Responding to a Cyber Incident: Insights from a Breach Coach

MEARIE Conference

Lyndsay A. Wasser, Partner
Head of Privacy & Data Protection
McMillan, LLP

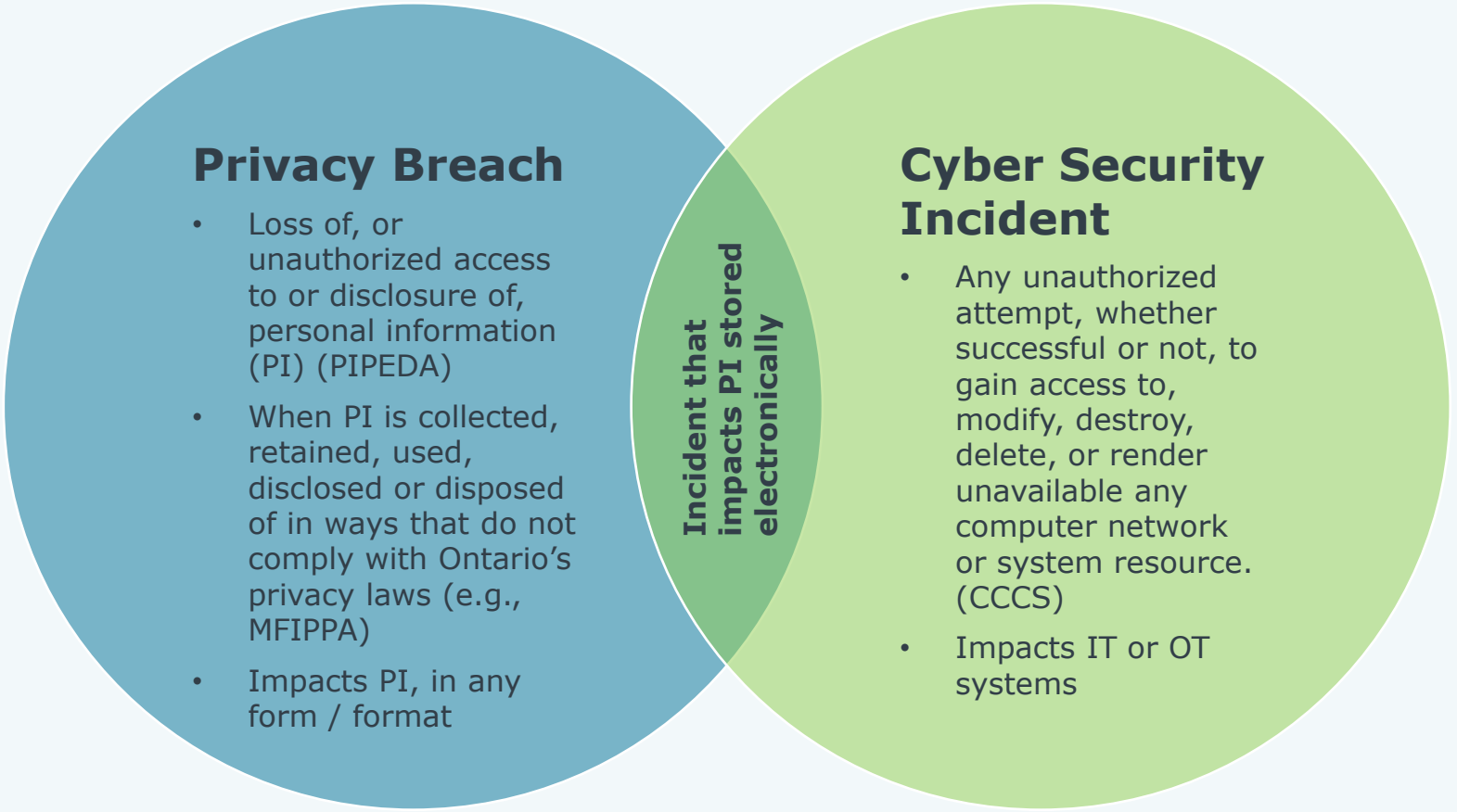
June 21, 2024

Agenda

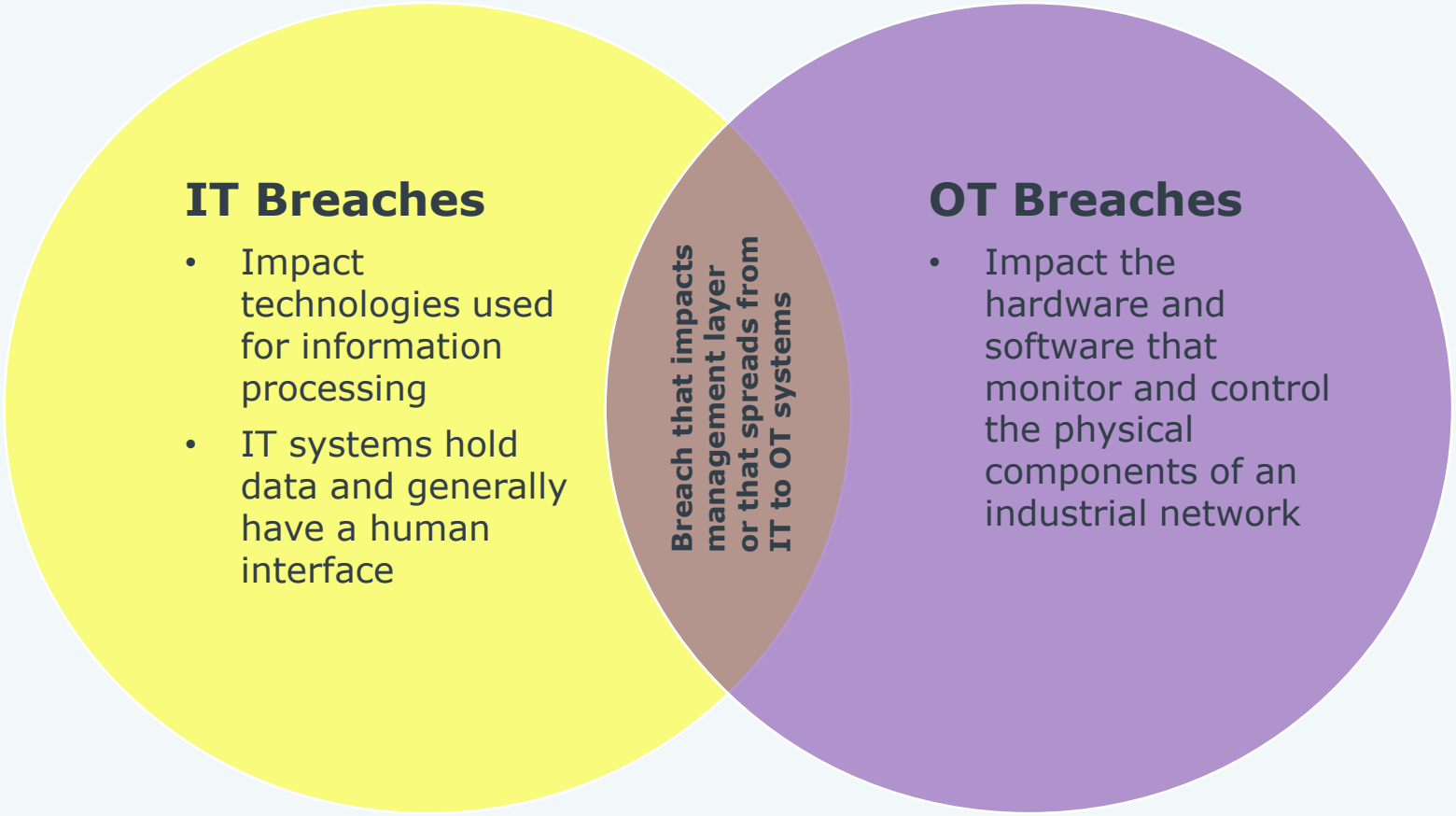
- Introduction
  - Types of Incidents
  - Threat Landscape
- Responding to a Breach
- Case Study #1 – TTC
- Case Study #2 – Colonial Pipeline
- Conclusion – Key Takeaways

Introduction

Privacy Breaches vs. Cyber Security Incidents



IT Breaches vs. OT Breaches



Threat Landscape – Electricity Sector

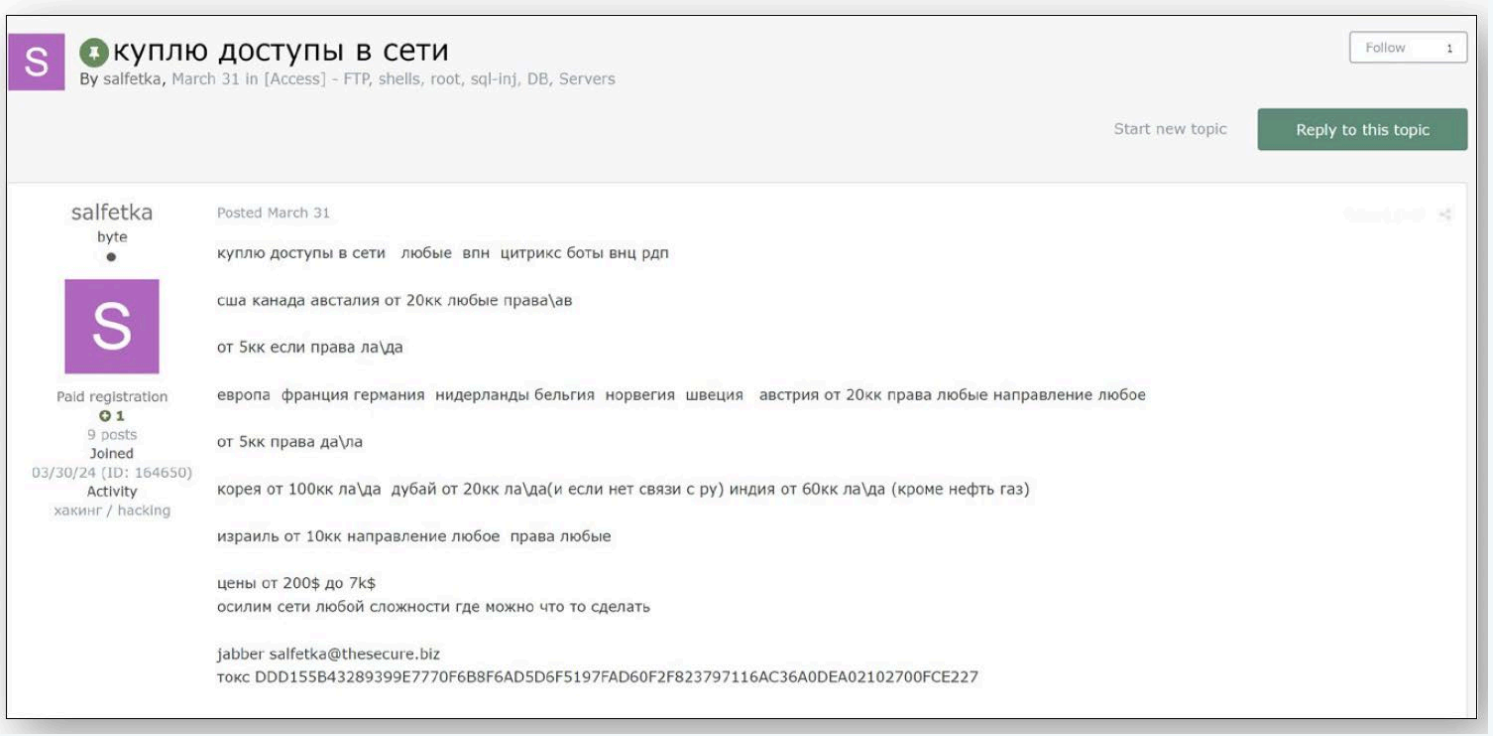
- Nation State cyber attacks
  - Russia, China, North Korea, Iran
- Social activists; environmentalists; terrorists
- Opportunistic threat actors; financially motivated hacker groups
- Internal threats; human error

Dark Web and Online Intelligence

Available services include:

- Monitoring of the dark web, the World Wide Web, chat groups, and social media for hackers and criminals soliciting, buying, and selling confidential information, user credentials, and access to your network.
- Receiving customized alerts that explain the risk, implications, and immediate remediation steps in real-time.
- Receiving monthly industry-specific intelligence reports.

VPN access to a Canadian energy company with $5m revenue listed on the darknet



On March 17, 2023, a user named "cozyTM" posted a notice offering VPN access to a Canadian energy company. The access includes data with Jira, internal Wikipedia, and more. The company has a revenue of over $5 million, and the price for this access is $1,700.

mcmillan

Responding to a Cyber Security Incident – Key Steps in Breach Response

Incident Response – The NIST Approach

Preparation
Implementing a series of tools (including a IR plan) ahead of time, so that you are ready to analyze, isolate, and respond to an incident.

Detection & Analysis
Identifying the type of threat and determining whether it is an incident. Also includes incident documentation and prioritization.

Containment
Isolating impacted systems and other appropriate measures to limit impact. Implement a long-term and a short-term containment strategy.

Eradication
Removing malware and deleting or securing compromised accounts.

Restoration
Restoring or rebuilding systems; Resuming normal operations.

Post-incident Updates
Considering lessons learned; Implementing improvements.

Incident Response – Ontario Cyber Security Framework

Incident Response – Privacy Regulators

Contain the Breach

Take immediate steps to contain the breach (e.g., stop unauthorized practice, recover records, revoke access, etc.)

Evaluate the Risks

Consider sensitivity of information, cause and extent of the breach, impacted individuals, and possible harms

Notification & Reporting

Where required or appropriate, notify impacted individuals, relevant government authorities, and possibly others

Prevention

Thorough security audit. Develop and improve safeguards and policies to reduce the risk of future incidents

Detection

- Detection - Identifying an actual or suspected cyber incident
- How are incidents detected?
  - IT alert – e.g., by an Intrusion Detection System (IDS), Security Information and Event Management (SEIM) solution, or Endpoint Detection and Response (EDR) solution
  - Reported anomaly or suspicious activity by an employee
- Ensure employees are trained to escalate potential incidents!

Investigation & Activation of IRT

- What should you do if a potential threat is detected?
  - Investigate **promptly**
  - Convene incident response team (IRT), where appropriate
  - Review insurance policy and call your insurer
  - Activate internal and external IT / OT experts, and implement immediate short-term containment
  - Engage legal at an early stage

Communication, Prioritization & Documentation

- Ongoing communication and collaboration is key
- Prioritization
  - Decisions will need to be made based on the needs of the business and the potential impact of foreseeable risks
- Documentation
  - Document the incident and steps taken to investigate, contain and remediate the incident – **But stick to the facts!**
  - Consider litigation risk and privilege strategy. Avoid creating "bad" evidence!

Analysis

- Consider:
  - The type of incident
  - The potential impact on individuals
  - Operational impact
  - Statutory requirements (e.g., MFIPPA, PIPEDA)
  - Regulatory requirements (e.g., OEB, IESO)
  - Litigation risk
  - Reputation and maintenance of customer trust

Notification & Reporting

- Privacy Breach – Reporting to the Regulators
  - PIPEDA
    - Office of the Privacy Commissioner of Canada
    - Mandatory where there is a "breach of security safeguards" and there is a real risk of significant harm to an individual
  - MFIPPA
    - Information and Privacy Commissioner of Ontario
    - Not currently mandatory, but the IPC takes the position that it should be notified of "significant breaches"

Notification & Reporting

- Cyber incident that impacts OT
  - Market participants must report certain incidents to IESO, including:
    - Events that may impact the reliability of the ICG
    - Events that meet the reporting criteria defined in NERC standard CIP-008: Cyber Security- Incident Reporting and Response Planning (if applicable)
  - IESO reports physical and confirmed cyber security incidents to the NERC Electricity Information Analysis Centre, and may report to the CCCS, the RCMP, the Ontario Ministry of Energy, local law enforcement, and other operating authorities
  - Certain incidents may need to be reported to the Electrical Safety Authority (e.g., if the incident causes a fire or explosion), or the OEB (i.e., Major Events)

Notification & Reporting

- In some cases, the incident may be reported to other organizations or governmental authorities that can potentially assist, such as:
    - The CCCS
    - The RCMP or other law enforcement
- It may also be necessary or advisable to notify:
    - Impacted individuals
    - Members of the public

Notification & Reporting - Potential, Upcoming Changes

- Bill 194 – *Enhancing Digital Security and Trust Act, 2024*
  - New breach reporting requirements for institutions subject to FIPPA (but not MFIPPA)
  - Lieutenant Governor in Council may make regulations requiring public sector entities to submit reports to the Minister or a specified individual in respect of incidents relating to cyber security
- Bill C-26 – *Critical Cyber Systems Protection Act*
  - New requirements, including cyber security incident reporting, for critical infrastructure, including for the energy sector
  - Applies to federal works, undertakings and businesses (e.g., interprovincial or international pipeline and power line systems, as well as nuclear energy systems)

Recovery & Restoration

- Occurs only after you have expelled the threat actors, rebuilt or restored affected systems and validated their integrity, deployed any relevant patches and updates, etc.
- Stakeholders are highly motivated to return to normal operations quickly
- Speed may be prioritized where there is an OT incident that impacts delivery of electricity, especially in inclement weather
- But beware of the risks of restoring systems before the threat is fully eradicated!

Post-Incident

- Review “lessons learned” and implement improvements
  - Update your incident response plan, based on what worked and what did not work
  - Conduct a thorough review of security controls to identify any other gaps
  - Implement improvements to safeguards and relevant policies
- Complete your documentation of the incident (including, where applicable, the mandatory breach record pursuant to PIPEDA)
- Post-incident activities may also include responding to a regulatory investigation and/or legal claims

Responding to IT vs. OT Cyber Incidents

Similarities

Both types of incidents:

1. Can have a significant impact on an organization
2. Require an IRT composed of different stakeholders/ specialists
3. Require consideration of reporting obligations
4. Involve setting priorities at an early stage

Also:

In each case the response will involve preparation, detection, analysis, containment, eradication, restoration and post-incident updates

Differences

But

1. The potential scale and impact of an OT incident is often greater
2. The composition of the IRT will differ
3. The specific reporting obligations differ
4. The priorities will differ (e.g., forensics versus restoring the delivery of electricity)

But:

Pure OT breaches generally do not impact personal information, and so privacy legislation does not typically apply

mcmillan

Case Studies

Case Study #1 – Cyber attack on the TTC

- Ransomware attack whereby a threat actor gained access to TTC systems (including PI) via a phishing attack
- TTC Response:
  - Intrusion discovered quickly; Immediate action to secure systems
  - Communicated promptly with employees
  - Developed a priority order to have devices "cleaned"
  - Identified the information that may have been taken within two weeks, and was able to determine what happened
  - Retained cybersecurity and forensic experts to investigate the breach
  - Notified impacted individuals (and offered identity protection service) and the Ontario IPC
  - Updated security measures and developed additional policies, standards and guidance
- The attack did not cause any significant disruption to transit service, or give rise to any risks to the public or TTC employees

Case Study #2 – Cyber Attack on Colonial Pipeline

- Ransomware attack likely caused by a stolen password for a legacy VPN profile that was no longer in use, and the lack of multi-factor authentication for remote access
- Breach went undetected for eight (8) days, thereby allowing the threat actor to penetrate deeper into Colonial's network
- Production was shut down for 5 days because Colonial could not determine how the breach occurred or how far it had progressed
- Colonial paid $4.4 million ransom for "imperfect" decryption key
- Incident led to fuel shortages for Eastern and Southern US states, in part due to "panic buying"
- Lessons Learned = The importance of:
  - A detection and response system
  - A ransomware response plan
  - An effective communication strategy

mcmillan

Conclusion

Key Takeaways

- Incidents can impact any organization or institution
- Being proactive can reduce the risk of catastrophic events
- An effective response is key to limiting financial and reputational damage, as well as operational impact, if an incident occurs
- Planning and preparation are essential to an effective and efficient response

Thank You

Q&A

Lyndsay A. Wasser

Privacy & Data Protection

Toronto

416.865.7083

Lyndsay.wasser@mcmillan.ca

mcmillan

Get in Touch

EMAIL

info@mcmillan.ca

LINKEDIN

@mcmillanllp

INSTAGRAM

@mcmillanllp

TWITTER

@mcmillanllp

If you have any questions about McMillan, or how we may help you with your legal needs, please get in touch with us.