PROTECTING AGAINST CYBERTHREATS

Marcus Troiano,
Cybersecurity Strategy Advisor

November 9, 2022 12:30 p.m. ET

WHAT'S UP NEXT

The 2nd Wednesday of the month
12:30pm eastern

- November 15 CONVERGE a Unique Virtual Networking Opportunity with Featured speaker Kevin Gangel, CEO of Unstoppable Conversations
- December 14: Exploring Canada's Entrepreneurship Ecosystem with Kayla Isabelle
- Now Available What's Up Wednesday recorded sessions
- CMC-Ontario Presentation Library PDF download of all past sessions

WHY JOIN?

MEMBERSHIP CONNECTS YOU

- CONSULTANTS
- NETWORK
- RESOURCES
- CERTIFICATION
- VISIBILITY
- DIFFERENTIATE

https://www.cmc-canada.ca/MembershipRegistration

A HIGHER LEVEL of management consulting ONTARIO | CMC | Un NIVEAU SUPÉRIEUR de conseil en management ONTARIO

ABOUT OUR PRESENTER

Marcus Troiano

- Highly experienced Cybersecurity Strategy Advisor with broad exposure internationally and in Canada over the past 7+ years with Mandiant Consulting, a Google Cloud Company
- Focused on overseeing and leading strategic security assessments, due diligence and portfolio company assessments, transformations, and CISO Advisory services
- Marcus is Mandiant's global lead for Strategic Program Assessment Services, and leads Mandiant Canada's Strategic Services team

What's UP? Wednesday
CMC

What's UP? Wednesday

CMC

PROTECTING AGAINST CYBERTHREATS

A HIGHER LEVEL of management consulting ONTARIO

CMC

Un NIVEAU SUPÉRIEUR de conseil en management ONTARIO

POLL 1

How many of you have actively been involved in helping your customers with Cybersecurity matters?

- Yes, I have been actively involved
- No, I have not been actively involved

Threat Landscape - FSI in the news

FSI data breaches & cyber attacks are common news stories

Insurance giant Aon confirms it has suffered 'cyber incident'

Oh the irony! Insurance companies, even those selling cyber insurance, are attack targets

March 2022

SCOTIABANK EMPLOYEES LEAKED CUSTOMER DATA. THE BANK IS CONTACTING AFFECTED USERS FOR SECURITY BREACH

July 2020

Criminals Resurrect A Banking Trojan To Push COVID-19 Relief Payment Scam

March 2020

How Even Emails Leave Robinhood Users Exposed to Financial Criminals

Savvy customers who ignore the latest data breach could pay dearly if they aren't careful.

November 2021

Some TurboTax Accounts Were Hacked Due To Poor Passwords

July 2021

Banking industry sees 1318% increase in ransomware attacks in 2021

September 2021

Major Chilean bank shuts down all branches following ransomware attack

There is a nationwide alert for future ransomware campaigns against Chilean companies.

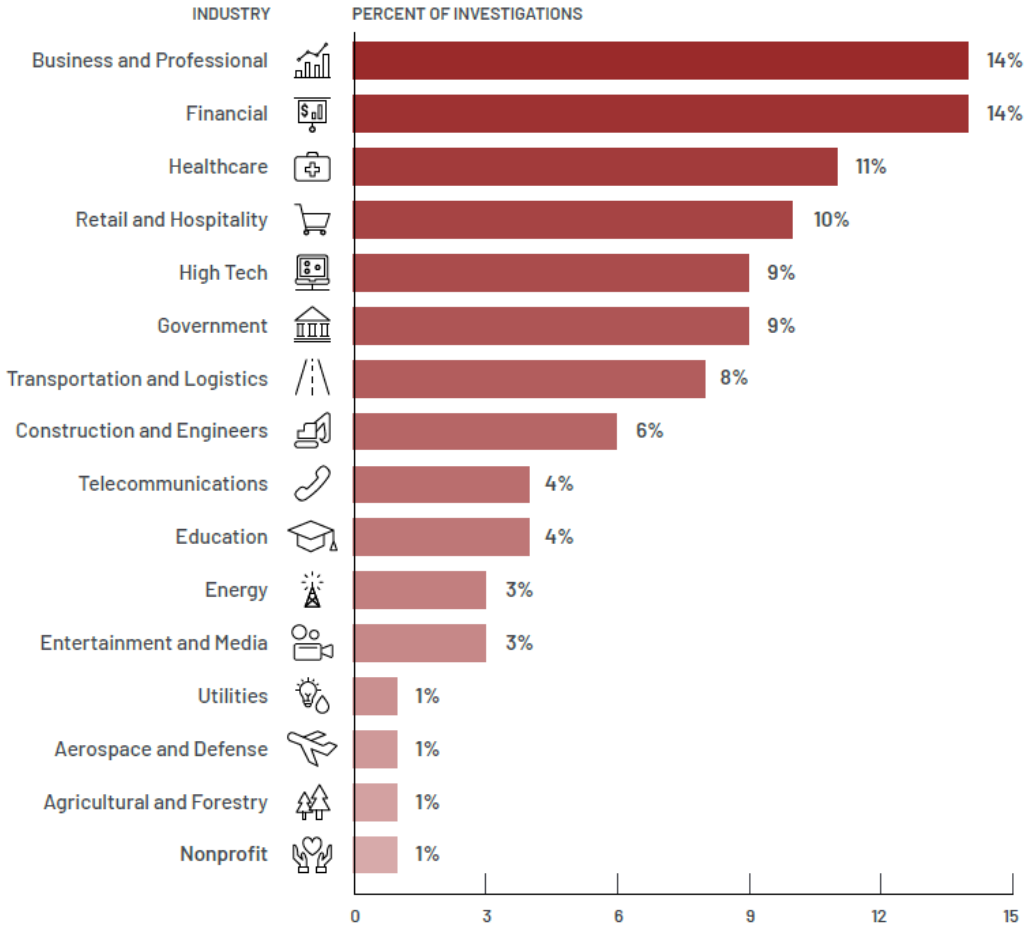
September 2020

Morgan Stanley faces data breach, corporate client info stolen in vendor hack

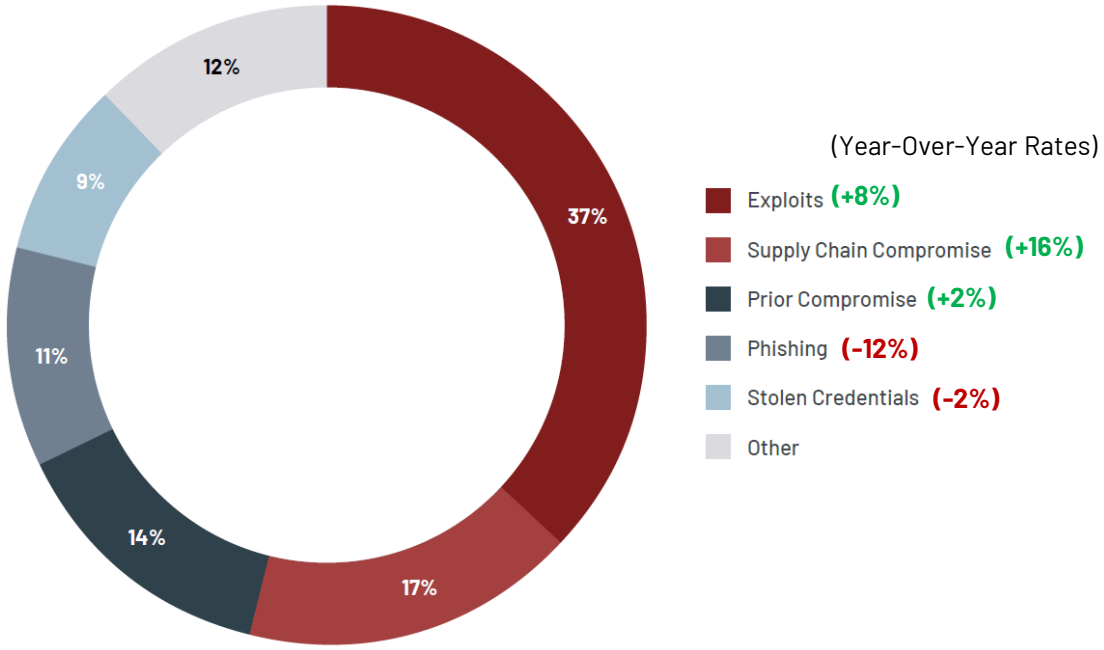
July 2021

Exploits & Supply Chain Attacks Are The New Normal

Business/Professional Services and FSI remain the top targeted industries globally. Retail and hospitality, healthcare and high tech round out the top five (5) industries favored by adversaries.



Initial Infection Vector, 2021 *(When Identified)*

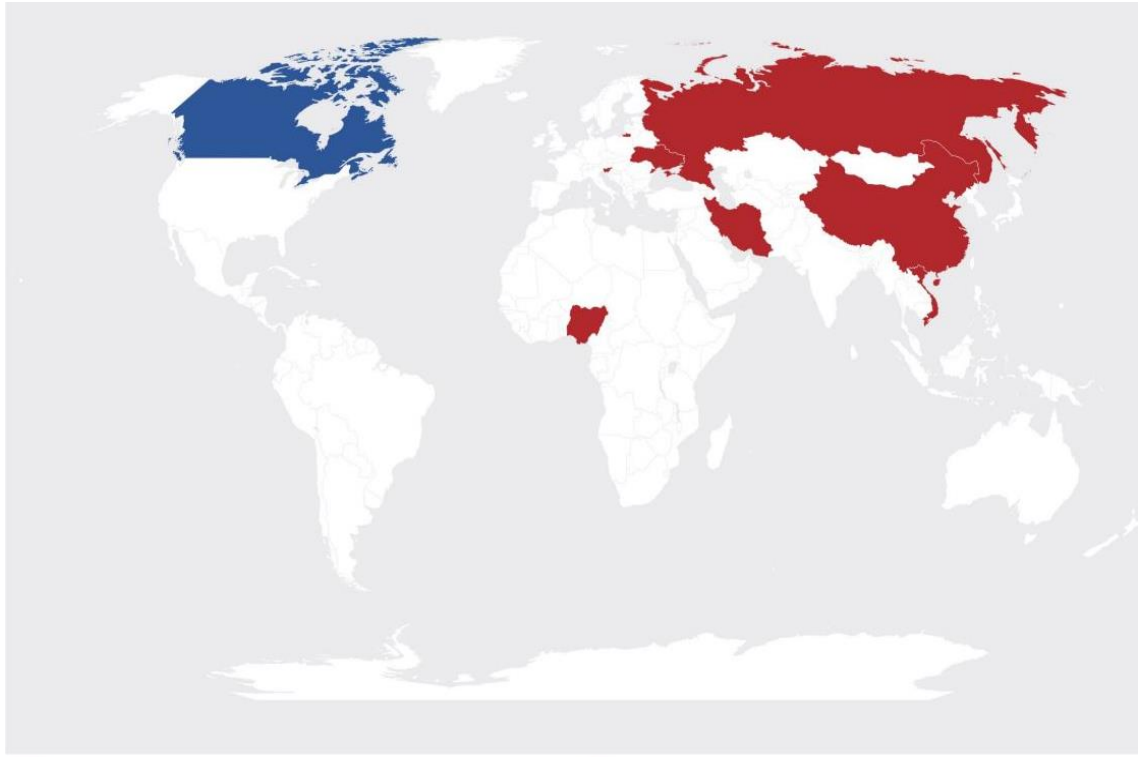


Focus on Canada

Canada has a very "typical" threat landscape, with FSI as its most targeted vertical

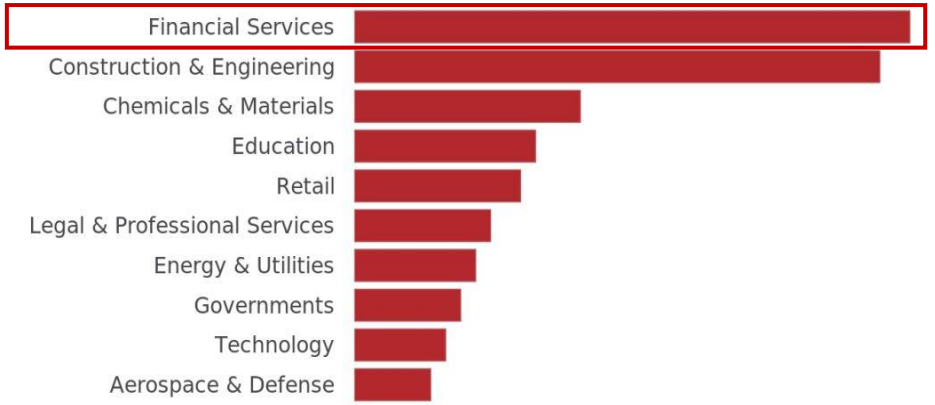
GEOGRAPHIC TARGETING

Typical "Big 4" targeting (Russia, China, Iran, N. Korea).
Other minor players include: Nigeria, Vietnam, Ukraine & other Eastern EU locations.

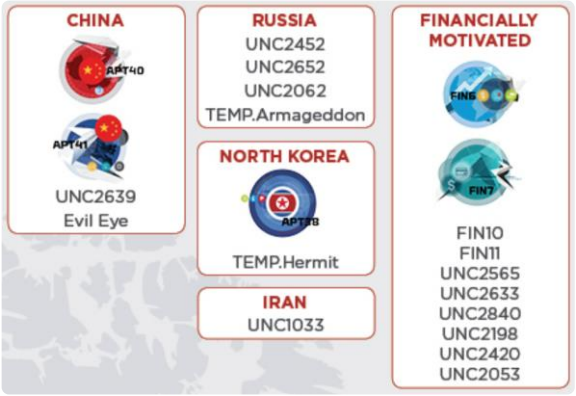


INDUSTRY TARGETING

FSI is consistently ranked #1, with financial gain as a constant motivation.



OBSERVED THREATS



MALWARE TARGETING

Russia-Ukraine Cyber Warfare Collateral Damage

The Ukraine cyber war is has brought operational resilience back into the spotlight

RUSSIAN CYBER NEXUS

Proxy warfare through cyber privateering

- Leverage cyber-criminal groups for foreign interventions.
- Privateering to dodge direct attribution.

High volume, loosely managed destructive attacks

- Almost exclusive focus on operational disruption & destruction.
- Limited accuracy considerations (low opsec).

Escalating threats against NATO & cyber warfare expansion

- Increase destruction & espionage attacks in EU countries (i.e.: Germany)
- Propagated / collateral damage from Ukraine-targeting attacks & malware.

CANADA THREAT PROFILE

NATO sanctions participation

- Russia has directly threatened aggressive response based on NATO sanctions.

Sub-warfare retribution attacks

- Destructive actors are likely to stay under direct cyber warfare thresholds.
- Energy, Agro., and FSI are still considered primary targets.

Geographical considerations

- Canada is a Russian neighbor.
- Canada is highly interconnected with the US and may be subject to direct or collateral damage.

Russian-backed privateering

FSI targeting likelihood at *Med-High*

Destructive actor

Custom malware (likely wipers)

*All threat intelligence from Mandiant.

Cloud Considerations

Cloud is the fastest evolving threat landscape

INITIAL ACCESS VECTOR

CREDENTIAL HIJACKING
- Credential re-use, theft, and resell
- Lateral movement from on-premise
- Phishing (or social engineering)
- Illicit consent grant by users

MISCONFIGURATIONS
- API attacks
- Exposed repository
- Exposed key / secrets
- Human error

VULNERABILITY EXPLOITATION
- Cloud vulnerabilities increasingly found as security research (and attacker) scrutiny increases

SUPPLY CHAIN COMPROMISE
- Leveraging existing trust relationships (vendors)
- Vulnerabilities in tools & software

DENIAL OF SERVICE – DOS/DDOS

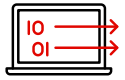
IoT-powered

Continually growing (new record each quarter)

Hacktivism-driven...

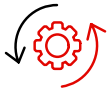
...or extortion driven

TOP CLOUD RISKS



1. **Data exposure**

2. **Account hijacking**



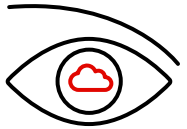
3. **Misconfiguration**

4. **Insider threat**

5. **Denial of Service (DOS)**

KEY CLOUD SECURITY TOPICS

Identity & Access Management (IAM)



Network & detection

Governance & Data handling

POLL 2

How many of your customers have migrated to the cloud?

- All of my customers have migrated to the cloud
- Some of my customers have migrated to the cloud
- None of my customers have migrated to the cloud

Canadian Cyber Regulatory Landscape

Federal & provincial legislations of Personal Information (PI)

FEDERAL LEGISLATION

Personal Information Protection and Electronic Documents Act
PIPEDA (2000)

- Federal privacy law for all interprovincial and international activities involving PI.
- Intra-provincial business coverage exceptions.

See infographic →

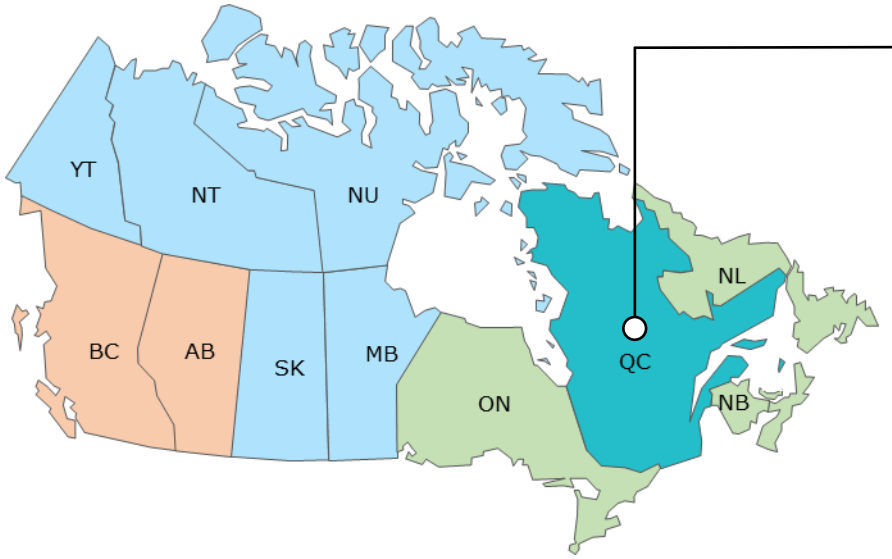
Digital Privacy Act
DPA (2015)

- Amendment to PIPEDA
- Mandatory breach reporting, notification, etc.

OSFI OVERVIEW

- Independent federal agency regulating and supervising FSI entities
- OSFI Advisory *B-13 Technology and Cyber Risk Management (2021)* requirements
- Requirement for incident reporting within 24 hrs

PIPEDA COVERAGE PER PROVINCE



- PIPEDA fully applied
- PIPEDA fully applied, except involving health information (PHI), as health-related privacy laws are in effect
- PIPEDA is not applicable outside of inter-provincial/national data processing [Follow Personal Information Protection Act – 2004]
- PIPEDA is not applicable outside of inter-provincial/national data processing

La Belle Province
Québec is subject to its own set of PI-handling regulations, such as:

- Québec Private Sector Act
- Québec Access Act
- Québec Information Technology Act
- Bill 64 (now called Act 25)

Most recent legislation

GDPR IN CANADA

The EU regulation (GDPR) is relevant for Canadian organizations that handle PI of individuals (i.e.: employees, clients) located in the EU.

The EU GDPR enforces a 72-hour reporting requirement for all breaches of PI.

UPCOMING LEGISLATIVE CHANGES

Bill C-26 — Bill C-26
Act Respecting Cyber Security (ARCS)

Bill C-27 — Bill C-27
Digital Charter Implementation Act (DCIA)

Strategic Considerations - Ransomware

Key metrics & trends observed

FASTER & INNOVATIVE THREAT ACTORS

21 Days	Global median dwell time (17 for FSI)
5 Days	Global median dwell time for ransomware only
514	Newly tracked malware families

EVIL AS A SERVICE

- Ransomware-as-a-Service (RaaS)
- Initial access-aaS
- Phishing-aaS
- DDoS-aaS
- Etc-aaS

Commoditized underground cyber market

RISE OF MULTIFACETED EXTORTION

POLL 3

Have you been exposed to Ransomware at a client organization?

- Yes
- No

Ransomware: Fundamental Challenges

Many organizations are not prepared to deal with a large-scale ransomware incident

Identify

Insufficient institutional understanding and management of ransomware risk

Detection:

- Delayed detection
- By the time the incident is escalated, ransomware is already deployed

Response

- Containment measures can not be implemented quickly
- Response playbooks are not in place
- Recovery effort destroys forensics data
- Resource scalability and staff burnout

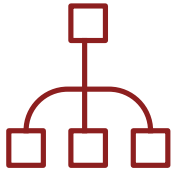
Protect:

- Active Directory and lateral movement hardening
- Endpoint hardening

Recover:

- Communication strategies do not scale
- State of backups
- Decision to pay to protect the data or recover keys
- Disaster recovery processes are not designed to survive large scale IT disruption
- Enterprise-wide password reset is slow

Key Ransomware Recommendations



Board

Manage the risk of disruption, destruction, and organization impact

Prepare for financial impact and ensure crisis plans are in place

Leverage experience from other incidents

C-Suite

Implement rigid response plans: Backups, Segregation, and Disaster Recovery

Continually test and assess information security capabilities

Empower analysts to perform their duties; give them the tools they need

IT Team

Establish Cyber Incident Response Plans and Playbooks

Establish offline backups and validate ability to recover from them

Develop and implement a privileged access management strategy

POLL 4

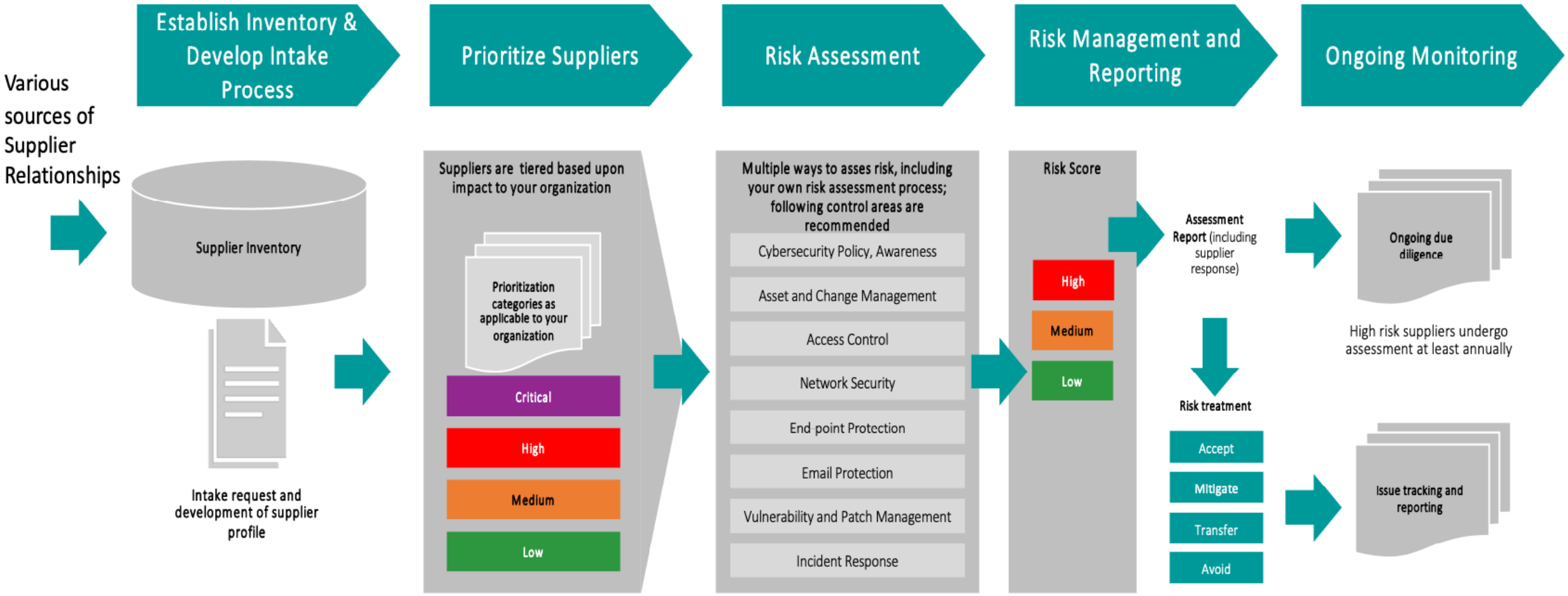
Do you feel your organization is prepared to respond to a Ransomware attack?

- Yes, we are prepared
- Some what prepared
- Not prepared

Baseline SCRM Approach

- Establish and integrate a formal Supply Chain Risk Management (SCRM) across the organization and define formal accountability.
- Program objectives: identify and manage the cyber security risk exposed to the organization through its suppliers.
- Supply Chain Risk Councils Proactively:
  - Review relevant risks and risk mitigation plans
  - Set priorities
  - Share best practices
  - Pilot initiatives
- Benefits of Councils:
  - Shared risk decision-making
  - Closer collaboration
  - Better understanding of risks by Leadership

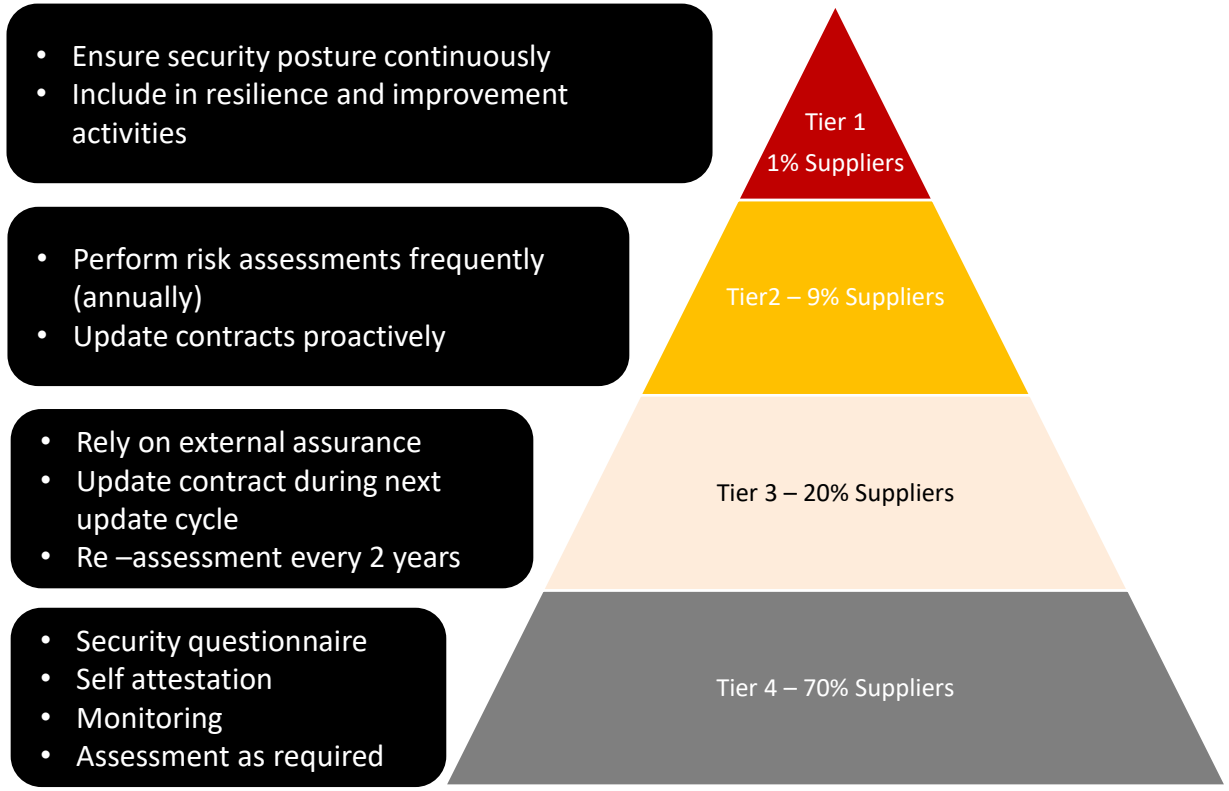
Supplier Risk Management End-to-End Process



Source: Health Industry Cybersecurity Supply Chain Risk Management Guide v2.0.pdf

Supplier Risk Tiering

- Revenue contribution of suppliers
- Whether a supplier processes critical data belonging to the acquirer, such as regulated data (e.g., PII, PHI) or intellectual property
- Revenue impact
- Operational Impact/Business Criticality/Geopolitical
- Reputational Impact
- Regulatory Compliance
- Volume of data a supplier has access to or hosts
- Whether a supplier has access to the acquirer's system and network infrastructure
- Whether a supplier can become an attack vector by being compromised and allowing threat actors access to the acquirer
- Whether a supplier can become an attack vector for the company's products or services delivered to customers



Software Supply Chain Risk Management – Key Practices

- Vendors should be required to participate in the National Vulnerability Database (NVD), including Common Vulnerabilities and Exposures (CVE) and Common Vulnerability Scoring System (CVSS), to characterize, categorize, and score vulnerabilities.
- Inclusion of the software vendor in dark web vulnerability, threat intelligence and breach monitoring services.
- All software updates should be signed by the vendor and should be verified for integrity prior to implementation.
- Software update process including details on the external connectivity requirements for downloading the software updates should be documented in the software security profile.
- If possible, updates should be pushed via an internal update server or endpoint patching solution after signature validation is conducted.
- The software should be associated with dedicated service accounts with least privileges required.

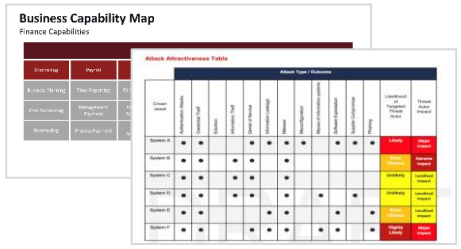
An Approach for Increasing Resilience

Protecting what matters is all that matters

CJ approach is divided in 4 phases:

Identification

Define, identify, and inventory business capabilities and core supporting systems.

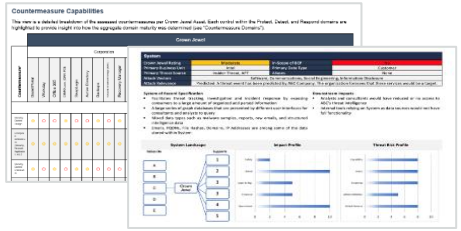


Risk Assessment

Assess identified systems across multiple impact categories.

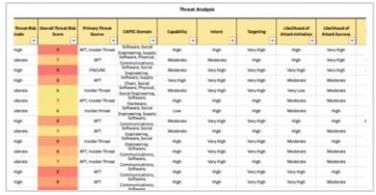
Countermeasures

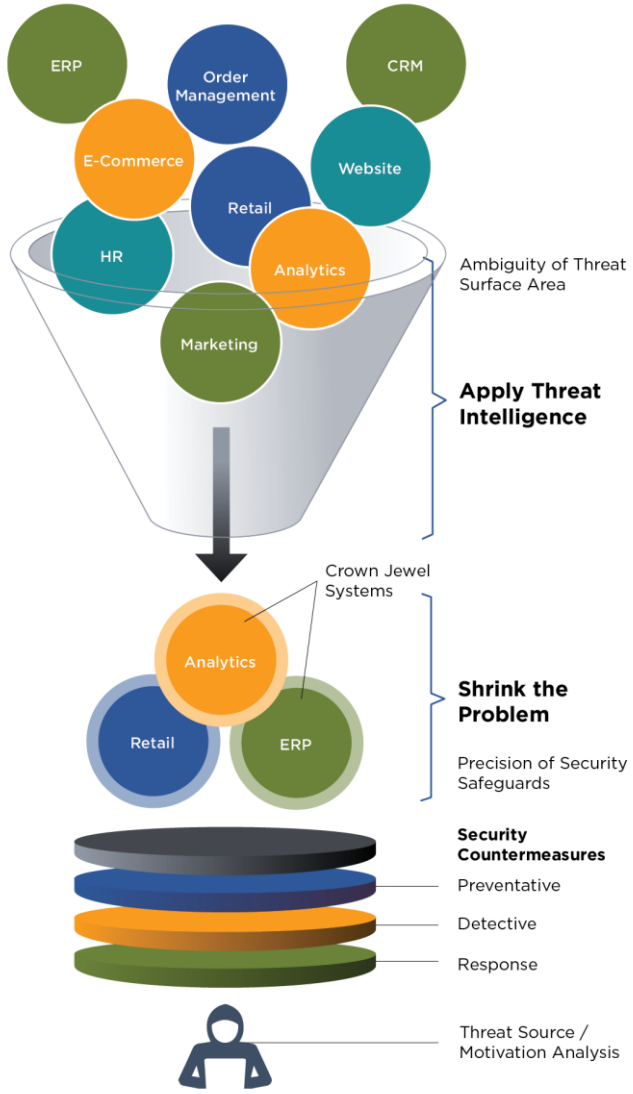
Identify security controls in place on each systems.



Reporting

Aggregate all inputs, provide executive and technical overview.





Conceptual Top-Down Progression

...And Now To Protect Those Crown Jewels

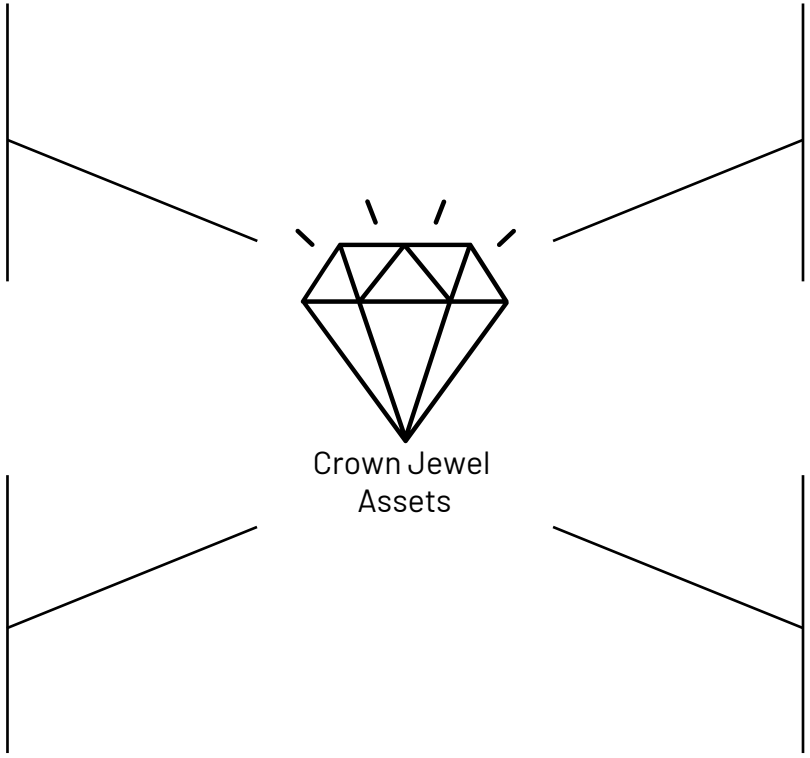
Leverage Mandiant's approach to ransomware defense on Crown Jewels first

1 ARCHITECTURE

- Network segmentation
- AD architecture
- Cloud architecture
- Identity & access management (IAM) program

2 SECURITY CONTROLS

- Email security
- Web security
- Endpoint controls
- Network controls
- Infrastructure management



3 INCIDENT RESPONSE

- Governance: IR Plan, Playbooks
- Rapid response capabilities
- Preparedness: TTX, purple teams
- Ransom strategy
- Most importantly: *Retainers*

4 RECOVERY PLANNING

- Backups
- Recovery testing
- BC & DR programs

Additional Industry Leading Practices

- Continuous **red teaming** of environments
- Requiring **dual factor authentication** on all remote access
- **Incident response plan** that addresses extortion as well as threat actor communications and payments
- Ongoing searches for **indicators of compromise** across the environment
- Inventorying **service accounts** and resetting passwords on a consistent basis
- Leveraging **threat intelligence** to make risk-based decisions and define the security strategy

Conclusion

Key Takeaways and Resources

There’s no single silver bullet: combination of people, process, and technology

1

KNOW YOUR CROWN JEWELS

- Strategic and structured approach
- Leverage defined frameworks such as NIST CSF, and more defined guidance frameworks on Cyber Risk, Ransomware, Supplier Risk Mgmt, etc.

2

PRIORITIZE YOUR SECURITY EFFORTS CORRECTLY

- Defense in depth approach
- Exercise your processes

3

YOU ARE NOT ALONE, HAVE FIREFIGHTERS ON STANDBY

- Incident Response Surge Support
- External Counsel
- Crisis Mgmt and Communications

THANK YOU!

Marcus Troiano – Cyber Strategy Practice Lead (Eastern Canada)

Marcus.Troiano@Mandiant.com

+1 647 885 0714

WHAT'S UP NEXT

The 2nd Wednesday of the month 12:30pm eastern

- December 14: Exploring Canada's Entrepreneurship Ecosystem with Kayla Isabelle
- January 11, 2023 Coming soon
- November 15 CONVERGE a Unique Virtual Networking Opportunity
  - Featured speaker Kevin Gangel, CEO of Unstoppable Conversations
- Now Available What's Up Wednesday recorded sessions
- CMC-Ontario Presentation Library PDF download of all past

THANK YOU

CMC
ONTARIO

INFO@CMC-ONTARIO.CA
HTTPS://CMC-CANADA.CA/ONTARIO