AON

ALIA Universal Cyber Coverage Webinar:

Cyber Loss Prevention Seminar

ALBERTA LAWYERS INDEMNITY ASSOCIATION

Welcome message

ALBERTA LAWYERS INDEMNITY ASSOCIATION

David Weyant, K.C.

President and CEO

Alberta Lawyers Indemnity Association

AON

An Introduction to the Team

Presented By:

Katie Andruchow, AON,
National Cyber Broking Practice Leader

Che Bhatia, AON,
Managing Director, Stroz Frieberg

Dan Elliott, ZURICH,
Principal, Cyber Security Risk Consulting

AON

Agenda

1

ALIA Universal Cyber Program

- Overview of Limits & Coverage
- Key controls concept

2

Cyber & Privacy Threat Landscape

- Threat Landscape
- Top Loss Trends
- Forward Looking Comments

3

How to Prepare and Protect

- Strategies to Handle Cyber Risk
- Tools to Handle Cyber Risk

Cyber Program Overview

AON

ALIA Universal Cyber Program Overview

Liability Claim Costs

	Deductible
$250,000 each Claim / $250,000 Aggregate each Law Firm **For Coverage 1. Security Liability Coverage**	$5,000
$250,000 each Claim / $250,000 Aggregate each Law Firm **For Coverage 2. Privacy Liability Coverage**	$5,000
$250,000 each Claim / $250,000 Aggregate each Law Firm **For Coverage 4. Regulatory Proceedings**	$5,000

https://www.lawsociety.ab.ca/lawyers-and-students/alberta-lawyers-indemnity-association/universal-cyber-coverage-program/cyber-coverage-faqs/

ALIA Universal Cyber Program Overview

First Party Response Costs

	Deductible
$35,000 each Claim / $35,000 Aggregate each Law Firm **For Coverage B Breach Cost coverages, Cyber Extortion Coverage**	$5,000

Maximum amount claimable per firm in a policy period is $285,000

Key Areas of Underwriting Focus, Aon's Recommendations

Key Areas of Underwriting Focus

Multi-Factor Authentication (MFA)	Endpoint Protection and Response (EDR)	Phishing Exercise/Cyber Awareness Training
Patch Management	Secure RDP/VPN	Incident Response Plan
Previous Incidents and Containment	Disaster Recovery/ Backups	Email Filtering

Aon's List of Critical Network Security Controls

1. Multi-factor authentication (MFA) for:
   Email, privileged accounts, all remote access
2. Security & phishing awareness training
3. Regularly Conducted Assessments
4. Properly configured URL filtering and email attachment sandboxing
5. Advanced endpoint detection and response (EDR) solution
6. 24/7 Managed SOC (Security Operations Centre)
7. Advanced malware detection tool that inspects network traffic
8. 16+ character service account and domain admin passwords
9. Lateral Movement Detection Tools
10. Properly configured security information and event management (SIEM) platform
11. Continuous security monitoring function
12. Business Resilience
13. Disabling accessibility of remote desktop directly from Internet

AON

Cyber & Privacy Threat Landscape

Aon Cyber Solutions – Stroz Friedberg
Che Bhatia, Managing Director
February 2023

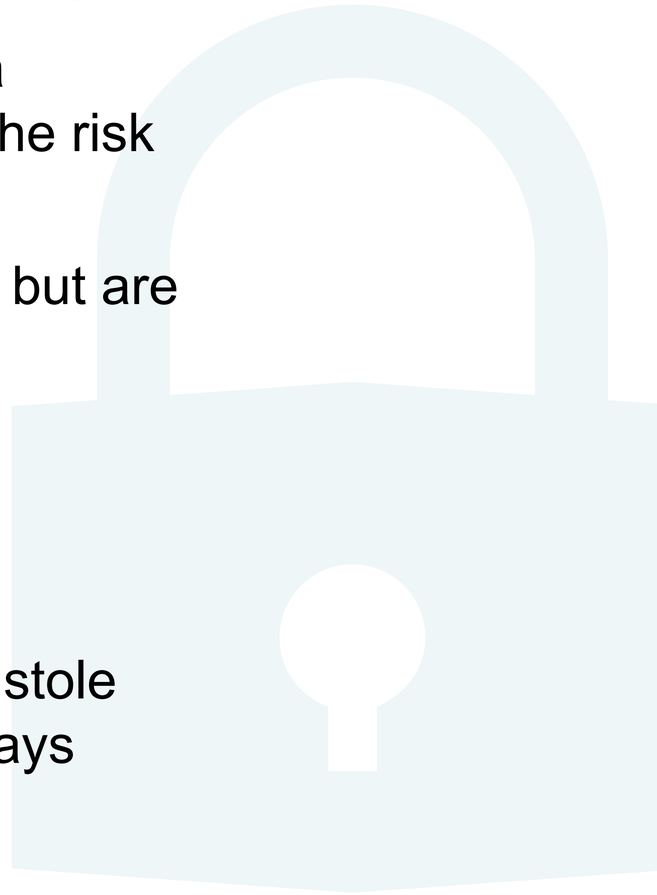
Understanding the Cyber Threat Landscape

- COVID-19 – forced most in the private and public sectors to lift and shift entire workforces in a very short period of time causing low hanging fruit for the attackers.
- Hybrid work environments are a greater risk. Confidential client information is spread widely across a distributed and virtual environment
- Ransomware continues to be an issue for law firms. Greater diversity of ransomware variants
- Targeting of Managed Security and Service Providers for downstream customers
- Professional services (like many industries) are having a tough time engaging and retaining cyber talent, and struggles with fewer resources keep organizations behind while cyber criminals are getting smarter with how to enter these systems
- Attackers are targeting organizations with large amounts of data. Law firms have massive amounts of organizational financial data, sensitive information regarding merger and acquisitions, client information, etc.
- Insider threats

Trend #1 – Ransomware, but Hold the Ransomware

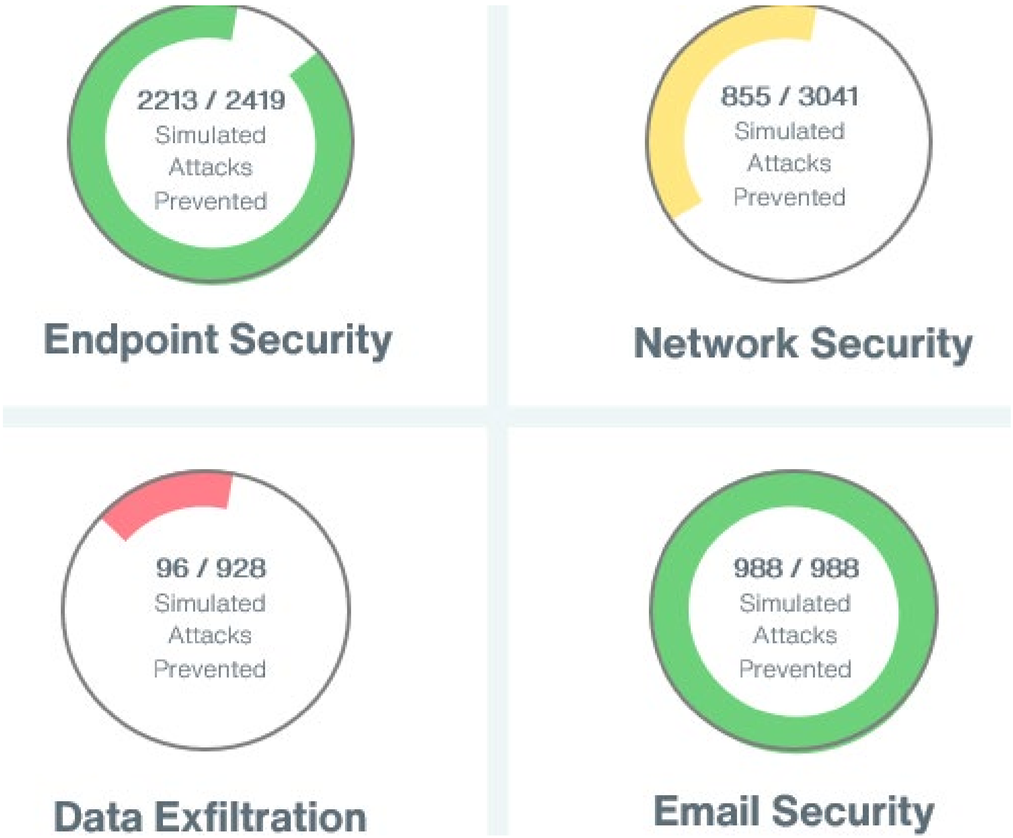
Overview

- Ransomware is still one of the most prominent threats affecting law firms
- Attacks against law firms are trending slightly down, and backup/data recovery trends are looking positive for firms proactively addressing the risk of ransomware
- Tactics and techniques of ransomware actors vary quarter to quarter, but are generally characterized by:
    - Opportunistic exploitation of newly discovered vulnerabilities
    - Increasing reliance on the threat of data theft to attempt ransom collection
    - In terms of data exfiltration, nearly all attackers who successfully stole data were observed staging and stealing data just hours or 1-2 days before executing ransomware



AON

Trend #1 – Ransomware, but Hold the Ransomware

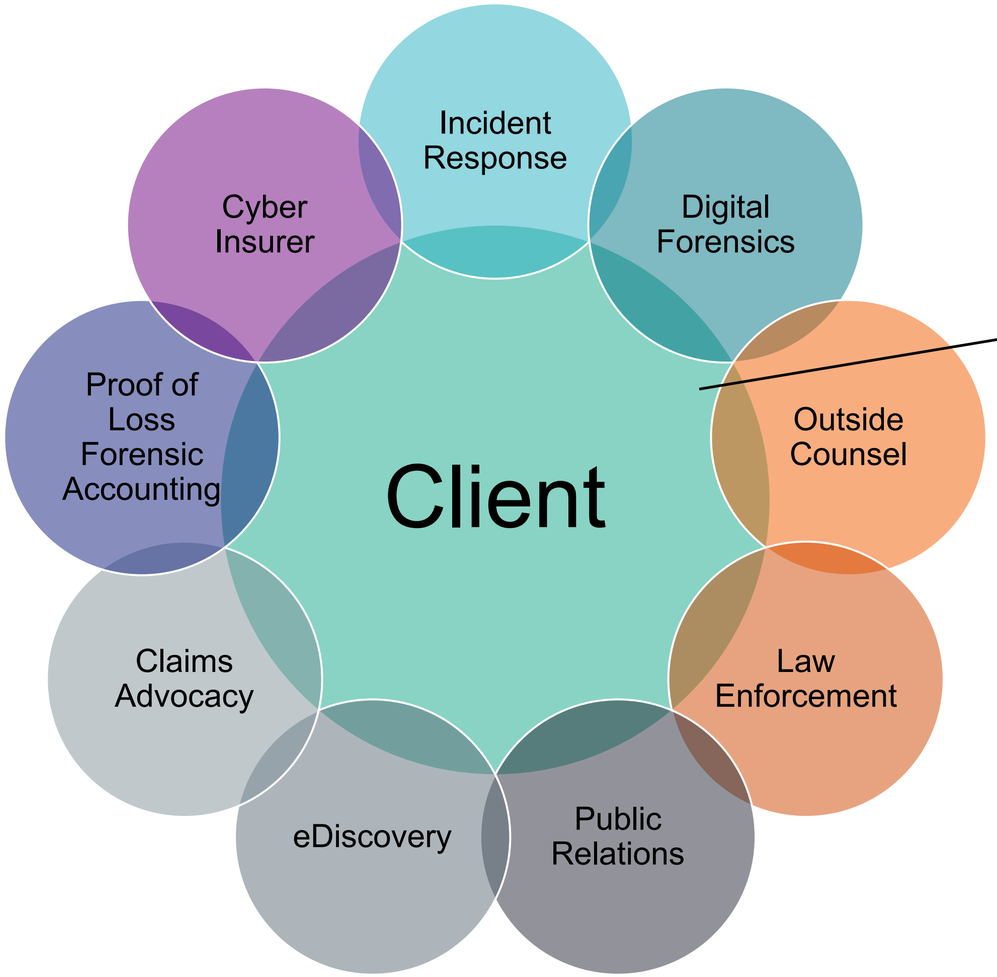


Staying Ahead of the Curve

- Ensure that security solutions, like EDR tooling or network monitoring, can be used to identify or proactively prevent massive data transfers
- Conduct attacker simulations to identify potential avenues through which a malicious actor could compromise organizational systems and attack critical assets.
- Leveraging a library of adversary tools and techniques to test the efficacy of your defensive controls at preventing attacks across the functional security domains of Endpoint Security, Network Security, Data Exfiltration, and Email Security.

AON

Trend #2 – Lack of Incident Response Preparedness



Incident/Breach Response Readiness:

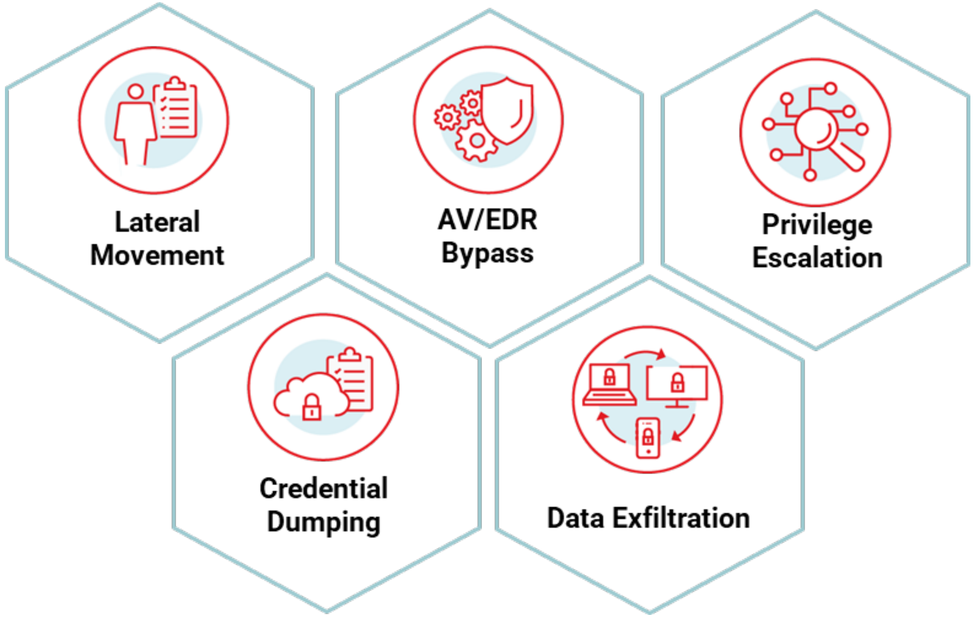
- IRP/BCP/DRP Review/Development
- Playbook Development
- Master Services Agreement
- Systems Readiness
- Cyber Tabletops/Threat Simulations
- SOC Optimization
- Stakeholder Placemats

AON

Early 2023 – Trends & Predictions for Law Firms

High Level Trends

- Attackers are capable of breaking or avoiding singular security controls
    - MFA bypassing, EDR avoidance, and use of administrative tools are still trending
    - Defense in depth is key, including controls at the application, host, and network levels
- Shame blogs, law enforcement takedowns and poor operational security by criminals means more and more breaches are being exposed to the world by 3rd parties



- Well-managed security controls continues to define the difference between and “intrusion” and a “data breach”
- The high watermarks in cryptocurrency markets + international market volatility informs viability and profitability of ransomware, extortion demands, and dark web markets
    - Attackers, especially organized criminal entities, run like businesses. These are more incentivized when the means of payout are high and traditional markets are lower
    - Economic factors also increase the temptation of financial insider threat in entry-level roles

AON

Cyber Risk
How to Prepare and Protect

Zurich Resilience Solutions – Cyber Services
Dan Elliott, Principal, Cyber Security Risk Consulting
February 2023

AON

General Ransomware Planning

More than 60% of Canadian companies were impacted by ransomware in 2021.
Data exfiltration in connection with ransom demands has now become normalized.

95% of CIOs admitted to struggling with developing a vision for digital change and upgrades

45% of CEOs have digital transformation and cyber risks on the top of their agenda

32% of businesses can respond to a breach immediately. Even “simple” attacks affect the business negatively for at least one full week

67% of CISOs think ransomware attacks are the most significant cyber risk they currently face

Sources of numbers: Marsh, Wavestone, CISO surveys 2021: The future of cyber survey from Deloitte; PWC’s Digital Trust Insights Survey; 2022 Gartner CIO Survey.; Telus Canadian Ransomware Study 2022.

Where are you spending for security?

11% The average spend on security of an organization's IT budget.

70% of incident costs incur for emergency assistance, IT forensics, data restoration and crisis communication assistance.

16% Average ransomware payment out of overall recovery costs

14x The exponential growth in ransom demands to SMEs from 2018 to 2021

Sources of numbers: CISO surveys 2019: The future of cyber survey from Deloitte; PWC's Digital Trust Insights Survey; 2019 Gartner CIO Survey; 2022 Heidrick CISO Survey.

Understanding your current state

Identify your Crown Jewels

What data or physical assets are most important in your business?

Contracts?

Client data?

What are the Threats?

Malicious actors?

Insider threat?

Criminal?

Vulnerabilities or Existing Controls?

What are the weaknesses or protections in place that will impact a threat reaching your core business?

Old equipment?

Inexperienced staff?

Lack of cyber controls?

Self Risk Assessment

Threat	Vulnerability	Asset	Impact	Likelihood	Risk	Control Recommendation
Malicious human interference - hacker High	PAM in place; servers are elevated priv; data encrypted at rest. Low	Student records (PII, academic audit, ACA, transcripts, etc.) Critical	Student records lose integrity; reputation loss; backups take 8 hours to reload if captured. Critical	Low External pentest and vulnerability test positive results	Medium Potential loss to the university is critical but significant controls in place.	Regularly test backups with full failover test. Continue external testing.
Infrastructure - Water intrusion High	Aging infrastructure/ maintenance scheduled High	Servers Critical	All services from Registrar's Office and Central Admin unavailable. Critical	Medium Flood of another building two years ago.	High Potential loss of $75,000 plus any reputational loss	Install water mitigation in server room. Press for water pipe upgrade in affected building.
Malicious human (interference) – DDOS attack Medium	Firewalls are configured; SOC monitoring; however multiple faculties are able to access website for editing and potential reconfig remotely Medium	Website Medium	Website resources and email addresses associated unavailable. Medium	Medium National statistics show increase in DDOS attacks within higher education	High Potential loss of $20,000 per hour	Monitor firewalls. Regularly assess configuration.
Malicious human interference – theft High	Decentralized IT resources with faculty; lack of visibility on software and configuration; Limited monitoring High	Research data at labs Medium	Research data could be lost or stolen. Medium	Medium Lack of visibility on faculty servers to fully assess	Medium	Offer faculties use of centralized university servers to lower cost and standardize security controls.

Determine Your Minimum Security Standard

Your unique footprint
How large is your organization?
Do you operate in the cloud or on-premise?
Do you have multiple vendors?

Your financial position
How much do you have to spend on cyber security?
What is your insurance coverage?
What do you have at risk?

Your brand equity
What are the expectations of your clients?
What is your reputational risk in an incident?
With which brands do you want to be associated?

Your people
What is the technology comfort level of your team?
Do you have a dedicated Information Security person or team?

Canadian Centre for Cyber Security

CIS Critical Security Controls

NCSC Cyber Essentials

ASD Essential Eight

Three Pillars of Cyber Security

Cyber Risk Assessments

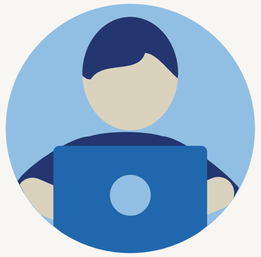
An assessment is focused on helping you understand and improve your risk to your core assets in three areas. The assessment enables you to:

Analyze your core business processes

Find weaknesses in your setup of controls

Benchmark the maturity of your cyber posture to industry peers

Identify and prioritize countermeasures



People

Executive leadership team education

User awareness training

Security team training

Hiring practice security guidelines

Access management

Technology

Recommendations for a range of specialized technology solutions

Process

Cyber security strategy

Capability road map

Policy and procedure development

Management metrics for cyber security

Essential Controls to Consider

Control	Question to ask yourself
Inventory and Control of Assets	Do you know what you own and/or for which you are responsible?
Patch Management	Do you have a formal process in place to update hardware and software?
Strong User Authentication (Multi-factor Authentication)	How do you access applications? Do you use more than a password?
Restrict Administrator Privileges	Do you use the same login to surf the internet as you do to install new software?
Data controls	What is your formal process to identify, classify, retain and dispose of data?
Backup and Encryption	Could you restore your key systems if they disappeared tomorrow?
Network Monitoring and Defence	Who is watching for unauthorized access while you are sleeping?
Employee Training and Testing	What is the frequency of your employee training? What is their understanding?
Incident Response Management	Do you know who to call on a really bad day?
Secure Mobile Devices	Do mobile devices have similar controls to workstations or is their access unfettered?
Testing (Penetration Testing or Vulnerability Assessment)	Do you have anyone verifying what you are doing?

Questions and FAQ

[Cyber Coverage FAQs – ALIA's webpage on the Law Society of Alberta Website]

[ALIACyber@aon.ca]

FAQ How to Report a Claim

Urgent crisis management and/or reporting of a claim/ circumstance

If urgent crisis management or legal advice is needed following a cyber attack: Please contact the designated incident response breach coach: **Designated Breach coach** **Imran Ahmad** 1-866 -BREACHX / 1-866-273-2249 nrfc.breach@nortonrosefulbright.com This contact information is toll-free and available to access 24 hours 7 days a week.	To provide formal notice of a claim or a circumstance to the insurer: Send claim details to: **Notification Email**: Claims@zurich.com Phone: 1-866-345-3454; Fax: 1-877-977-8077 Zurich Insurance Company Ltd First Canadian Place, 100 King Street West Suite 5500, P.O. Box 290 Toronto, ON M5X 1C9

FAQ

In a loss scenario can I utilize my own vendor for incident response?

- All incident response work should be done by firms on the vendor panel established by Zurich

- If there are conflicts of interest or unique needs to procure work outside the panel, this will be assessed on a case-by-case basis either during the claim consultation process or in advance of a loss by contacting ALIAcyber@aon.ca

AON

Thank You!