Vantage

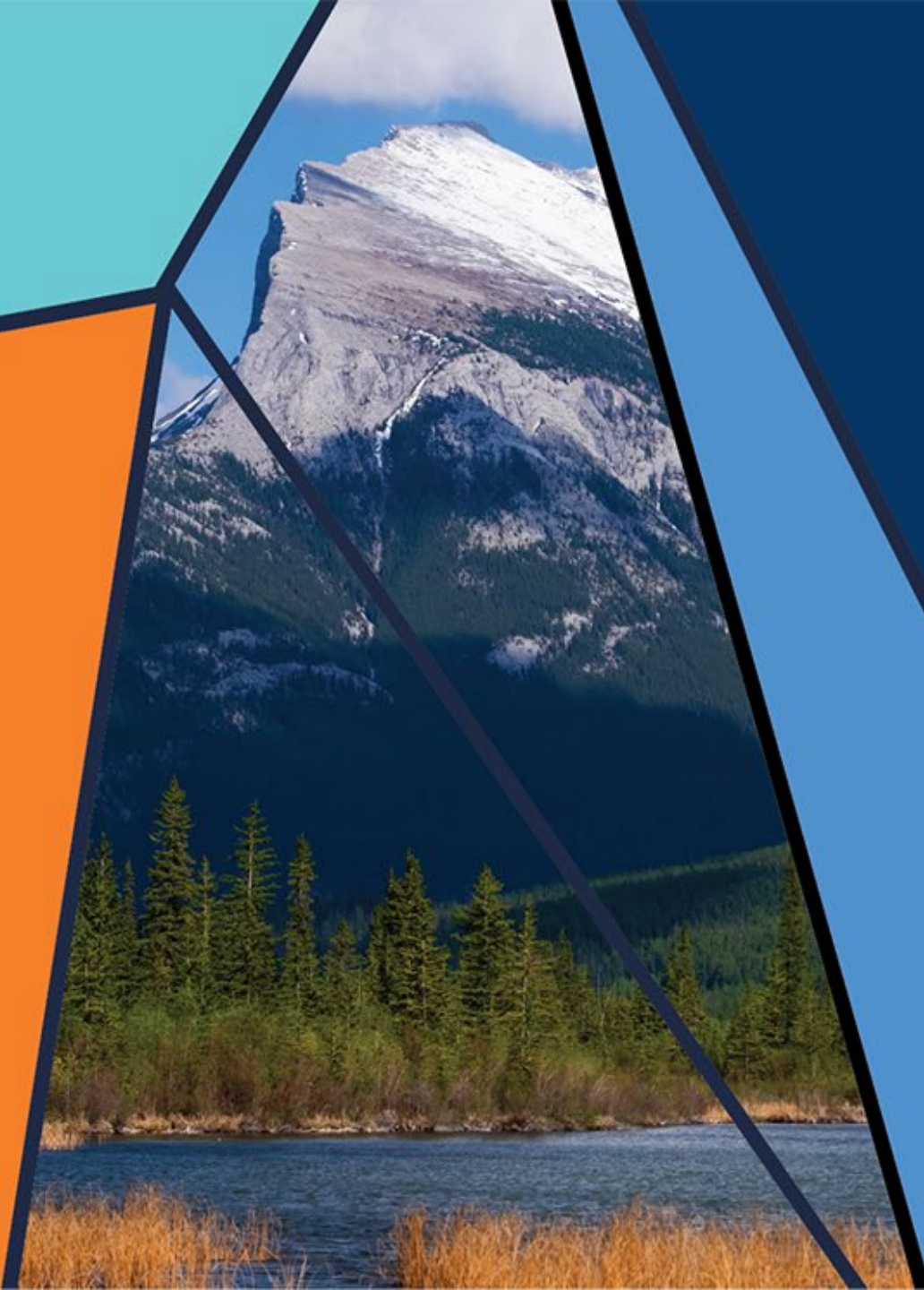
Lapp strong & secure 60 years

AIMCo

Building Value for Public Pensions

Cybersecurity and Ransomware

Is Your Organization Cyber Savvy



Ooops, Your Files have been Encrypted

Your network has been infected!

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

To decrypt your files you need to buy our special software - **General-Decryptor**

Follow the instructions below. But remember that you do not have much time

General-Decryptor price

the price is for all PCs of your infected network

Time is over

* You didn't pay on time, the price was doubled

Current price

259289 XMR

≈ 100,000,000 USD

Monero address: 86u2HFPhvXt5PycXDh1zSKJ3xa6dmRu9FCH;

* XMR will be recalculated in 2 hours with an actual rate.

Alberta Pension Services Corporation

Introduction

- Alberta Pensions Services Corporation (APS) provides administrative services to more than 500 participating employers and over 370,000 members and pensioners across Alberta.
- Located in Edmonton, Alberta
- Approximately 340 employees

Vice President, Information Services and Technology
Joined APS in June 2014 with over 30 years of IT Industry experience.
Certified Project Management Professional (PMP) and ITIL Certified.

Cyber Team:

- Michelle Desnoyers -Corporate Information Security Officer
- Maharaj Vinayagam - Senior Cybersecurity Specialist
- Jamie Macnaughton – IT Security and Risk Management

Key Activities in 2021

- **Pandemic response, *secure Work From Home* and continuous monitoring of Provincial Operation Centre and AHS direction to ensure safety on-premise and remotely.**
  - **Enforced VPN** – Transition to GlobalProtect VPN for applicable managed APS devices, including client users.
  - **Strong passwords** – delivery of user password education and transition to stronger passwords for user and service accounts.
- **Continuous improvements of:**
  - **Business Resilience** – supported by robust **Change Management** and **Release Management.**
  - **Enterprise Security Management Platform** – suite of services (such as email threat protection) which adaptively protect against, and rapidly detect and respond to, cyber-related events 24/7.
  - **Managed Security Information and Event Management (SIEM)** - a 24/7 service monitoring security event logs and alerting on potential security incidents.
  - **Vulnerability Management Program** – process establishment for scanning and assessment, web application security testing, zero-days, and penetration testing.
- **Continuous development and delivery of the Security Education and Awareness Program, utilizing training modules, simulated phishing campaigns, and promotional activities.**
- **Pension System Disaster Recovery test – successful execution of a DR test, including pension payroll.**
- **Ransomware readiness – acquisition of cyber insurance for enhanced response capabilities, plus internal dynamic tracking of current controls and improvements for cyber events and IT disruption protection and response readiness.**

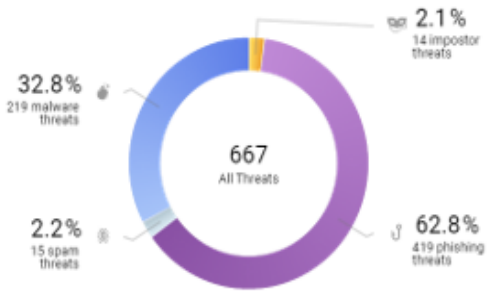
IT Security & Risk Management Dashboard

Enterprise Security Management Platform

APS continued to be targeted by global high-volume phishing email campaigns, as well as individually targeted malicious emails.

Email Threat Categories

99.9% pre-delivery protection rate (1047/1048).



Email Threat Types by Message Volume

Nominal reduction in 'All Messages' from previous quarter.

Cybersecurity Incidents / Managed SIEM

In this quarter, there was no impact to the availability of systems due to security events.

- **SIEM Alerts (Total: 24)**

Severity 1	-	0 (Critical)
Severity 2	-	0 (High)
Severity 3	-	11 (Medium)
Severity 4	-	13 (Low)
Severity 5	-	0 (Informational)

Business Resilience

- **Crisis Management:** Five tabletop exercises for Q2 2022
- **Disaster Recovery:** Next Compass test planned for Q2 2023
- **Business Continuity:** Included in tabletop exercises for Q2 2022
- **Plan Maintenance:** Plans updated as changes occur

IT Risk Register

- **High Rated Risks (Total: 1)**

New	- 0	Raised	- 0
Closed	- 0	Lowered	- 0

Security Awareness & Education

- **Training modules**
  Security Beyond the Office – 100%
- **Phishing simulations**
  Users who reported suspicious emails – 54%
  Users who clicked phishing link – 7%
  Users who were compromised – 2%
- ***New in 2022 - training and phishing reporting includes APS and plan corporation staff.***

Change Management

- **Change Requests – 99.0% success rate (Total: 279)**

Standard	-	249
Normal	-	24
Urgent	-	5
Emergency	-	1

Up and Coming

- **Vulnerability Management**
  Patching compliance, APS security rating
- **Third Party Risk Management**
  Key vendor security ratings

Key Activities 2022

Cyber Resilience

- **Ransomware Readiness**
- **Russia/Ukraine Conflict Cyber Risk**
- **Cloud Services**

Continuous monitoring and actions to strengthen cyber resilience from associated cyber attacks.

Crisis Management Exercises

Engagement for facilitated crisis management tabletop exercises.

1. IT Disruption - System failure
2. Business Disruption - Pension payment delay
3. Business Disruption - Employee strike
4. Cyber Incident – Ransomware
5. Cyber Incident – Privacy breach

Initiatives

- **Compass D6 Upgrade**
- **Third Party Risk Management**
- **Identity & Access Management**
- **Cloud Services**

Ransomware Readiness

Business Resilience
- Business Continuity Plans + Orientation & Training
- Compass Disaster Recovery Plans & Tests
- Crisis Management Tabletop Exercises + Board Playbook
- IT Change Management & Compass Release Management

Security Services
- Advanced Email Threat Protections (including DMARC)
- Advanced Endpoint Protection (Anti-virus/malware)
- Next-Generation Firewalls + Web Application Firewalls
- Managed SIEM* (24x7)

Vulnerability Management
- Vulnerability Scanning & Remediation + Patch Management
- IT Risk Register + Governance/Risk/Compliance (GRC)
- Web Application Security Testing
- Security Rating Service – Self & Key Vendors

Incident Response
- Annual External Security Testing (Penetration Testing)
- Cybersecurity Incident Response Management & Process
- Cyber Insurance (Breach Response Services)
- Ransomware Protected Backups + Restore Testing

Security Education & Awareness
- Quarterly Education to Staff and Plan Clients (except Q4)
- Quarterly Phishing Simulation Campaigns + 'Report Phish'
- Annual Cybersecurity Awareness Month and Events
- Cybercommunity – CCTX, CyberAlberta + Partners & Peers

Identity & Access Management
- Strong Password Policy + Multi-Factor Authentication
- Enforced VPN on APS-Managed Devices
- Privileged Access Management & Reduction Improvements
- Identity & Access Management Program Development

*SIEM – Security Information & Event Management

IT Security & Risk Management Progress and Direction

Current State - 2022

Very good business resilience program and security controls maturity; continuous improvement.

- Best in class email, malware, and network protections
- Good security awareness and education program
- Good internal and external audit outcomes

- Cyber insurance / breach response services
- IT Security & Risk Management Dashboard
- Support Agile APS / secure WFH

Objectives - 2022

- Introduction of more Microsoft security services and expansion of other services
- Robust, practiced incident and crisis management response

- Full vulnerability management program with vulnerability prioritization
- Collaboration with key vendors for security ratings improvements
- Identity proofs of concept for lifecycle management

Target State – 1 to 3 Year Plan

- Optimized security services with automated response
- Network segmentation
- Full ransomware readiness and proven continuity options for pension payroll / Compass

- No preventable major business impacting incidents
- End to end management of all identities
- Coordinated vendor management for third party (supply chain) risk management

Questions

Alberta Investment Management Corporation

Introduction

- AIMCo manages investments for 32 clients which include pensions, endowments and government funds in the Province of Alberta.
- Headquarters in Edmonton, Alberta. Offices in Calgary, Toronto, London and Luxembourg
- Around 575 employees
  - Cyber security team size is 5 FTE

Director Technology Platforms and Security

Joined AIMCo in 2014 and is an Information Security professional with over 15 years of security experience.

- Certified Information System Security Professional (CISSP)
- Information Systems Security Architecture Professional (CISSP-ISSAP)
- Certified Information Systems Auditor (CISA)
- GIAC Certified Incident Handler (GCIH)
- GIAC Certified Perimeter Protection Analyst (GPPA)
- GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)

Key Principles in our Cyber Program

- Defense in Depth
  - If one layer fails, there are subsequent processes, systems and tools to prevent a breach
- Leverage investments in tools that you already have in place
  - Invest in tools that integrate well
- Keep it simple
- Directors can use the NIST Cyber Security Framework (CSF) elements
  - Identify, Protect, Detect, Respond, Recover

NIST Cybersecurity Framework (v1.1)

Identify

Threat Risk Assessments

- What are our crown jewels and where do they reside?
- Which Threat actors want to compromise these crown jewels?
- What are the skills sets of these threat actors?
- What controls do you have in place to protect these systems?
- Where are my gaps?

Protect

Robust User Awareness Training

- Targeted training for sensitive positions
- Continuous communication on relevant topics
- Simulated Phishing and fake Multi-Factor Authentication (MFA) prompt exercises

Identity Protection

- MFA on all external portals and system with sensitive data
- Single identity provider

Malware Protection

- Enhanced Email security; Don’t stop at standard email filtering
- Advanced end-point protection which provides the data needed for incident response
- All internet traffic filtered in-bound and outbound

Detect

User Behavior Analytics

- Build baseline of normal activity, detect when user activity outside of normal
- Key to insider threat detection

Threat Hunting

- Dedicated team actively looking for compromise inside environment
- Assume you are already breached

Honey Pots

- Fake documents, systems, or other type of data that looks enticing to attackers.
- Cheap and low effort but very effective

Respond and Recover

Cyber Security Incident Response Plan

- Plan should be a framework for how the organization will respond
- Designated a tactical and strategic team
- Clear lines of decision making and communication

Tabletop Exercises

- Real-world scenarios
- Involvement from executives and board is important

Protected and Tested Backups

- Data backups separated from regular production systems
- Backup often; Test restoration often
- Ensure storage locking is enabled on backup systems

Assurances Over Security Program

- Validate the effectiveness of your security program on a regular basis
- Penetration testing with appropriate scope
  - Attackers aren't only limited to specific systems, during certain hours
- Change it up
  - Regularly change the security firms performing your testing
  - Change timing of tests so Analysts don't plan to be extra only during pentest window
- Educated 2nd and 3rd line defenses within the organization
- Specific audits for high impact systems (SWIFT)
- 3rd party outsource arrangement provide assurances of their security programs

Emerging Risks and Hot Topics

3rd Party Outsourcing

Like many companies, AIMCo is seeing most of it's new or upgraded systems move outside of our datacenters, into 3rd party hosted environments. This introduces new risks associated with Cyber Security that need to be managed, including:

Lack of visibility and control over 3rd party hosting environments cyber security.

Larger target for cyber criminals and nations states

Potential reduction in incident response capabilities in case of breach.

In order to mitigate these risks, AIMCo has a well-defined review process for the hosting organization cyber security capabilities and strict requirements for 3rd party assurances.

Talent Shortage

We are facing a wide-spread shortage of skilled cyber security professionals across the industry.

- A significant factor behind data breaches are the lack of highly skilled cybersecurity professionals
- Global shortage of 3.5 million cyber security professionals

How we manage?

- Provide training path for new grads
- Leverage managed service providers with security expertise

Questions

How can you evaluate the effectiveness of your organizations cyber security program?

Take-Aways

1. Cyber Hygiene
2. Table-Top Exercises
3. Cyber Focused Business Continuity Plans
4. Security Framework
5. Audit / Control Testing
6. Organizational Cyber Awareness Training
7. Board Involvement
8. Expertise on Board
9. Get Help and Ask Questions

Thank-You