Cyber-Readiness and Response: Preparing for the Next Cyber Attack

Charles Morgan and Susan Wortzman

Monday, January 24, 2022
12:00 pm EDT

Charles Morgan
Partner, Co-Lead, Cyber/Data Group
514-397-4230
cmorgan@mccarthy.ca

Susan Wortzman
Lead, MT>3, a Division of McCarthy Tétrault
416-642-9025
swortzman@mt3.ca

Agenda

1. The Role of the Corporate Counsel
2. Pre-planning Incident Response
3. Cyber Response

1. The Role of the Corporate Counsel

- Before an incident occurs, Corporate Counsel's role is to assist the board to ensure accountability and oversee risk management
- Setting priorities and identifying major investments (allocation of scarce resources)
- In the event of a security incident, Counsel will have an integral role with the implementation of policies, procedures and other responses to mitigate the consequences of the incident.
- The board should be notified as soon as possible once a material incident has occurred

1.1 The First Line of Defence

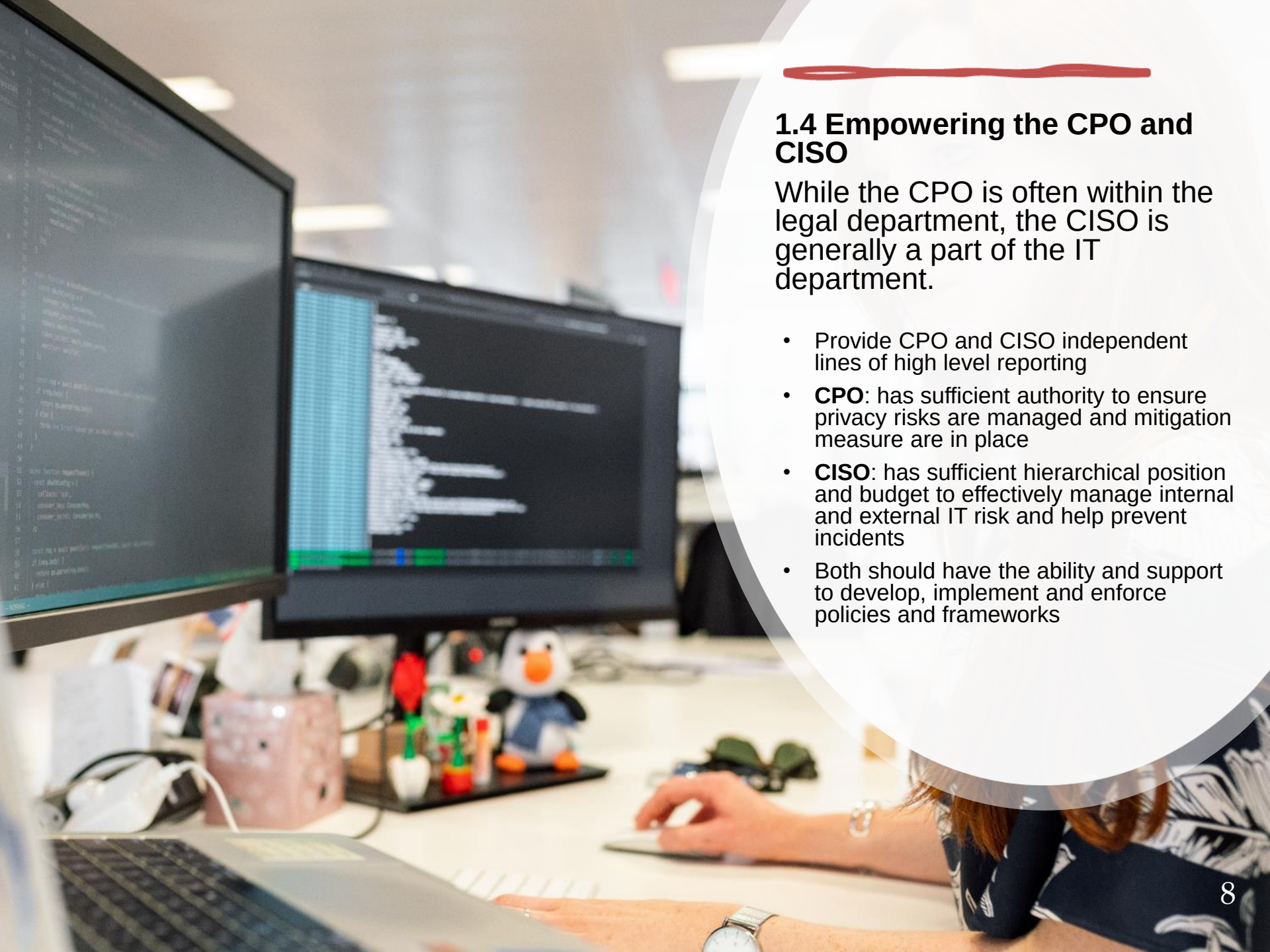
- **First line of defence:** departments that own and manage risk
- This means that operational managers:
  - are responsible for maintaining effective controls and for executing procedures on a day-to-day basis
  - identify, assess, control, and mitigate risks
  - guide the implementation of internal policies and procedures
  - are responsible for implementing corrective actions
- E.g. production, marketing, service delivery)

1.2 The Second Line of Defence

- **Second line of defence:** managers that oversee risks
- This means that the overseeing functions:
  - ensure the first line of defense is properly designed, in place, and operating as intended
  - alert operational management to emerging issues and changing regulatory and risk scenarios
  - monitor internal controls, reporting, compliance, and timely remediation of deficiencies
- E.g. risk management team, compliance department, internal legal counsel

1.3 The Third Line of Defence

- **Third line of defence:** functions that provide independent assurance.
- This means that the internal audit function:
  - provides the governing body and senior management with comprehensive assurance
  - should have the highest level of independence and objectivity within the organization
  - provides assurance on the effectiveness of governance, risk management, and internal controls
  - evaluates if the first and second lines of defense are achieving risk management and control objectives



1.4 Empowering the CPO and CISO

While the CPO is often within the legal department, the CISO is generally a part of the IT department.

- Provide CPO and CISO independent lines of high level reporting
- **CPO**: has sufficient authority to ensure privacy risks are managed and mitigation measure are in place
- **CISO**: has sufficient hierarchical position and budget to effectively manage internal and external IT risk and help prevent incidents
- Both should have the ability and support to develop, implement and enforce policies and frameworks

1.5 Empowering the CPO and CISO

- Privacy/Data Security risk impact assessments are key risk management tools
- Document potential impact to Privacy/Data Security risks before projects start
- Update impact assessments before changes are implemented
- Ensure projects and changes are within the
- Empower CISO and CPO to intervene, change or stop projects

1.6 Vendor Management (Suppliers)

- Carefully assess agreements under which vendors will handle your organization’s data (templates and checklists)
  - Privacy and IT Security
  - Data Location
  - Control over subcontracting
  - Breach notification
  - Limitation of liability
  - Insurance
- Have relevant vendor agreements assembled and ready in anticipation of a data breach.

1.7 Vendor Management (Key Customers/Clients)

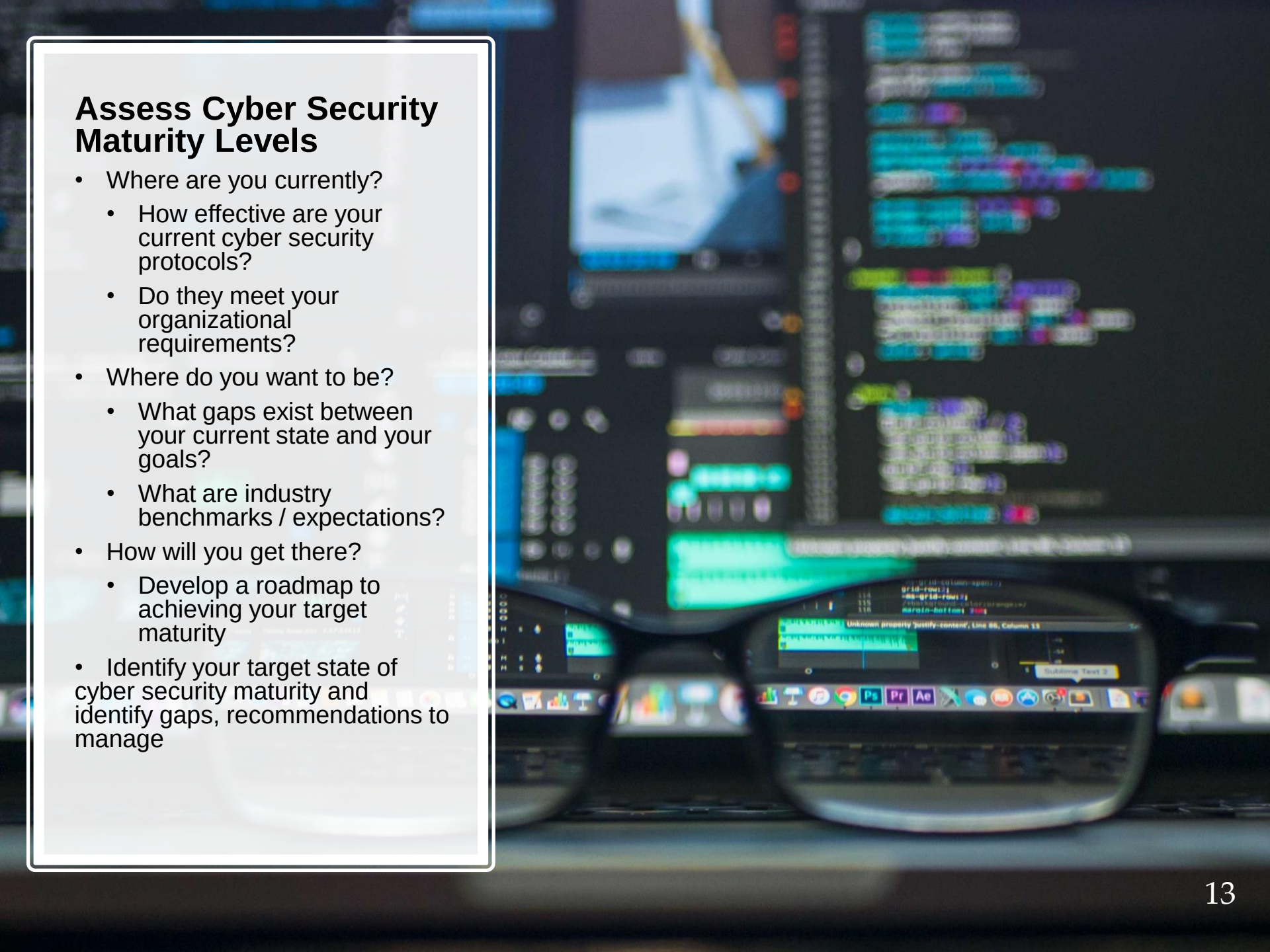
- Include considerations for key client relationships in incident response plan
- Work with key customers/partners to collaboratively and proactively manage cyber risk
- Understand and track key customer/client contracts to identify applicable obligations and ensure appropriate actions are taken:
    - breach notification obligations
    - risk allocation and liability

2. Assessing Your Risk Profile

- Identify threats and risks to your organization
  - Who might attack?
  - How might they attack?
  - Where will they attack?
  - What are they after?
- Ensure the “Crown Jewels” are protected
  - What is the cost to the business if these are breached?
- Create an Risk Profile
  - Map targeted information to likely attackers and assign a risk value – high/medium/low

Assess Cyber Security Maturity Levels

- Where are you currently?
  - How effective are your current cyber security protocols?
  - Do they meet your organizational requirements?
- Where do you want to be?
  - What gaps exist between your current state and your goals?
  - What are industry benchmarks / expectations?
- How will you get there?
  - Develop a roadmap to achieving your target maturity
- Identify your target state of cyber security maturity and identify gaps, recommendations to manage

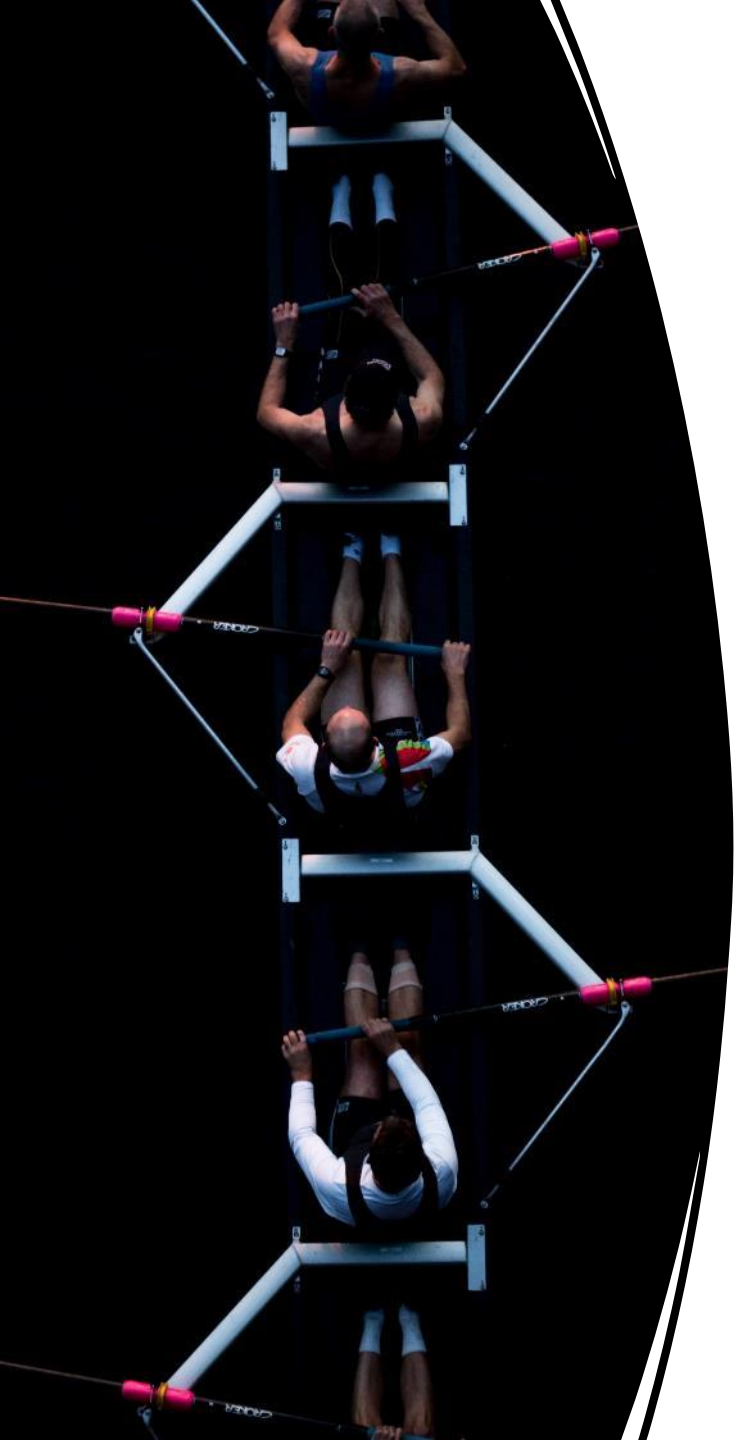


2.1 Pre-planning Incident Response

- **Cyber response plan:** have an *actionable* step-by-step plan for addressing incidents (with accountable parties)
- **Prepare a template incident log** aligned with record retention rules (bearing in mind privilege concerns)
- **Prepare template notification letters** aligned with notice requirements
- **Have a living list** of other persons who require notice, including the board, insurers, and other parties as required under contract

2.1 Incident Response Playbook

- Framework for assessing potential for “real risk of significant harm” (or “RROSH”) and recording the assessment in a way that minimizes privilege risks
- Detailed but **actionable** step-by-step plan for addressing incidents, including stopping incident, escalation to external advisors, insurance notices, recovering data, remediation of immediate issue and collateral issues
- Can be tiered to differentiate between minor and major incidents
- Should account for all applicable laws → is the clock ticking on notice to regulators?
- Regular table-top exercises and debriefs allow you to stress-test and update procedures



2.2 Pre-planning Support Team(s)

- Gather contact information and assign responsibilities for internal and external resources (IT security, legal, human resources, PR/GR, project management).
  - Backups are essential because of vacations, availability issues
  - Having parallel work streams often essential in context of big breaches
  - Avoid overloading key contacts - not everything should be dropped in the privacy officer’s or CISO’s lap
- Ideally, there should be internal/external pairing for efficiency
- External teams should be identified beforehand, including establishing service provider contracts that can be signed on short notice to maximize privilege in early days
- Tension between fixing the problem and privilege protection

2.3 Pre-plan Call Centre/Credit Monitoring

- These services are among the most expensive cost outlays during a breach –even if they are often of questionable benefit to affected individuals
- Consider negotiating for call centre/credit monitoring services before incidents occur →advance bids?
- Have contracts ready and where possible, fix rates in advance, building in mechanisms to account for low take-up
- Microsites are a great standardized way to disseminate information →consider having a template site ready in case of an emergency
- Consider how to safely share information in event of a breach –commissioners expect meaningful sharing, but there are risks of secondary breaches, phishing, etc.

3. Cyber Response

- **Be proactive**: minimize data collection and retention – you can't lose what you don't have.
- **Be ready**: plan for a breach/loss, in advance.
- **Pre-determine your team of experts:** technical; legal; PR.
- **Stop the bleeding**: close the door, permanently.
- **Determine and then control your story**, and tell it: to your customers, to the Board, to the Regulator (and later, to the Court).
- **The lawyers, and privilege**, are important. But a fast, thoughtful response is job one.

3.1 Assembling the Right Internal Team

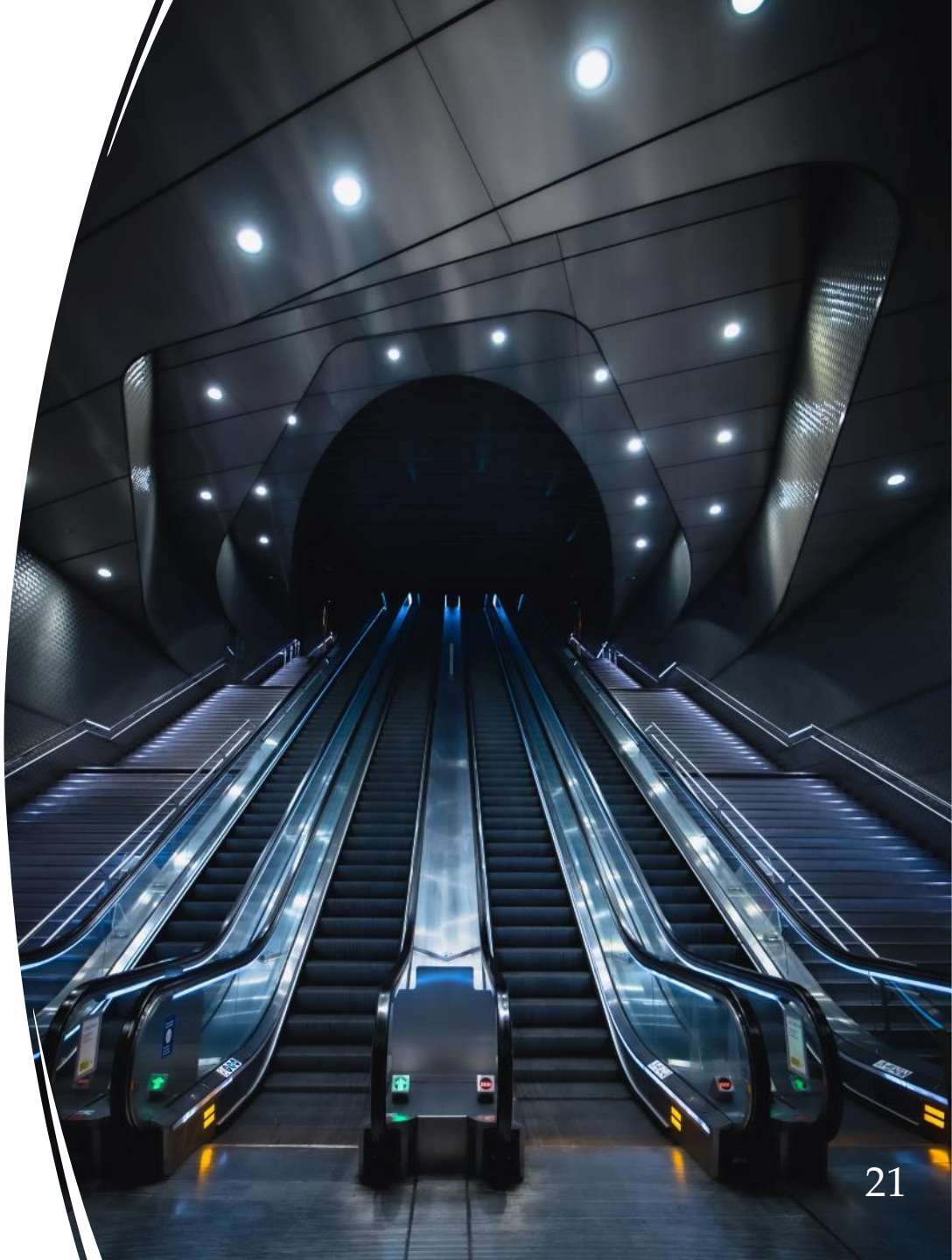
- **Executive management**: should have broad authority so that the process can advance quickly
- **Legal investigation team:** should be led by in-house and external counsel, with support of technical experts
- **IT and security team**: should perform the technical response and remediation work
- **Digital forensics team**: should investigate the incident (usually a third party consultant)
- **Communications and PR team**: should coordinate the communication efforts to all parties

3.2 Assembling the Right External Team

- **External counsel**: should have cyber/data expertise
- **Digital forensics team**: should have capability to provide technical response, forensics and remediation advice
- **Public relations firm**: should have expertise with similar organizations
- **Staffing services**: should be able to provide qualified replacement or supplemental personnel
- **Call centre services**: should have capacity to provide quality on-demand services

3.3 Escalation Criteria

- Understand and communicate incident life cycle management within the organization
- Establish criteria and process to evaluate and escalate an incident to senior management
- Incorporate and document RROSH assessment



3.4 Insurance

- Have insurance experts who will advise on what steps should be taken with regards to the cyber insurance policy review, notifications and coordination with insurers
- Evaluate insurance policies to understand coverage for different types of incidents
- Use insurance as a risk management tool

3.5 Class Actions

- The small number of experienced Canadian plaintiff class action firms will assess your breach
- Data breaches are a classic mass event – a single corporate failure, with identical effect on many individuals (says the Plaintiffs' lawyer….)
- A class action is a legal leveraging tool, turning 1000's of small (alleged) losses into one lawsuit, efficient for publicity and Court review
- Judges worry about corporate over-retention and misuse of data, and lax security

Questions?

Feedback Form

Please complete the feedback form:
https://app.getresponse.com/survey.html?u=hSVRV&survey_id=1543203