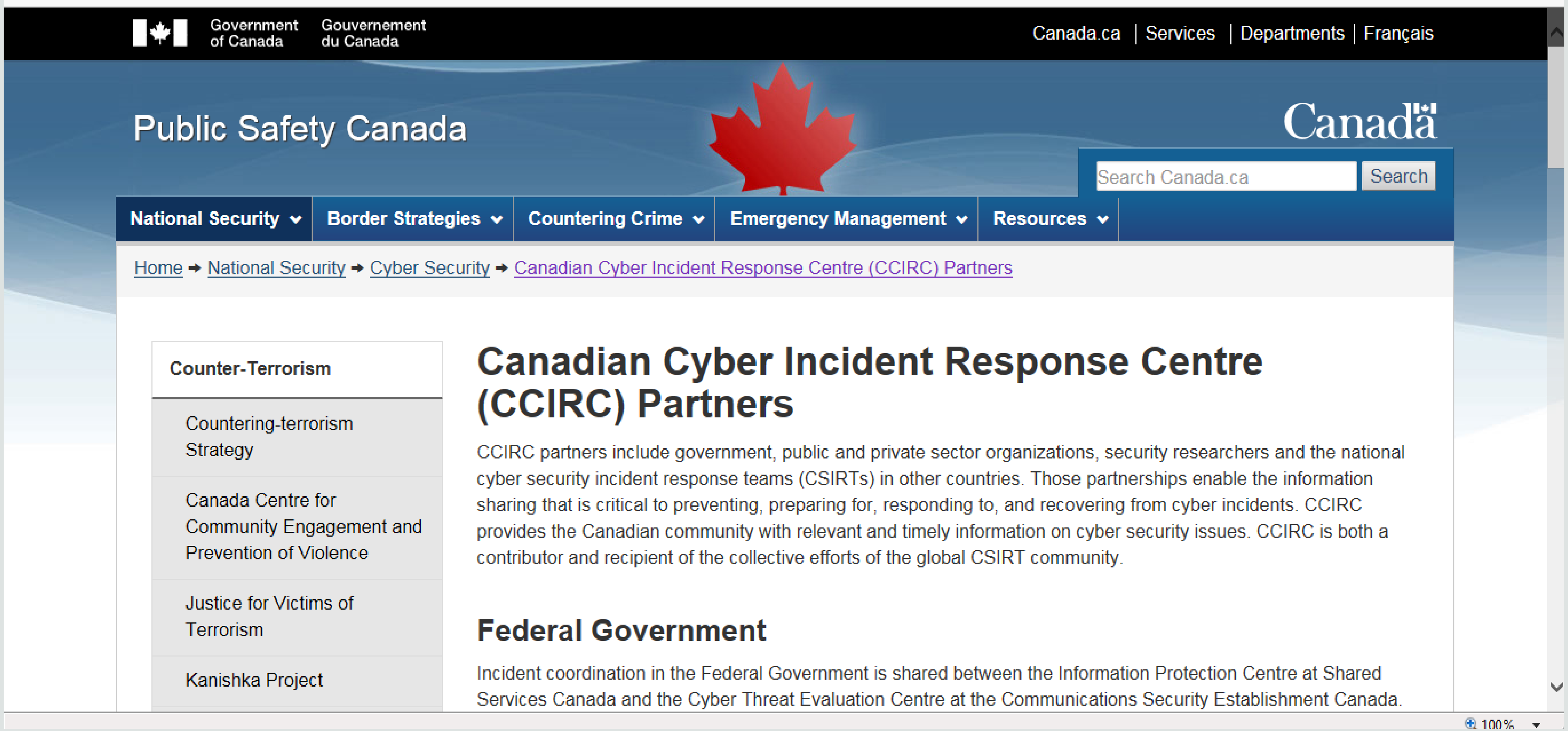
Your download will begin immediately after submitting the form, check your Downloads directory for the document.

A link to the IRP template will also be provided after completing our survey following this webinar.

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

Additional Resources

CCIRC



Government of Canada
Gouvernement du Canada
Canada.ca | Services | Departments | Français
Public Safety Canada
Canadä
Search Canada.ca
Search
National Security
Border Strategies
Countering Crime
Emergency Management
Resources
Home → National Security → Cyber Security → Canadian Cyber Incident Response Centre (CCIRC) Partners
Counter-Terrorism
Countering-terrorism Strategy
Canada Centre for Community Engagement and Prevention of Violence
Justice for Victims of Terrorism
Kanishka Project
100%

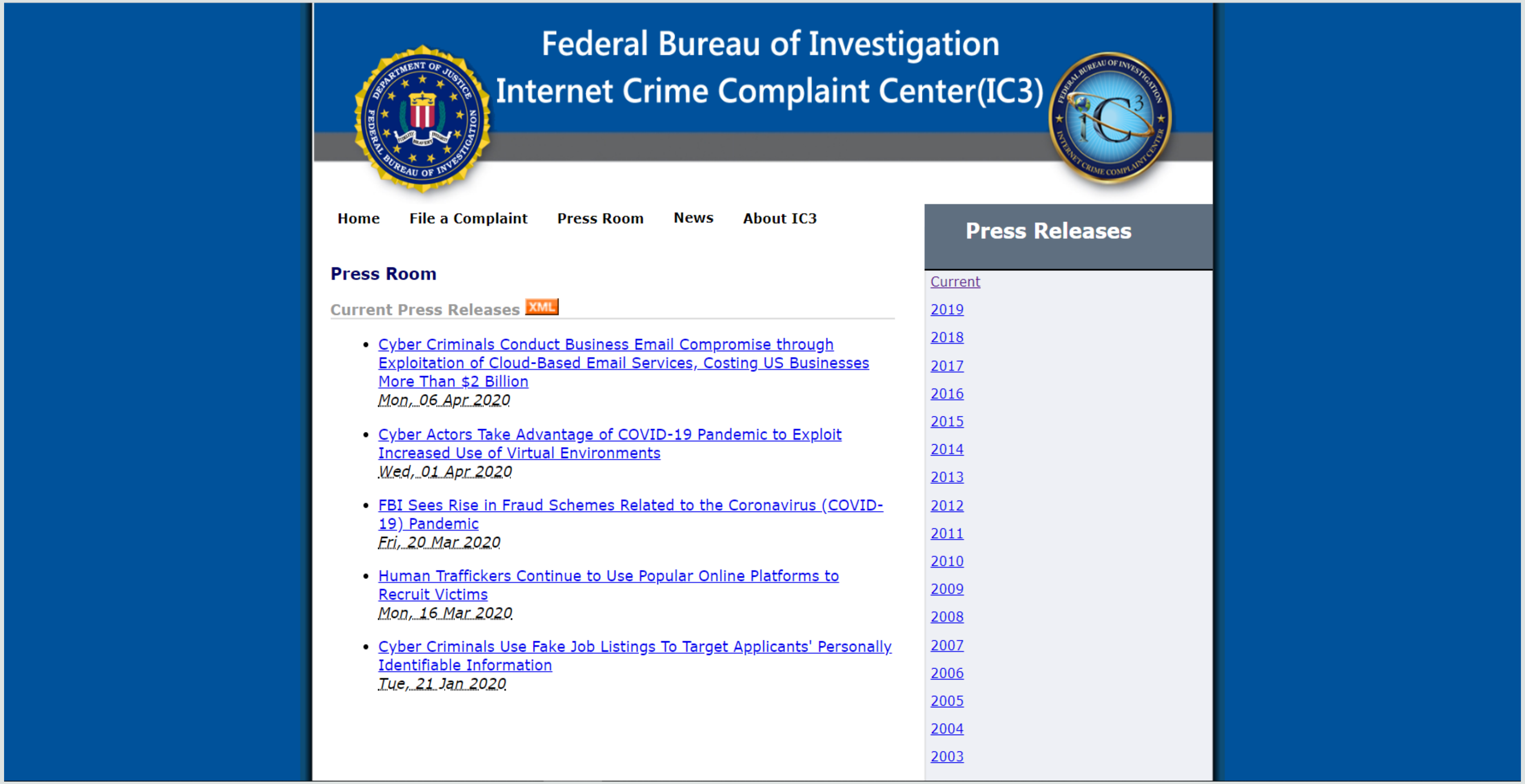
Canadian Cyber Incident Response Centre (CCIRC) Partners

CCIRC partners include government, public and private sector organizations, security researchers and the national cyber security incident response teams (CSIRTs) in other countries. Those partnerships enable the information sharing that is critical to preventing, preparing for, responding to, and recovering from cyber incidents. CCIRC provides the Canadian community with relevant and timely information on cyber security issues. CCIRC is both a contributor and recipient of the collective efforts of the global CSIRT community.

Federal Government

Incident coordination in the Federal Government is shared between the Information Protection Centre at Shared Services Canada and the Cyber Threat Evaluation Centre at the Communications Security Establishment Canada.

FBI IC3



Federal Bureau of Investigation
Internet Crime Complaint Center(IC3)

Press Room

Current Press Releases XML

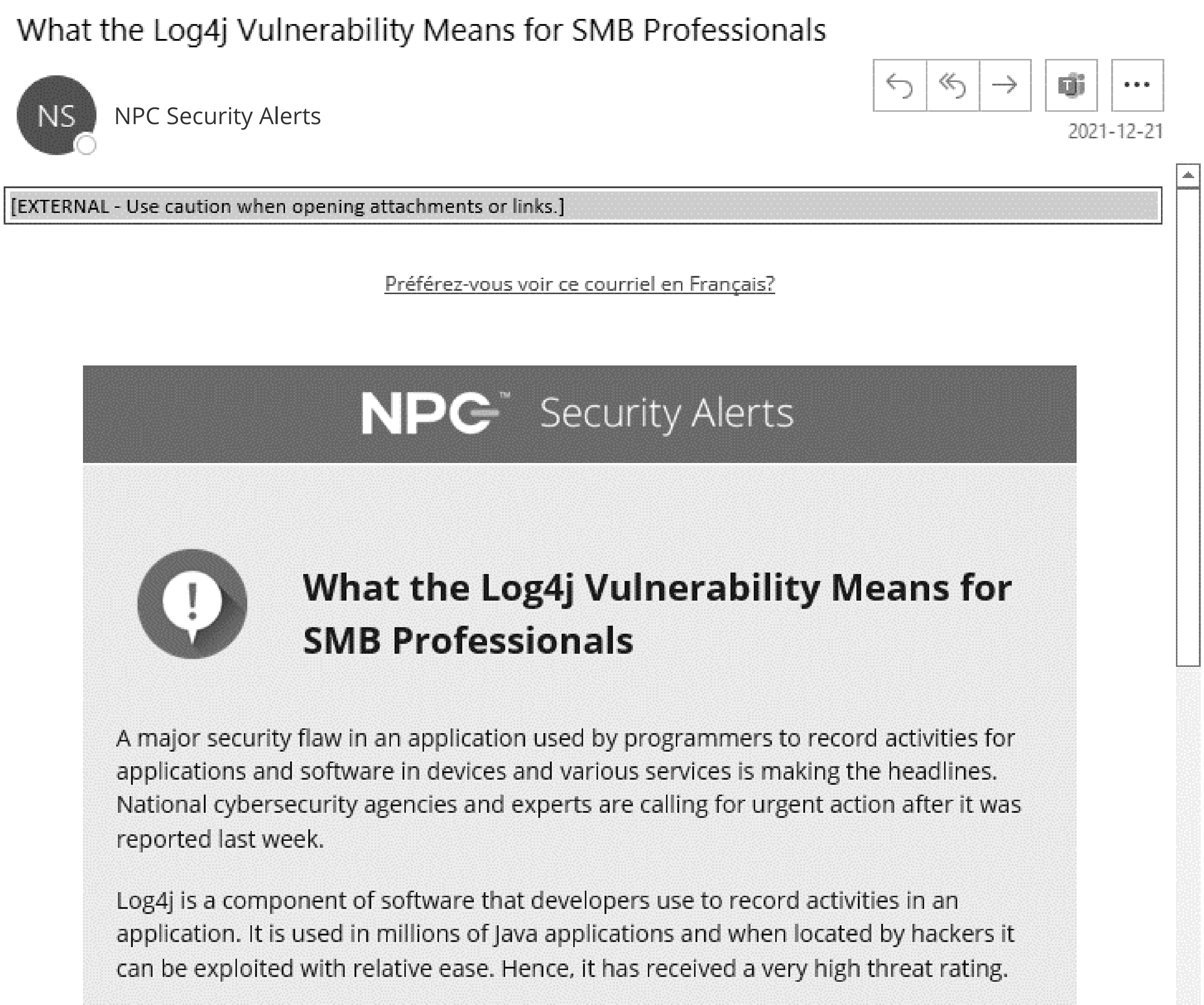
- Cyber Criminals Conduct Business Email Compromise through Exploitation of Cloud-Based Email Services, Costing US Businesses More Than $2 Billion
  Mon, 06 Apr 2020
- Cyber Actors Take Advantage of COVID-19 Pandemic to Exploit Increased Use of Virtual Environments
  Wed, 01 Apr 2020
- FBI Sees Rise 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

NPC Security Alerts

npcdataguard.com/alerts



What the Log4j Vulnerability Means for SMB Professionals

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.

Upcoming NPC Webinars

→ npcdataguard.com/webinars

June 28th 1pm ET (30-minutes)	NPC DataGuard Solutions Overview
July 18th 1pm ET (60-minutes)	10 Steps to Secure Your Business from Ransomware
July 20th 1pm ET (30-minutes)	NPC DataGuard Solutions Overview
August 16th 1pm ET (60-minutes)	Implementing and Managing the Secure Hybrid Workplace
August 18th 1pm ET (30-minutes)	NPC DataGuard Solutions Overview

NPC Webinars Recordings

→ npcdataguard.com/webinars

Enhancing Password Security and the Power of MFA

Work Securely from Anywhere with Microsoft 365

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

Five-Step Checkup for Your Cyber Protection

& 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