Cybersecurity Risk Management for Municipalities

David Bruyea - CIBC

Senior Vice-President, Chief Information Security Officer and Chief Security Officer

Note:
This presentation is for informational purposes only and should not be treated as comprehensive. Your circumstances may require you to engage an independent security specialist to ensure suitable best practices are engaged by your organization.

Biography

David Bruyea has over 30 years of Financial Services experience in Canada and the United States. David joined CIBC as a full time employee in 1988 and has held a variety of business, technical and executive management positions within the Bank.

David's current role at CIBC is Senior Vice-President and Chief Information Security Officer and Chief Security Officer. In this role, he uniquely combines the disciplines of Information Security, Physical Security and the management of several other operational risk types within CIBC to support CIBC's business strategy.

David holds a Bachelors Honor's Cooperative degree in Mathematics/Computer Science - Business Administration Option from the University of Waterloo.

Agenda

1. In the news
2. Who & what to be worried about?
3. Who are the targets?
4. Five cyber and fraud scenarios to watch out for
5. Protecting your organization: Where to start?
6. How to protect my organization? A few practical tips…
7. Final thoughts
8. Q&A

In the news…

Cyber attacks and security incidents continue to increase; profit-motivated criminals looking to steal money or data, or impact your operations

THE GLOBE AND MAIL

Ontario Provincial Police warn of **ransomware attacks** on municipal governments (Sept 2018)

CBC

FBI charges men in 2016 **ransomware** attack on University of Calgary (Nov 2018)

CTV NEWS

Capital One target of massive **data breach**; 6 million Canadians impacted (July 2019)

MONTREAL GAZETTE

Desjardins: Rogue employee caused **data breach** for 2.9 million members (June 2019)

STRATFORD THE BEACON HERALD

Personal information safe after **cyber-attack** at Stratford city hall (Apr 2019)

SEAWAY NEWS

Cornwall's cyber infrastructure **attacked daily** (July 2019)

Global NEWS

Town of Midland back to normal operations after **cyberattack** (Sept 2018)

OTTAWA CITIZEN

Hackers swarm around Ottawa City Hall (Aug 2019)

CBC

Statistics Canada says the national rate of **police-reported extortion rose 44 percent** in 2018 (Jul 2019)

NATIONAL POST

City of Burlington falls for $503,000 **phishing scheme** (June 2019)

Who & what to be worried about?

Threat Actors

- Nation States
- Hackers & Hacktivists
- Organized Crime
- Insiders (malicious, or non-malicious)

Attacks are often simple; clicking on a link in an email or surfing the internet leads to a virus or ransomware

Tactics and Threats

Social Engineering

- **Phishing (email, voice, text)**
- **Spear-Phishing**
- Eavesdropping
- Tailgating
- Baiting (eg. USB keys)
- Dumpster diving

Malware / Virus

- **Malicious Software**
- **Ransomware**
- Spyware
- Worms
- Key loggers
- Watering holes
- Trojan horses

Insider threats

- **Malicious and non-malicious insiders**
- **Poor security hygiene**
- Data leakage (theft) or data corruption

Denial of Service

- Distributed Denial of Service (DDoS)
- “Botnets”

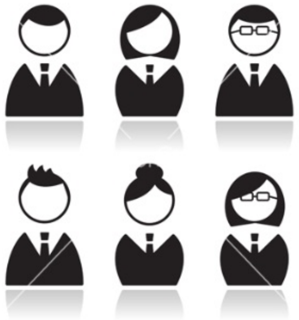
Exploits

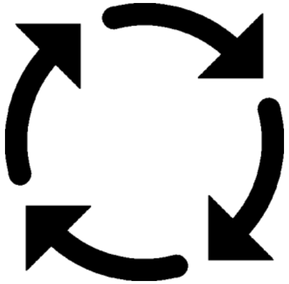
- Code that takes advantage of software vulnerabilities
- “Zero-day” exploits

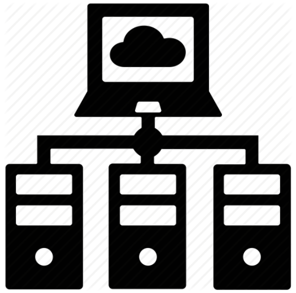
Who are the targets?

Attacks target **all dimensions** of the organization, leveraging both cyber and traditional fraud techniques.

People	Processes	Technology
Social engineering, Insider threats (malicious or human error)	Learn your processes and supply chain to exploit weaknesses	Exploit vulnerabilities in systems, attack highly protected assets







Five cyber & fraud scenarios to watch out for

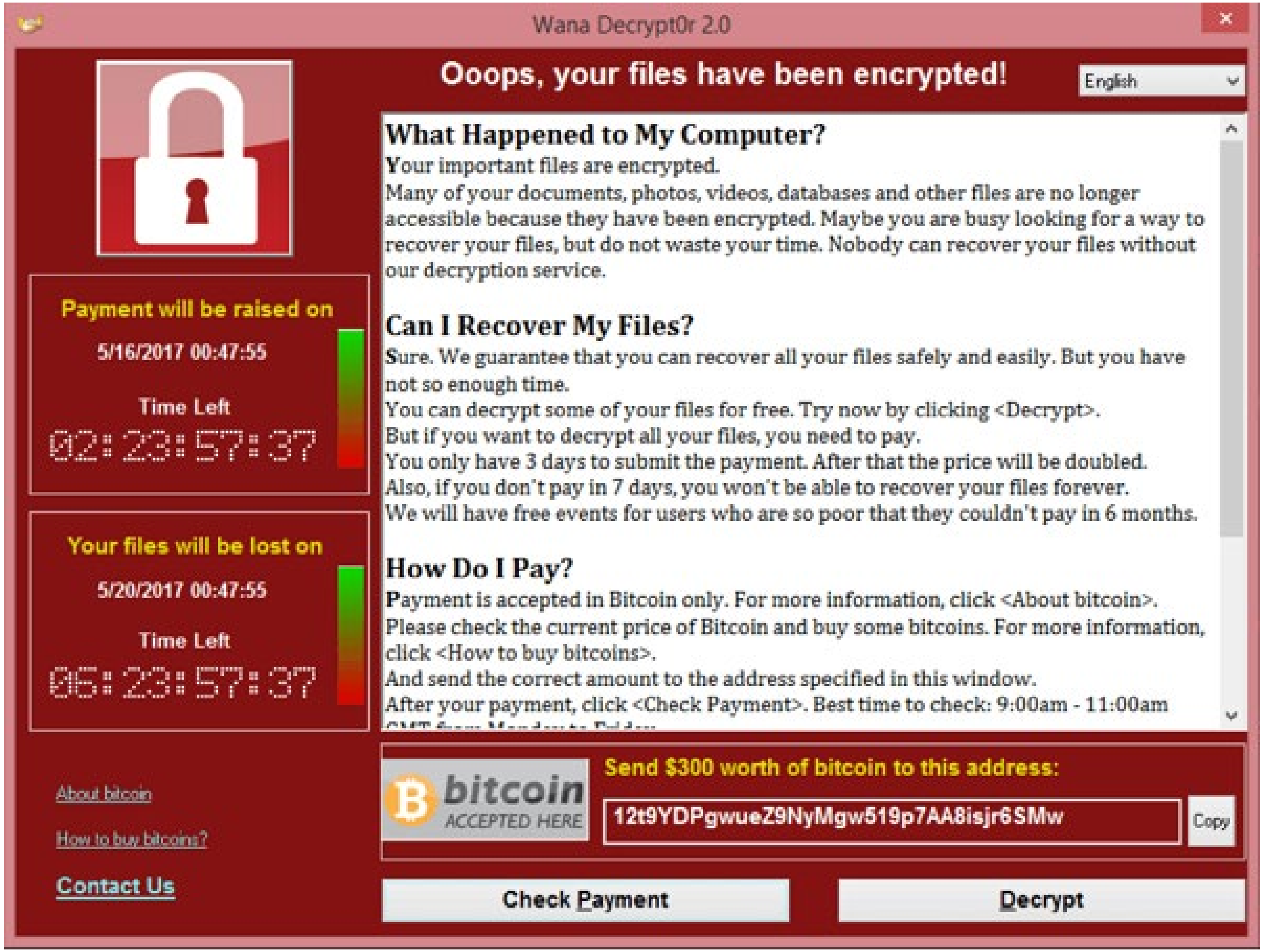
1 Social Engineering, Phishing & Malware

- Tactic is not going away; cost-effective attack vector for cyber criminals
- Includes both general (commodity) and targeted phishing
- Leverage social media (eg. LinkedIn) to learn about potential targets
- **Goal: extortion (ransomware, or business disruption), steal data or commit fraud (eg. malware or keyloggers to track your actions)**

TIPS:

- Layers of security defense are required; both technical controls and a strong cyber resilient employee culture
- Security awareness & education:
  - **“Trust but verify”**
  - Phishing simulations, educating on phishing/cyber threats
  - Managing your social media (what and who you share data with)
  - Protecting your passwords
  - How to report an incident (real or suspected)

Example: ransomware (extortion to ‘unlock’ or decrypt your data)



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

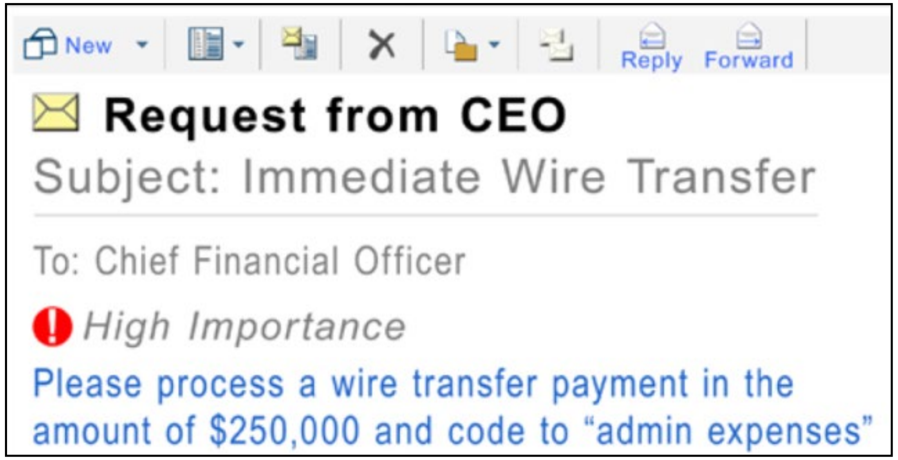
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

- Screenshot of WannaCry ransomware, May 2017
- Infected ~200K computers across 150 countries
- Cybercriminals leverage crypto-currencies (eg. BitCoin) for payment to maintain anonymity

Five cyber & fraud scenarios to watch out for

2 Transaction Instruction or Wire Payment Fraud

- “**Business Email Compromise**” scenarios, impersonation of…
  - **CEO:** email to lower level employee to transfer money
  - **Supplier**: request to change banking information with invoice to be paid
  - **Employee**: email to HR requesting change in payroll information



Request from CEO

Subject: Immediate Wire Transfer

To: Chief Financial Officer

! *High Importance*

Please process a wire transfer payment in the amount of $250,000 and code to “admin expenses”

TIPS:

- Verify payment instructions via a trusted alternative method
- Ensure key employee groups are aware of fraud schemes, and know how to handle urgent requests
- Require multiple approvers for high risk transactions
- Strong vendor governance; periodic validation of contact info

FBI Report (May 7, 2018): BEC is the top internet crime in reported dollar loss ($676MM in 2017) [1]

[1] FBI Internet Crime Report. https://www.fbi.gov/news/stories/2017-internet-crime-report-released-050718

Five cyber & fraud scenarios to watch out for

3 Cheque Fraud

- Intercepted cheques that are altered, counterfeited, or forged
- <u>TIPS:</u>
  - Ensure physical cheque stock is secured, don’t use window envelopes
  - Segregate duties in payment processes
  - Leverage digital banking services

4 Overpayment Fraud

- Fraudster impersonates vendor, advises they have “wired” too much money and requests a repayment. The “wire” is really a fake cheque (or no payment), and client wires back the overpayment before validating.
- <u>TIPS:</u>
  - Be cautious when dealing with overpayments
  - Wait for cheque or money order to clear before processing anything

5 Internal Fraud

- Varies by industry and type of company, eg. “book-keeper” fraud, shrinkage, point-of-sale fraud, etc…
- <u>TIPS:</u>
  - Eliminate “single trust” points for high risk processes/functions
  - Ensure processes account for vacations, emergencies, etc…

Protecting your organization: where to start?

Risks to Data

- Loss, compromise or misuse of sensitive, confidential data (client, intellectual property)
- Unauthorized access to systems

Risks to System Availability

- Business disruption; cyber attack on key systems (applications, databases, services)

Risk of Fraud

- Manipulation of people or systems leading to fraudulent transactions or market manipulation

Understanding your key risk scenarios allows organizations to tailor their defenses better and focus in on key areas, networks or systems

(a risk-based approach)

How to protect my organization? A few practical tips…

There is no silver bullet to defend against cyber and fraud attacks.
A comprehensive, balanced approach is required. Some examples:

Foundational Cybersecurity Practices

- Basic security controls go a long way (eg. anti-virus, anti-malware, patching, security monitoring)
- Build a security and fraud awareness culture: educate your employees
- Classify your data, know where it is (internally and externally), and protect it
- Limit access to information (who is allowed to do what)

Protect from Fraud & Insider Threats

- Ensure clear accountabilities/ownership of controls
- Consider your risk appetite: what is a low vs high value account or transaction?
- Enforce segregation of duties; use multiple approvers for high risk accounts/transactions
- Consider the need for personnel screening

Final thoughts…

- ✓ **Build resilience in your organization:** measure and test your processes and systems, including business continuity plans. It is not a matter of "if" but "when" an incident will happen.
- ✓ **Be ready to adapt:** safeguarding your company is an ongoing challenge as the threat, business/technology and regulatory landscape is constantly evolving.
- ✓ **Engage Senior Leadership and the Board:** Cybersecurity and Fraud **must** be on their agenda.
- ✓ **Get help:** external cyber and fraud expertise can deliver capabilities for you.

A few public resources:

- Canadian Anti-Fraud Centre (CAFC)
- Public Safety Canada: Get Cyber Safe, Enhancing Canada's Critical Infrastructure Resilience to Insider Risk
- Aligning your capabilities to industry frameworks (eg. NIST Cybersecurity Framework)

Note:
This presentation is for informational purposes only and should not be treated as comprehensive. Your circumstances may require you to engage an independent security specialist to ensure suitable best practices are engaged by your organization.

Q&A

GREAT QUESTION!