Marsh

Cyber Security: Lessons learned from 2020 - 2022

Ransomware, security controls, and insurance

Friday, October 14, 2022

A business of Marsh McLennan

Today’s panelists

Julien Ducloy

Senior Vice President,
Marsh Advisory – Cyber Practice Lead

Anupam Rawla

Consulting Director,
Marsh Advisory – Consulting Solutions

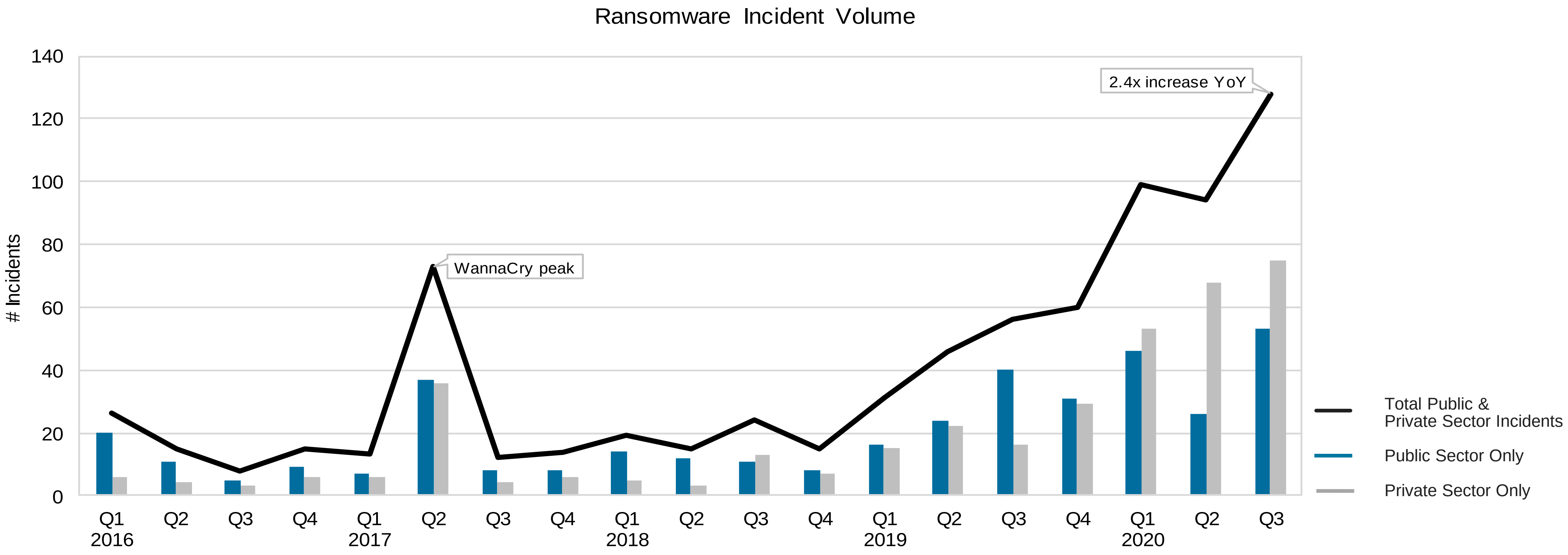
Agenda

1. Cyber Risk Environment
2. Insurance Industry Response
3. Cyber controls: What organizations need and why
4. Examples of Cyber Attacks
5. Zoom on Cyber Incident Best Practices

Cyber Risk Environment

Ransomware Incident Frequency Increased Significantly

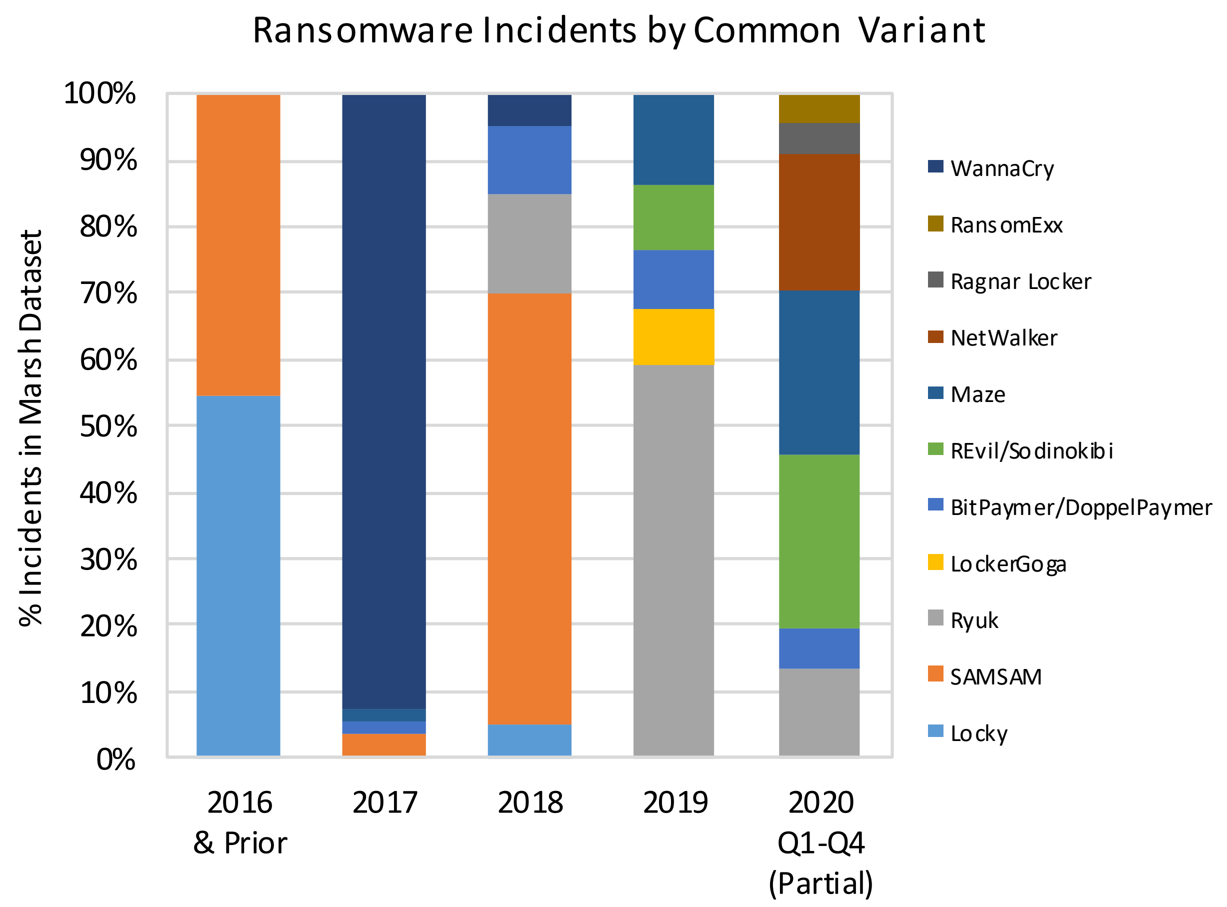
Year-over-year increase in incidents impact both public and private sectors



Public sector is defined as Healthcare, Government, Not for Profit.

Ransomware: Rising Sophistication & Severity

New & emerging variants and increased loss costs are driving the evolution of underwriting

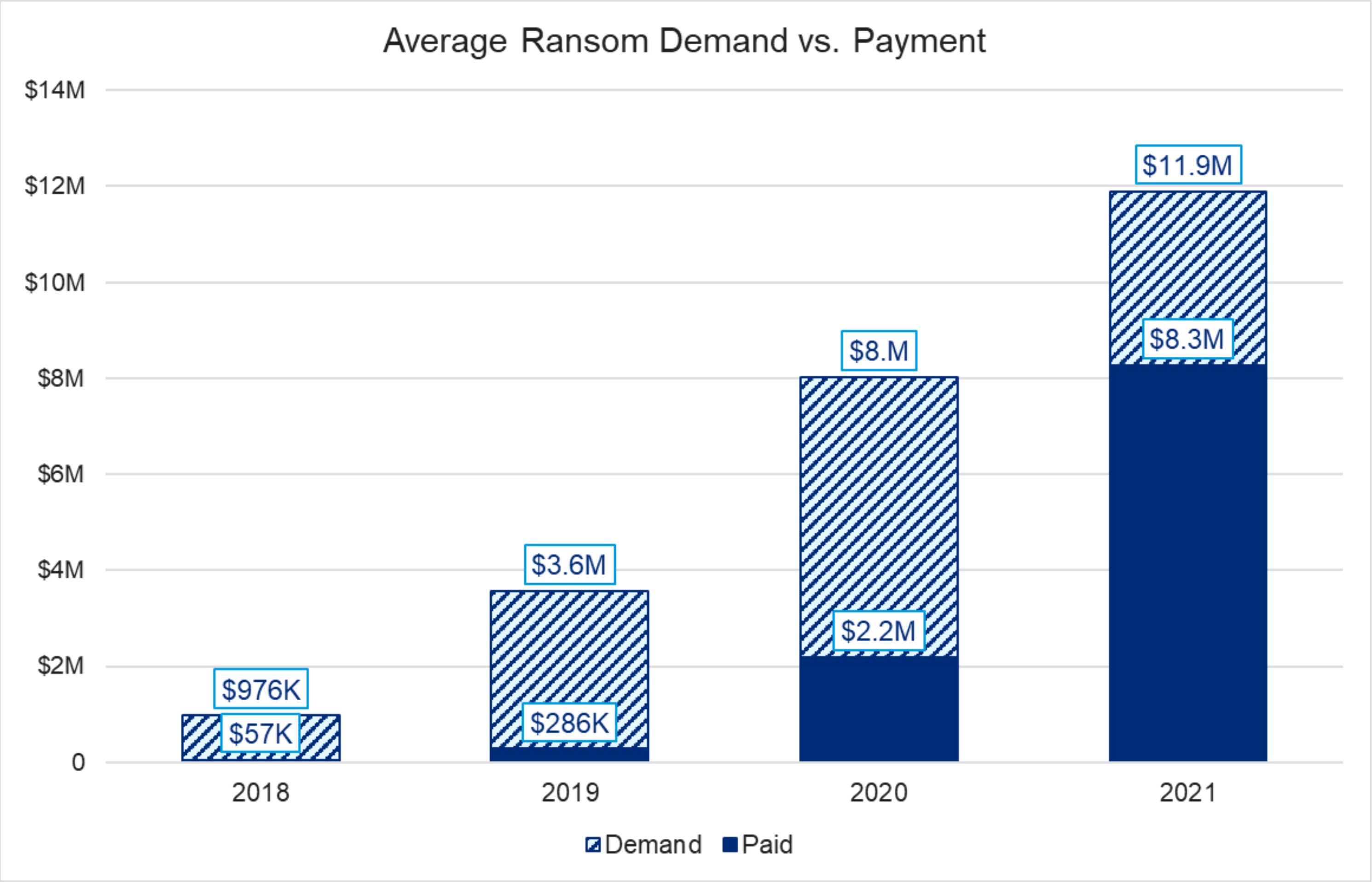


Note: on average, 46% of incidents in the collected dataset are classified as known variants, and 54% of incidents are unclassified and not depicted in this chart.

Q1 2022 Ransomware Update

Ransom Demand vs. Payment

- **The difference between the average ransom demanded and paid** is decreasing as threat actors more effectively attack targets
- **77% of ransomware cases** involved data exfiltration in Q1 2022
- **63% of victims who paid a ransom to prevent dissemination of their compromised data** in Q1 2022 never received evidence that the data was actually deleted
- **Average downtime following an event reached 26 days**, up from 18.2 days in Q4 2021
- **$211K was the average ransom payment** for small to mid-sized companies in Q1 2022
- **86% of victims** reported that the attack they suffered caused a loss of business and corresponding revenue



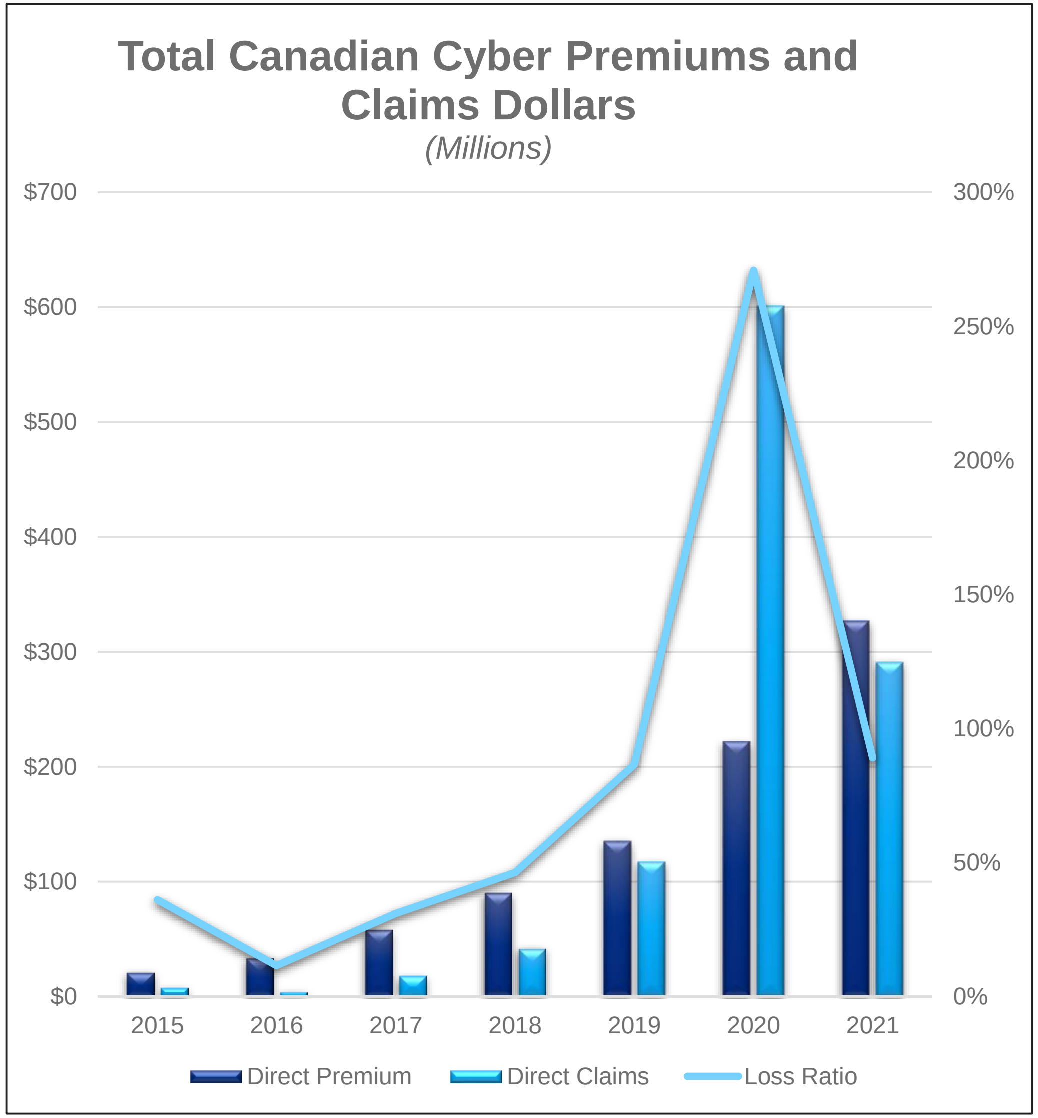
Source: MMC Cyber Risk Analytics Center

Marsh

Additional sources: Coveware Blog Q1 2022; Sophos

Insurance Industry Response

Cyber Market Loss Ratios in Canada



Source: OSFI - https://www.osfi-bsif.gc.ca/Eng/wt-ow/Pages/FINDAT-pc.aspx

Cyber Insurance Profitability – Loss Ratios

Sample of 2020 and 2021 Canadian Insurer Cyber Gross Loss Ratios as reported to OFSI

For All Insurers in 2020: ~$601M in direct cyber claims incurred; Only ~$222M in cyber premiums collected

AIG	2020: 223% 2021: 86%
Allianz	2020: 258%***
AXA XL Insurance Reinsurance	2020: 52% 2021: 32%
AXIS	2020: 41% 2021: 26%
CHUBB®	2020: 104% 2021: 148%

CNA	2020: 133% 2021: 319%
LLOYD'S	2020: 364% 2021: 109%
TRAVELERS	2020: 548% 2021: 187%
ZURICH®	2020: 129% 2021: 68%

Source: Canadian data as reported by the Office of the Superintendent of Financial Institutions

**Gross Loss Ratio = Direct Written Premium/Direct Claims Incurred

***Allianz announced that they will be exiting all financial lines in Canada in order to support their long term sustainability.

Insurers’ Ransomware supplements

The origin of the 12 control areas we highlight

Controls Requested by Insurers:	Insurer 1	Insurer 2	Insurer 3	Insurer 4	Insurer 5
MFA-Controlled Access	✓	✓	✓	✓	✓
Secured & Tested Backups	✓	✓	✓	✓	✓
Patched Systems & Applications	✓	✓	✓	✓	✓
Filtered Emails & Web Content	✓	✓	✓	✓	✓
Protected Privileged Accounts	✓	✓	✓	✓	✓
Protected Network	✓	✓	✓	✓	✓
Secured Endpoints	✓	✓	✓	✓	✓
Logged & Monitored Network	✓	✓	✓	✓	✓
Phishing-Aware Workforce	✓	✓	✓		✓
Managed Vulnerabilities	✓	✓	✓	✓	
Hardened Device Configuration	✓		✓	✓	
Prepared Incident Response	✓	✓			✓

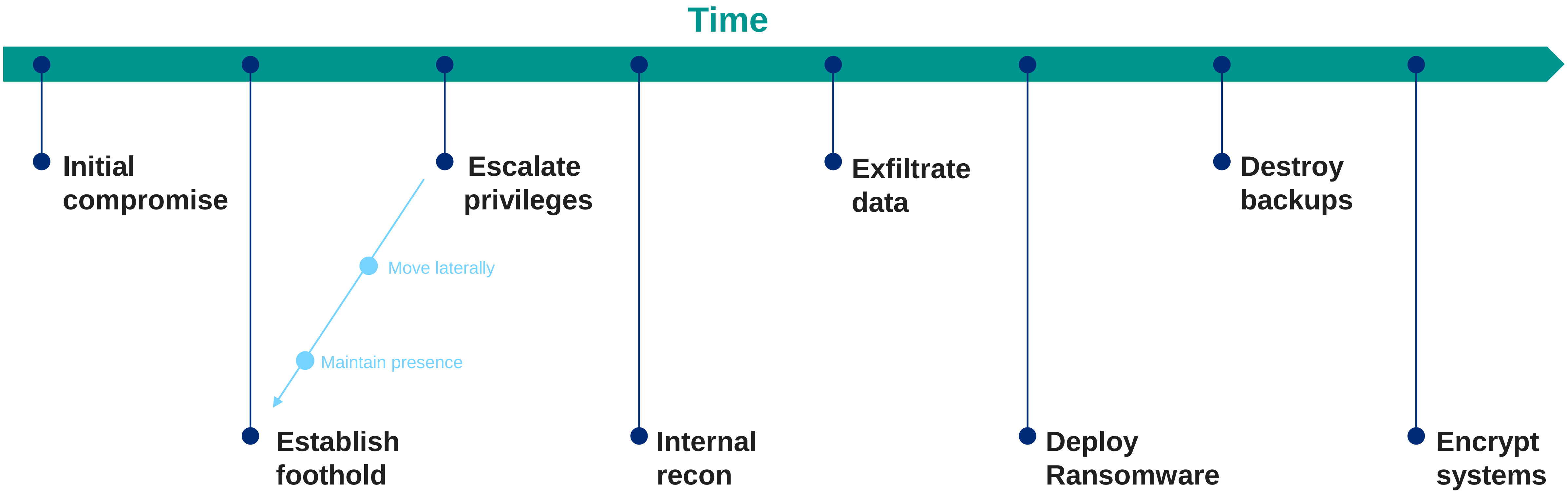
We conducted a detailed analysis of the Ransomware supplemental questionnaires requested by cyber insurers and identified these 12 control areas

Cyber Controls

What are the top cyber controls and why?

Anatomy of a targeted ransomware attack

In the attackers’ shoes



Time

Initial compromise

Establish foothold

Escalate privileges

Move laterally

Maintain presence

Internal recon

Exfiltrate data

Deploy Ransomware

Destroy backups

Encrypt systems

Top 12 Cybersecurity controls

Multifactor authentication for remote access and admin/privileged controls

Endpoint Detection and Response (EDR)

Secured, encrypted, and tested backups

Privileged Access Management (PAM)

Email filtering and web security

Patch management and vulnerability management

Cyber incident response planning and testing

Cybersecurity awareness training and phishing testing

Hardening techniques, including Remote Desktop Protocol (RDP) mitigation

Logging and monitoring/network protections

End-of-life systems replaced or protected

Vendor/digital supply chain risk management

Note: Each insurance carrier has their own specific control requirements that may differ by company revenue size & industry class. For more on the Cyber hygiene see: [Cyber hygiene controls critical as cyber threats intensify (marsh.com)]

Multifactor authentication for remote access and admin/privileged controls

MFA makes login credentials more resistant to:

- Password guessing
- Password compromise
- Brute force attack

Getting access to systems and networks is *exponentially more difficult* with MFA - it requires another level of attack that is not that of ransomware and financially motivated attackers

Endpoint Detection and Response (EDR)

An “endpoint” is a user system or a server

Most of ransomware attacks start on endpoints

EDR is the new AV (Anti-Virus)

The level of protection provided by an efficient EDR is very high

MDR and XDR are the new EDR

Secured, encrypted, and tested backups

Backups are the lifeline of the organization

If backups are lost an attacker has a huge leverage to get the ransom

Secured backups means:

- Offline or “air gapped”
- Protected with MFA
- Access credentials separated from Active Directory (AD)

Recent and tested backups also go a long way to limit BI impact

Privileged Access Management (PAM)

Privileged or Administrative Credentials are the keys to IT kingdom

A ransomware attack cannot be successful without compromising it

These credentials need to be specially protected:

- Protected by MFA or Vault
- Used only when required
- Named accounts only, no generic or “service” account
- Monitored activity

Email filtering and web security

Most of the ransomware attacks come through email attachments, malicious links, or vulnerable web browsers

Attacks can be blocked before they reach the user system (endpoint)

It means:

- Controlling origin of emails
- Filtering attachments and links
- Filtering access to web pages

Patch management and vulnerability management

A vulnerability in a system is comparable to an open door in a facility

Attackers leverage vulnerabilities to get initial access to an organization, or to move laterally inside it and get higher privileges for their attack

Patches' importance depends on how much the related vulnerability could help an attacker – how much it is "exploitable"

Standard recommendations are:

- Critical patches to be applied within 24-72hrs
- High severity patches to be applied within 7 days

Cyber incident response planning and testing

This is equivalent to a building's fire evacuation plan, routes and fire drill

Even if this is a "soft" control the ROI is very significant in case of attack, as good decision making and speed contain the impacts

Bad decision making during a cyber incident leads to:

- Increased incident management costs
- Longer recovery time and higher business impact
- Higher privacy or third party related liability
- Higher reputational impact and loss of clients

Cybersecurity awareness training and phishing testing

The most common tactics hackers use to carry out ransomware attacks are email phishing campaigns, RDP vulnerabilities, and software vulnerabilities - *Cybersecurity & Infrastructure Security Agency, 2021*

It is assumed that 50% of attacks start with a phishing email

It is possible to get a workforce at a high rate of awareness through education and testing campaigns

Hardening techniques, including Remote Desktop Protocol (RDP) mitigation

Hardening systems means to close every door, window, or vent that shouldn’t be open, change factory locks settings and default pin codes, and teach tenants how to handle requests so access is granted only to authorized people

It means having a “secure baseline” for systems and control any change

It reduces the ability of an attacker to hop from system to system

It increases chances to detect attackers as they are slower and noisier

Logging and monitoring/network protections

This is the CCTV, recording system and security guards of the IT

All actions performed on and between systems can be recorded and monitored

Early security incidents and attacks in preparation can be detected, contained and investigated

And even ahead of monitoring – having network protection means:

- Security devices to detect and block attacks (Firewalls, Intrusion Detection/Prevention Systems, EDR, etc.)
- Maintaining different zones with restricted movements between zones (network segmentation)

End-of-life systems replaced or protected

End-of-life (EOL) system means that the manufacturer doesn’t repair it anymore

When a new vulnerability is found (i.e. every day), there’s no more patch

It means that a door is open in your building and you cannot close it – then very convenient for ransomware attackers

For example: Windows 7 is EOL since Jan 2020, when Windows 10 is planned to be supported until 2025

If an EOL system cannot be replaced, it requires specific protection

Vendor/digital supply chain risk management

Supply chain is newest and extremely efficient attack vector

You might have heard of Solar Winds, Accellion and Kaseya breaches

These are large scale supply chain attacks

Attackers gets into one system, generally at a high cost (investment) and then leverage it to get into multiple organizations (10,000’s) at once

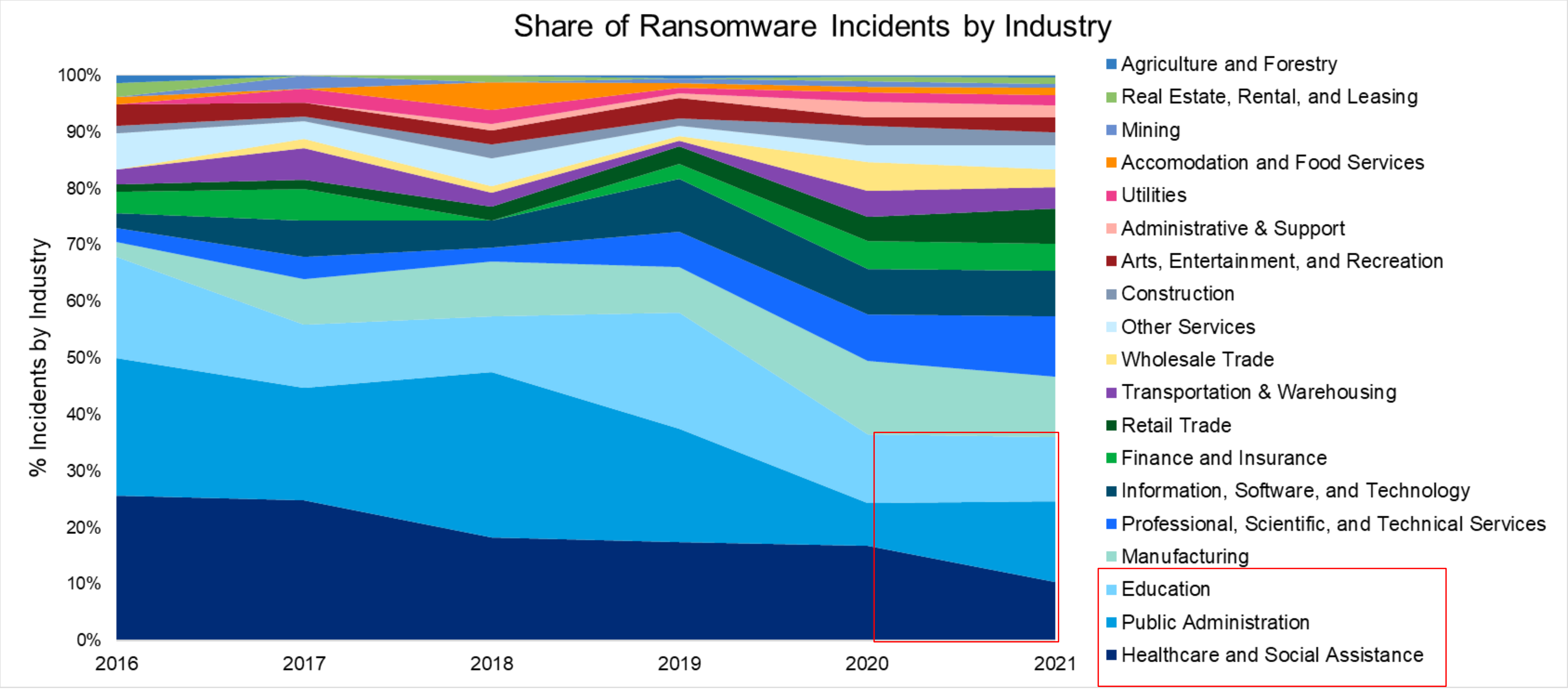
There are also smaller supply chain attacks using a poorly protected supplier to get into a large organization (for example using an insecure HVAC maintenance remote connection)

Managing digital supply chain risk is mostly comparable to classic supply chain risk management, with a few technical tweaks, for example on remote connections or in case of in-house software development

Examples of Cyber Attacks

Ransomware Incidents By Industry

Q1 2022 Ransomware Update



Marsh

Additional sources: Coveware Blog Q1 2022; Sophos

Cyber Attacks in North America - Public Sector

The ransomware trend has grown over the past few years and is not yet decreasing

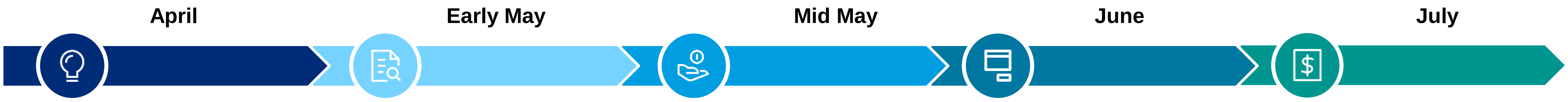
2016		
	Nov	University of Calgary, Alberta Canada
2017		
	Dec	Mecklenburg Country. North Carolina
2018		
	Feb	Davidson County, North Carolina
	Mar	Atlanta City
	May	Wasaga Beach, Ontario Canada
	Sept	Midland, Ontario Canada Mekina, Quebec Canada
	Oct	West Haven, Connecticut
2019		OWSA, Jacksonville, North Carolina
	Mar	Jackson County, Georgia Albany, New York
	Apr	Augusta, Maine Greenville, North Carolina Imperial County Stratford, Ontario Canada
	May	Baltimore, Maryland
	Jun	Riviera Beach, Florida Lake City, Florida The Nation, Ontario Canada
	Jul	Georgia Administrative Office of the Courts
	Aug	Texas
	Nov	Iqaluit, Nunavut
2020		
	Jan	Tillamook County Oregon, Ransomware attack Municipality of Westlake-Gladstone, MB, Theft of funds
	Mar	Torrance, Cal, Ransomware attack
	Jun	City of Florence, Alabama, Ransomware attack Knoxville, TN, Ransomware attack
	Sept	Key West, FL, Ransomware attack
	Oct	Mt. Pleasant, MI, Ransomware attack
	Nov	Saint John, N.B.,- Ransomware attack Delaware County, Pennsylvania, Ransomware attack
	Dec	NYC, Department of Education, Ransomware attack
2021	Jan	Toronto, ON, third party software vulnerability exploit
	Feb	Oldsmar, FL, water system hacked to poison the people (raised sodium hydroxide levels to 100x the normal level)
	Mar	City of Buffalo, NY, Ransomware attack
	Apr	Resort Municipality of Whistler (RMOW), BC, Ransomware attack Regional Municipality of Durham, ON third party software vulnerability exploit
	May	City of Tulsa, OK, Ransomware attack
	Jul	Joplin, Mo., City Government, Ransomware attack Grass Valley, California, Ransomware attack
	Sept	Jersey City Municipal Utilities Authority, NJ, Ransomware attack
	Oct	City of Clarence-Rockland, ON, Ransomware attack

Marsh

Color Legend: Incident in US ; Incident in Canada

Ransomware in Canada – Attack on a Municipality

What is disclosed by the town on its website



April

Discovery

The town’s computer system was compromised in April which left about 10 servers locked.

Early May

Investigation

External consultants were hired to provide guidance on security matters, assisting with the virus decryption, and conducting the post-incident analysis.

Mid May

Ransom Payment

After several communications the cyber criminals accepted an offer of 3 bitcoins (~ $35,000) for 4 servers.

June

System Restore

The town rebuilt a new network and has since updated its anti-malware protection and invested in an new email security solution to reduce exposure to phishing and spam emails.

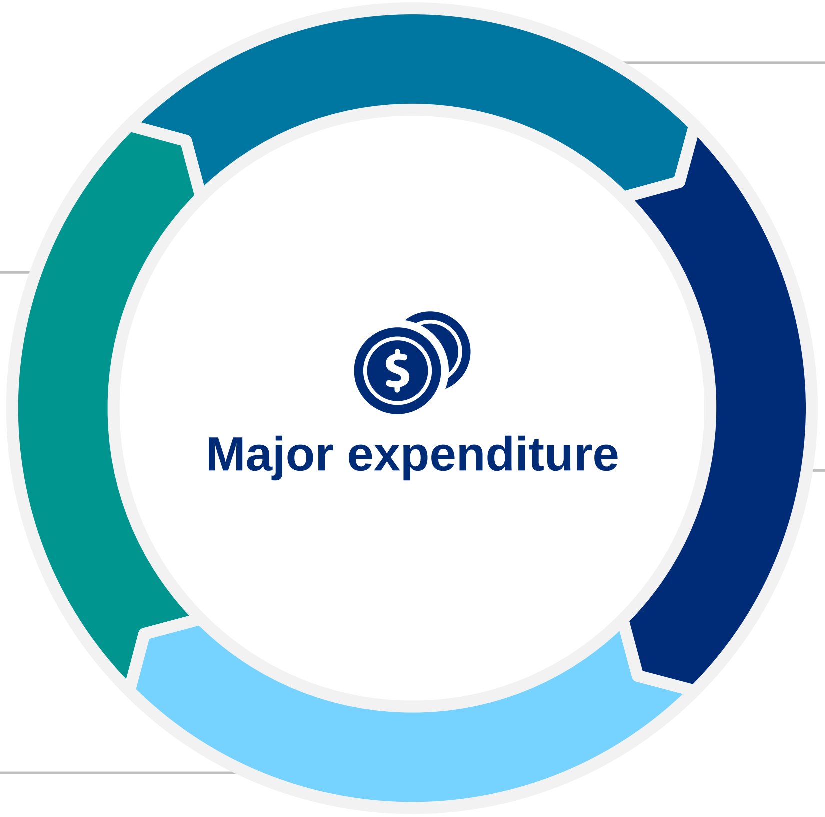
July

Aftermath

The financial impact is estimated as ~ $250,000 which include but not limited to: hiring external consultants; reprogramming of the Town’s Security Access system; various purchase of IT devices and computer hardware; internal productivity loss; etc.

Ransomware in Canada – Attack on a Municipality (Cont.)

What is disclosed by the town on its website



60%

Internal productivity losses

Losses that result from personnel being paid but unable to perform their duties

15%

External Support

External resources applied to identifying extent of incident and technical details

10%

Internal staff overtime

Additional cost of additional resourcing from internal employees

15%

Ransom payment

3 bitcoins paid for 4 servers that are determined necessary.

Ransomware attacks in Canada – Example of a large scale attack

What is publicly known

A large public organization suffered from a ransomware attack by the end of 2019

The security systems in place did not detect the virus

Due to the systems being centralized, the ransomware had impacted other linked organizations and services, and over 20 communities as well

Close to a 1,000 physical and virtual on-premises servers and about 5,000 workstations were encrypted

Nearly 40,000 people in the area were impacted as public services were shut down

IT had to rebuild the network as the ransom was not paid by the institution. Nine months after the attack, IT had not been able to fully restore all its systems (email, particular)

The impact of the ransomware attack is estimated to be more than $7M (this includes service contracts, purchases of hardware and software, staff overtime, etc.)

Cyber Incident Best Practices

Incident Management

Top Ten Practices… 1/3

Build an Incident Response Plan

- Assign a team
- Define incident assessment and escalation process
- Set a communication Plan
- Maintain a contact list
- Define response procedures
- Prepare to track timeline and decisions

Conduct Incident Response Exercise

- Conduct yearly incident response exercises
- Allow the team to practice its response to cyber incident scenario
- Use response tools and procedures
- Provide training as you onboard new team members

Establish Incident Response Relationships

- Have relationships with Incident Response vendors such as breach coach, forensic firms, managed service providers
- Have relationship with other stakeholders such as Privacy officer/Legal Counsel, senior management team
- Develop these relationships before incident rises

Maintain Asset Inventory and data map

- Assemble an inventory of devices and software
- Map the locations where sensitive data is stored
- Keep it current

Incident Management

Top Ten Practices… 2/3

Implement Incident Response Technology

- Implement technical solutions to detect, monitor, contain and respond to incidents
- The solutions include Endpoint Detection and Response (EDR) and Security Information & Event Management (SIEM) with alerting and monitoring

Collect and Protect Activity Logs

- Collect, monitor, store and protect logs such as system, user and network events
- Monitor activities to detect abnormal behaviour
- Analyze security events to qualify and investigate security incidents

Backup Systems and Data

- Maintain offline copies of critical systems and data
- Regularly test the integrity of backups
- Secure backups with encryption and control access

Prepare for Disaster Recovery

- Document procedures on how to restore systems from backups
- Test at least annually the ability to restore critical systems and data

Incident Management

Top Ten Practices… 3/3

Conduct User Awareness Campaigns

- Conduct regular cyber risk awareness campaigns including risk bulletins and trainings on how to report anomalies and incidents.
- Conduct phishing exercises regularly, test and educate users on current phishing attacks

Get Cyber Insurance

- Purchase insurance to get expert support in incident response
- Protect your organization from financial losses stemming from cyber incidents

Q&A

Marsh

Marsh is a business of Marsh McLennan.

This document and any recommendations, analysis, or advice provided by Marsh (collectively, the “Marsh Analysis”) are not intended to be taken as advice regarding any individual situation and should not be relied upon as such. This document contains proprietary, confidential information of Marsh and may not be shared with any third party, including other insurance producers, without Marsh’s prior written consent. Any statements concerning actuarial, tax, accounting, or legal matters are based solely on our experience as insurance brokers and risk consultants and are not to be relied upon as actuarial, accounting, tax, or legal advice, for which you should consult your own professional advisors. Any modelling, analytics, or projections are subject to inherent uncertainty, and the Marsh Analysis could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. The information contained herein is based on sources we believe reliable, but we make no representation or warranty as to its accuracy. Except as may be set forth in an agreement between you and Marsh, Marsh shall have no obligation to update the Marsh Analysis and shall have no liability to you or any other party with regard to the Marsh Analysis or to any services provided by a third party to you or Marsh. Marsh makes no representation or warranty concerning the application of policy wordings or the financial condition or solvency of insurers or re-insurers. Marsh makes no assurances regarding the availability, cost, or terms of insurance coverage.

A business of Marsh McLennan