CYBER ALBERTA

CYBER COMPROMISE CHECKLIST: A GUIDE FOR ALBERTA BUSINESSES

V1.0

Cybersecurity incidents, such as ransomware or network intrusions, can severely impact your business. If your organization experiences an attack, it's crucial to take swift, structured action to minimize damage and recover effectively. Below are the steps of recovery from a cybersecurity incident.

☐ IMMEDIATE ACTIONS AFTER AN ATTACK

- **Isolate the Incident**: Disconnect affected systems from the network to prevent further spread.
- **Assess the Impact**: Identify which systems or data have been compromised.
- **Document the Incident**: Record key details, such as when the attack started, which systems were affected, and any suspicious activity.
- **Do Not Engage with Attackers**: Avoid responding to ransom demands until consulting cybersecurity professionals.

☐ ENGAGING WITH CYBER INCIDENT RESPONSE TEAMS

For professional guidance on recovering from an attack, consider reaching out to trusted cybersecurity firms. These experts can help:

- Contain the attack.
- Recover compromised data.
- Conduct forensic investigations.

Tip: Alberta businesses should keep a list of pre-vetted cybersecurity firms or incident response providers on hand for rapid access in emergencies.

☐ REPORTING A CYBERSECURITY INCIDENT

Timely reporting is essential to help law enforcement track any weird disrupt criminal activities, and to receive the support necessary for recovery.

- **Contact Your Local Police**

  For **Calgary-based businesses**, reach out to the Calgary Police Service Cybercrimes Investigative Team:

  - **Non-Emergency Line**: +1 (403) 266-1234
  - **Online Reporting**: Submit non-urgent reports, including cybercrime, via the CPS Online Reporting Portal (https://www.calgary.ca/cps/community-programs-and-resources/crime-prevention/reporting-online-crime.html).

  For **Edmonton-based businesses**, report incidents to the Edmonton Police Service Cybercrime Unit:

  - **Non-Emergency Line**: +1 (780) 423-4567

- **Online Reporting**: Submit non-urgent reports via the EPS Online Reporting Portal (https://www.edmontonpolice.ca/ContactEPS/OnlineCrimeReporting).

For other jurisdictions, please reach out to your local police service or the RCMP.

- **Notify the Canadian Anti-Fraud Centre (CAFC)**
  Report incidents of fraud, ransomware, or cyberattacks to the CAFC. The CAFC collects information on cybercrimes to support investigations across Canada.
  - **Website:** https://www.antifraudcentre-centreantifraude.ca
- **Notifying the Canadian Centre for Cyber Security (CCCS)**
  Businesses should also report incidents to the Canadian Centre for Cyber Security (CCCS) for expert advice and assistance. Reporting to the CCCS contributes to national threat intelligence and improves Canada's overall cybersecurity resilience.

  The CCCS provides:
  - Cyber incident response guidance.
  - National cybersecurity threat intelligence.
  - Access to federal resources for breach recovery.
  - **Website:** https://cyber.gc.ca/en/

- **Legal and Compliance Notification**

  In some cases, businesses may have additional obligations, such as notifying the Office of the Information and Privacy Commissioner of Alberta (OIPC) if personal data has been breached.
  - Website: https://www.oipc.ab.ca
- **Reporting to CyberAlberta**

  Alberta businesses are encouraged to report incidents to CyberAlberta, which collaborates with law enforcement and provides guidance on system recovery and future prevention.
  - Email: cyberalberta@gov.ab.ca
  - **Website**: www.cyberalberta.ca

  CyberAlberta can assist with:
  - Coordinating with law enforcement
  - Providing guidance on breach recovery
  - Connecting businesses with cybersecurity resources
  - Liaising with the CCCS on behalf of the organization