

are you
FUTURE READY?

Cyber Security Battlefield BOMA Industry

Presented by:
Danny Timmins



MNP Technology Solutions





AGENDA

•
•
•

Cyber Security Overview

Cyber Crime Tactics and Techniques

- Hacking (Penetration Testing)
- Social Engineering (Malware/Phishing)

Staying Focused and How

MNP CYBER



- Est. 2000
- Today over 55 dedicated individuals nationally

“Top 24
Security
Partners in
North
America”
CRN Magazine



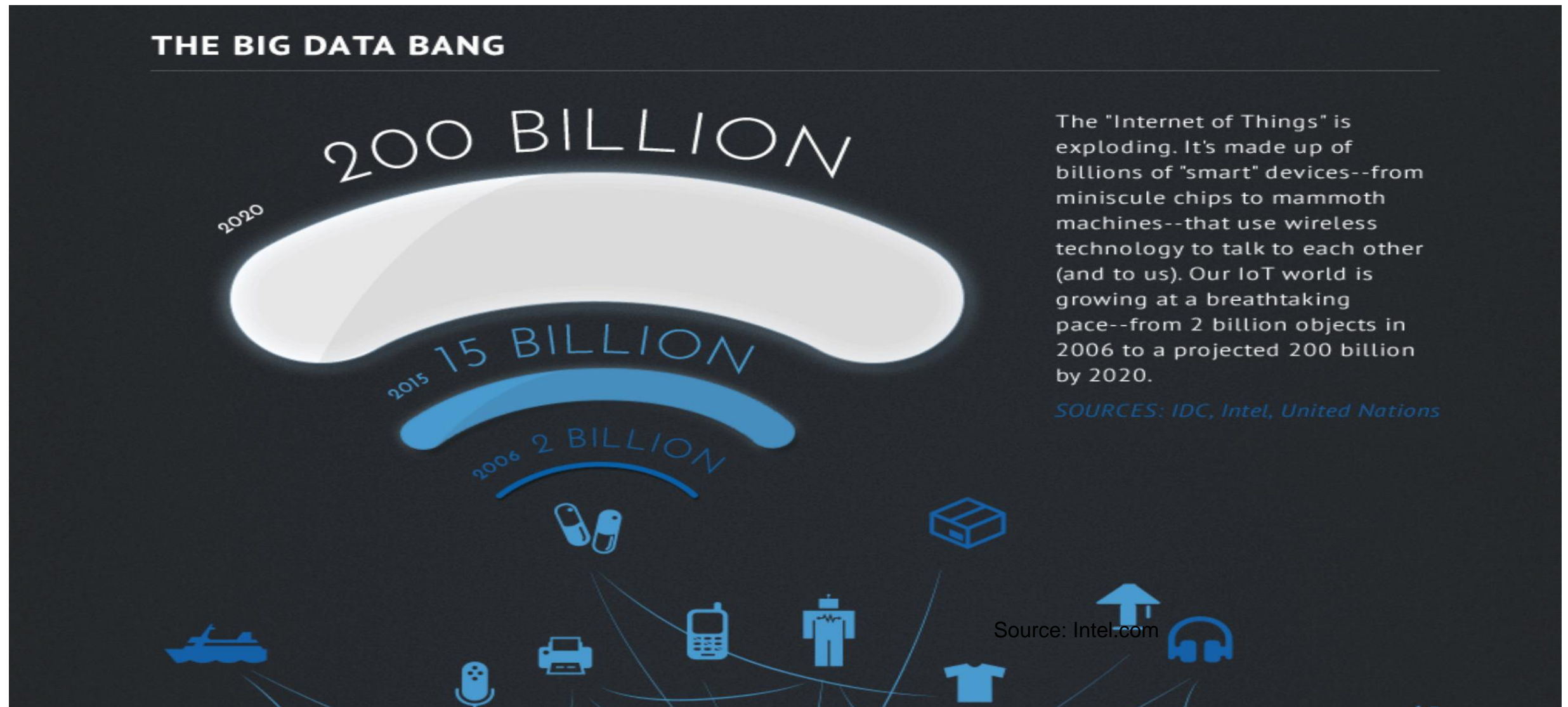
Privacy

- >Appropriate safeguards in place
- >Fines based on records loss
- >Everyone – even small business



Canada's Mandatory Privacy Breach Reporting Requirements coming into force November 1, 2018

Internet of things is, and will be a business Challenge.



Pwned = Stolen & Compromised

322
pwned websites

5,558,182,518
pwned accounts

83,079
pastes

90,414,182
paste accounts

Largest breaches



711,477,622 [Onliner Spambot accounts](#)



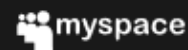
593,427,119 [Exploit.In accounts](#)



457,962,538 [Anti Public Combo List accounts](#)



393,430,309 [River City Media Spam List accounts](#)



359,420,698 [MySpace accounts](#)



234,842,089 [NetEase accounts](#)



164,611,595 [LinkedIn accounts](#)



152,445,165 [Adobe accounts](#)



131,577,763 [Exactis accounts](#)



125,929,660 [Apollo accounts](#)

Recently added breaches



24,990 [Rbx.Rocks accounts](#)



14,609 [Società Italiana degli Autori ed Editori accounts](#)



858 [WPSandbox accounts](#)



22,477 [Joomla! Art accounts](#)



326,714 [Mac Forums accounts](#)



846,742 [Baby Names accounts](#)



1,274,051 [Wife Lovers accounts](#)



342,913 [Facepunch accounts](#)

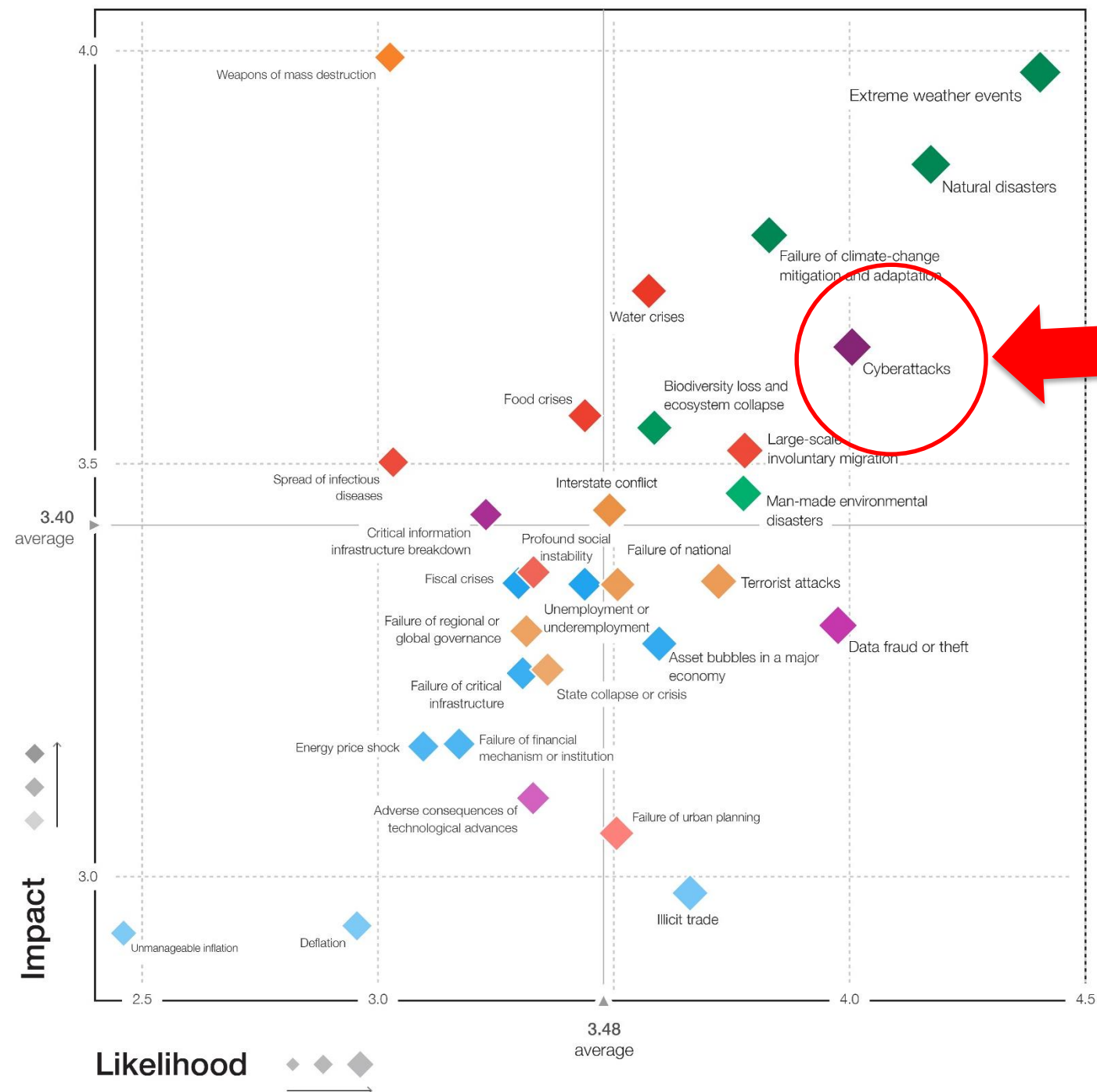


125,929,660 [Apollo accounts](#)



7,687,679 [Digimon accounts](#)

Figure I: The Global Risks Landscape 2018



COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

Insight Report

The Global Risks Report 2018 13th Edition

Top 10 risks in terms of Likelihood

- 1 Extreme weather events
- 2 Natural disasters
- 3 Cyberattacks
- 4 Data fraud or theft
- 5 Failure of climate-change mitigation and adaptation
- 6 Large-scale involuntary migration
- 7 Man-made environmental disasters
- 8 Terrorist attacks
- 9 Illicit trade
- 10 Asset bubbles in a major economy






3rd

Top 10 risks in terms of Impact

- 1 Weapons of mass destruction
- 2 Extreme weather events
- 3 Natural disasters
- 4 Failure of climate-change mitigation and adaptation
- 5 Water crises
- 6 Cyberattacks
- 7 Food crises
- 8 Biodiversity loss and ecosystem collapse
- 9 Large-scale involuntary migration
- 10 Spread of infectious diseases

6th

Categories

-  Economic
-  Environmental
-  Geopolitical
-  Societal
-  Technological

Source : World Economic Forum Global Risks Perception Survey 2017–2018.

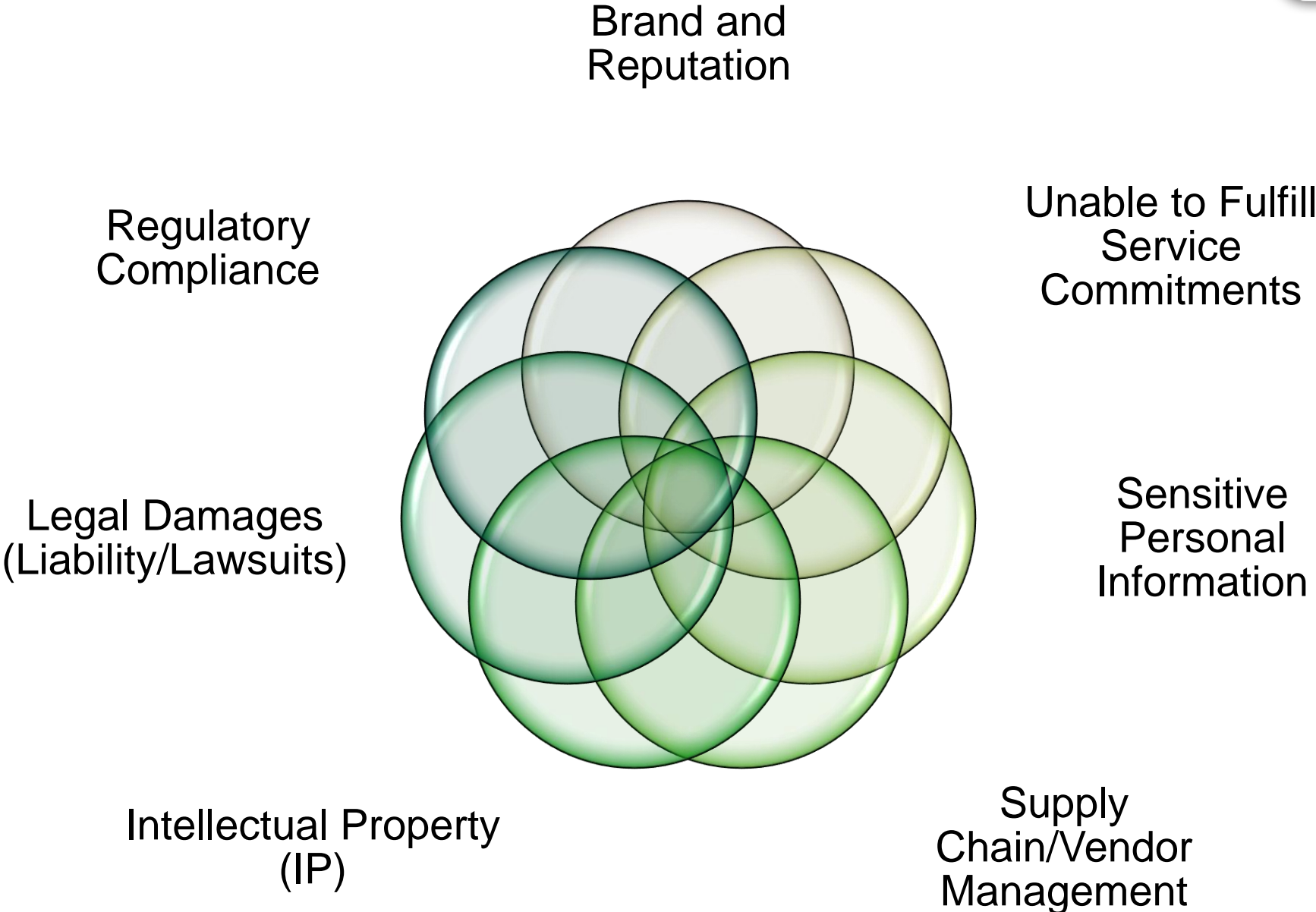
Note : Survey respondents were asked to assess the likelihood of the individual global risk on a scale of 1 to 5, 1 representing a risk that is very unlikely to happen and 5 a risk that is very likely to occur. They also assess the impact on each global risk on a scale of 1 to 5 (1: minimal impact, 2: minor impact, 3: moderate impact, 4: severe impact and 5: catastrophic impact). See Appendix B for more details. To ensure legibility, the names of the global risks are abbreviated; see Appendix A for the full name and description.

Stats Canada

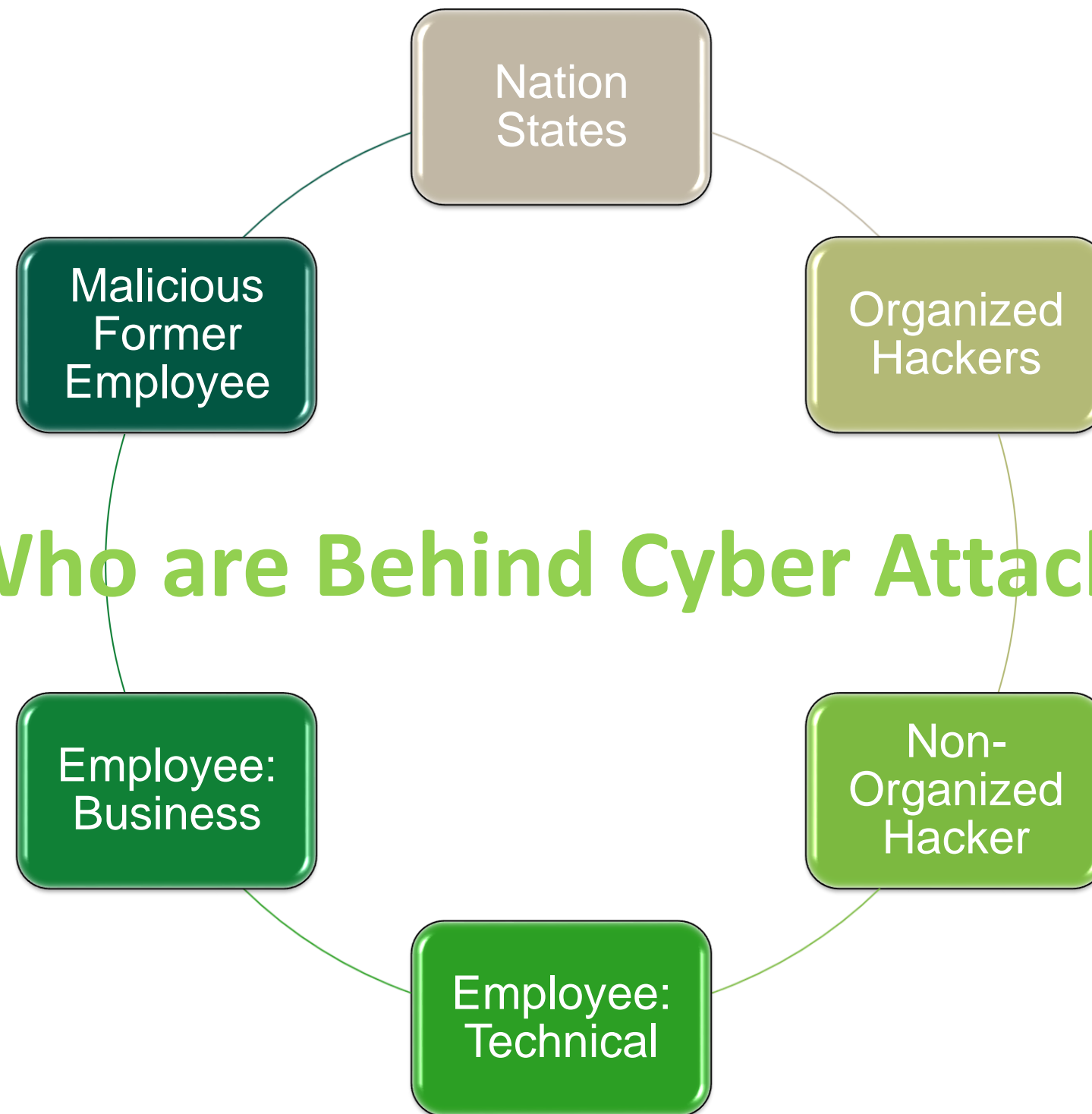
The survey found that in 2017:

- Canadian businesses spent a total of \$14 billion to prevent, detect and recover from cyber security incidents.
- Two out of ten (21%) Canadian businesses were impacted by a cyber security incident.
- Almost six out of ten (58%) businesses impacted by cyber security incidents experienced some downtime.

What does being a target mean...



Who are Behind Cyber Attacks?



Security Threat Landscape

- **Attackers find value in sensitive information**
 - Personal
 - Financial
 - Intellectual Property
- **Challenging to protect against today's threats**
 - Attacks originate from various sources
 - Avenues of attack continue to evolve



Property managers downplay cybersecurity threats

If a building operating system is breached, any party in supply chain could be liable

Friday, January 6, 2017

By Rebecca Melnyk

Sponsored Content

National Technology

Commercial Real Estate Is Unprepared For A Major Cyberattack

June 14, 2018 | SIOR | Travis Gonzalez, Writer

Want to get a jump-start on upcoming deals? Meet the major players at **one of our upcoming national events!**



RISK MANAGEMENT

Real estate firm Essex Property reports data breach

Judy Greenwald

9/30/2014 12:00:00 AM

Equifax Hack: The Real Estate Industry Is Just As Vulnerable



Bisnow Contributor ⓘ

We are the world's #1 source for commercial real estate news

Forbes

POST WRITTEN BY

Lara O'Keefe

- As smart cities begin to expand, it is becoming essential that real estate developers and investors keep cybersecurity top of mind.
- Smart buildings can improve building and tenant efficiency, but can also leave company and tenant information vulnerable to attacks.

US Electric Grid Hacked By Targeting Of Hundreds Of Small Government Contractors And Subcontractors

Posted at 1:02 pm on January 14, 2019 by [Elizabeth Vaughn](#)

 Share On Facebook

 Share On Twitter



Russian hackers initiated a complex plan to hack the US Electric grid by targeting a small construction company, All-Ways Excavating USA, located in Salem, Oregon. The

Spy agency expects foreign actors to attempt to sway public opinion online 

<https://www.ctvnews.ca/politics/spy-agency-expects-foreign-actors-to-attempt-to-sway-public-opinion-online-1.4207164>

Canada's cyber spy agency is warning that in 2019—an election year—foreign countries are "very likely" to try to sway Canadians' public opinion with misinformation online.

Hackers Targeting Third-Party Vendors on Amazon

 Damien

Amazon is spending millions of dollars to prevent hacking and online banking fraud.

However, even with all of their cryptographic technology and network security measures, the e-commerce giant has not saved its third-party vendors from hacking and fraud.

In recent weeks, [according to the Wall Street Journal](#), there have been hackings targeting the growing



Hackers have been making waves after hitting active and inactive Amazon vendors' accounts and taking profits in the thousands.

Let's take a closer look!

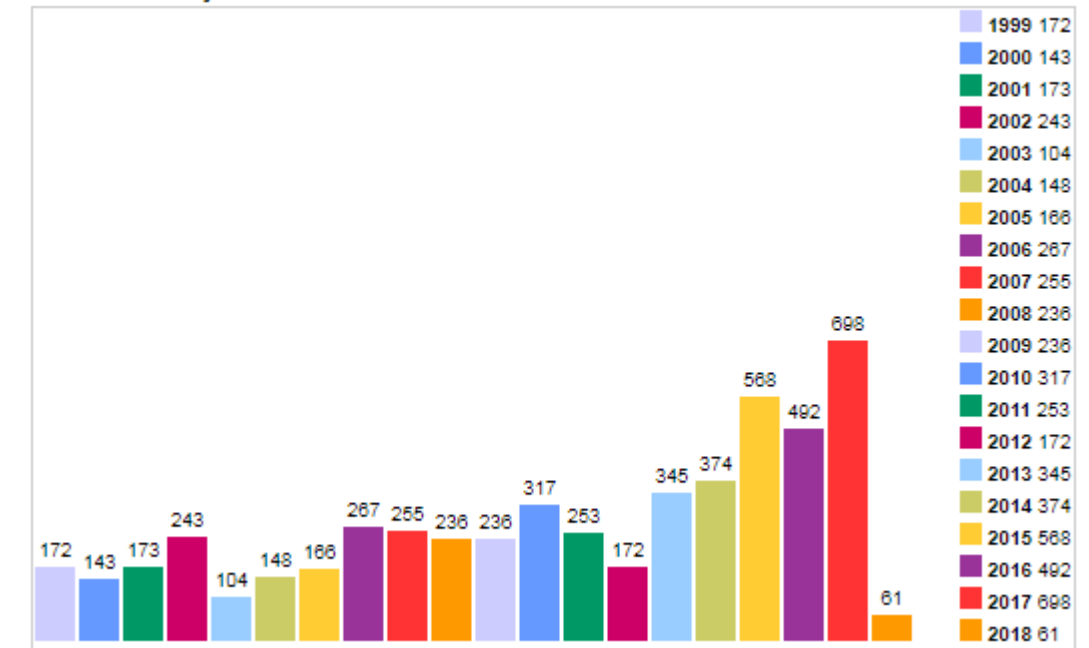
Hacking or Ethical Hacking

- **Internet is a big place**
 - Every “bad guy” is milliseconds from your firewall or application
 - Attackers are probing your IT systems right now
- **Vendors are releasing security patches on a monthly basis to fix vulnerabilities**
 - It can be difficult to keep up with missing patches
- **This doesn't include other security vulnerabilities (e.g., weak passwords, mistakes, etc.)**
- *Have you given permission*

Microsoft : Vulnerability Statistics

[Products \(461\)](#) [Vulnerabilities \(5491\)](#) [Search for products of Microsoft](#)

Vulnerabilities By Year



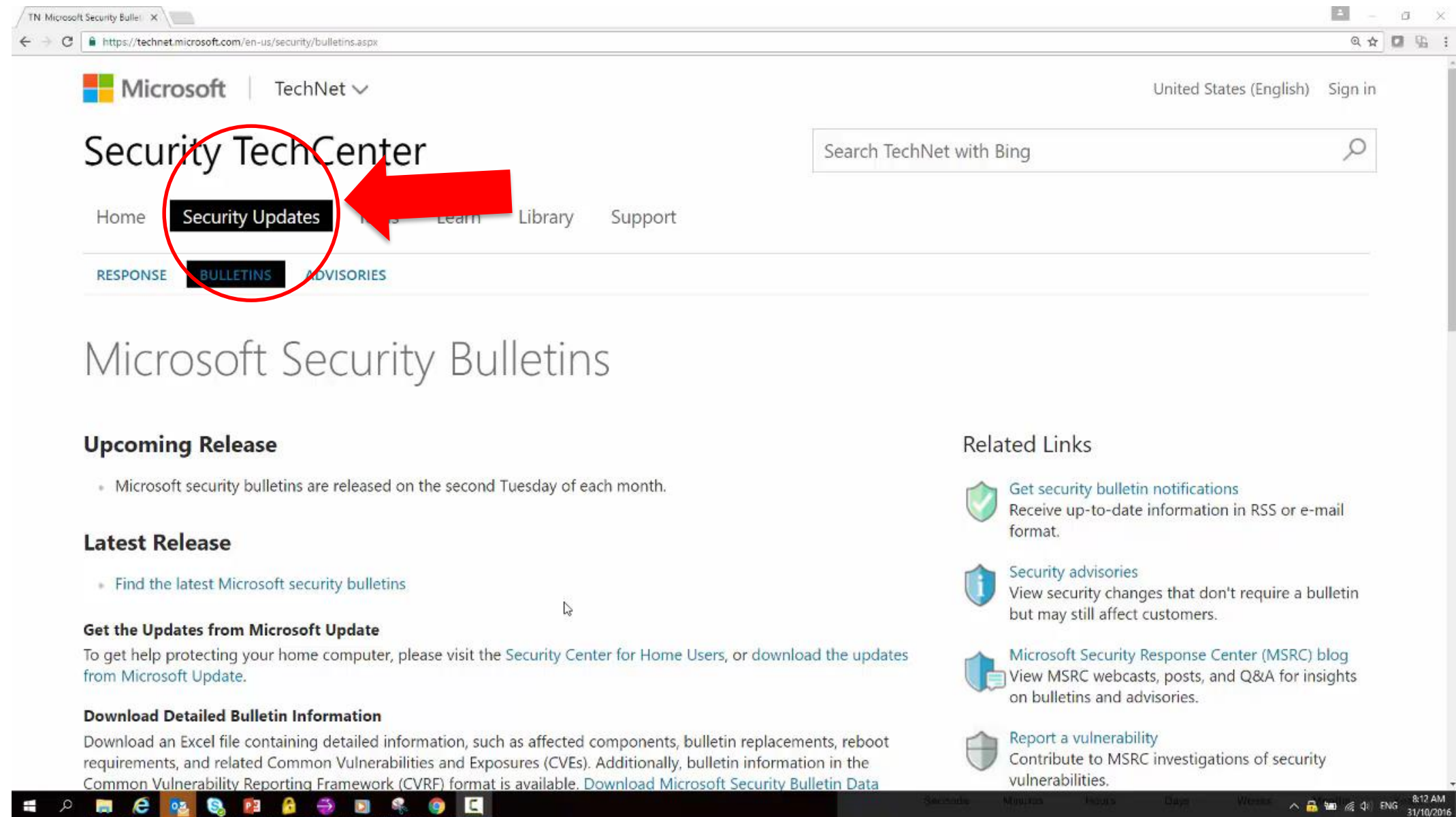
Moodle : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

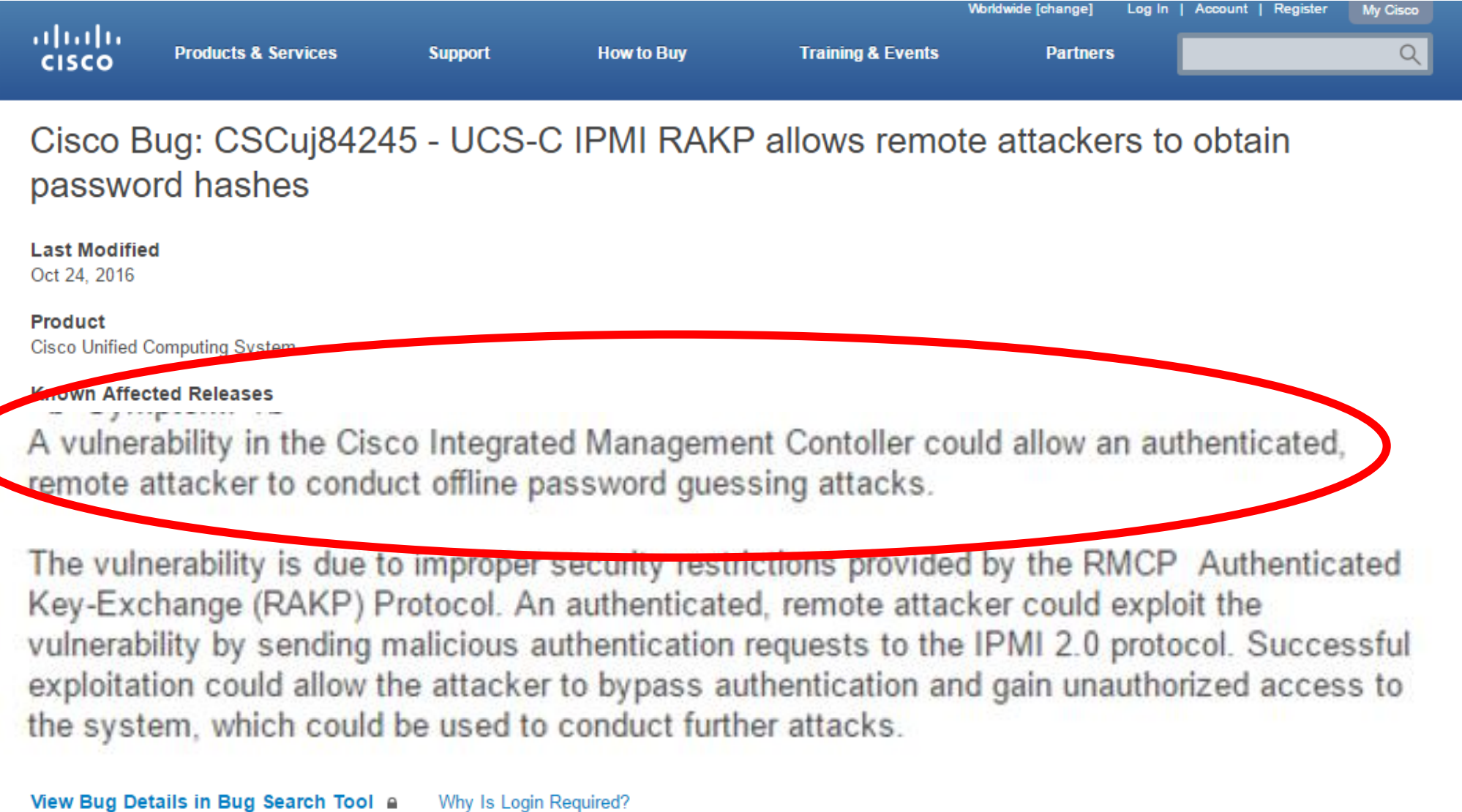
Sort Results By : [CVE Number Descending](#) [CVE Number Ascending](#) [CVSS Score Descending](#) [Number Of Exploits Descending](#)

Total number of vulnerabilities : 350 Page : 1 (This Page) 2 3 4 5 6 7

Almost ALWAYS Starts with a Vulnerability



Example #1 of a Penetration Test



The image shows a screenshot of a Cisco bug report page. A red oval highlights the "Known Affected Releases" section, which contains the text: "A vulnerability in the Cisco Integrated Management Controller could allow an authenticated, remote attacker to conduct offline password guessing attacks." Below this, a paragraph explains that the vulnerability is due to improper security restrictions provided by the RMCP Authenticated Key-Exchange (RAKP) Protocol. At the bottom, there are links to "View Bug Details in Bug Search Tool" and "Why Is Login Required?".

Worldwide [change] Log In | Account | Register | My Cisco

CISCO Products & Services Support How to Buy Training & Events Partners

Cisco Bug: CSCuj84245 - UCS-C IPMI RAKP allows remote attackers to obtain password hashes

Last Modified
Oct 24, 2016

Product
Cisco Unified Computing System

Known Affected Releases

A vulnerability in the Cisco Integrated Management Controller could allow an authenticated, remote attacker to conduct offline password guessing attacks.

The vulnerability is due to improper security restrictions provided by the RMCP Authenticated Key-Exchange (RAKP) Protocol. An authenticated, remote attacker could exploit the vulnerability by sending malicious authentication requests to the IPMI 2.0 protocol. Successful exploitation could allow the attacker to bypass authentication and gain unauthorized access to the system, which could be used to conduct further attacks.

[View Bug Details in Bug Search Tool](#) [Why Is Login Required?](#)

TobTu News Cracker Leaderboard Tools Beta Donate About

- ☒ a-z
- ☒ A-Z
- ☒ 0-9
- ☐ Symbol 14 !@#\$%^&*()_+=
- ☐ Symbol 18 '~{}[]\|;':",./?
- ☐ Space

Character Set:

abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789

Length:

7

Passwords:

32

Generate Passwords

Calculate Hashes

Passwords:

password1
password2
password3
password4

NTLM Hashes:

5835048CE94AD0564E29A924A03510EF
E22E04519AA757D12F1219C4F31252F4
BD7DFBF29A93F93C63CB84790DA00E63
F9187D82A9D623E60EF231B384D6F861
31D6CFE0D16AE931B73C59D7E0C089C0

LM Hashes:

E52CAC67419A9A2238F10713B629B565
E52CAC67419A9A22F96F275E1115B16F
E52CAC67419A9A221B087C18752BDBEE
E52CAC67419A9A22EA36BEE89599AE2E
AAD3B435B51404EEAAD3B435B51404EE



“Hashinator”

26 lower case letters (a-z)

26 upper case letters (A-Z)

10 digits (0-9)

8 Characters

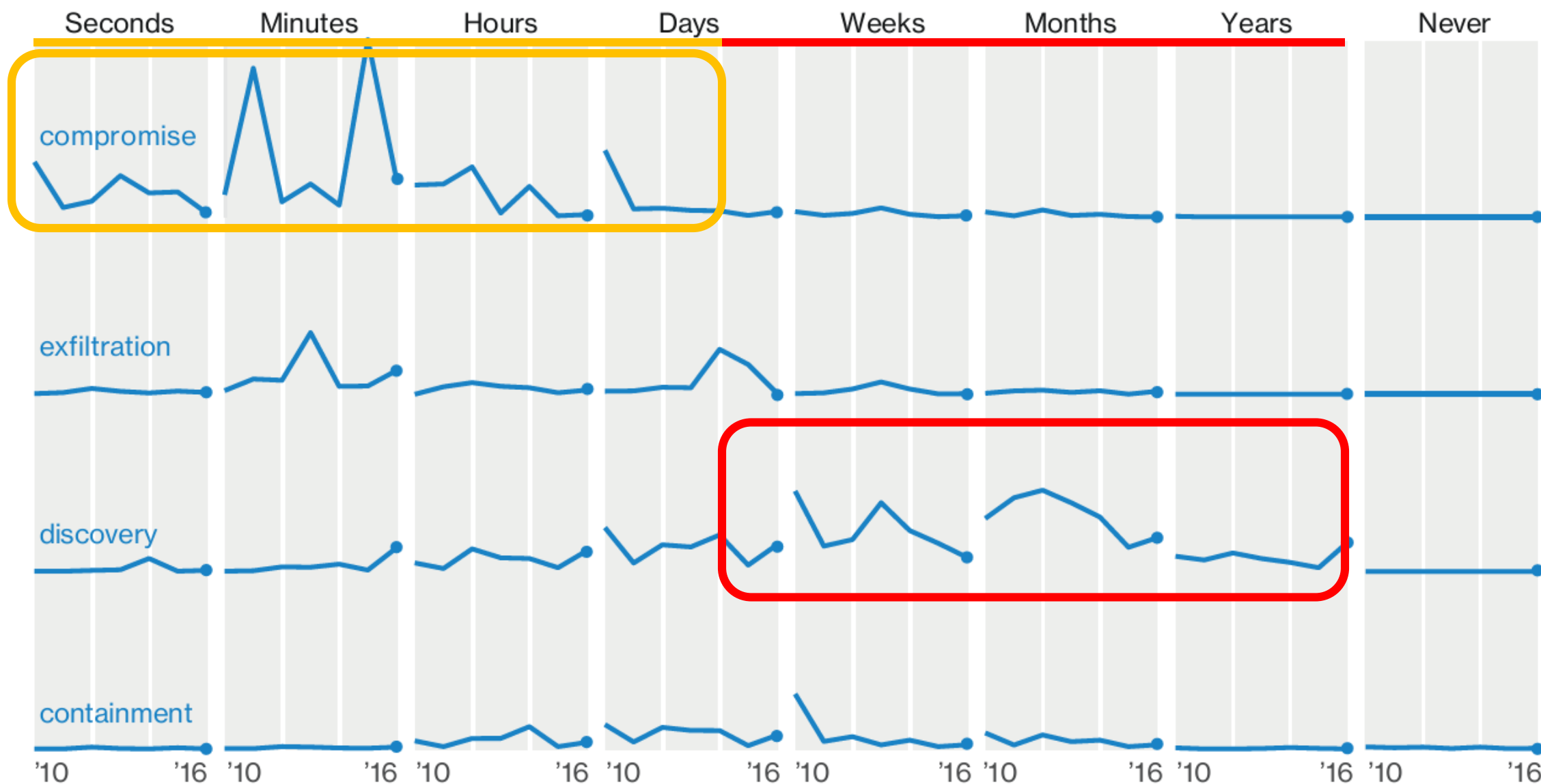
$$26 + 26 + 10 = 62$$

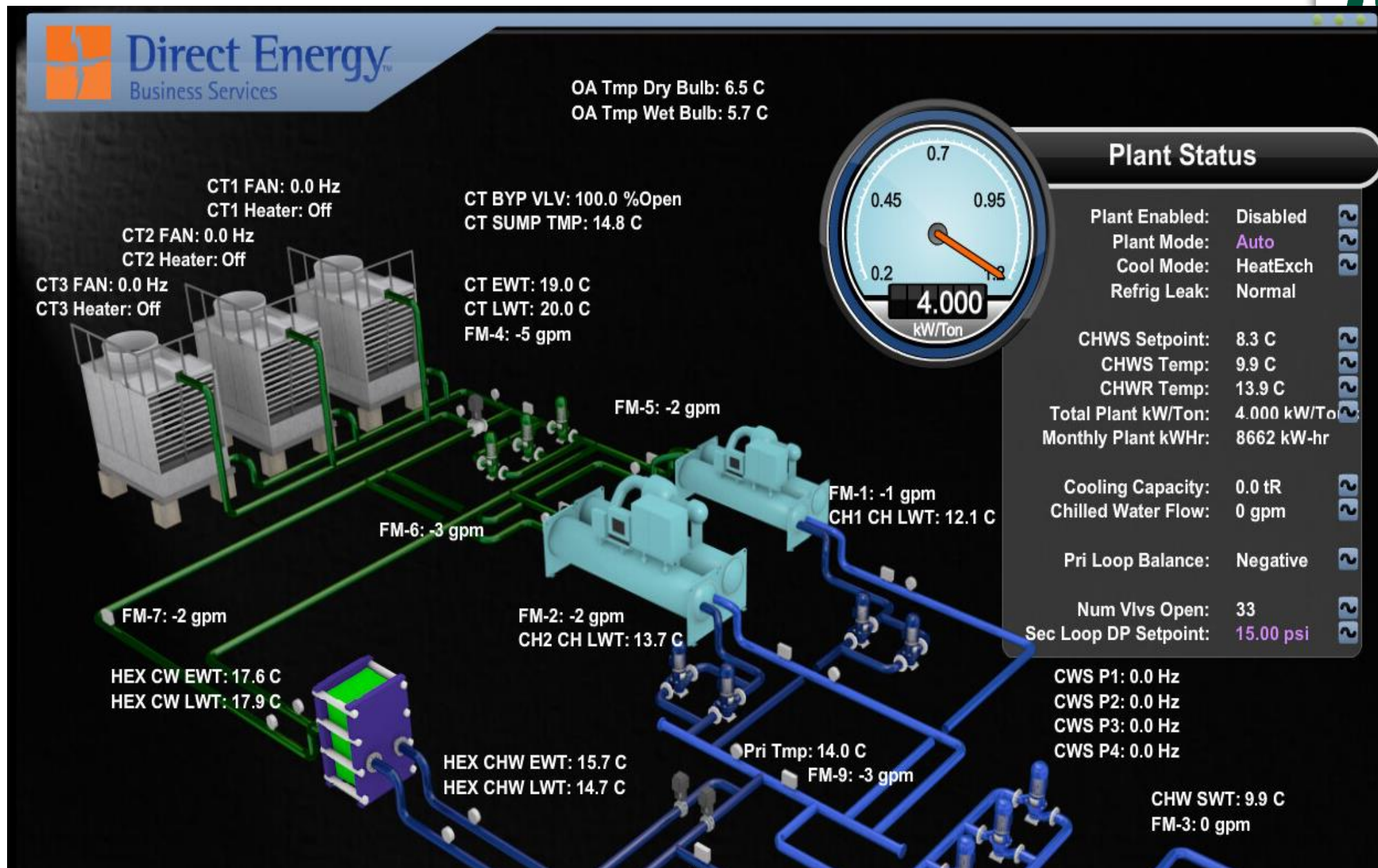
$$62^8 = 218,340,105,584,896$$

...or < 2 days

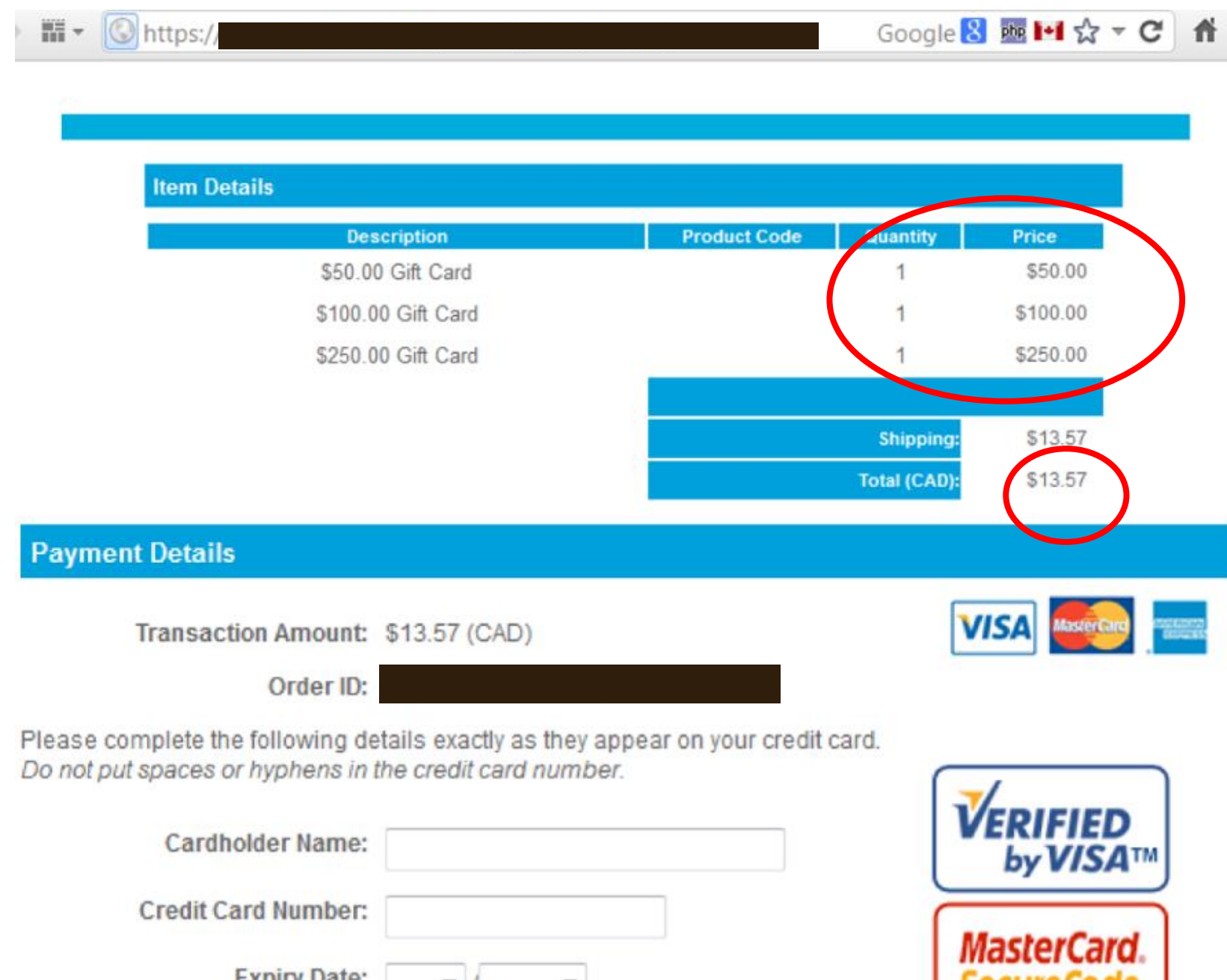


Security Threat Landscape





Example 2: Programming Error



https:// [redacted] Google [php] [Canada flag] [star] [refresh] [home]

Item Details

Description	Product Code	Quantity	Price
\$50.00 Gift Card		1	\$50.00
\$100.00 Gift Card		1	\$100.00
\$250.00 Gift Card		1	\$250.00

Shipping:	\$13.57
Total (CAD):	\$13.57

Payment Details

Transaction Amount: \$13.57 (CAD)

Order ID: [redacted]

Please complete the following details exactly as they appear on your credit card.
Do not put spaces or hyphens in the credit card number.

Cardholder Name:

Credit Card Number:

Expiry Date: /

VISA MasterCard American Express

VERIFIED by VISA™

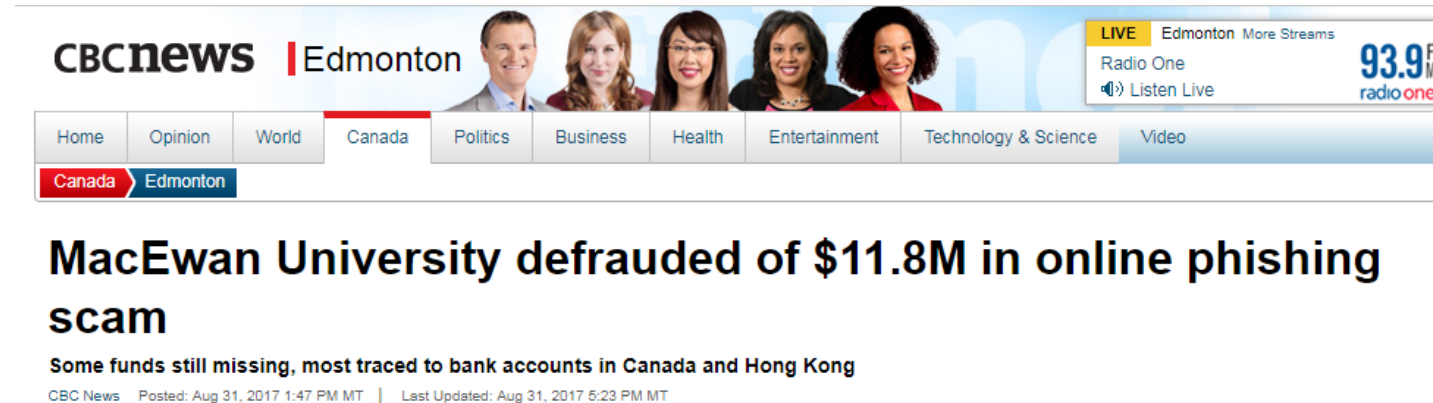
MasterCard

Why is Hacking so easy?

- Businesses are not patching their systems. This includes:
 - Applications – both Web & Mobile
 - Network & Computer Devices
- Businesses are not discovering a breach quickly to mitigate

Social Engineering

- **A hacking technique**
 - Used by attackers to obtain sensitive electronic information (e.g., passwords) from a victim
 - Convinces victims to provide information through “social” manipulation
- **Attacks pray on peoples’ inherent trustworthiness and inclination to be helpful**
- **Increase in “supply chain” attacks**
 - Attackers targeting business relationships



Verizon's data breach investigations team finding that 90 percent of breaches trace to a phishing or other social engineering attack

DO
NOT
FEED_{the}
PHISH



Why is Social
Engineering so
easy?



Example Phishing



Survey Monkey <survey@monkey.ca>
Mandatory employee survey


To

Hi,

This is a mandatory employee survey. Please fill out the following:

[Survey](#)

Thanks!



My Surveys Examples ▾ Survey Services ▾ Plans & Pricing

Upgrade ▾

Create Survey

Please enter your name:

Name

Start!

Get Survey Help, Ideas & Tips

- Learn how to survey like a pro
- Find more survey tools to help you
- Why use Question Bank?

Get Help





Community: [Developers](#) • [Facebook](#) • [Twitter](#) • [LinkedIn](#) • [Our Blog](#) • [Google+](#) • [YouTube](#)

About Us: [Management Team](#) • [Board of Directors](#) • [Integrations](#) • [Newsroom](#) • [Office Locations](#) • [Jobs](#) • [Sitemap](#) • [Help](#)

Policies: [Terms of Use](#) • [Privacy Policy](#) • [Anti-Spam Policy](#) • [Security Statement](#) • [Email Opt-In](#) • [Accessibility](#)

Language: **English** • [Español](#) • [Português](#) • [Deutsch](#) • [Nederlands](#) • [Français](#) • [Русский](#) • [Italiano](#) • [Dansk](#) • [Svenska](#) • [日本語](#) • [한국어](#) • [中文\(繁體\)](#) • [Türkçe](#) • [Norsk](#) • [Suomi](#)

Copyright © 1999-2016 SurveyMonkey



From: linkedin.com <message-wk881425ffjm55@linkedin.com>
Subject: Mark Andronas at Payroll Processing wants to connect on LinkedIn
Date: June 2, 2011 12:55:01 PM GMT+03:00
To: Mickey Boodaei
Reply-To: message-wk881425ffjm@linkedin.com

LinkedIn

I'd like to add you to my professional network on LinkedIn.

- Mark Andronas

Neal Collins
Vice President, Strategy & Corporate Development at Payroll Processing
Greater Chicago Area

Confirm that you know Neal

© 2011, LinkedIn Corporation

From: Lawrence Reed
Date: May 26, 2011 1:29:03 PM GMT+03:00
To: Mickey Boodaei
Subject: Invitation to connect on LinkedIn

LinkedIn

Mickey,

I'd like to add you to my professional network on LinkedIn.

- Lawrence

Lawrence Reed
Independent Consultant
London, United Kingdom

Confirm that you know Lawrence

© 2011, LinkedIn Corporation

Tue 30/10/2018 10:03 AM

admin.support@staplesprocessing.ca

Confirmation #:314767VW

nmins

problems with how this message is displayed, click here to view it in a web browser.
download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.



Order confirmation #:314767VW PAID

Hi Danny Timmins

Customer: **Danny Timmins**

Payment type: **Credit Card**

Order: **#:314767VW**

Currency: **CAD**

Invoice date: **18 October 2018**

**Please be informed that your transaction is confirmed.
Please check invoice and update your information.**


The payment will appear on your card statement

<http://bit.ly/2ejgiws>
Click or tap to follow link.

PPSOLUTE

[View Invoice](#)

.ly is
from
Libya



From: CanadaPost <Peter@sfseomedia.biz>
Sent: November 14, 2018 12:36 PM
To: Danny Timmins <Danny.Timmins@mnp.ca>
Subject: Shipment Notification #3 - CanadaPost

Dear client,

Canada Post is sorry to inform you that we could not deliver your package to your place area on 13 , November 2018 because no one was available at time of delivery to sign for item, and you could not be reached on a phone.

You can schedule redelivery of your item to the same address after visiting any Canada Post office that is conveniently located to you and bringing a printed shipping invoice.

The shipping invoice is available to download at the following link:

[http://akliquefiednaturalgas.biz/
lololololol/trolololo/index.php?id=17090](http://akliquefiednaturalgas.biz/lolololol/trolololo/index.php?id=17090)
Ctrl+Click to follow link

www.canadapost.ca/pqotools/apps/customers/personal/deliveryInvoicePrint?prnt=a1s4

If the order is not picked up within 72, it will be sent back.

This is an automatically generated email, please do not reply.

Best regards,

2018 Canada Post

Does it
look like
Canada
Post?

From: canadapost.ca <Marcus@tasteofspring.biz>

Sent: November 14, 2018 5:30 PM

To: Danny Timmins <Danny.Timmins@mnp.ca>

Subject: Canada Post - Delivery Notification #2

Dear customer,

Unfortunately, we could not hand over your order to your place area on 13 , November 2018 because no one was available at the delivery address to sign for item, and you could not be contacted.

You can schedule redelivery of your item to the same address after visiting any Canada Post office in your area and bringing a printed shipping invoice.

To view and download the shipping invoice,

<http://badbusinesspractices.biz/123123lololll/traasssaavfdve11241vwsv/index.php?id=112233>
Ctrl + Click to follow link

following link:

www.canadapost.ca/pqotools/apps/customers/personal/deliveryInvoicePrint?prnt=a1s4

If the parcel is not picked up within 72, it will be sent back.

This is an automatically generated message, please do not reply.

Best regards,

2018 Canada Post

Does it
look like
Canada
Post?



What are they trying to do?

Typically two things:

1. Get you to give them your username and password
2. Get you to click on a link where Crimeware is downloaded onto your systems without you noticing. The malware could be described as:
 - Spyware
 - Denial of Service
 - C&C – Command & Control
 - BackDoor
 - Ransomware
 - Cryptojacking



Scammers pose as company execs in wire transfer spam campaign

Innocent-looking payment requests could result in financial loss for companies as finance department employees targeted with fraudulent emails.

By: **Sean Butler**  SYMANTEC EMPLOYEE

Created 28 Oct 2014

 0 Comments |  Translations: [Português](#) |  Share



CBCnews | Edmonton



LIVE Edmonton More Streams
Radio One **93.9** FM
 Listen Live **radio one**

Home Opinion World **Canada** Politics Business Health Entertainment Technology & Science Video

Canada Edmonton

MacEwan University defrauded of \$11.8M in online phishing scam

Some funds still missing, most traced to bank accounts in Canada and Hong Kong

CBC News | Posted: Aug 31, 2017 1:47 PM MT | Last Updated: Aug 31, 2017 5:23 PM MT

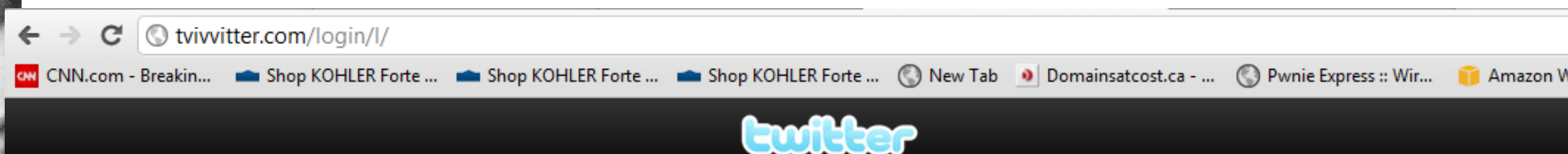
Twitter...or was that Tvivviter

Direct messages › with [REDACTED]



53m

Hey someone is saying nasty rumors about you...
[thniiidxuaajgkeppflgbfxktw.plz.re](https://t.me/thniiidxuaajgkeppflgbfxktw)



Your session has timed out, please re-login.

Username or email

Password

☐ Remember me

Sign in

 tvivitter.com/login/l/

Already Using Twitter Via SMS?

[Activate Your Account »](#)

[About](#) [Help](#) [Blog](#) [Status](#) [Jobs](#) [Terms](#) [Privacy](#) [Businesses](#) [Media](#) [Developers](#) [© 2011 Twitter](#)



How Strong is Your Password?

TEST YOUR PASSWORD SKILLS!

Are you hackable or uncrackable?



Play our password game.

Test your strong password here*

**Determine Your
Password Strength*

*We will not retain information
entered into this password grader.
The password you enter is checked
and graded on your computer. It is
not sent over the Internet. Just the
same, be careful where you type
your passwords anywhere online.*


GRADE MY PASSWORD!

Newsroom



USA (English) ▾

TIP 3: Clicky McClicker



ASHLEY Woods

Manager, Customer Support at EPAM - DEP
Dallas, Texas | Computer Software

Previous JP Morgan FCS, Teradata Aster
Education University of Dallas

Accept invitation


Send ASHLEY InMail

65 connections

in


https://www.linkedin.com/in/ashley-woods-351797117

WIN ME!



LIKE AND SHARE





Accept invitation

Send ASHLEY InMail

65 connections

in

https://www.linkedin.com/in/ashley-woods-351797117



You can use Google Images

- Use Google Images to verify and validate pictures

Google

← → ↻ https://www.google.ca/?gws_rd=ssl

ASHLEY Woods 2nd

Manager, Customer Support at EPAM - DEP
Dallas, Texas | Computer Software

Previous JP Morgan FCS, Teradata Aster
Education University of Dallas

[Accept invitation](#) [Send ASHLEY InMail](#) 65 connections

<https://www.linkedin.com/in/ashley-woods-351797117>

Google Canada

Google Search I'm Feeling Lucky

Help Canada make the world better, faster. [Enter the Google.org Impact Challenge.](#)

Google.ca offered in: [Français](#)





NBC AFFILIATES | REPORTING | SHOPTALK

Reporter Deborah Sherman Out At Denver's KUSA



By Merrill Knox on Nov. 22, 2011 - 12:35 PM  1 Comment

Deborah Sherman, a reporter at KUSA, has been cut loose at the Denver NBC-affiliate because of a “personnel issue,” the [Denver Post](#) reports.

Sherman joined KUSA’s investigative reporting team in 2003. Her last day at the station was reportedly last week, though management has refused comment on the circumstances surrounding her departure.

“We’re not going to comment on people who are leaving or have left the station,” KUSA news director Patti Dennis [said](#).

The *Post* reports Sherman “is said to have great contacts but not the easiest professional temperament,” saying a memo from station management to KUSA staffers fueled rumors that Sherman was shown the door due to her connection to [several controversial stories](#) she has reported on in the past.



Top 10 Considerations



Have you and your executives quantified business risk? What is the impact to those assets if breached? How to better prioritize budget & resources?



Have you developed and implemented the appropriate cyber security safe guards: Have you considered threat detection (AI)? What is the impact of moving to the Cloud? How safe are IoT devices?



Have you understood your potential exposure by engaging cyber security consultants “ethical hackers” to hack your organization? (Networks, Applications, Mobile)

Top 10 Considerations



Can you demonstrate a solid Cyber Incident Response plan which enables you to respond to a breach? If yes, have you tested it by doing a table top exercise?



Have you ever considered a Cyber Security Advisor to help set standards, recommendations and policies?



Do you have a clear understanding of your Supply Chain (Vendor/Third Party) Contracts. Have you done an assesemnt on their maturity? Begin with the IT focused contracts?

Top 10 Considerations



Have you considered purchasing cyber security-specific insurance to protect against the ramifications of any major breaches? Is it focused on the key business risks identified if breached?



Is your data reinforced by a business continuity plan including data backup & data recovery. Is the data stored offline & offsite? Have you tried restoring it?

Top 10 Considerations



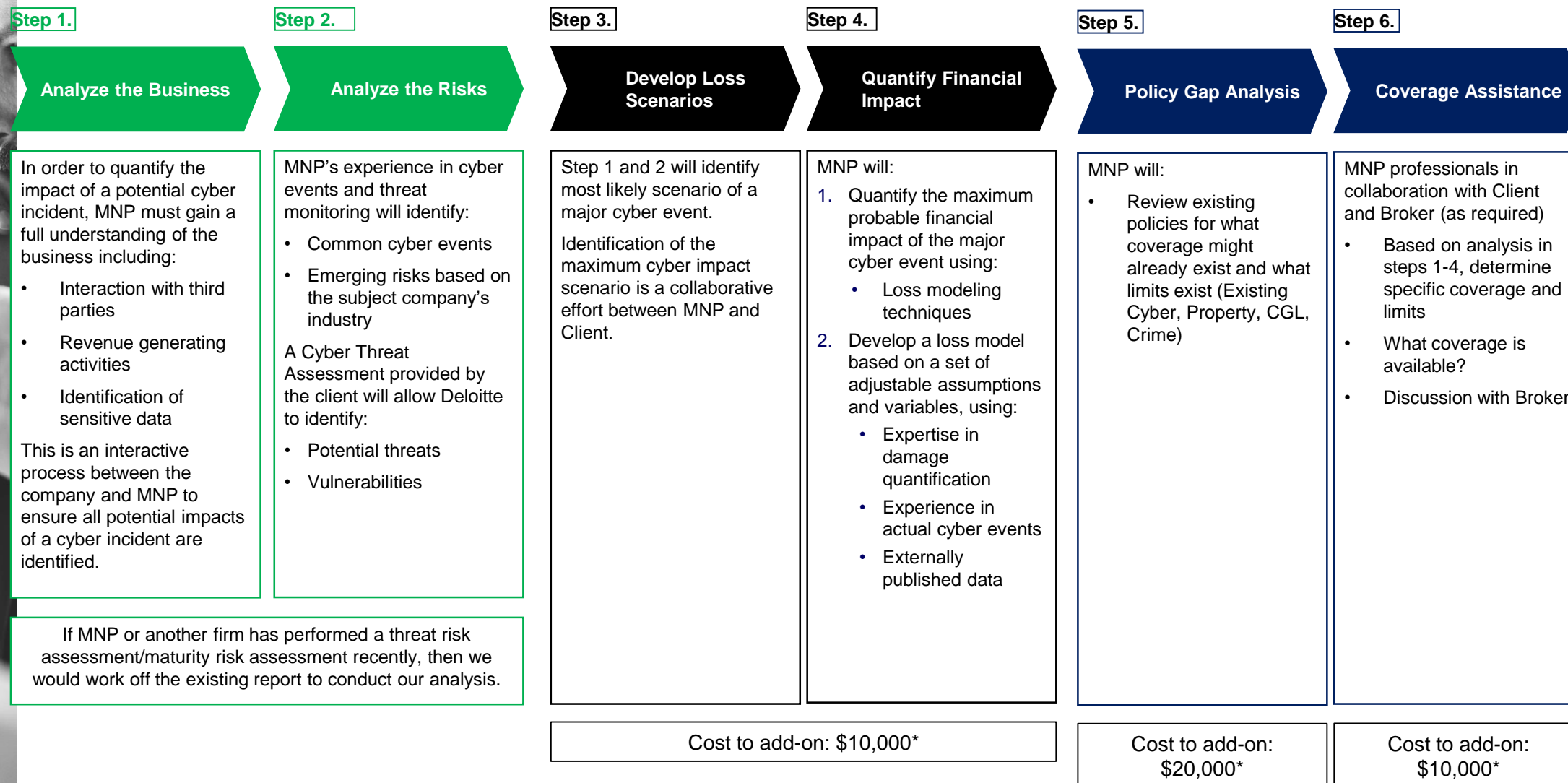
**How sophisticated are your Cyber Security Educational Training, practices and procedures?
Are you making it personal?**



Are you patching? Who has access to what? Do you have a shadow IT problem? Are your IT assets all accounted for? These are other major challenges that exist in Cyber Security today.

Insurance Advisory

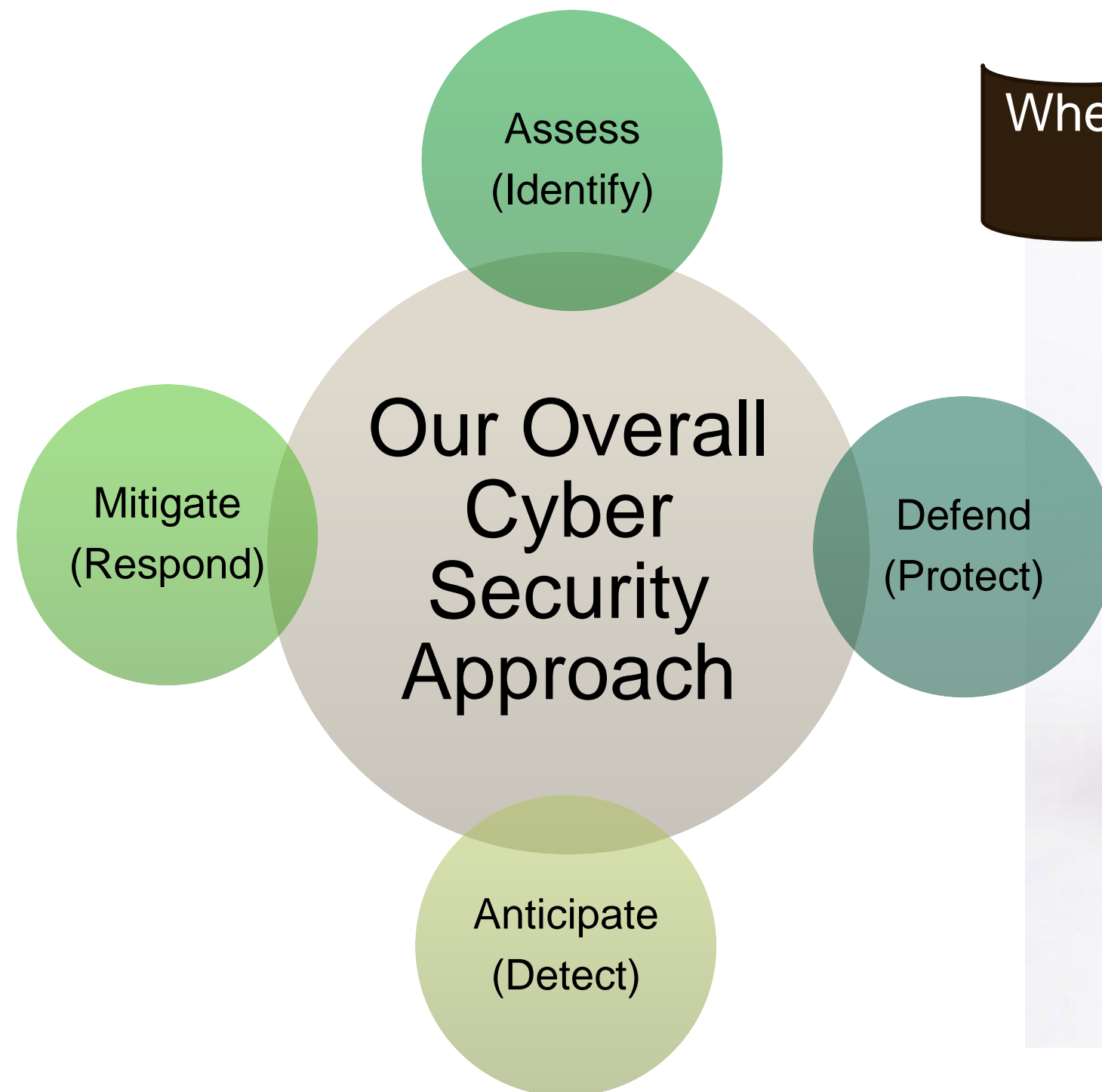
Stand-Alone Services – Cyber Insurance Assessment



*Cost have been estimated

Page 46

Where do YOU sit!



Personal Cyber Security Check List

- ✓ Create strong PW – use a minimum of 12 characters (Capitals, numbers, special characters).
- ✓ Keep your systems updated with latest software.
- ✓ Run Anti-Virus, Anti-Malware.
- ✓ Back Up your systems (local, cloud, offsite..).
- ✓ Have a Firewall if possible.
- ✓ Two Step Verification .

Personal Cyber Security Check List

- ✓ Have your computer or mobile set to auto lock out.
- ✓ Never click on something you don't know.
- ✓ Don't add people to your profiles that you don't know.
- ✓ Sensitive browsing should only be done from a trusted network. i.e.: banking
- ✓ Be wary of any phishing or social engineering attempt (smishing, vishing etc.).

Questions?

