Prevent Cyber Attacks Canadian Home Builders Assocaition

MNP Cyber Security Presentation

Presented by: Danny Timmins, National Cyber Security Leader November 2017

ACCOUNTING > CONSULTING > TAX





Cyber Security MNP Technology Solutions





- Cyber Security Overview
- Cyber Crime Tactics and Techniques
 - Hacking (Penetration Testing) Ο
 - Social Engineering (Malware/Crimeware) Ο
 - **Red Teaming** Ο
- Considerations







Lessons from the field

- Canada's 5th Largest Accounting | Tax | Consulting
- 4500 Team Members
- 80 Offices coast to coast
- 55 Cyber Security Professionals Nationally









MNP is more than an Accounting Firm

- **Digital Strategy**
- Portal Development
- Business Continuity

- **IoT**
- Cyber Security & Risk
- Workplace Collaboration •
- CRM/ERP lacksquare
- Cloud Strategy

- **Data Analytics**
- DevOps
- Auditing



Operational Technology

Page 4



Predictions

 \geq 99% of vulnerabilities exploited will continue to be the ones known by security/IT professionals.

 \succ The single most impactful enterprise activity to improve security will be patching.

 \succ The second most impactful enterprise activity to improve security will be removing web server vulnerabilities.



Page 5



Predictions

 \geq Internet of Things will grow to an installed base of 20.4 billion.

> A third of successful attacks experienced will be on their shadow IT resources.

 \succ Companies are using more than 15 times more cloud services to store critical company data than CIOs were aware of.

 \geq Nearly eight in ten (77%) of decision makers admit to using a third-party cloud application without approval.



Page 6

What's happening...

Canada's new privacy laws will require breach notice and affect private sector operations in Canada. (Digital Privacy Act)...do you know how safe your client data is?

Canada's privacy watchdog planning to pro-actively investigate companies

Excerpt: Canada's privacy watchdog is transforming the way it has pursued protective measures for more than 15 years, planning to more actively go after companies and other organizations for privacy concerns. And it has renewed calls for an update t... Show more



Canada's privacy watchdog planning to pro-actively investigate companies

Commissioner Daniel Therrien also repeated his call for changes to federal law that would give his office the ability to issue orders and

ACCOUNTING > CONSULTING > TAX



7



What's happening in the industry?

Damages have started to increase in Canada – Class Action Suits are here - Casino Rama is an example30+ Million

Cyber Insurance...how much do you need ... is it focused on the correct areas?

ACCOUNTING > CONSULTING > TAX



Page 8



Business

Threat of cyberattacks 'more worrisome than all the other stuff': Bank of Canada governor

Stephen Poloz shared his unease at a time when governments, central banks and the private sector around the world are searching for new strategies to counter hacks.



Page 9



What's happening in the industry?

Mandatory cyber audits coming for publicly traded companies in Canada.... US is pushing hard – its coming

Payment Card Industry (PCI) already has compliancy. IE: Best Western Motels - have been targeted-very limited security

Equifax 140M plus - 100+ thousand in Canada....patch management said to be the issue...mishandled from the start of the breach...directing clients to a phishing site



Page 10

Who are Behind Cyber Attacks?

- Nation States
- Organized Hackers
- Non-Organized Hacker
- Employee: Technical
- Employee: Business
- Malicious Former Employee

**89% of breaches had financial or espionage motive





Page 11



Some Risks to Consider

- Brand and reputation
- Unable to fulfill service commitments
- Strategic plans, engineering drawings, RFP's, Proposals, etc.
- Supply Chain/Vendor Management
- New Automation deployments IoT (Internet of Things) – Life Safety Systems – automated systems, elevators, exhaust
- Privacy Personal Identification Information (PII)
- Regulator Compliance
- Intellectual Property (IP)
- Payment Systems (Ecommerce or Point of Sale)



Page 12



Cyber-attacks have:



ACCOUNTING > CONSULTING > TAX



Page 13

Who's making the decisions

JUL 13, 2015 @ 01:42 PM 11,527 VIEWS

Why Cybersecurity Leadership Must Start At The Top



Frontline, CONTRIBUTOR Dispatches on Cybersecurity FULL BIO V Opinions expressed by Forbes Contributors are their own.

JUL 1, 2016 @ 04:21 AM

7,294 VIEWS

It's Time To Think Of Cybersecurity As A Business Enabler

8 6 9 10 8



William H. Saito, CONTRIBUTOR

I write about cybersecurity, innovation & Japan. FULL BIO V Opinions expressed by Forbes Contributors are their own.

ACCOUNTING > CONSULTING > TAX



Page 14



Let's take a closer look!

ACCOUNTING > CONSULTING > TAX









What is Hacking?

- The EXPLOIT of a technical vulnerability
- Human error (still a vulnerability)
- Can involve chaining together a series of weaknesses
- Performed without owner permission





What is Penetration Testing?

- Similar to hacking except owner gives permission
- Attempt to gain access to sensitive information or resources
- Steps can include:
 - Information gathering
 - Vulnerability enumeration
 - Vulnerability exploitation / Privilege Escalation
 - Exploration / Lateral Movements
- Performed against defined scope
- Measures Network(s) and Application(s) resiliency
- Overall goal to improve security posture



Page 17

Almost ALWAYS Starts with a Vulnerability

Microsoft TechNet V	United St
Security TechCenter Search Tech	hNet with Bing
Home Security Updates Tools Learn Library Support	
RESPONSE BULLETINS ADVISORIES	
Microsoft Security Bulletins	
Upcoming Release	Related Links
Upcoming Release Microsoft security bulletins are released on the second Tuesday of each month.	Related Links Get security bulletin notification Receive up-to-date information
Upcoming Release Microsoft security bulletins are released on the second Tuesday of each month. Latest Release	Related Links Get security bulletin notification Receive up-to-date information format.
Upcoming Release Microsoft security bulletins are released on the second Tuesday of each month. Latest Release Find the latest Microsoft security bulletins 	Related Links Get security bulletin notification Receive up-to-date informatic format. Security advisories View security changes that do but may still affect customers.

To get help protecting your home computer, please visit the Security Center for Home Users, or download the updates from Microsoft Update.

Download Detailed Bulletin Information

e 📴 🕄 🛤 😚

12

Download an Excel file containing detailed information, such as affected components, bulletin replacements, reboot requirements, and related Common Vulnerabilities and Exposures (CVEs). Additionally, bulletin information in the Common Vulnerability Reporting Framework (CVRF) format is available. Download Microsoft Security Bulletin Data

C



Report a vulnerability Contribute to MSRC investigations of security vulnerabilities.

ACCOUNTING > CONSULTING > TAX





23

Microsoft Security Response Center (MSRC) blog

🔨 📅 🛲 🍕 🕼 ENG





Defining the "zero-day" (software) threat

A security hole in software that is not yet known to the software maker or to Information Security vendors

NO PATCH - NO SIGNATURE

Zero-day vulnerability

Code that attackers use to take advantage of a zero-day vulnerability to compromise a system for their benefit

DROP - CONTROL - DISABLE

Zero-day exploit

The term "zero-day" refers to the number of days that the software vendor has known about the hole - ZERO.



arabilities

Vulnerability

ovacs on November 01, 2016



Recommend 24

Google has disclosed a Windows zero-day vulnerability after Microsoft failed to release a patch within the 7-day deadline the search giant gives vendors when it finds a flaw that is actively exploited by malicious actors.

ACCOUNTING > CONSULTING > TAX



Google Discloses Windows Zero-Day



Page 19

Example 1: Penetration Test

					1	Worldwide [change]	Log In	Account Reg
	cisco	Products & Services	Support	How to Buy	Training & Events	Partners		
	Cisco E passwo	Bug: CSCuj842 ord hashes	45 - UCS-	C IPMI RAKI	P allows remot	e attackei	rs to	obtain
	Last Modifie Oct 24, 2016	d						
	Product Cisco Unified (Computing System						
	Known Affec	cted Releases						
(A vulner remote a	ability in the Cis	sco Integrat uct offline p	ed Manageme bassword gues	ent Contoller cou sing attacks.	ıld allow ar	n aut	thenticat

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?









What Can You Do with Hash?

TobTu	News	Cracker	Leaderboard	Tools	Beta	Donate	About	
✓ a-z ✓ A-Z ✓ 0-9 Syn Syn Spa	nbol 14 nbol 18 ce ter Set:	!@#\$%^8 `~{}[] \:;"	&*0+= '<>,.?/					
abcdefg	hijklmno	opqrstuvwx	ZABCDEFGHIJI	KLMNOPC	RSTU	VWXYZ01	23456789	•
Length 7 Passwo	: P 3 rds:	asswords: 32	Generate	Password	s	Calculate	Hashes	Hashes:
passwo passwo passwo passwo	rd1 rd2 rd3 rd4		5835048CE94AD E22E04519AA75 BD7DFBF29A93F F9187D82A9D62 31D6CFE0D16AE	0564E29A 7D12F121 93C63CB8 3E60EF23 931B73C5	924A03 9C4F31 4790DA 1B384D 9D7E0C	510EF 252F4 00E63 6F861 089C0	E520 E520 E520 AAD3	AC67419A9A2238 AC67419A9A22F9 AC67419A9A221B AC67419A9A22EA 3B435B51404EEAA
PwDum	ip Form	nat:						

password1:E52CAC67419A9A2238F10713B629B565:5835048CE94AD0564E29A924A03510EF::: password2:E52CAC67419A9A22F96F275E1115B16F:E22E04519AA757D12F1219C4F31252F4::: password3:E52CAC67419A9A221B087C18752BDBEE:BD7DFBF29A93F93C63CB84790DA00E63::: password4:E52CAC67419A9A22EA36BEE89599AE2E:F9187D82A9D623E60EF231B384D6F861::: :AAD3B435B51404EEAAD3B435B51404EE:31D6CFE0D16AE931B73C59D7E0C089C0:::









"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



ACCOUNTING > CONSULTING > TAX





INF0: approaching final keyspace, workload adjusted

f7a0df1801200002f63d0c38641adeaee22884a29096a179270c2b069e96b48fa8314f2a1927111e 8db2de615edd11e3b960a80c0db8b7ec140561646d696e:0686e03152b9cef46e48fc82e94279cb0 6eec7ab:w rk

Session.Name;	sellash cat
Status	Cracked
Rules.Type	Generated (90000)
Input.Mode:	File (/root/projects/ /working.txt)
Hash.Target:	f7a0df1801200002f63d0c38641adeaee22884a29.
Hash.Type:	IPMI2 RAKP HMAC-SHA1
Time.Started:	Mon Jan 4 18:51:01 2016 (2 secs)
Speed.GPU.#1:	5054.6 kH/s
Speed.GPU.#2:	5233.3 kH/s
Speed.GPU.#3:	5281.1 kH/s
Speed.GPU.#4:	5252.1 kH/s
Speed.GPU.#5:	5239.2 kH/s
Speed.GPU.#*:	26060.2 kH/s
Recovered:	1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress:	52308480/110880000 (47.18%)
Rejected:	0/52308480 (0.00%)
Restore.Point:	0/1232 (0.00%)
HWMon.GPU.#1:	35% Util, 39c Temp, 20% Fan
HWMon.GPU.#2:	61% Util, 34c Temp, 30% Fan
HWMon.GPU.#3:	59% Util, 42c Temp, 30% Fan
HWMon.GPU.#4:	61% Util, 37c Temp, 30% Fan
HWMon.GPU.#5:	36% Util, 43c Temp, 20% Fan





U/P Leads to Full VM Infrastructure

🖸 💽 🏠 Home 🕨 🚮 Inve	entory 🕨 🗊 Inventory			
ID.20.255.70 BACnet Controller core-01 core-03 core-04 core-05 core-06 core-07 core-08 core-09 core-10 core-10 core-10 cores_production_vmware Dashboard Server Desktop Triacta Workstation VMware vCenter Server Ap vSphere Management Assis	Getting Started Summary Virtu Manufacturer: Model: CPU Cores: CPU Cores: Processor Type: License: Processor Type: License: Cores per Sockets: Cores per Socket: Logical Processors: Hyperthreading: Number of NICs: State: Virtual Machines and Templates: vMotion Enabled: VMware EVC Mode: vSphere HA State Host Configured for FT:	Cisco Systems Inc Cisco Systems Inc C260-BASE-2646 20 CPUs x 2.393 GHz Intel(R) Xeon(R) CPU E7- 2870 @ 2.40GHz VMware vSphere 5 Enterprise Plus - Licensed for 2 physic 2 10 40 Active 8 Connected 17 N/A Disabled @ N/A N/A	Performance Configuration CPU usage: 1802 MHz Memory usage: 84191.00 MB Storage Dr Image: datastore1 Network Tr Network St St St	Local Users & Groups Events Per Capacity 20 x 2.393 GHz Capacity 130953.90 MB rive Type Capacity on-SSD 2.17 TB Pre andard port group andard port group
	Active Tasks: Host Profile: Image Profile: Profile Compliance: DirectPath I/O: Commands	N/A ESXi-5.5.0-20140302001-st ? N/A Supported C	Fault Tolerance Fault Tolerance Version: Total Primary VMs: Powered On Primary VMs: Total Secondary VMs: Powered On Secondary VMs:	5.0.0-5.0.0-5.0.0 Refresh Virtual Machine Counts 0 0 0

ACCOUNTING > CONSULTING > TAX





MNP.ca



Once Access is Gained... Then We "Pivot"



ACCOUNTING > CONSULTING > TAX



Page 25

Access to HVAC System...



ACCOUNTING > CONSULTING > TAX

Plant Sta	tus	\supset	
Plant Enabled: Plant Mode: Cool Mode: Refrig Leak:	Disabled Auto HeatExch Normal	222	
CHWS Setpoint: CHWS Temp: CHWR Temp: otal Plant kW/Ton: nthly Plant kWHr:	8.3 C 9.9 C 13.9 C 4.000 kW/T 8662 kW-h	้ริเยร	
Cooling Capacity: hilled Water Flow:	0.0 tR 0 gpm	212	
Pri Loop Balance:	Negative	~	
Num Vlvs Open: .oop DP Setpoint:	33 15.00 psi	212	
WS P1: 0.0 Hz WS P2: 0.0 Hz WS P3: 0.0 Hz WS P4: 0.0 Hz			
CHW SW FM-3: 0 g	/T: 9.9 C jpm		e 26



Example 2: Programming Error

🖬 🔹 💽 https:// Google 8 🔤 🖬 ☆ ▾ C 🖌 א



ACCOUNTING > CONSULTING > TAX







What is Social Engineering?

- An act that influences a person to take an action
- Used by attackers as it consistently works
- There is no patch for untrained users
- Performed against defined scope
- Three types of Social Engineering:
 - Phishing
 - Vishing
 - Impersonation
- Measures how well People identify SE attacks -

ACCOUNTING > CONSULTING > TAX









Example Phishing



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

Hi,

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

Survey

Thanks!

ACCOUNTING > CONSULTING > TAX











Mon 26/06/2017 11:42 AM

Linkedin Updates <messages-noreply@portal-linkedin.com>

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

inked in "	
respond?	would like to connect on LinkedIn. How would you like to
2	Associate Director, IT, ITIL, I Corporation
are receiving Reminde	emails for pending invitations. Unsubscribe

Figure 2: Email 'being forwarded' to the recipients

ACCOUNTING > CONSULTING > TAX









Example 1: Phishing

Sign In to Online Ban	king for Busi	iness		
Customer ID:				
User ID:				
Password:				
	Forgot my passy	word		
Sign In				
			usteer	
		Secure Y	our Browser	

ACCOUNTING > CONSULTING > TAX





Page 31



Use the hover technique

Hi Everyone,

Due to the recent weather events in the Miami are numbers on whether or not you will be ettending. located on The uid=Imnofhbx lease clic Click or tap to follow link.

http://agm.mnp.ca

The AGM website is accessible to partners only and attendance.



Never click on URL's sent in emails...if you must, make sure you "hover" over the URL to see the REAL destination





	Hello, my name is XXXXX. I attached. I look forward to s Sincerely yours, XXXXX	Resume eeing you.
Thu 13/07/2017 8:28 A	M	
SF	@yahoo.com>	
\bigcirc	Resume	
o 🥝 Danny Timmins		
etention Policy MNP Deleted Items 30 d	lays (30 days)	Expires 12/08/2017
This item will expire in 5 days. To You forwarded this message on 1.	keep this item longer apply a different Retention Policy. 3/07/2017 6:02 PM.	
Pdf 439 KB		
Hi Dan,		

Please find attached a copy of my resume. I would like to learn more about MNP and current opportunities within the marketing team.

Thanks and have a good day,







Example 5: Fake AV / Cryptolocker



ACCOUNTING > CONSULTING > TAX



Page 34



The following are some of the FAKEAV programs that the KOOBFACE botnet pushes:

- Safety Center. This offers two types of license:
 - One-year license: This is worth US\$59.95.
 - Lifetime license: This is worth US\$79.95.





Page 35

How Strong is Your Password?

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!

ACCOUN

TEST YOUR PASSWORD SKILLS!

2







Executive Wire Fraud

Social Engineering w/o Malware

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



5 Votes



Social Engineering Attackers Deploy Fake Social Media Profiles



ASHLEY Woods

Manager, Customer Support at EPAM - DEP

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

Dallas, Texas | Computer Software

- Previous JP Morgan FCS, Teradata Aster
- Education University of Dallas

Accept invitation

Scare

Send ASHLEY InMail

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



ACCOUNTING > CONSULTING > TAX











Tip #3 – Google Images

- Use Google Images to verify and validate pictures





٩





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 NBCaffiliate 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.











What is Red Teaming?

- **Contains aspects of Penetration Testing and Social Engineering**
- Performed with the permission of the owner \bullet
- Typically full-scope, multi-layered attack simulation
 - Penetration Testing
 - Social Engineering
 - Physical Security Controls
- Designed to measure resiliency of People, Network(s), and ullet**Application(s) during a real-life attack**
- Attacks are performed simultaneously ullet
- **Overall goal to identify gaps and improve Incident Response** ${\color{black}\bullet}$



Page 41



Considerations



ACCOUNTING > CONSULTING > TAX





Page 42

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 infrastructure to protect your organization and maintain your clients' confidence?

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

ACCOUNTING > CONSULTING > TAX



Can you demonstrate a solid Cyber Incidence 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 (Virtual Chief Information Security Officer-VCISO) to help set standards and policies?

Do you have a clear understanding of your Supply Chain/Vendor/Third Party Management Strategy & Contracts; beginning with the IT focused contracts?

ACCOUNTING > CONSULTING > TAX



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

ACCOUNTING > CONSULTING > TAX



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

Do you have a patching and shadow IT strategy? Two of the biggest problems that exist in Cyber Security today.



Page 46



Cyber Security Services

Offensive Security (Red Team)

- **Penetration Testing**
- **Blended Threat Attack Exercises**
- Social Engineering
- **Vulnerability Assessments**

Defensive Security (Blue Team)

- Enterprise Network Security
- Network, Wireless and Security Architectural Design
- Perimeter and Data Center Security
- Data Loss Prevention and Data Encryption
- Email / Web Content Filtering and Malware Protection
- Secure Access and Authentication
- End Point Security and Encryption
- Wireless, BYOD and Network Access Control
- Security Hardening Standards and Guidelines
- Virtualization and Cloud Computing Standards and Guidance
- Security Awareness Training

Forensics

- Data Retrieval from hard drives, servers, laptops, cell phones, etc.
- E-Discovery Service for Court Admissibility

Risk Management

- Quantitative Threat and Risk Assessment (based on probabilities and industry statistics
- Qualitative Threat and Risk Assessment (based on matrix approach)
- **Cloud Security Checklist**
- **Privacy Impact Assessments**
- MTA (Maturity Threat Analysis)
- Information Security Framework Development
- Assessment and Review against ISO27k, NIST, CSF or CSC 20
- Policy, Process, Procedure and Documentation Development

Payment Card Industry (PCI) Compliance

- Scope Discovery
- Gap Analysis and Readiness Review
- On Demand Consulting and Remediation
- PCI Report on Compliance Validation (ROC)
- PCI SAQ Review and Sign Off
- **External ASV Scanning**
- Annual Maintenance (Business as Usual)

Managed Services

- Cyber Security Administration
- Perimeter Threat Prevention (firewall, IPS, anti-virus, web application firewalls, etc.)
- 2-Factor Authentication
- Log Management





Questions?

Danny Timmins National Leader Cyber Security

Danny.Timmins@MNP.CA

