



# Post-Mortem Report – Security Incident

## BOO-SEC-2025-0587

**Company:** Bank of Ontario

**Date of Incident:** May 23, 2025

**Date of Resolution:** May 26, 2025

**Report Author:** Ravi Khurana, IR Lead

**Last Updated:** May 30, 2025

**Confidentiality:** INTERNAL – Security & Compliance Use Only

---

## 1. Executive Summary

On **May 23, 2025**, Bank of Ontario experienced a **critical cybersecurity incident** involving unauthorized access through a **compromised employee VPN account**. The attacker exploited a **legacy MFA fallback mechanism** to gain access to internal engineering systems and exfiltrate **non-production customer staging data**. The incident was promptly detected via **Cisco SecureX**, contained in under 18 hours, and resolved through coordinated efforts between **Bank of Ontario Security Operations**, **Cisco Services**, and **Deloitte's Cyber Risk Advisory** team.

---

## 2. Timeline of Events

Date/Time (EST)	Event Description
<b>May 23, 03:26 AM</b>	Cisco SecureX flags anomalous VPN login ("impossible travel")
<b>03:45 AM</b>	SOC Analyst Leila Farhani confirms session fingerprint mismatch
<b>04:14 AM</b>	Incident escalated to IR Lead; Deloitte and Cisco engaged
<b>05:10 AM</b>	Cisco Talos confirms RDP activity and suspicious curl requests
<b>06:45 AM</b>	Forensic memory dump via Carbon Black shows AWS S3 exfil endpoint
<b>08:15 AM</b>	Affected endpoint quarantined via Cisco AMP

**11:00 AM** VPN credentials reset and legacy MFA fallback disabled

**May 26, 08:00 PM** Incident marked as contained and closed

---

## 3. Incident Details

### 3.1 Root Cause

- User `r.thompson@bankontario.net`'s password was reused from a past breach (LinkedIn 2023).
- MFA fallback was still permitted on the legacy VPN gateway, allowing OTP token use without biometric verification.
- The attacker used a **Tor exit node** to conceal geolocation and bypassed normal velocity heuristics.

### 3.2 Affected Systems

- VPN Gateway: `vpn-gw2.bankontario.net`
- Endpoint: `INT-ENG-BETA04.bankontario.net`
- AWS S3 exfil endpoint:  
`https://s3.eu-west-1.amazonaws.com/bk-dump/boo.tar.gz`

### 3.3 Data Impact

- **Data Accessed:** Internal CSV file (`customer_staging.csv`) with 28,000 anonymized records used for test workloads.
  - **No PII, PCI, or PHI** exposed.
  - **No systems encrypted or altered** – this was a data reconnaissance + exfiltration scenario.
-

## 4. Detection and Response

Tool/Team	Role
Cisco SecureX	Detected anomalous VPN login via impossible travel analytics
Cisco Talos	Provided IOC and threat actor profiling
Cisco AMP & Secure Endpoint	Quarantined infected host automatically
Carbon Black	Used by Deloitte to perform memory dumps and file analysis
Deloitte Forensics	Conducted host-based investigation and threat containment

---

## 5. Remediation Actions

### Immediate

- Disabled legacy VPN fallback MFA across the enterprise
- Revoked credentials and reset passwords for all VPN-enabled users
- Blocked known Tor exit nodes via Cisco Secure Firewall
- Decommissioned exposed dev endpoint **INT-ENG-BETA04**

### In Progress

- Replacing legacy VPN with Cisco Duo SSO & device-aware policies
  - Upgrading SecureX playbooks to include user session fingerprinting
  - Integrating behavioral analytics from Umbrella + Talos into SIEM
-

## 6. Lessons Learned

Observation	Action Taken
MFA fallback introduces undue risk	Disabled fallback paths and auditing all auth flows
VPN access lacked geo-fencing controls	Added Secure Access with Cisco Duo conditional policy enforcement
Endpoint data staging environments not properly isolated	Engineering now sandboxed via Cisco SD-Access microsegmentation
Password reuse remains a recurring weakness	Rolled out password manager & policy education campaign

---

## 7. Business Impact

- **Data Classification:** Internal test data only
  - **Customer Communication:** Not required
  - **Regulatory Reporting:** Logged internally, not subject to mandatory FINTRAC/FIPPA reporting
  - **Downtime:** None
  - **Reputation Risk:** Minimal due to lack of customer impact
- 

## 8. Cost Summary

Item	Estimated Cost
Deloitte IR services (48h)	CAD \$27,000
Cisco CX Retainer Response	Covered under annual IR contract
Internal resource time (120h)	CAD \$11,500

Training & Infra Hardening	CAD \$18,200
<b>Total</b>	<b>~\$56,700 CAD</b>




---

## 9. Preventive Measures Roadmap

Task	Owner	Deadline
Deploy Cisco Duo for all external access	CyberSec Ops	June 10
Rewrite incident playbooks in SecureX	SOC Team	June 15
Formalize threat simulation tabletop	Deloitte + IR Team	July 1
Complete Zero Trust Policy Implementation	CIO Office	July 15

---

## 10. Approval & Sign-Off

Name	Role	Signature
Amira Dosanjh	VP Cybersecurity Operations	
Ravi Khurana	Incident Response Lead	
Kate Young	Deloitte Partner	
Sanjay Mehta	Cisco CX IR Services Lead	