Aon Cyber Solutions

SARM ANNUAL CONFERENCE

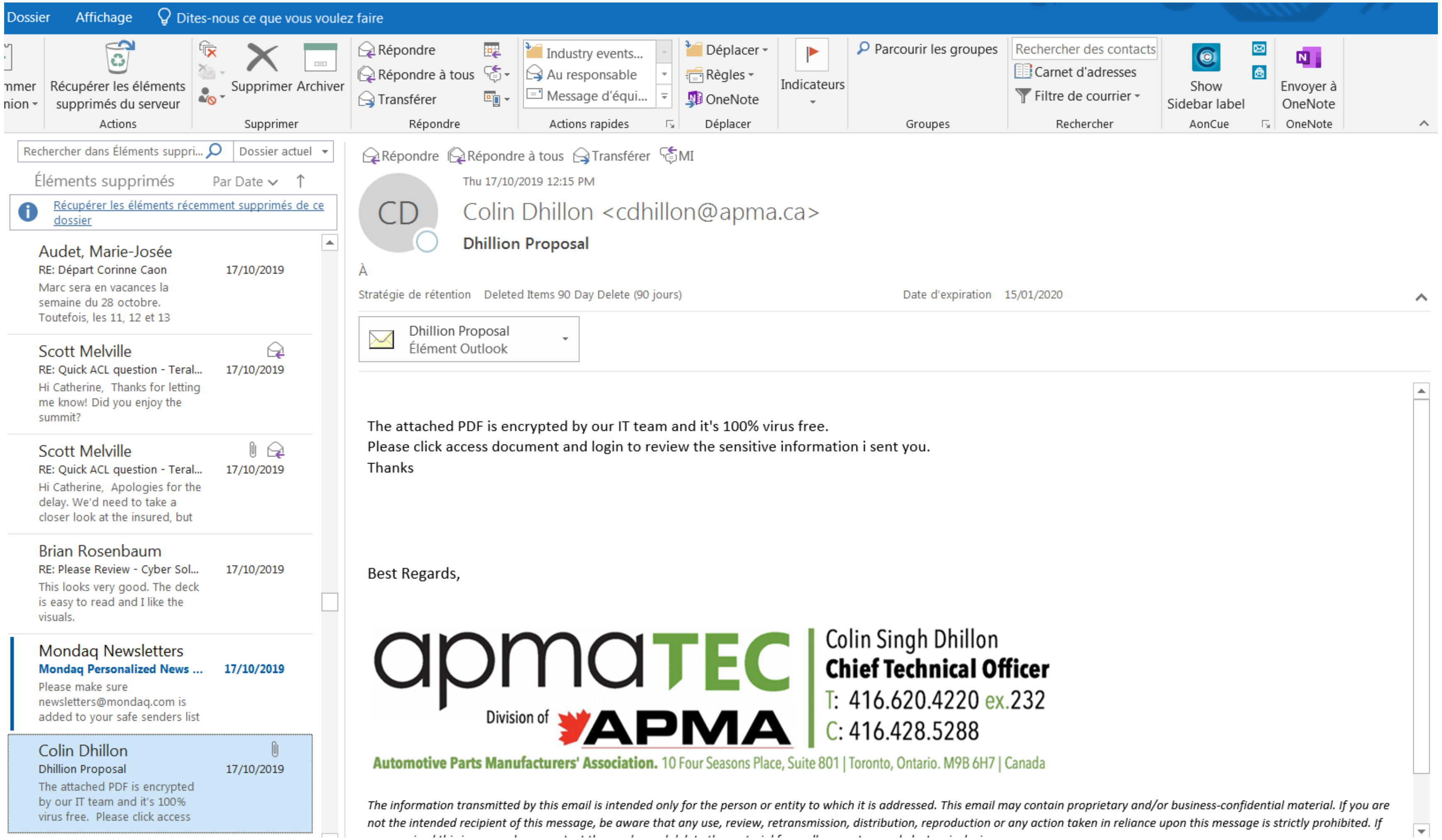
MARCH 9th 2020

Agenda

1. Acceleration of cyber threats
2. Threat topography
3. What it means for municipalities
4. What data is at risk
5. Pillars to Cyber Resilience
6. What to do if you experience a breach
7. Quick overview of the cyber insurance policy

Acceleration: or what is a « Viral Infection »

Hackers are more sophisticated



Audet, Marie-Josée
RE: Départ Corinne Caon 17/10/2019
Marc sera en vacances la semaine du 28 octobre. Toutefois, les 11, 12 et 13

Scott Melville
RE: Quick ACL question - Teral... 17/10/2019
Hi Catherine, Thanks for letting me know! Did you enjoy the summit?

Scott Melville
RE: Quick ACL question - Teral... 17/10/2019
Hi Catherine, Apologies for the delay. We'd need to take a closer look at the insured, but

Brian Rosenbaum
RE: Please Review - Cyber Sol... 17/10/2019
This looks very good. The deck is easy to read and I like the visuals.

Mondaq Newsletters
Mondaq Personalized News ... 17/10/2019
Please make sure newsletters@mondaq.com is added to your safe senders list

Colin Dhillon
Dhillion Proposal 17/10/2019
The attached PDF is encrypted by our IT team and it's 100% virus free. Please click access

Thu 17/10/2019 12:15 PM
Colin Dhillon <cdhillon@apma.ca>
Dhillion Proposal

Stratégie de rétention Deleted Items 90 Day Delete (90 jours) Date d'expiration 15/01/2020

The attached PDF is encrypted by our IT team and it's 100% virus free.
Please click access document and login to review the sensitive information i sent you.
Thanks

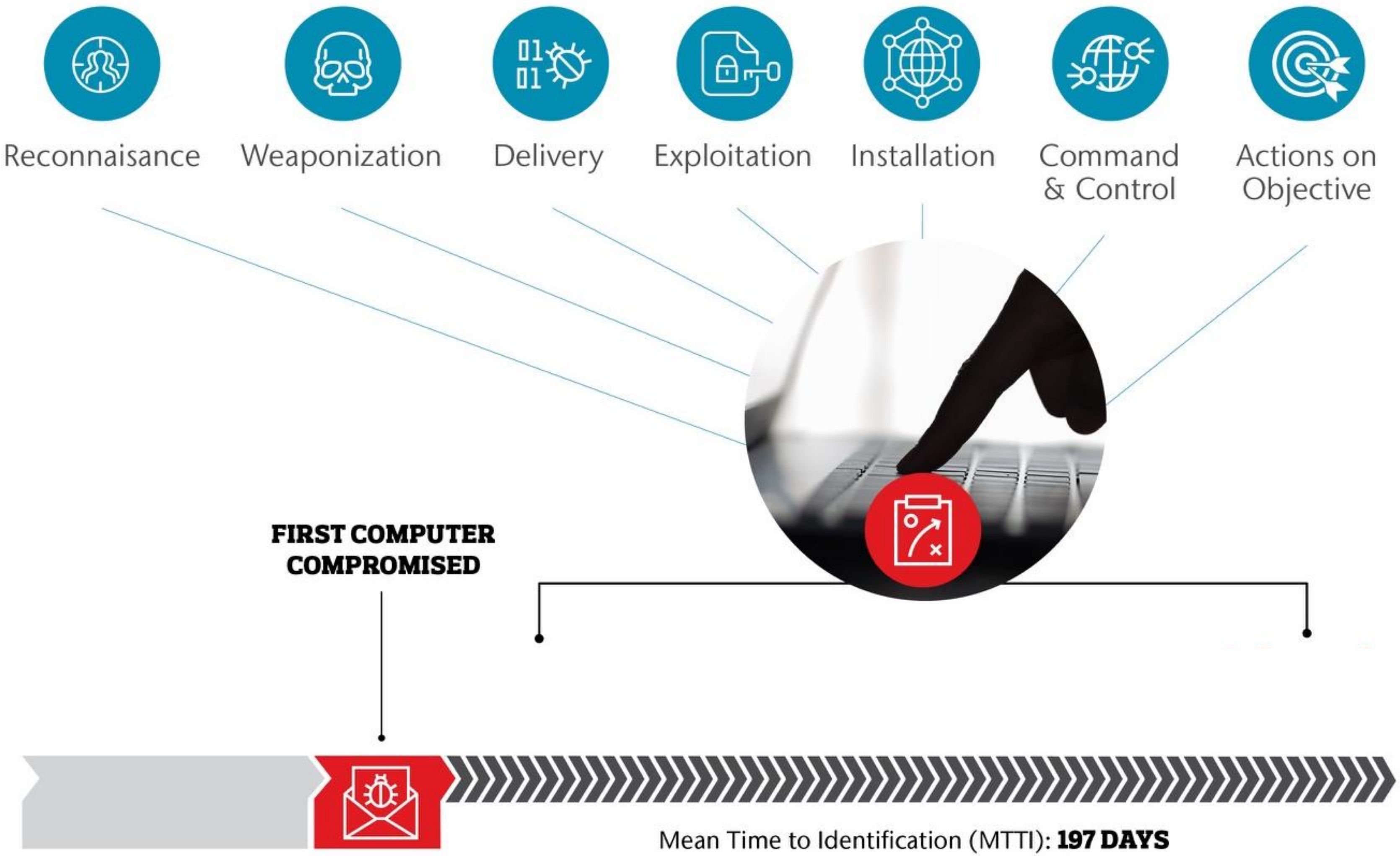
Best Regards,

apmaTEC
Division of APMA

Colin Singh Dhillon
Chief Technical Officer
T: 416.620.4220 ex.232
C: 416.428.5288

Automotive Parts Manufacturers' Association. 10 Four Seasons Place, Suite 801 | Toronto, Ontario. M9B 6H7 | Canada

The information transmitted by this email is intended only for the person or entity to which it is addressed. This email may contain proprietary and/or business-confidential material. If you are not the intended recipient of this message, be aware that any use, review, retransmission, distribution, reproduction or any action taken in reliance upon this message is strictly prohibited. If



Reconnaisance

Weaponization

Delivery

Exploitation

Installation

Command & Control

Actions on Objective

FIRST COMPUTER COMPROMISED

Mean Time to Identification (MTTI): **197 DAYS**

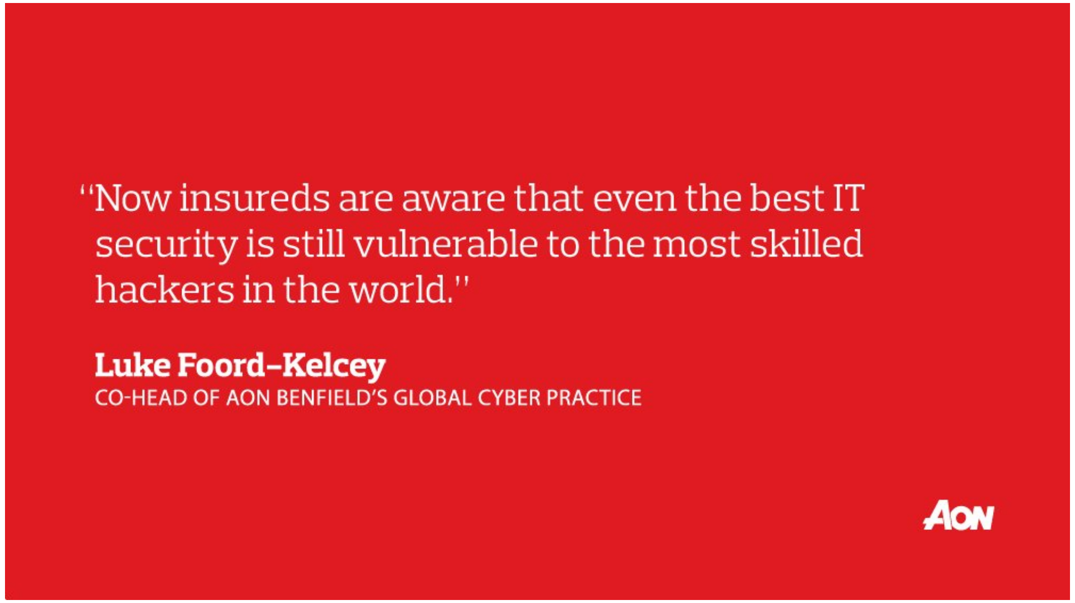
Mean Time to Containment (MTTC): **69 DAYS**

2018 Cost of Data Breach Study: Impact of Business Continuity Management
Benchmark research sponsored by IBM | Independently conducted by Ponemon Institute LLC

We are not in Kansas anymore…

If cybercrime was a country, it would rank 13th in GDP

(Cybercrime report by Bromium & McGuire, according to 2018 GDP data from the World Bank)



"Now insureds are aware that even the best IT security is still vulnerable to the most skilled hackers in the world."

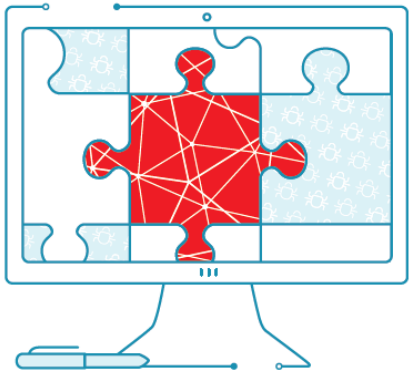
Luke Foord-Kelcey
CO-HEAD OF AON BENFIELD'S GLOBAL CYBER PRACTICE

Acceleration of cyber threats

1. Cyber attacks are increasing in frequency and magnitude

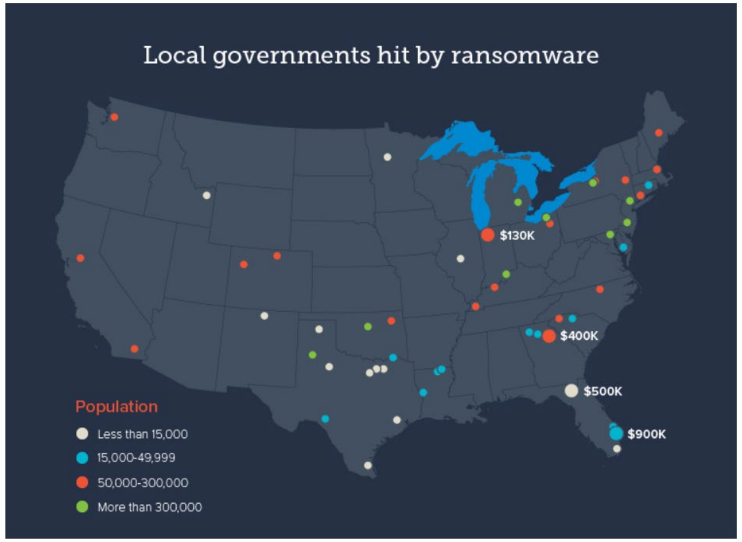
2. Cyber crime is an economy

3. Influence of the socio-political context



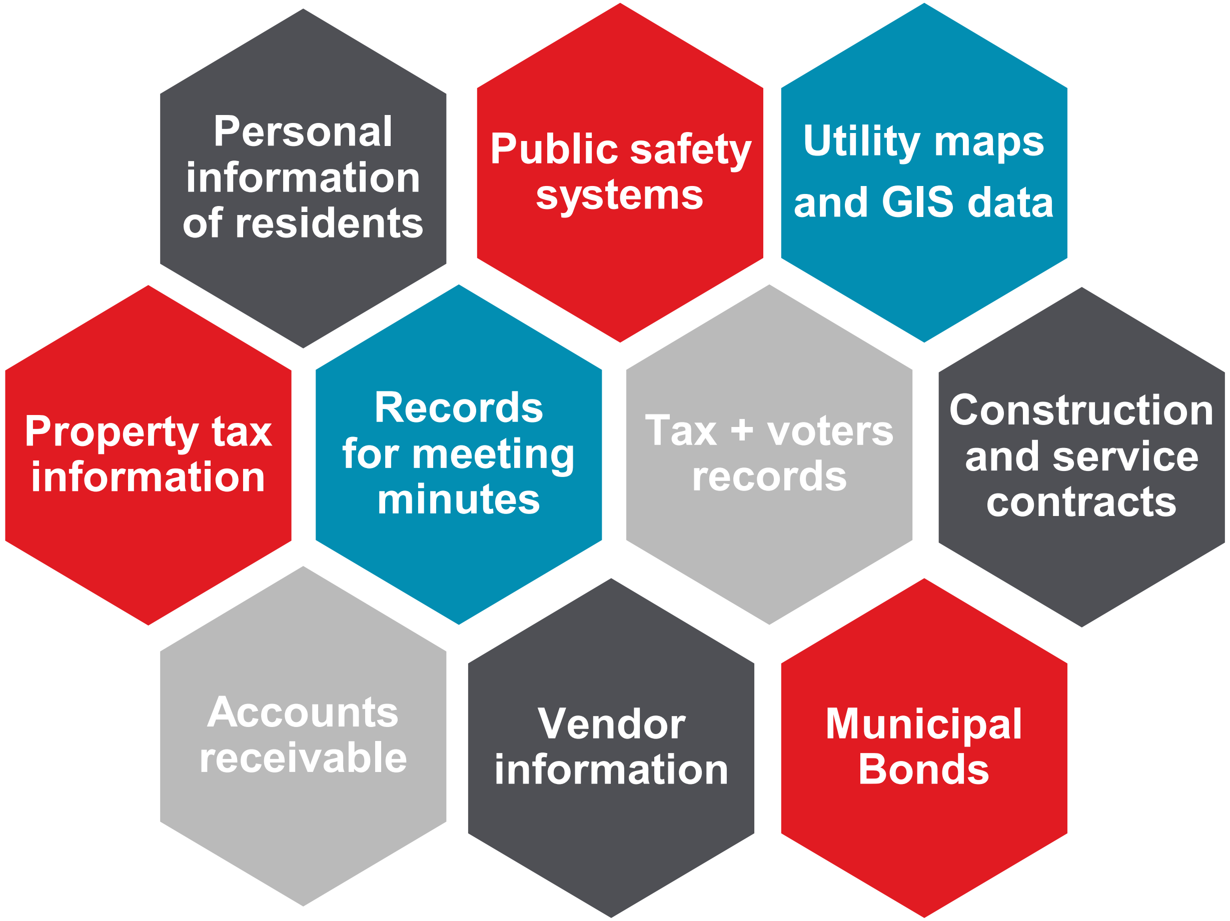
What it means for Municipalities

- 1 in 4 local governments will fall to ransomware
- Ransomware hit over 70 US municipalities (Jan to Sept 2019)
- 24% were municipalities of populations under 15,000



Source: US statistics from IT security firm Baracuda Networks

What data is at risk



Personal information of residents

Public safety systems

Utility maps and GIS data

Property tax information

Records for meeting minutes

Tax + voters records

Construction and service contracts

Accounts receivable

Vendor information

Municipal Bonds

Case Study: Ontario Municipality Ransomware attack in 2018

Ransom Payment	$34,950
Computer Consultants	$37,181
Physical Security Vendor	$4,725
IT Purchases	$1,901
Third-Party Software Vendors	$9,590
Internal Staff Overtime	$31,370
Internal Productivity Losses	$132,042
Total Cost of Ransomware Incident	**$251,759**

Source: CTV News. 24 July 2018 and Canadian Municipal Government Meeting Agenda (24 July 2018)

Pillars to Cyber Resilience

Assessment

Baseline understanding of all network and system vulnerabilities.

Prevention

Best practices to reduce the likelihood and potential damage of a cyberattack.

Response

Prompt and efficient response to reduce the impact of a cyber incident.

Assessment

CYBER CENTRE **LEARNING HUB**

FOSTERING EXCELLENCE IN CYBER SECURITY

Canadian Center for Cyber Security

NIST National Institute of Standards and Technolc
U.S. Department of Commer

CYBER ESSENTIALS

Assessment: Managed Service Provider (MSP attacks)

- We are back to a feodal system
- APT10 (China) and other State-Sponsored actors = MONEY
- Victims include:
  - IBM, CGI, Rio Tinto, American Airlines, Deutsche Bank, Allianz SE, …

Prevention

- How to maximize IT security with limited budgets?
- Better spending money on cyber hygiene, than lawyers or ransoms.

Good quality cyber hygiene

- Password management
- Stay current on security updates
- Regular backups
- Awareness and education
- If it is suspicious… investigate!
- Insurance (crisis response)

Prevention: What makes a strong password

- Unique
- Hard to guess
- At least 10 characters
- Mix of upper and lower cases
- Letters, numbers and symbols

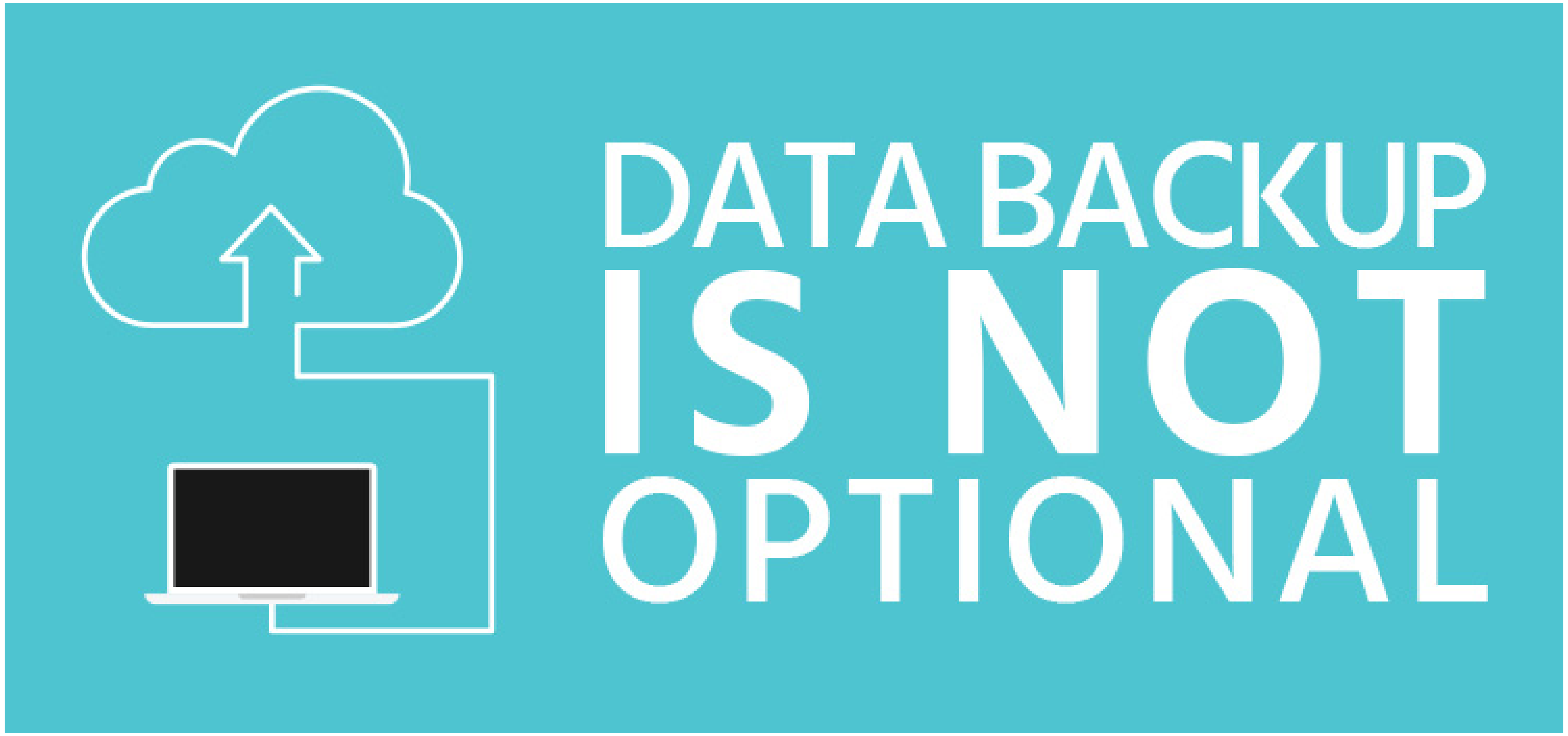
Hint: this is also valid for “at home” devices and systems!

Prevention: Strong password example

MsitB&ho7!

Passphrase: **M**y son is the **B**est & he’s only 7 !

Prevention: Regular backups



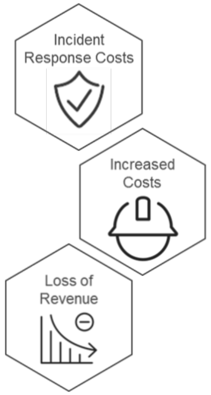
Response: What to do if you experience a breach

- Legal advice (*Breach coach*)
- Expert IT investigation (*Forensic*)
- Notification and call center
- Mitigation (ID tefth and credit monitorign)
- PR and communication experts

Quick overview of the cyber policy

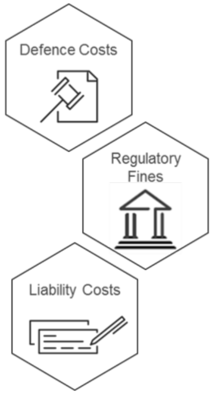
First party

- Incident Response
- Cyber extortion
- System Damage and digital asset restoration
- Network Business Interruption / Dependent BI
- System Failure

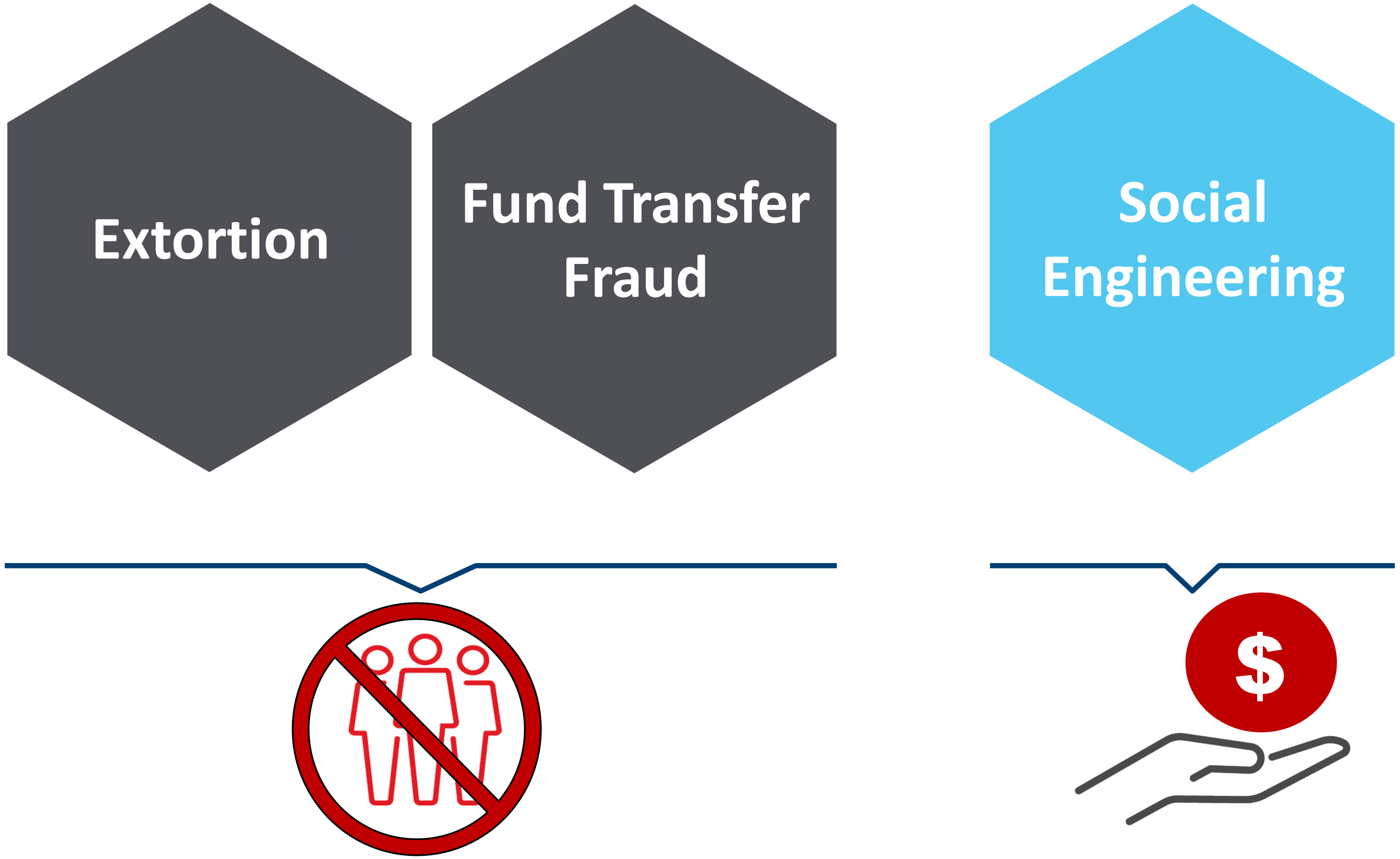


Third party

- Network Security and Privacy Liability
- Privacy Regulatory Fines and Penalties
- Media Liability
- PCI Fines and Penalties
- Breach Event Expenses (notification, credit monitoring)



Cyber policy answer to cyber crime



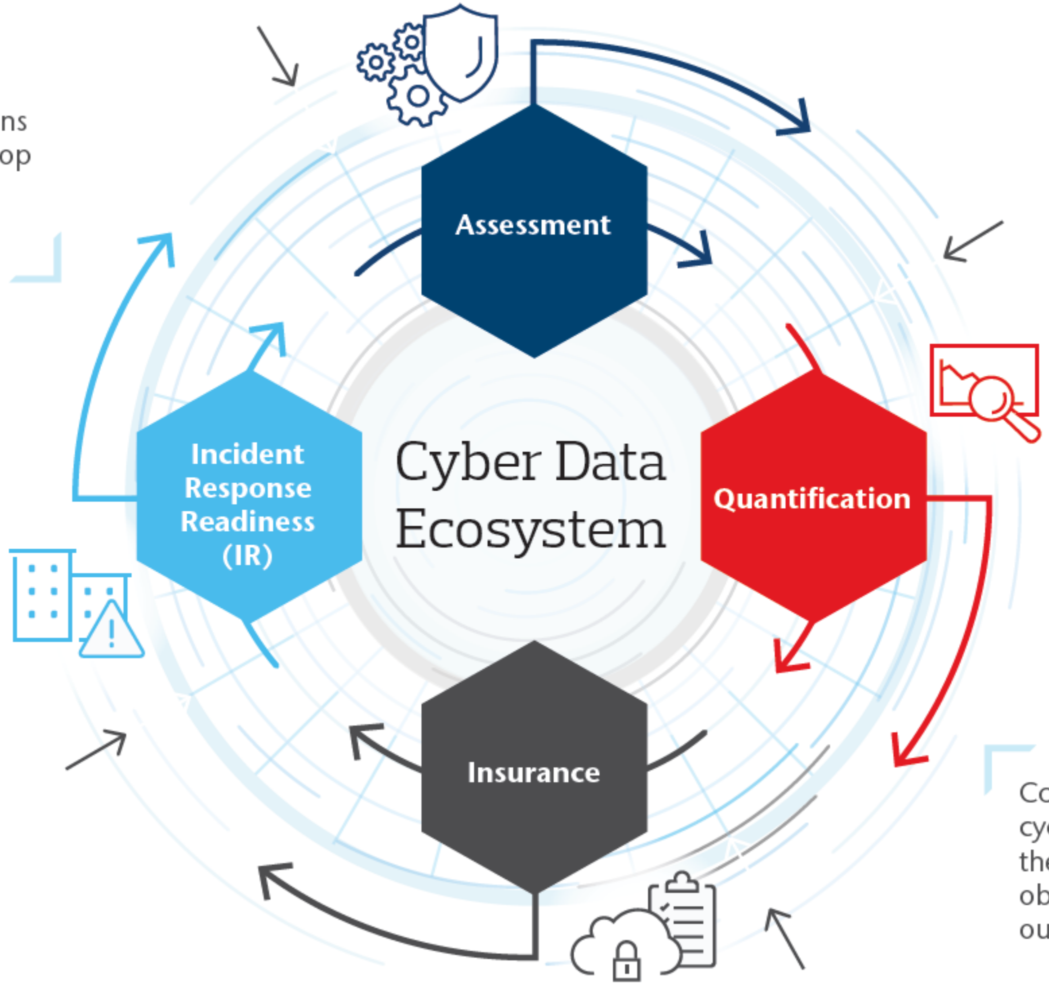
Extortion

Fund Transfer Fraud

Social Engineering

In Conclusion

Organizations enter the loop at different points.



Continuously cycle through the loop to obtain better outcomes.