

Cyber Breach:
Choose Your Own Response

Ryan Duquette, CFE
Partner, Security and Privacy Risk Consulting
RSM Canada

Speaker – Ryan Duquette, Partner, Security and Privacy Risk Consulting

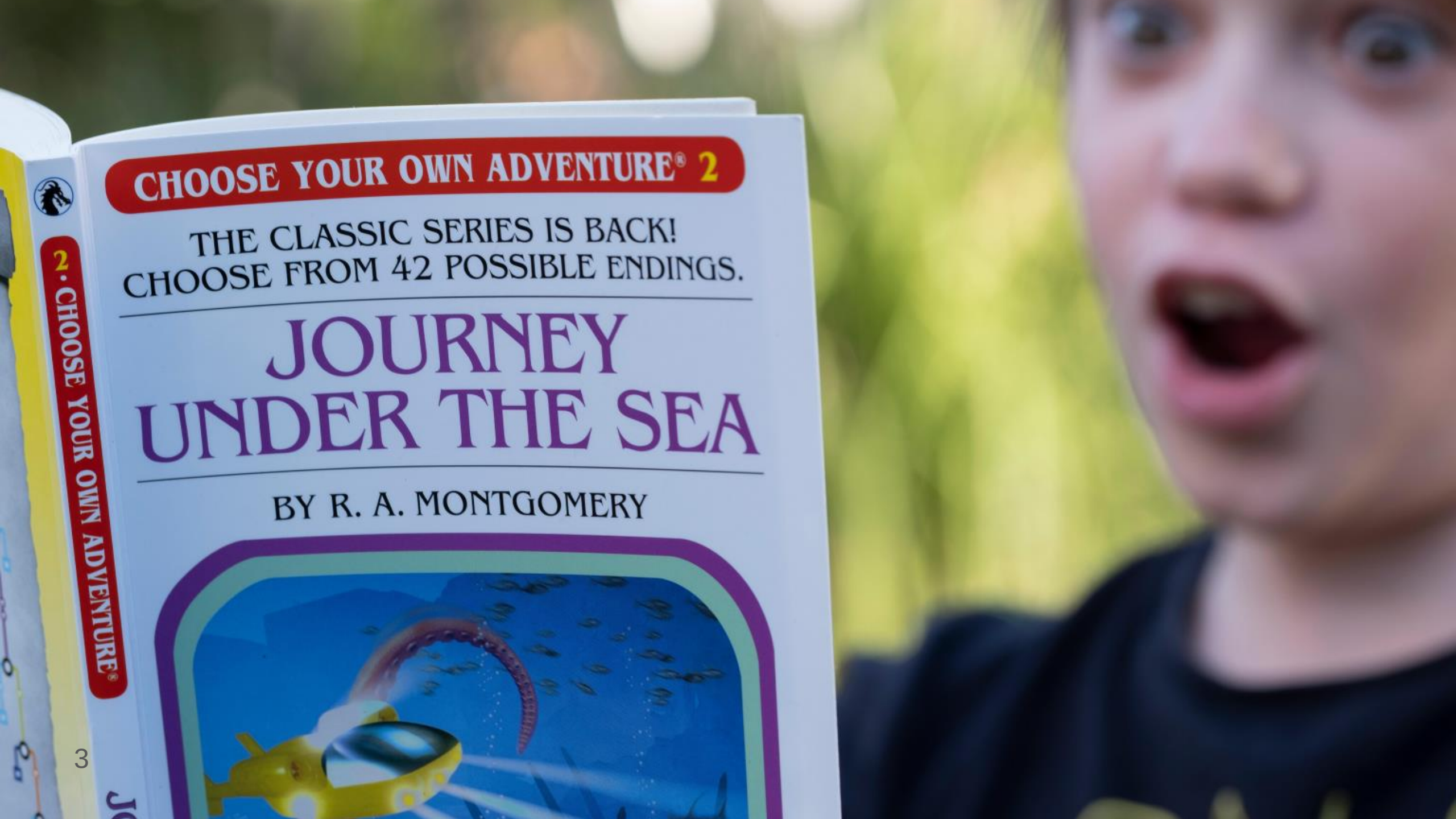


- Seasoned professional within the investigations and cybersecurity fields
- Focuses on litigation support, cyber-incident response, privacy and cyber-technology risks, digital forensics, and cyberfraud matters
- Works with clients involved in workplace investigations and civil litigation matters including intellectual property theft, HR investigations, and data breaches
- Over twenty years of experience as investigator; previously worked as a police officer focusing on cybercrime and fraud cases

- Certified Forensic Computer Examiner (CFCE)
- Certified Fraud Examiner (CFE)
- EnCase Certified Examiner (EnCE)
- Magnet Certified Forensics Examiner (MCFE)
- Level II (Secret) Government of Canada Security Clearance

Contact Details: ryan.duquette@rsmcanada.com
416 706 2273
LinkedIn: ryanduquettemsc
Twitter: @RyanDuquette4n6

© 2021 RSM Canada Consulting LP. All Rights Reserved.


CHOOSE YOUR OWN ADVENTURE® 2
THE CLASSIC SERIES IS BACK!
CHOOSE FROM 42 POSSIBLE ENDINGS.
JOURNEY UNDER THE SEA
BY R. A. MONTGOMERY
2 · CHOOSE YOUR OWN ADVENTURE®

Agenda

- Cyber-incident stats (just a few!)
- Choose your own breach
- Debrief and next steps
- Questions

- 2 – 15 min breaks

© 2021 RSM Canada Consulting LP. All Rights Reserved.

Defining cybersecurity

> “A blend of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access.”

© 2021 RSM Canada Consulting LP. All Rights Reserved.

The facts

- Cybersecurity is a business issue, not a technical problem
- The landscape is complex, and competing drivers are common
- Business enhancing actions can quickly lead to disruption
- Complex controls can hamper success

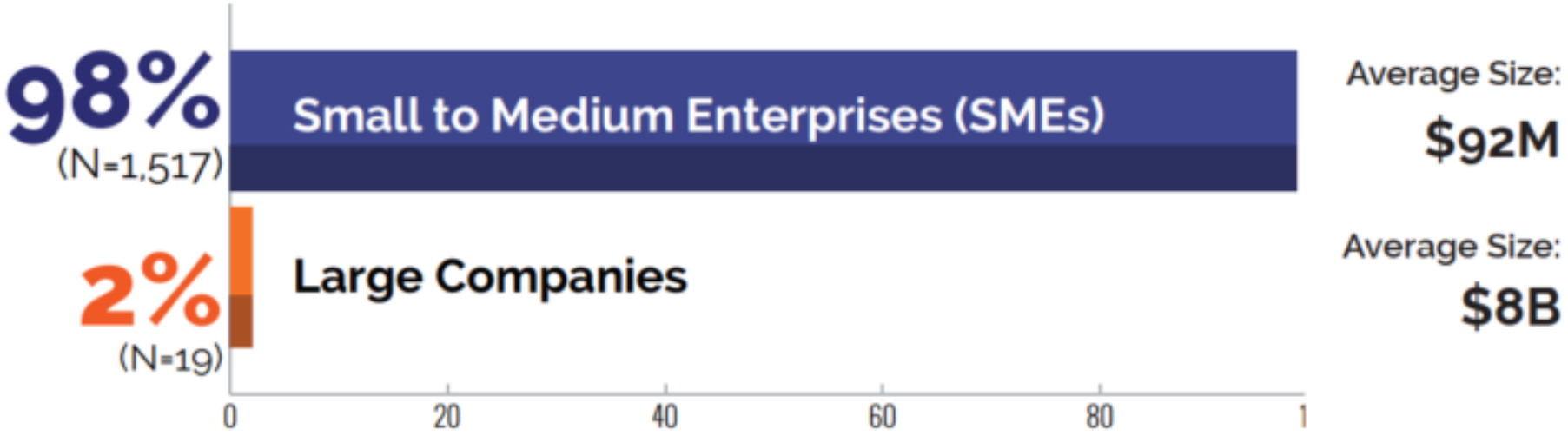
© 2021 RSM Canada Consulting LP. All Rights Reserved.

“Why isn’t this easier?”

- Regulatory obligations
- Evolving technology
- People

© 2021 RSM Canada Consulting LP. All Rights Reserved.

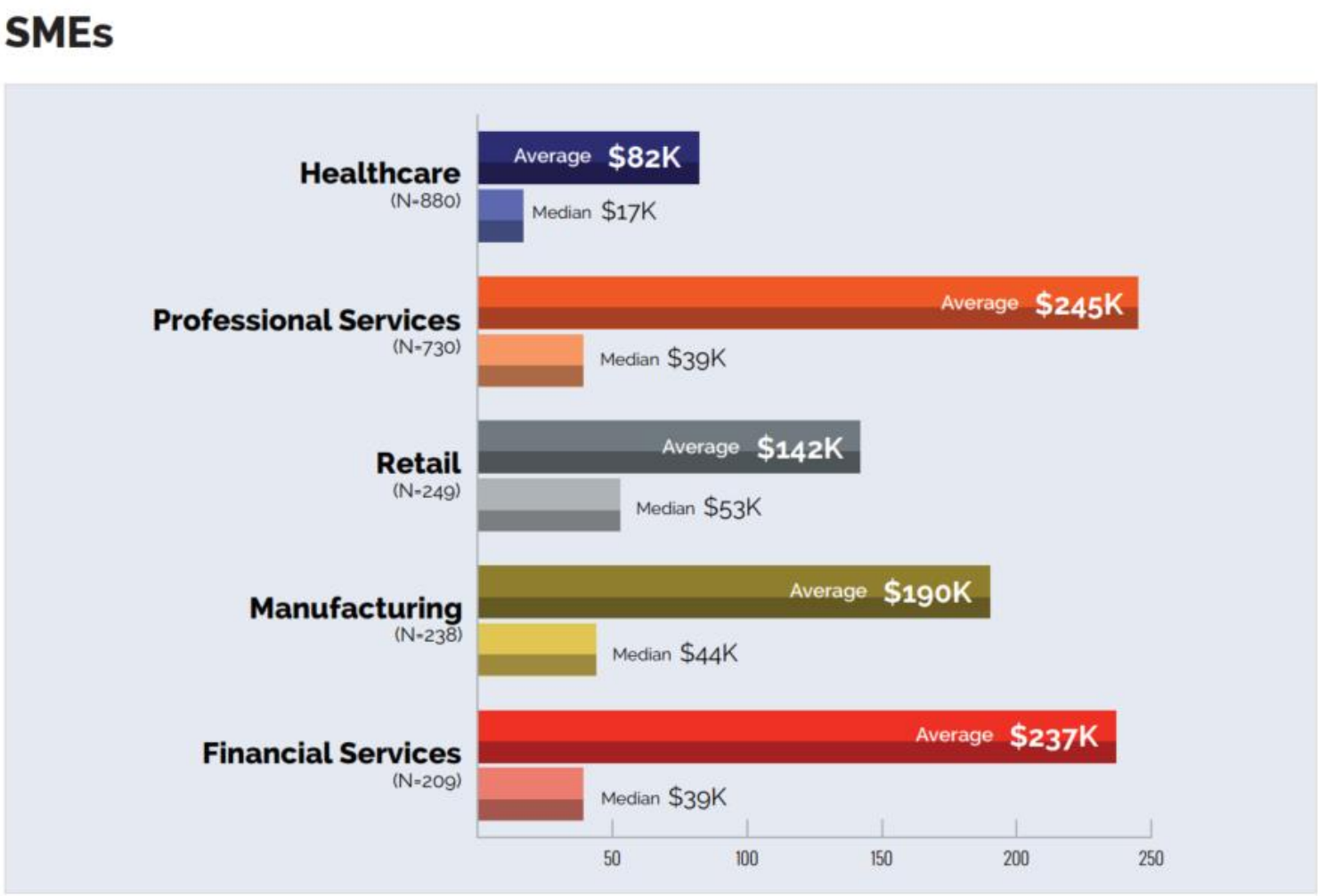
Company Size – 2020



Source: Netdilligence 2020 report

© 2021 RSM Canada Consulting LP. All Rights Reserved.

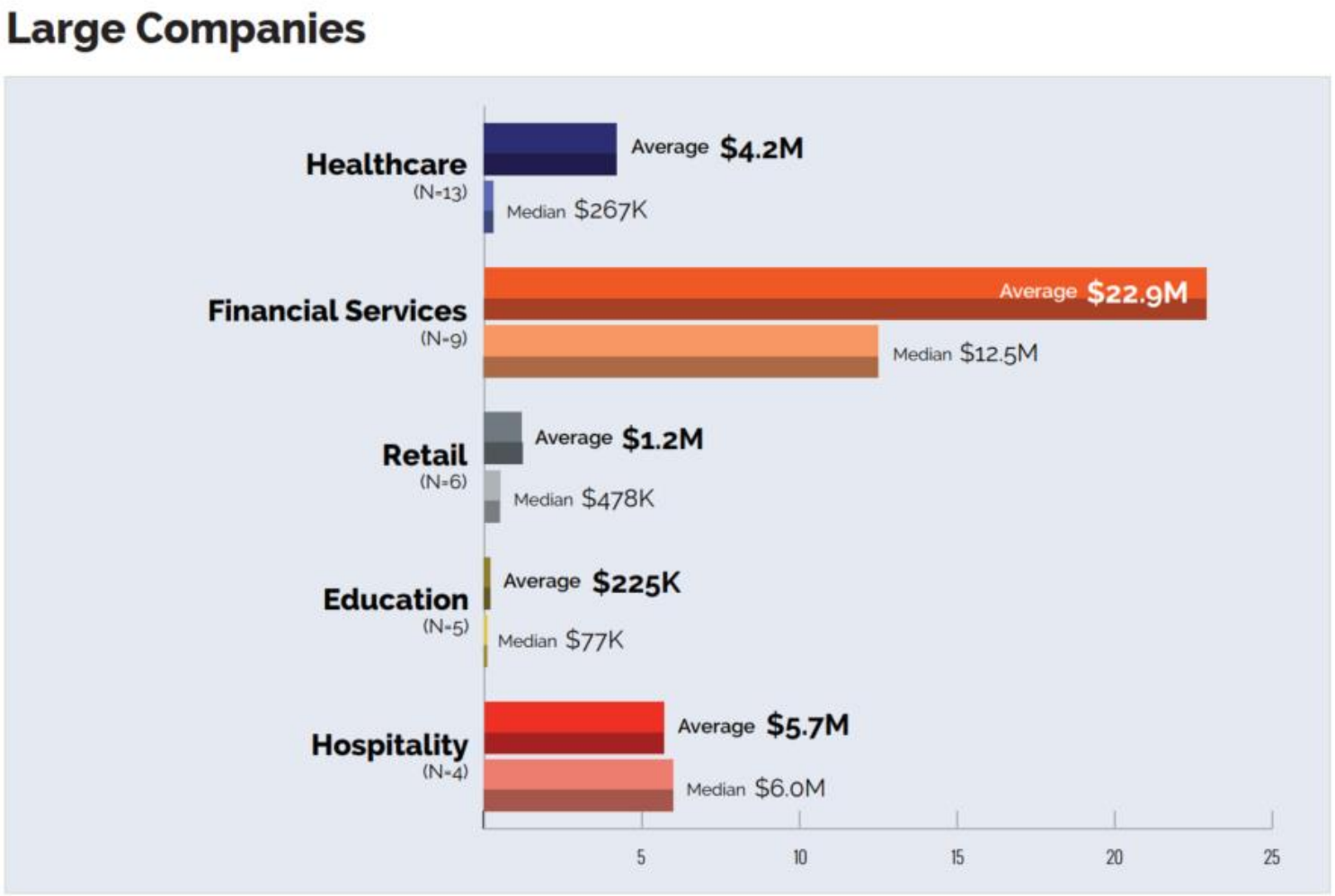
Average cost SME– 2020



Source: Netdilligence 2020 report

© 2021 RSM Canada Consulting LP. All Rights Reserved.

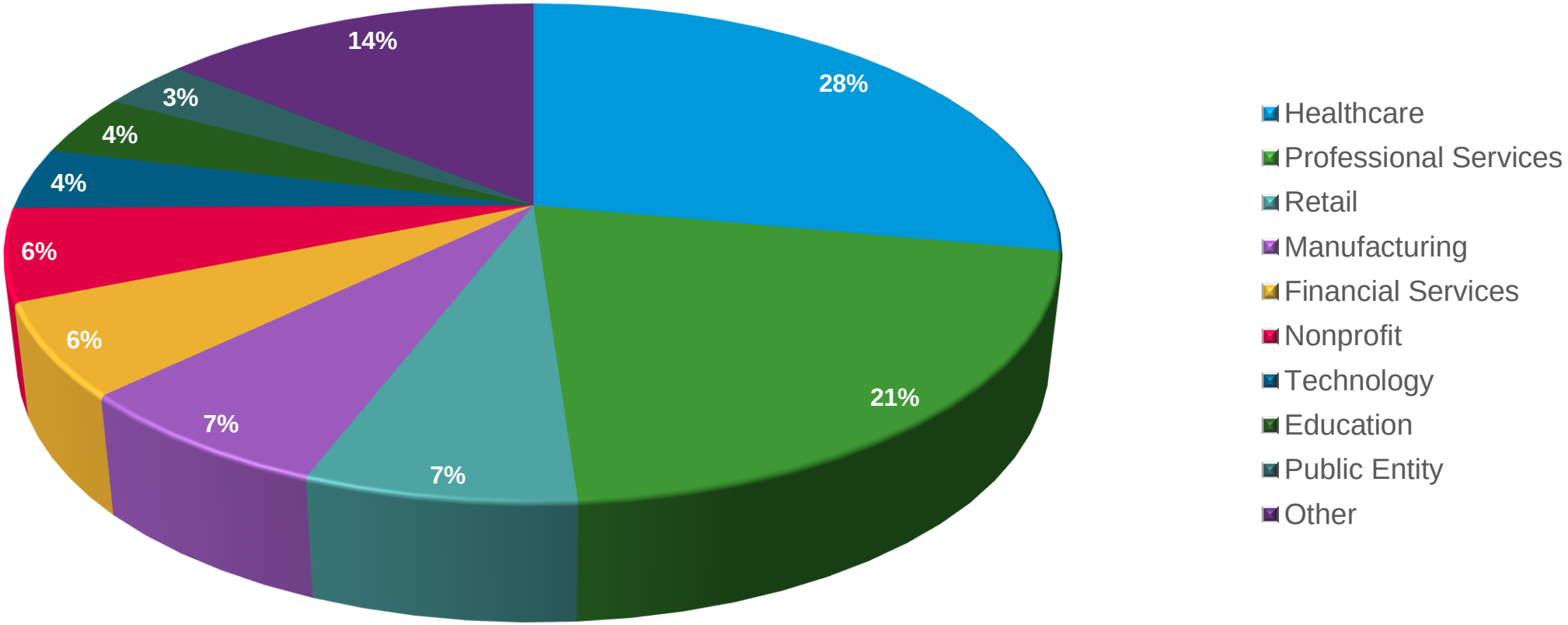
Average cost Large Companies– 2020



Source: Netdilligence 2020 report

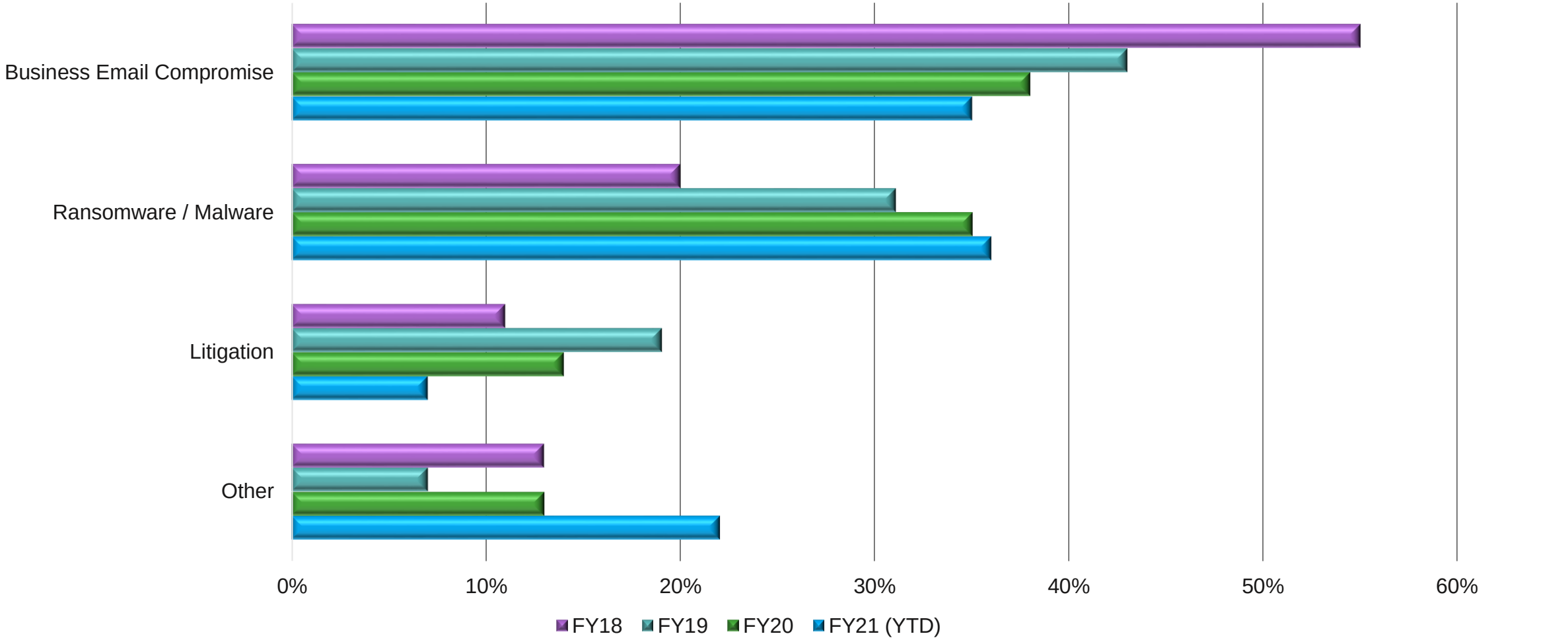
© 2021 RSM Canada Consulting LP. All Rights Reserved.

Cyber Incidents – Sectors (Over 3%) 2015-2019 (SMB)



© 2021 RSM Canada Consulting LP. All Rights Reserved.

RSM Cyber Response Incident Types (FY18 – FY21)



© 2021 RSM Canada Consulting LP. All Rights Reserved.

Ransomware Over The Years

HISTORY

- 1989 AIDS Trojan
- AIDS researcher gave out 20,000 infected floppy disks World Health Organization's AIDS conference attendees
- US$189 to a post office box in Panama
- 31 years later, healthcare industry remains a top target



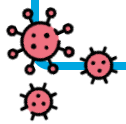
DISRUPT

- 2016 WannaCry
- Attack took advantage of a weakness in the Microsoft Windows operating system
- Hit around 230,000 computers globally
- US$300 – 600 in Bitcoin requested or files would be permanently deleted



EVOLVE

- Covid19 Tracker App – requested Android phone permissions in order to show live Covid19 tracking info
- Once successfully granted all permissions, it locked the phone and displayed a ransom note
- Ransom requested US$100 - 250 per device



© 2021 RSM Canada Consulting LP. All Rights Reserved.

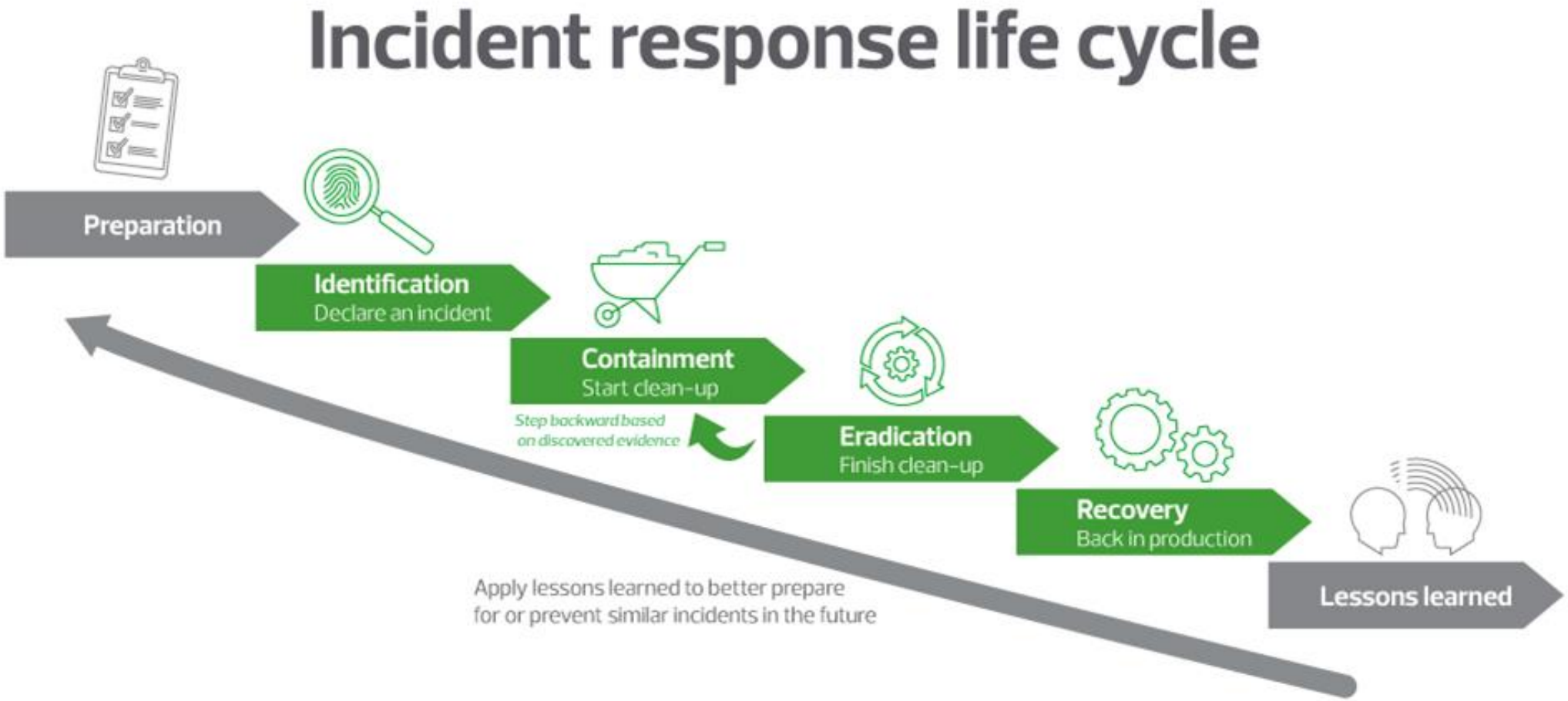
Ransomware

- Victims: 2020 – First ¾ $233,817, last ¼ $154,108
- 6,300 dark web marketplaces selling ransomware
- 45,000 products – averaging $10.50
- $6+ million in ransomware sales – well over 1+ billion in payouts

www.zdnet.com/article/ransomware-payments-are-going-down-as-more-victims-decide-not-to-pay-up

© 2021 RSM Canada Consulting LP. All Rights Reserved.

Incident Response Life Cycle



© 2021 RSM Canada Consulting LP. All Rights Reserved.

Changing mindset

“It’s the IT person’s job to protect the company”

© 2021 RSM Canada Consulting LP. All Rights Reserved.

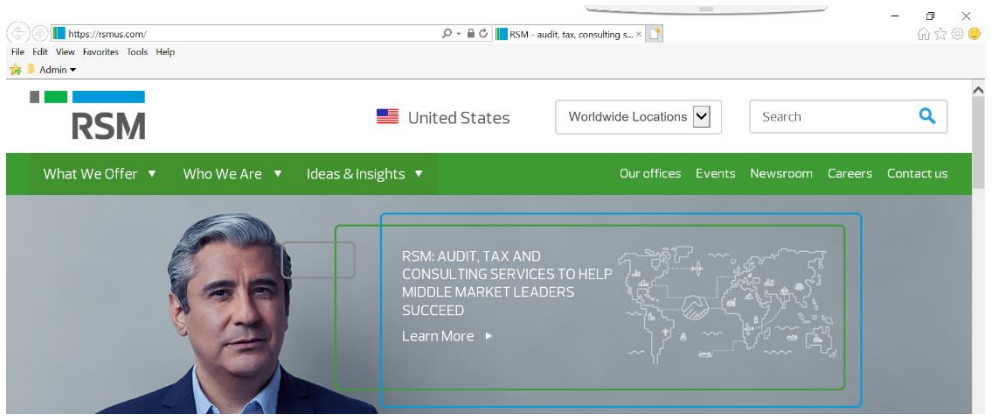
Changing mindset

"It's up to all of us to protect the organization"

© 2021 RSM Canada Consulting LP. All Rights Reserved.

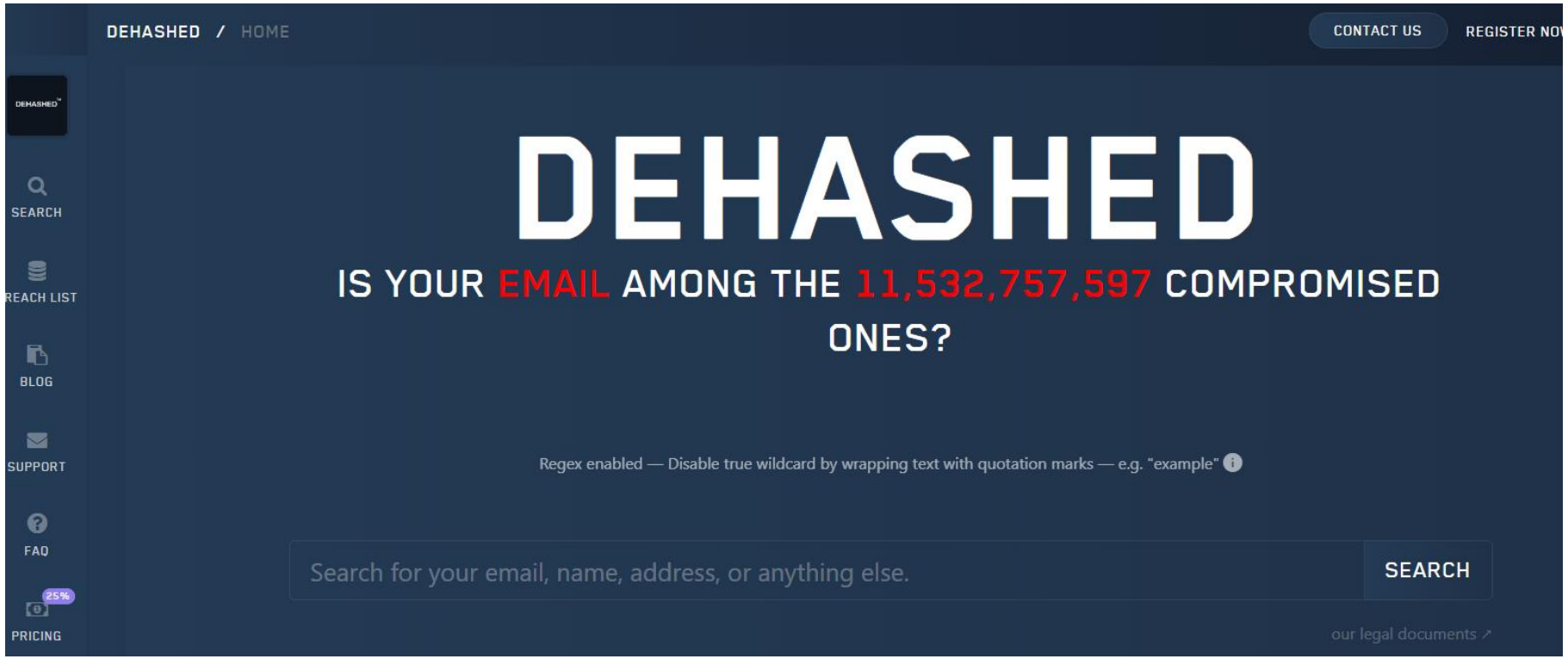
How are you being targeted?
Social Engineering





© 2021 RSM Canada Consulting LP. All Rights Reserved.

How are you being targeted?
Reused Creds



© 2021 RSM Canada Consulting LP. All Rights Reserved.

EXERCISE: RANSOMWARE/MALWARE

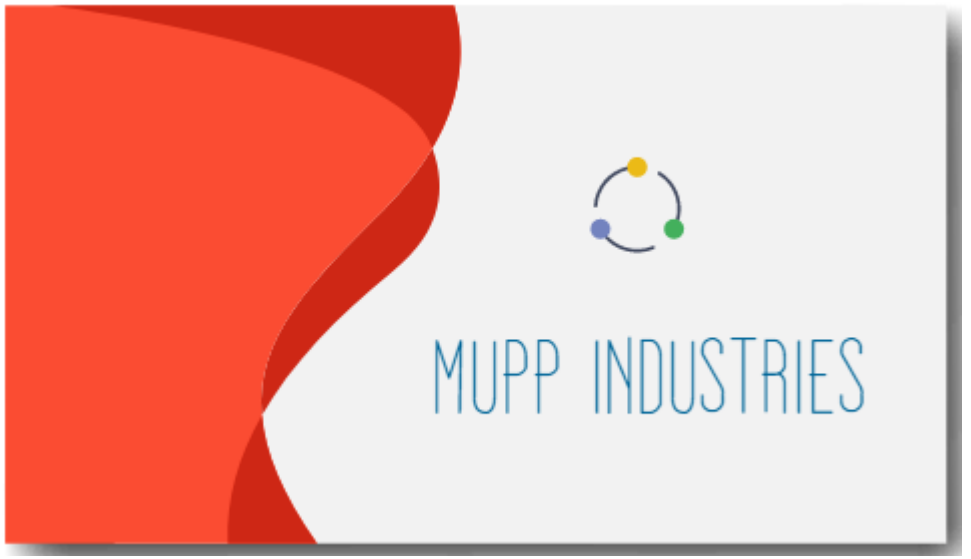
© 2021 RSM Canada Consulting LP. All Rights Reserved.

Ransomware – Scenario

You are a senior leadership member of Mupp Industries Ltd, which is a U.S. based organization and focuses on the manufacturing and distribution of proprietary scientific devices.

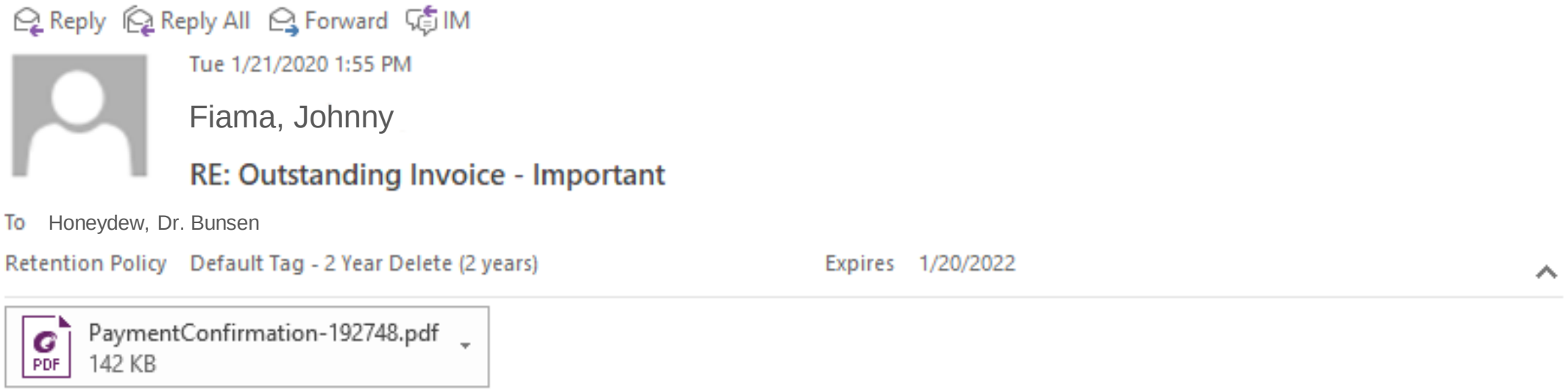
Mupp is privately owned by J. P. Grosse.

Mupp has offices across the country and employs approximately 2,500 people.



© 2021 RSM Canada Consulting LP. All Rights Reserved.

Invoice Email – Attachment



© 2021 RSM Canada Consulting LP. All Rights Reserved.

Ransomware – Scenario

Does this look like a standard email?

- Why?
- What parts look suspicious?

© 2021 RSM Canada Consulting LP. All Rights Reserved.

Should you report this activity to your IT dept?



Try Again

You chose to not report the suspicious activity to your IT department and now the entire environment has been encrypted by ransomware…

- Always make your IT department aware of any suspicious or malicious activity right away. Doing so can minimize an incident's impact.

© 2021 RSM Canada Consulting LP. All Rights Reserved.

Ransom Note

Event: Help Desk Ransomware Call

Description: On Friday, February 1, at 4:36 p.m., a user within the HR department calls the service desk stating that there is a ransomware note on his screen. He was opening attachments for work, and at first, he thought nothing of it.

© 2021 RSM Canada Consulting LP. All Rights Reserved.

Ransom note

Your computer has been infected!



Your documents, photos, databases and other important files **encrypted**



To decrypt your files you need to buy our special software - [redacted]*-Decryptor*



You can do it right now. **Follow the instructions below.** But remember that you do not have much time

[redacted]-Decryptor costs

You have 1 day, 05:07:19

* If you do not pay on time, the price will be doubled
* Time ends on May [redacted]

Bitcoin address: [redacted]

Current price [redacted] BTC
≈ [redacted] USD

After time ends [redacted] BTC
≈ [redacted] USD

* Amount in BTC will be recalculated in 3 hours with an actual rate.

© 2021 RSM Canada Consulting LP. All Rights Reserved.

Impact

- What type of data does this employee have access to?
- What is the employee's organizational role?
- Is there a risk of spreading or pivoting throughout the environment?
- Is there impact to the user's inability to continue work?
- Are any files accessible?

© 2021 RSM Canada Consulting LP. All Rights Reserved.

Incident Declaration

By 5 p.m., your IT department has determined that all the company's main servers and systems have been encrypted. Users are unable to access the company email system, file storage system, network servers, etc.

© 2021 RSM Canada Consulting LP. All Rights Reserved.

Incident Declaration

- How was it determined that there was an incident?
- Was it possible to correlate other information?
- What immediate actions will prevent the spread of ransomware?

© 2021 RSM Canada Consulting LP. All Rights Reserved.

RESPONSE PHASE: INCIDENT PRIORITIZATION AND MOBILIZATION

© 2021 RSM Canada Consulting LP. All Rights Reserved.

What’s an IRP?

- Incident Response Plans (IRPs) provide a consistent framework to quickly and efficiently respond to and mitigate the harm resulting from a potential or confirmed cybersecurity incident.



- Identifies responding personnel
- Assigns responsibilities
- Outlines required SLA’s

© 2021 RSM Canada Consulting LP. All Rights Reserved.

IRP Team



© 2021 RSM Canada Consulting LP. All Rights Reserved.

Yes, you have an IRP – but now what

- Great, you have an Incident Response Plans (IRP), however
  - Where is it contained?
  - Have you run through it with various playbooks?
  - Have you included alternative forms of communications?
  - Do you have external third-party providers on it?
    - If so, have they seen it?
  - How often is it updated for
    - Changes in staff/technology/vendors, etc?
  - Have all members with roles/responsibilities in the IRP seen it and signed off on seeing it?

© 2021 RSM Canada Consulting LP. All Rights Reserved.

Incident Recovery

- On or offsite backups?
- How often are backups taken?
- How long to restore from backup?
- Who is responsible?
- How often is the restore process exercised?

© 2021 RSM Canada Consulting LP. All Rights Reserved.

Failed Backup

The networking team has attempted to restore the affected systems using old system backups. When working to restore they were alerted that the primary snapshots/backups have been deleted.

At this point your IT team has determined that Mupp has suffered a cyber breach, however, other than files being encrypted, nothing else is known at this point.

© 2021 RSM Canada Consulting LP. All Rights Reserved.

No Cyber Counsel / Breach Coach

Although Internal / External counsel is not required, none of your communications will be protected under attorney-client privilege. You will also not benefit from the guidance counsel can provide on what constitutes as PII, PHI, PCI, or other protected / regulated data and when notification is required.



Continue

© 2021 RSM Canada Consulting LP. All Rights Reserved.

Incident Recovery



BREAKING NEWS

Your organization is penalized for neglecting to notify the regulatory entity of the breach. In addition, your organization's reputation has been damaged with this news

Try Again

© 2021 RSM Canada Consulting LP. All Rights Reserved.

Incident analysis

New note from attacker saying they have 34 GB of company data that they are going to release into the wild unless ransom is paid.





© 2021 RSM Canada Consulting LP. All Rights Reserved.

Does your company store IP or other PII?

Are you sure your company doesn't?

Personally Identifiable Information (PII): Information that can be used together to distinguish a specific individual (name, address, SSN, etc.)

Intellectual Property (IP): Proprietary information that is kept confidential and used for the benefit of the organization (Secret Recipe, System scripts, etc.)

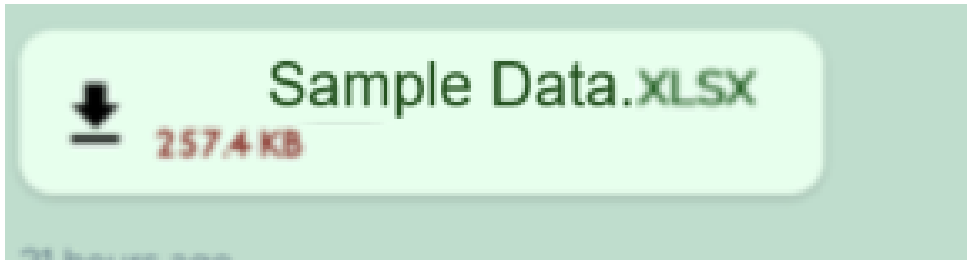
Yes

No

© 2021 RSM Canada Consulting LP. All Rights Reserved.

Incident analysis

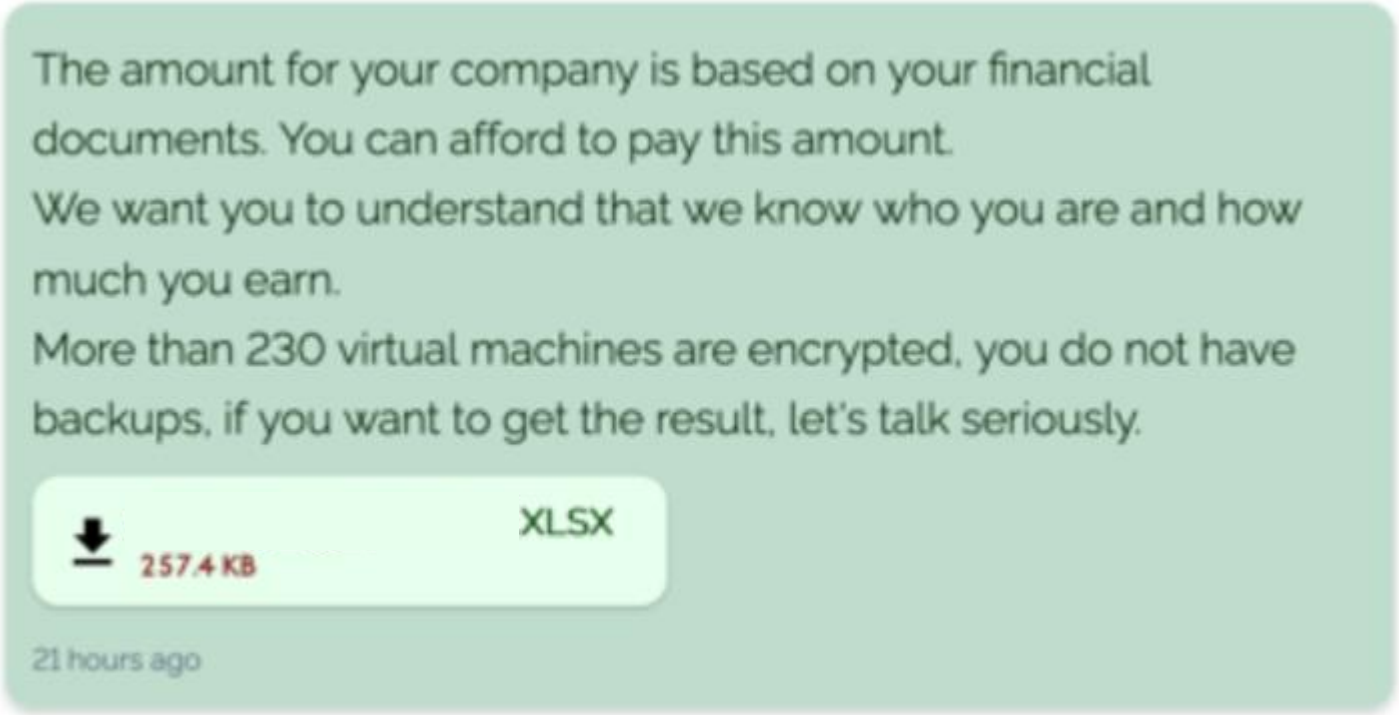
- Ask attackers for proof of life, and you determine that Mupp IP and PII of staff and clients are contained within the data breach.



© 2021 RSM Canada Consulting LP. All Rights Reserved.

Ransom

$1,200,000 USD



© 2021 RSM Canada Consulting LP. All Rights Reserved.

You’re paying the ransom

Many organizations choose to pay ransoms in order to recover encrypted and deleted data. However you need to make sure this doesn't violate contractual obligations or company guidelines / morals.



OFAC Advisory Warns of Civil Penalties for Ransomware Payments

Tuesday, October 13, 2020

OVERVIEW

The US Department of Treasury’s Office of Foreign Assets Control (OFAC) issued an advisory alert on October 1, 2020, that serves as a warning to entities who have been or will be the victim of a ransomware attack. The five-page advisory states that any company that pays a

Continue

© 2021 RSM Canada Consulting LP. All Rights Reserved.

You’re not paying the ransom

Many organizations choose not to pay ransoms due to company ethics, recommendations by government entities, or a number of other reasons.

Unfortunately, the data being held ransom is data that was lost in the deleted backups and now cannot be recovered. Do you pay now?

Continue

© 2021 RSM Canada Consulting LP. All Rights Reserved.

Performing a forensic investigation of an incident

Pros	Cons
System familiarity	No subject matter expertise in Forensics
Lines of communication previously established	Potential to trample on forensic evidence
Quick availability and response	Faster doesn’t always mean better
Proprietary software knowledge	No forensic background to preserve/analyze

© 2021 RSM Canada Consulting LP. All Rights Reserved.

Forensic analysis

- Is forensic analysis performed at all?
- Who performs the analysis?
- Is it based on priority or another criteria?
- When is it performed? How soon do you take action?
- How does analysis lead to indicators of compromise?

© 2021 RSM Canada Consulting LP. All Rights Reserved.

Forensic analysis

- Forensic analysis shows:
  - Attack came from phishing email (invoice)
  - Attackers were in the network for 1 month
  - Attackers looked at more than the data that was contained within the 34 GB
  - Attackers navigated across every server

© 2021 RSM Canada Consulting LP. All Rights Reserved.

CYBERSECURITY

© 2021 RSM Canada Consulting LP. All Rights Reserved.

The objective

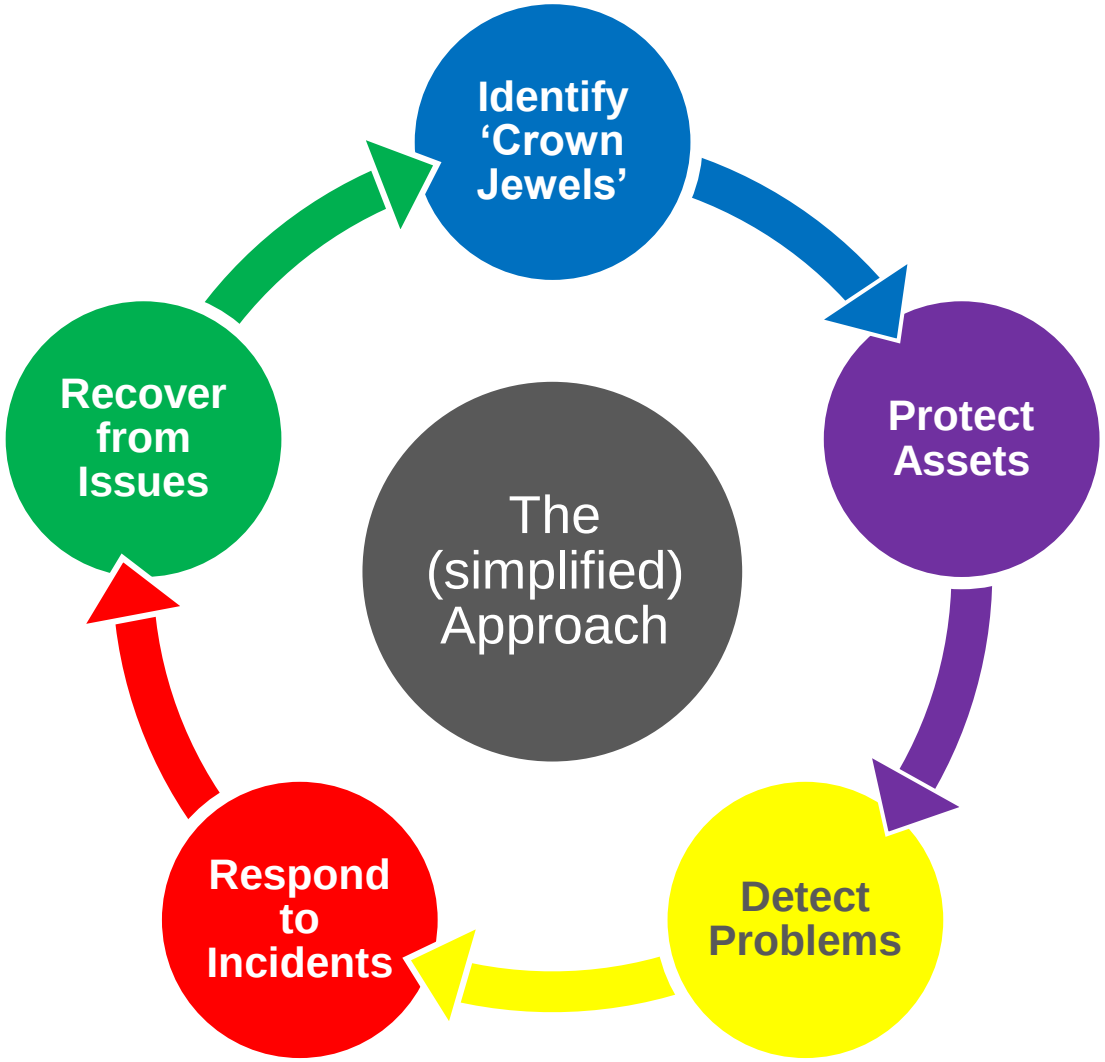
Mature processes, methods, tools and skills, working in unison, with a common goal.

Resulting in:

Well trained people, following **well** developed procedures, using **well** implemented technology

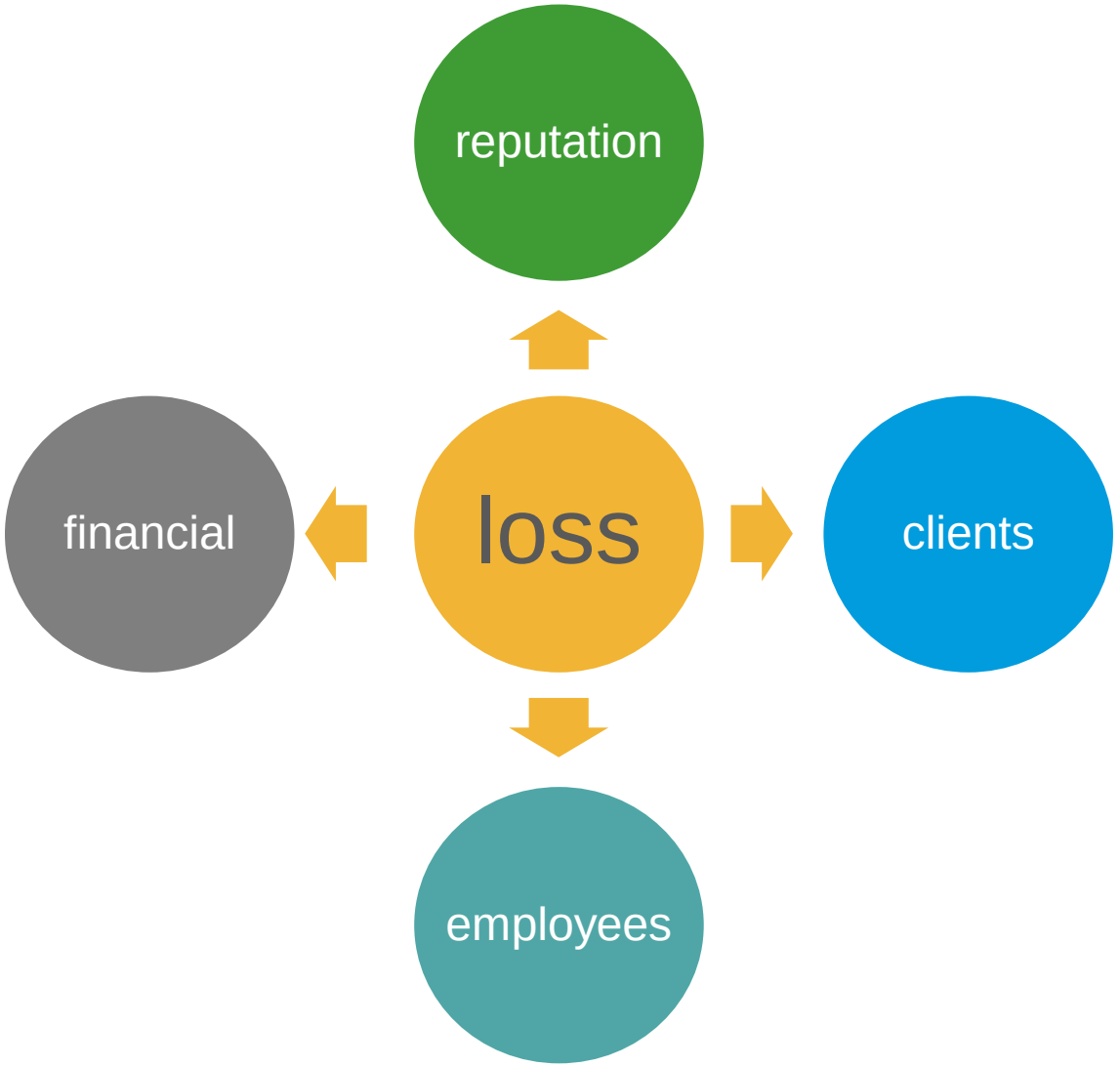
© 2021 RSM Canada Consulting LP. All Rights Reserved.

A framework for cybersecurity (and assessments)



© 2021 RSM Canada Consulting LP. All Rights Reserved.

Risks



© 2021 RSM Canada Consulting LP. All Rights Reserved.

Choices

1. Very secure



3. Low cost

2. Very functional

You can only pick two

© 2021 RSM Canada Consulting LP. All Rights Reserved.

Things to think about

- Understand the data
- Be sure of your obligations
- Think of the risks
- Introduce appropriate controls
- Consider the technology
- Do you need it?

© 2021 RSM Canada Consulting LP. All Rights Reserved.

Things to do

- [x] Back up
- [x] Insider Threat Program
- [x] Have a plan
- [x] Test your environment
- [x] Train your staff
- [x] Have a team
- [x] Consider cyber coverage

© 2021 RSM Canada Consulting LP. All Rights Reserved.

Contact Information



Ryan Duquette

Partner, Security and Privacy Risk Consulting

ryan.duquette@rsmcanada.com

647.730.2673

© 2021 RSM Canada Consulting LP. All Rights Reserved.

THANK YOU FOR YOUR TIME AND ATTENTION

© 2021 RSM Canada Consulting LP. All Rights Reserved.