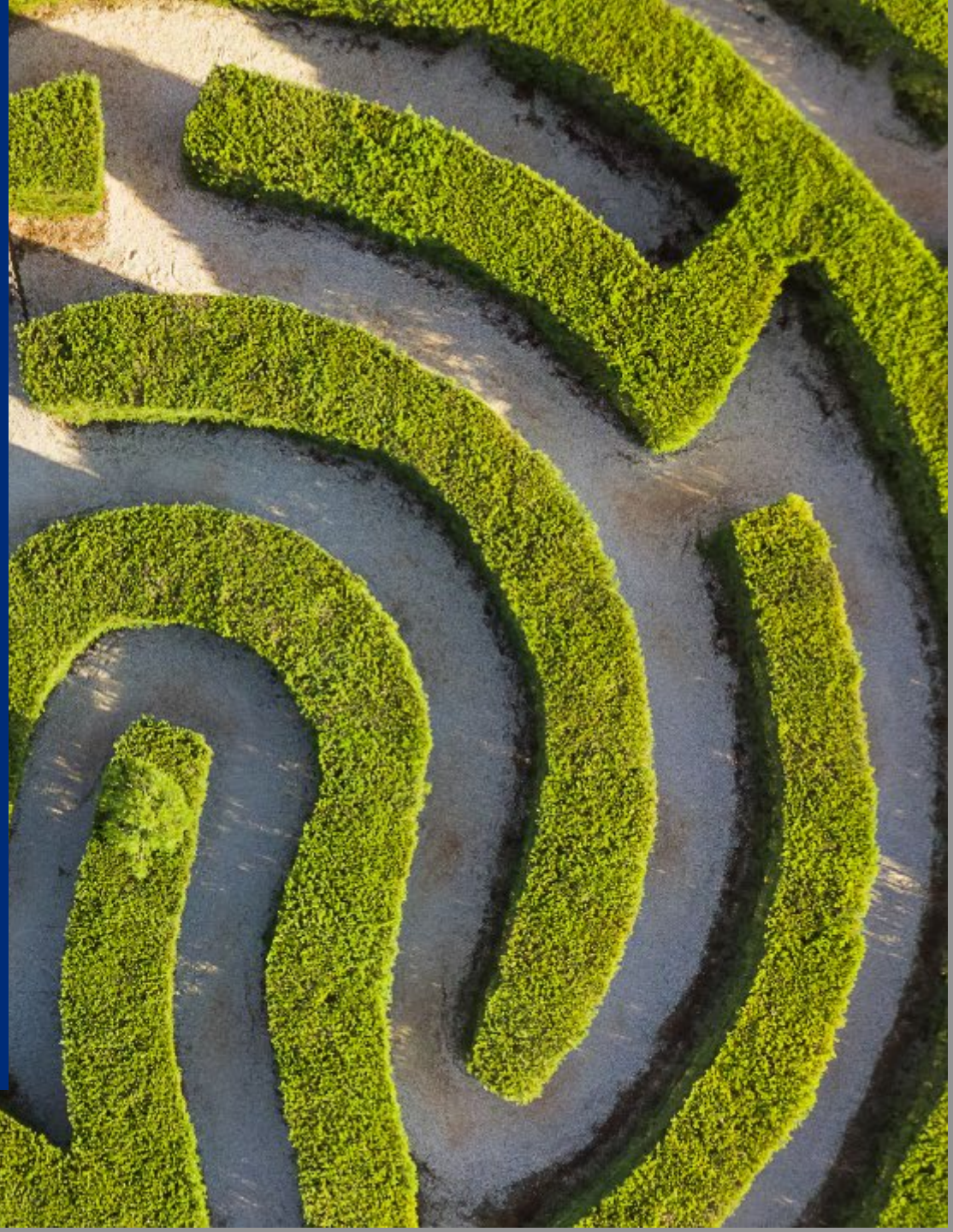
Marsh

Managing Cyber Risk in an Evolving Threat Landscape

2022 Public Risk Conference

Jonathan Weekes, CRISC
National Cyber Growth Leader
Marsh Canada Limited
April 28, 2022



1. Threat Landscape Update and Stakeholder Concerns
2. 5 Questions Organizations Should be Asking
3. Top 12 Security Controls
4. Q&A

Agenda

Threat Landscape Update and Stakeholder Concerns

1

Cyber seismic shifts are interconnected, constantly evolving

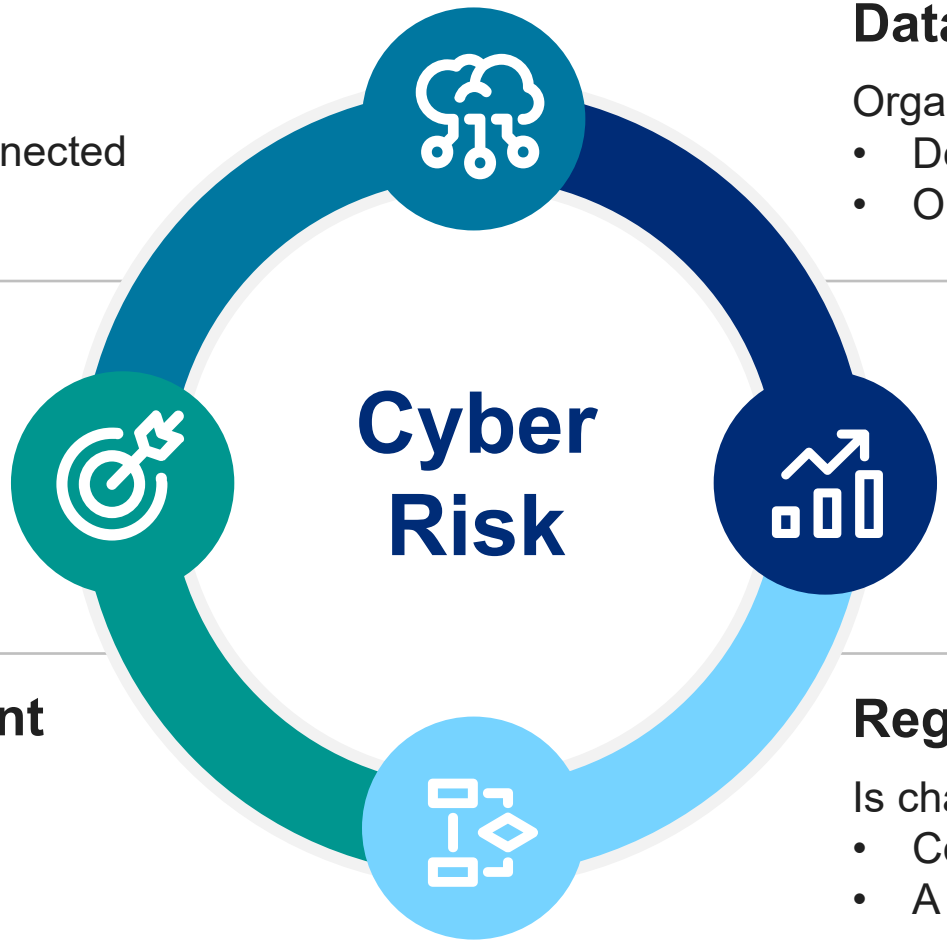
Technology and data are redefining possibility in a dynamic landscape, creating risks and opportunities

Technology

Organizations are:
- Increasingly interconnected
- Critically dependent
- Innovative

Data

Organizations are:
- Deriving greater value
- Outsourcing care



Threat environment

Is characterized by:
- Ransomware
- Supply chain attacks

Regulatory environment

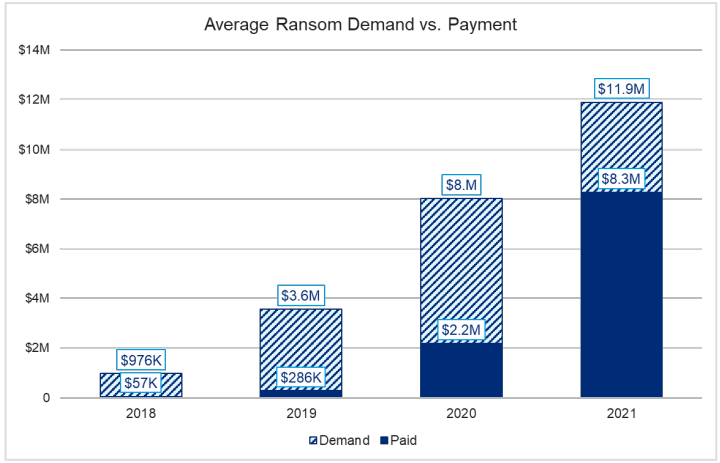
Is characterized by:
- Constant evolution
- A patchwork approach

2022 Cyber Risk Environment

Dominated by ransomware, regulations & supply chain cyber risk

Increasing controls drive improved outcomes, but drive more focus on ransomware sophistication:

- **42% of ransomware victims had viable backups in 2021** – up from 23% in 2020 – meaning more companies were able to avoid paying ransoms.



- **The difference between the average ransom demanded ($11.9M)** and the **average ransom paid ($8.3M)** is decreasing as sophistication has grown (aided by data exfiltration) and threat actors more effectively attack targets.
  - Large insurer: $40M paid
  - Oil pipeline: $4.4M paid
  - Infrastructure: $50M demanded
  - Food manufacturer: $11M paid
  - Chemical distribution:$4.4M paid
  - Tech hardware: $50M demanded

Systemic risk concerns intensify:

- **Aggregation** exposure a concern for underwriters
- **Systemic loss** – possible cyber risks:
  - Common vulnerabilities – in hardware or software
  - Common dependencies – vendors (such as cloud providers) and software
- **Cyber/digital supply chain vulnerabilities** are driving increased scrutiny: SolarWinds, Accellion, Microsoft Exchange, Kaseya & Log4j

Privacy regulations evolve; patchwork approach remains:

- **GDPR** fines are growing (~$27M BA, ~$24M Marriott, ~$41M H&M)
- **CCPA** (California Consumer Privacy Act) and similar legislation (i.e. VA CDPA) allow for private rights of action with per consumer statutory damages and require additional compliance efforts
- **BIPA** (IL Biometric Information Privacy Act) litigation is expensive and is on the rise with increased use of biometric identifiers, especially for employee access – driving additional underwriting questions. 45 states have existing / pending biometric privacy legislation.

Sources: Coveware Ransomware Blog & MMC Cyber Analytics Center

Attacks are increasingly more difficult to manage

80%

Of companies that paid ransomware demands experienced another attack*

27%

Of companies that suffered a material attack were successfully attacked again within 12 months***

61%

Of companies that suffered severe business disruption report that they were unable to remediate the compromise**

86%

Of companies that fell victim to additional significant attacks were found to have more than one unique attacker in their network***

* Cybereason June 2021 Report
** August 2021 Team Cymru Ponemon State of Threat Hunting Report
*** 2018 FireEye M-Trends Report

The questions we hear

from CEOs

“How resilient is our organization, really?”

“Have we got a good grip on our critical assets and their vulnerabilities?”

“Are we working with the right people?”

The questions we hear

from CFO/Treasury

“What’s our financial exposure?”

“How does our level of spend compare to our peers?”

“Is there a better way to demonstrate the ROI of our cyber spend?”

“Could a different risk strategy help us deal with rising cyber insurance costs?”

The questions we hear

from CROs

“How can I persuade colleagues that cyber’s a risk issue, not just a security one?”

“Are we retaining and transferring the right risks?”

“How can modelling and analytics help us measure risk better?”

“How can you support me on complex cyber claims?”

The questions we hear

from CIOs and CISOs

“Objectively, how good are our current partners?”

“How can I benchmark our investment to build a business case?”

“Where can I get reliable, timely, actionable threat intelligence?”

“How do I get our people to have better data discipline and cyber hygiene?

5 Questions Organizations Should be Asking

How are we at risk?

What risk strategies are right for us?

How can we build cyber resilience?

What insurance do we need? How much?

Who are the right advisors to trust? Are they the best for us?

- Accurately identify and quantify risks
- Align on risk and performance
- Use a scorecard
- Model specific loss scenarios (privacy, business interruption, ransomware)
- Ensure future-readiness with trend insights / threat indicators

How are we at risk?

- Assess security
- Model potential loss scenarios
- Align on a shared appetite for risk
- Develop an evidence-based retain / transfer strategy
- Determine the most economic insurance structure
- Benchmark against peers

What risk strategies are right for us?

How can we build cyber resilience?

- Proactively approach risk management
- Align on people and systems, planning and budgeting
- Receive help with response, recovery, and return to resilience
- Stay informed with timely global threat intelligence updates

- Define the role for insurance / risk transfer
- Develop a bespoke program
- Creatively approach policy innovation, limit negotiations, and underwriting changes
- Drive data-driven negotiations
- Benefit from price and admin efficiencies

What insurance do we need? How much?

Who are the right advisors to trust? Are they the best for us?

- Monitor the cyber hygiene of vendors
- Access the open market of cybersecurity vendors
- Objectively assess potential appropriate, compatible, and effective vendors

Top 12 Security Controls

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

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

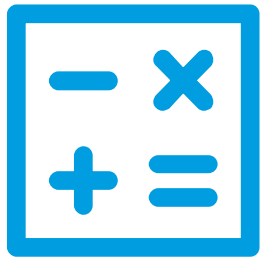
These are large scale supply chain attacks

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

How to build consensus and drive a faster, more efficient and more informed path toward cyber resilience



Measure potential economic impact of cyber events; model loss scenarios

Assess leading inputs on the cyber threat landscape

Frame out cyber risk profile

Document, analyze and prioritize critical event scenarios

Curate best-for-you experts to address issues and pain points

Q&A

A business of Marsh McLennan