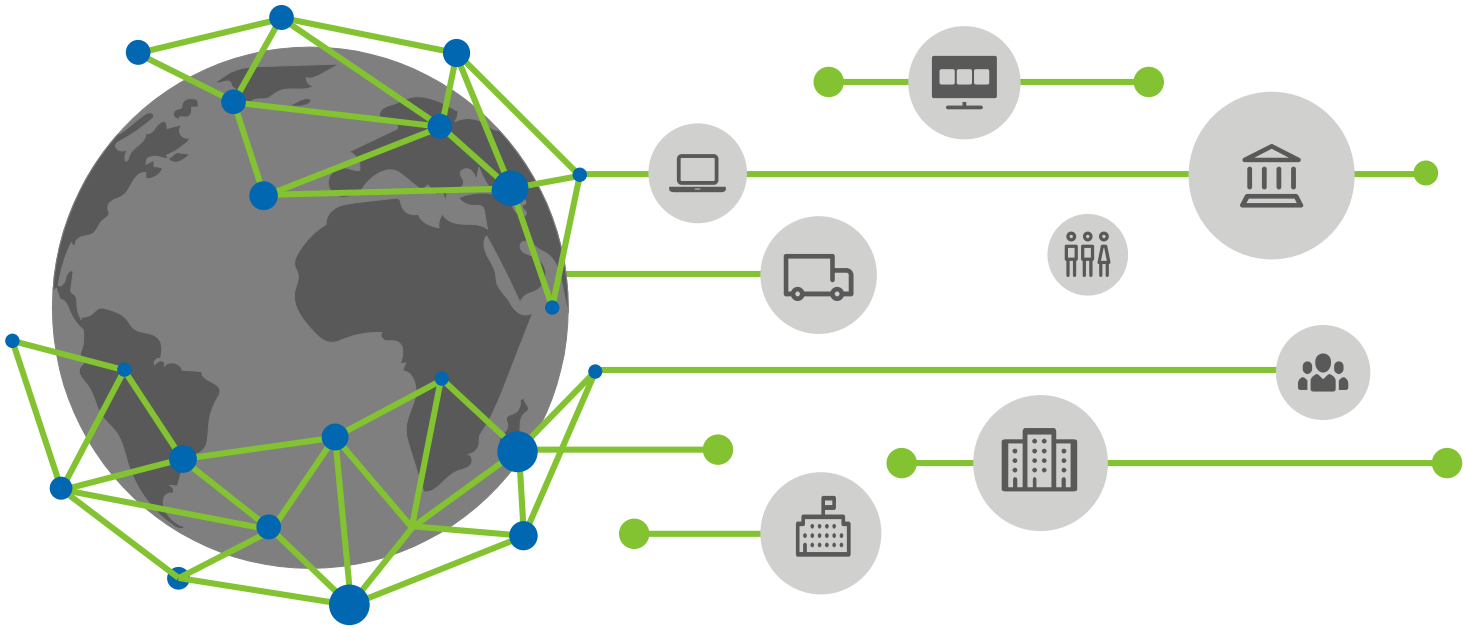
Deloitte.



# Incident Management Review

Table of contents
PNS incident management review

# Background

# Engagement summary
# Work performed to date

Throughout November and December Deloitte facilitated a no-fault, lessons learned discussion for the Province of Nova Scotia (PNS). The contents of this report are not recommendations or opinions of Deloitte. No review or audit was conducted, rather Deloitte facilitated discussions and documented the observations of PNS staff and provided input with respect to leading practices for discussion by PNS.


- Conducted interviews with key stakeholders
- Surveyed various staff related to the incident
- Conducted a workshop with relevant staff

- Created a report that includes issues identified by PNS staff matched to leading practices identified by internal Deloitte experts for PNS to discuss and consider

# Information gathering activities background

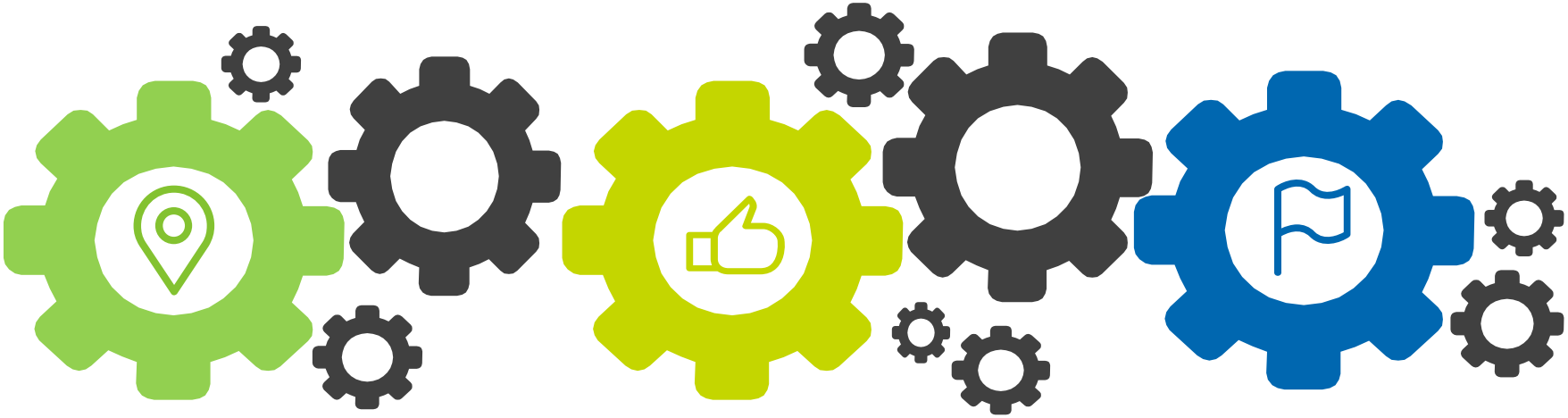
## Context for the interviews, survey, and workshop


Throughout the interviews, survey, and workshop PNS staff were asked to discuss areas for improvement as well as successes during three different time-frames: the pre-incident period, the discovery period, and the response & post-incident period. The following slides are the recommendations as identified by PNS staff in the working session matched to industry leading practices.

Improvements that could potentially be implemented in regards to culture, systems, or processes can take a considerable amount of time and resources to implement. It should be noted that not all potential improvements listed in the following slides represent activities or processes that were not present whatsoever during the response. They may simply be an enhanced version of an action, activity, or process that was already deployed during the response.

# Our understanding

## Overview of the conditions leading up to, discovery, and response to the incident



### Pre-incident (Launch – April 5)

- Long-standing relationship with vendor
- Vendor did not activate monitoring or reporting features
- Standard privacy impact assessment performed internally
- Threat risk assessment commissioned by the department but not performed until after go-live

### Discovery (April 6-7)

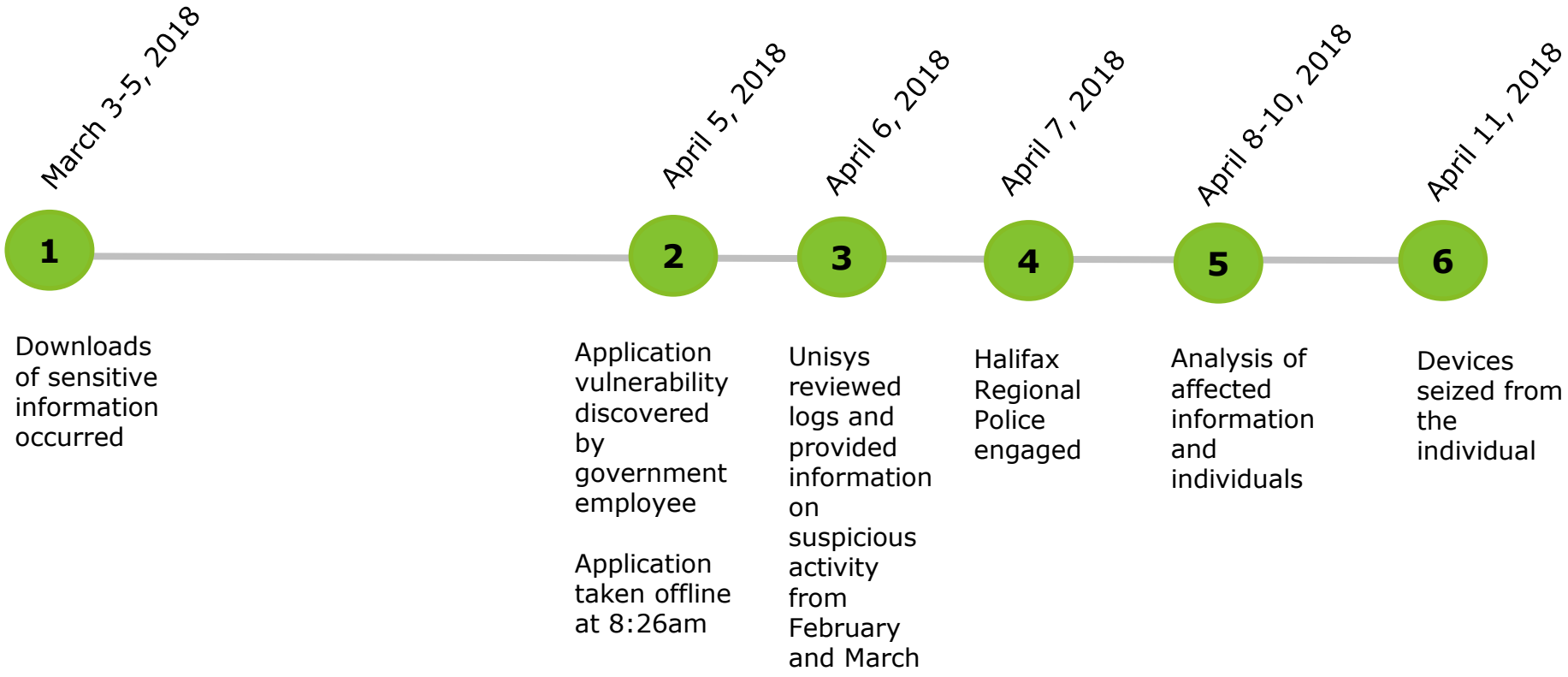
- Application vulnerability was discovered by a Public Archives employee while accessing the application at home
- Un-encrypted URL allowed users to navigate to and download sensitive private information
- Upon review of activity logs, discovered that all file downloads were requested by one IP address (believed to be the same individual) over a 4-5 day period
- At this time there was a lack of clarity about how documents were shared or used
- System was taken offline at 8:26am April 5th and has not been reinstated

### Response & post-incident (April 8 – Present)

- Conference calls occurring over the weekend following discovery
- Incident center established where response team convened
- Review of information compromised and individuals affected completed. Separated data into three categories.
- Contacted Halifax Regional Police (HRP) on April 7th, who launched an investigation.
- Notified Privacy Commissioner
- Currently working to strengthen security requirements and processes

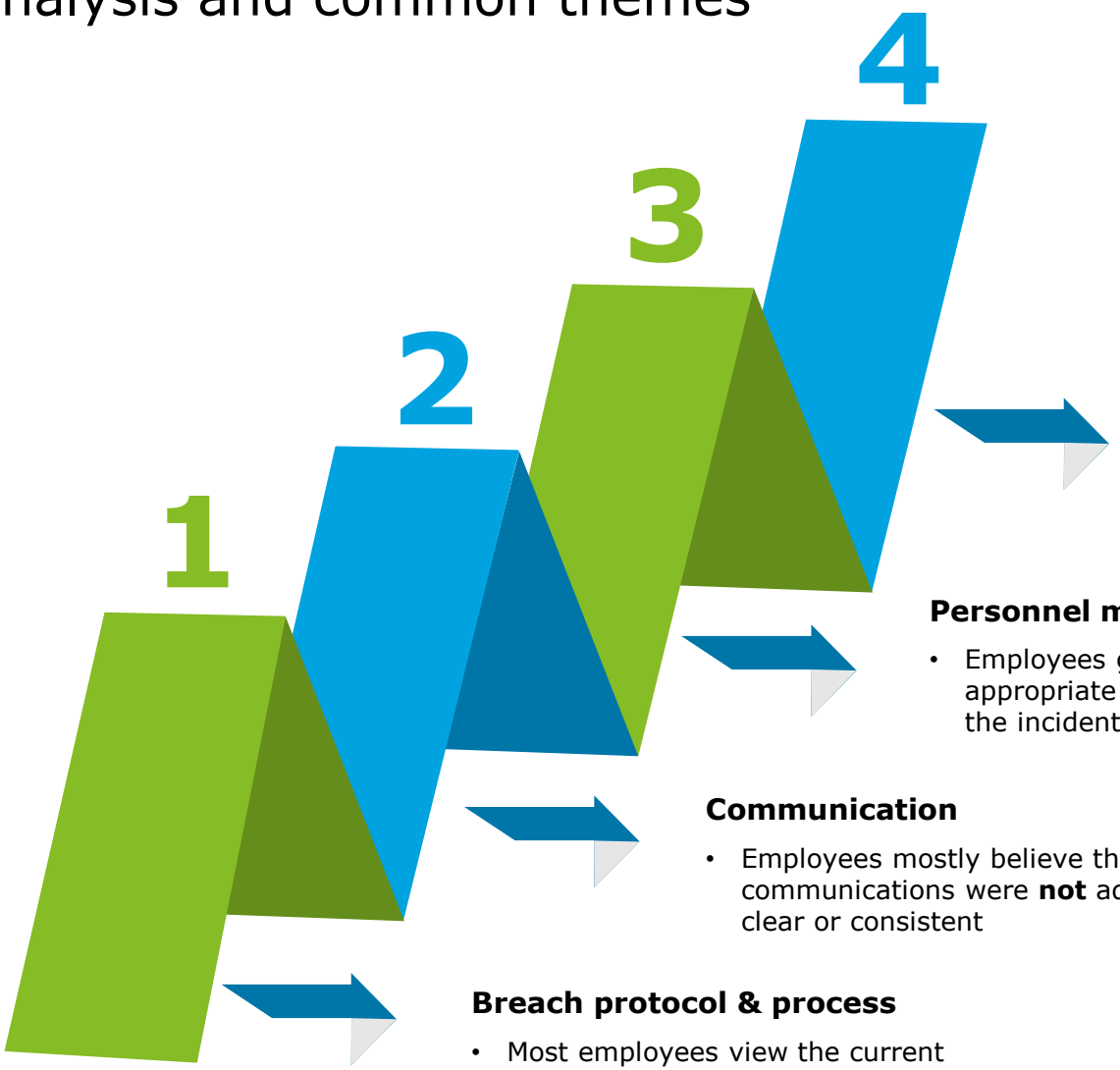
# Timeline

## Key events throughout the incident discovery and response



# Survey results

# Survey results
# Analysis and common themes




**Breach protocol & process**

- Most employees view the current protocol as adequate

**Communication**

- Employees mostly believe that external communications were **not** adequately clear or consistent

**Personnel management**

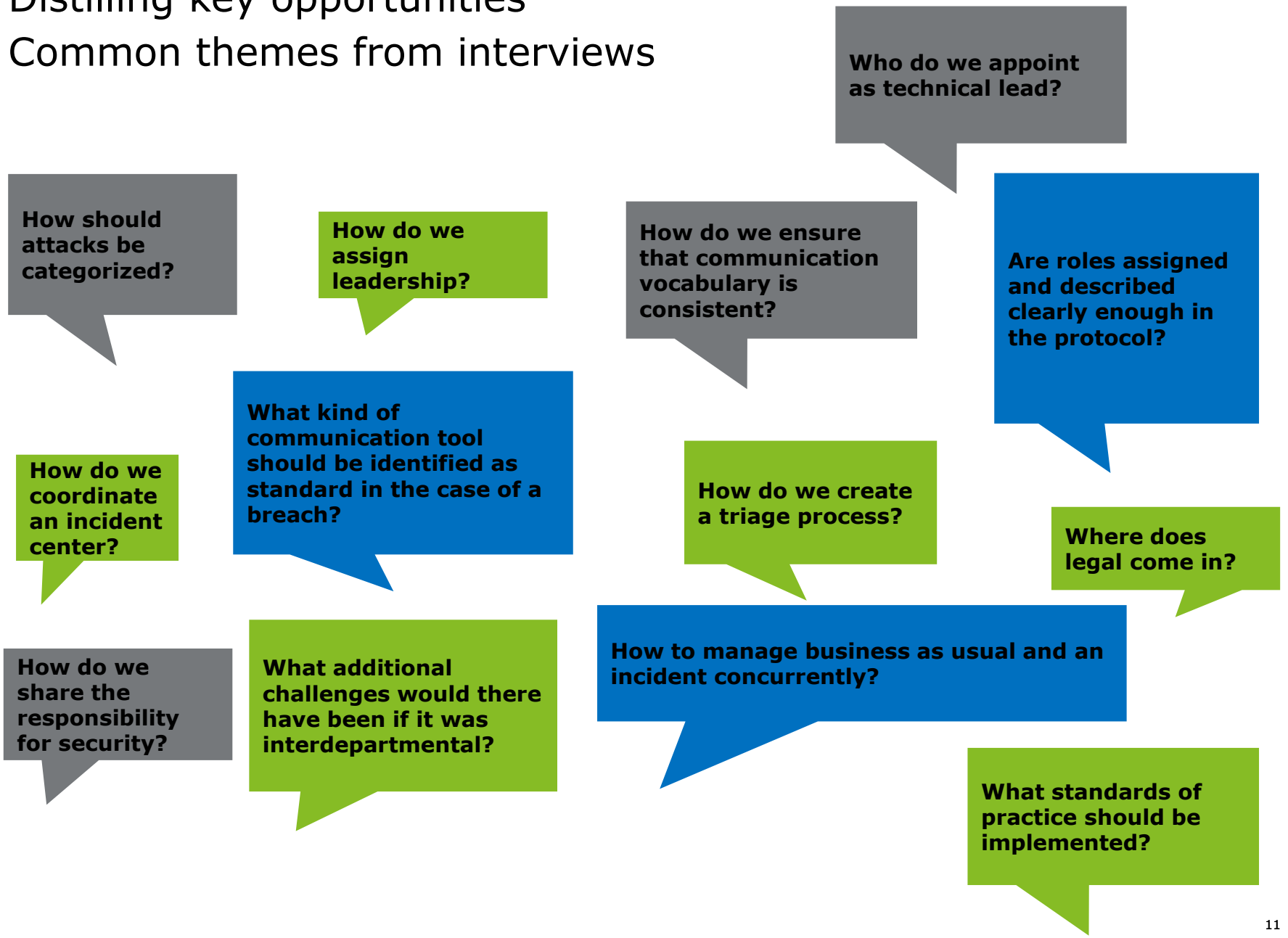
- Employees generally believe that appropriate personnel were involved in the incident response

**Roles & Responsibilities**

- Employees tend to believe that roles and responsibilities were **not** sufficiently defined during incident response

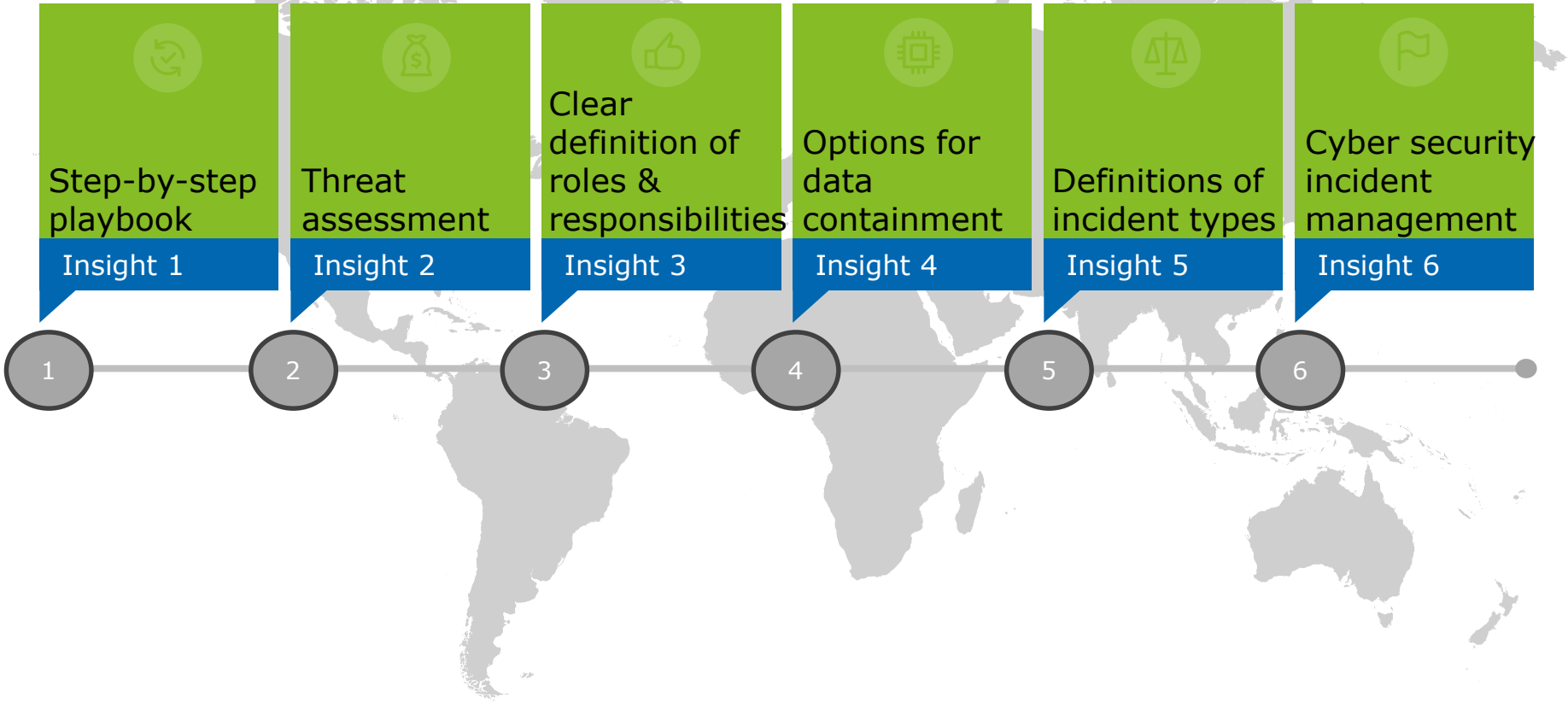
# Key themes

# Distilling key opportunities
# Common themes from interviews



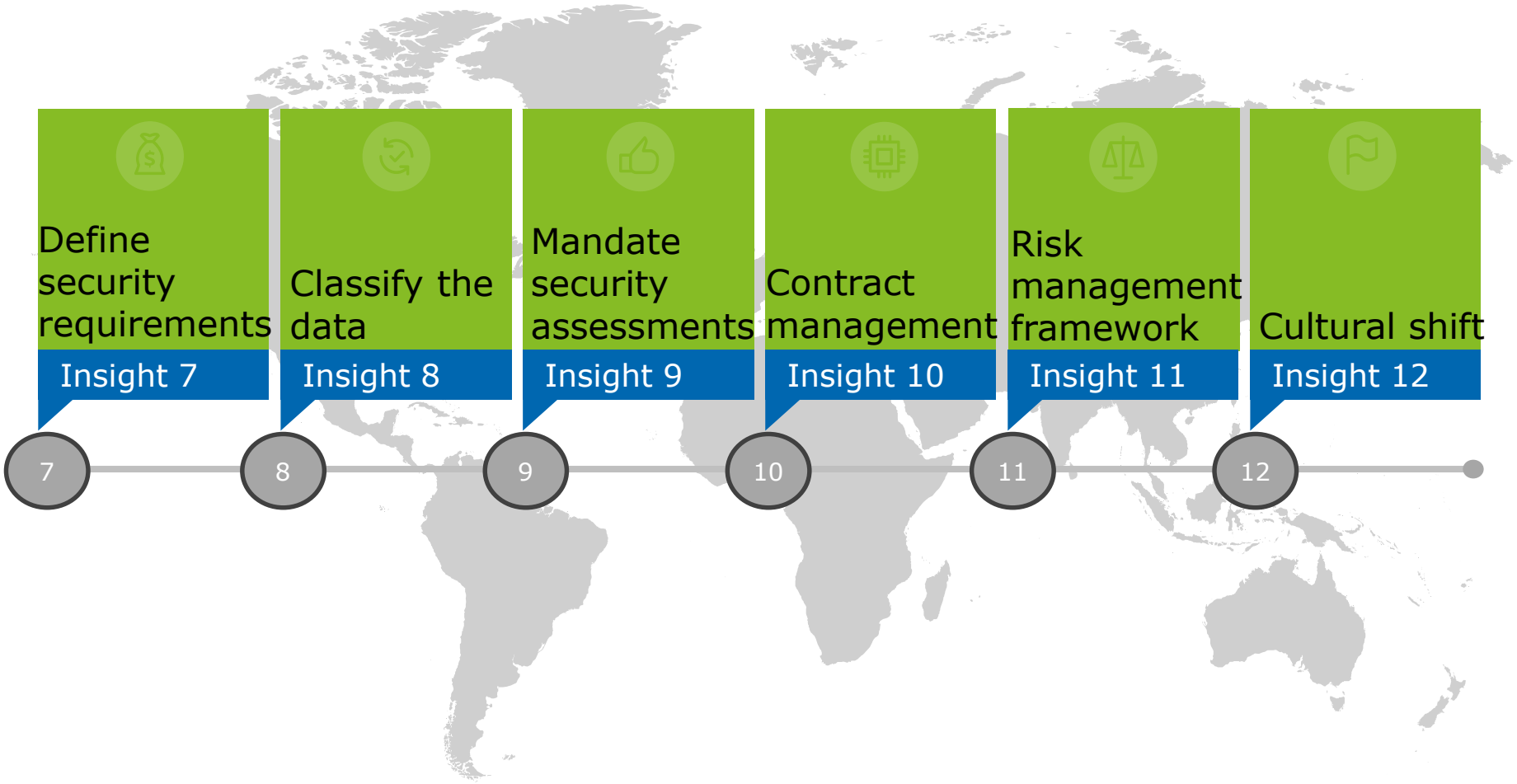
# Strengthening of incident protocol
## Improvements desired

While conducting interviews with key stakeholders, we identified the following 12 areas of improvement for the incident protocol. The opportunities identified are for consideration, however they do not represent a structured methodology or workflow.



# Strengthening of incident protocol (Cont.)

## Improvements desired



# Incident response successes

## Activities that generated positive outcomes throughout the response

**Activities to continue**

- **Employee reporting of application gaps**
- **Application of the privacy breach protocol**
- **Dividing teams in the current way (Privacy and Cybersecurity & Risk Management)**
- **Taking relevant systems offline immediately**
- **Sending notification letters promptly**
- **Requesting and receiving support from outside the department (e.g. Justice)**
- **Incorporating lessons learned into daily work**
- **Focusing on awareness that processes are public for maximum transparency**

# Key insights – **Pre-discovery**
# Matched to best practices

In the tables that follow Deloitte has matched desired improvements as identified by PNS to industry best practices. These best practices are sourced from industry recognized leading authorities such as the National Institute of Standards and Technology Computer Security Incident Handling Guide or the COBIT (Control Objectives for Information and Related Technology) standards.

| Observation | Improvement desired | Industry leading practice |
|---|---|---|
| 1. Step-by-step playbook | 1. Inclusion of emergency contact information for all relevant stakeholders and departments<br>2. Plans should account for different scenarios such as breach within government infrastructure and different departments or systems | 1. Organizational communication flows should be mapped<br>2. Asset vulnerabilities should be identified and documented, internal and external threats should be identified and documented |
| 2. Threat assessment | 1. Development of a methodology to evaluate severity of threats and sensitivity of data<br>2. Criteria to determine likelihood and consequences of potential impact | 1. Threats, vulnerabilities, likelihoods, and impacts should be used to determine risk<br>2. Risk responses should be identified and prioritized |
| 3. Definition of roles and responsibilities | 1. Definitions of who has the authority to assess nature of information breached<br>2. Guidance to define "responsible parties"<br>3. Inclusion of cyber security personnel in protocol<br>4. Define a team that will response to an incident for each system | 1. Information security roles & responsibilities should be coordinated and aligned with internal roles and external partners<br>2. Personnel should know their roles and the order of operations when a response is needed |

# Key insights – **Pre-discovery (Cont.)**
# Matched to best practices

| Observation | Improvement desired | Industry best practice |
|---|---|---|
| 4. Cyber security management | 1. Conduct table-topping, training, and practice privacy breaches to prepare for further breaches<br>2. Update the protocol to include guidance for cyber security attacks | 1. Vulnerability management plans should be developed and implemented<br>2. All users should be informed and trained in system security<br>3. Response plans (incident response and business continuity) and recovery plans (incident recovery and disaster recovery) should be in place and managed |
| 5. Define security requirements | 1. Ensure stronger understanding of functionality (what a program should do) vs anti-functionality (what it should specifically not do)<br>2. Defining expectations for monitoring and reporting requirements | 1. Information systems and their functions are catalogued<br>2. System configuration change controls are in place |
| 6. Classify the data | 1. Evaluation and documentation of the nature of content and the sensitivity of data<br>2. Determination of potential impacts of a breach | 1. Adoption of a security categorization of information and information systems<br>2. Adoption of an impact map |

# Key insights – **Pre-discovery (Cont.)**
# Matched to best practices

| Observation | Improvement desired | Industry best practice |
|---|---|---|
| 7. Mandate security assessments | 1. Development of guidance for required PIAs, TRAs, and/or vulnerability assessments<br>2. Scalable PIAs and TRAs | 1. Conduct, document, review, disseminate, and regularly update risk assessments<br>2. Conduct business/process level, and information system level threat assessments |
| 8. Communication management | 1. Clarify communications processes between corporate security and law enforcement<br>2. Develop clearer definitions for when to consult legal | 1. Share information in a way that is consistent with response plans<br>2. Voluntary information sharing should occur with external stakeholders to achieve broader cybersecurity awareness and to ensure transparency<br>3. Events should be reported consistent with established criteria |
| 9. Risk management framework | 1. Create a process to declare something a major incident<br>2. Implementation of a risk management framework<br>3. Equipping the business with tools and resources needed to assess data and related risks | 1. Adoption of an impact map<br>2. Organizational risk tolerance should be determined and clearly expressed<br>3. Adoption of NIST 6 step risk management framework |

# Key insights – **During response**
# Matched to best practices

| Observation | Improvement desired | Industry best practice |
|---|---|---|
| 1. Definitions of roles and responsibilities | 1. Determine an incident leader earlier than in this incident, especially if multiple executives are involved in the future<br>2. Appoint a technical leader and functional leader if necessary<br>3. Establish expectations for staff responsibility distribution (business as usual vs. incident response) | 1. A team manager and deputy should be appointed, in addition to a technical leader (if necessary)<br>2. Personnel should know their roles and the order of operations when a response is needed |
| 2. Data containment | 1. Outline and provide guidance on the different options for data containment<br>2. Define civil vs. criminal circumstances | 1. Data-at-rest and data-in-transit should be protected, protections against data leaks should be implemented<br>2. Incidents should be categorized consistent with response plans |
| 3. Definitions for incident types | 1. Define language to classify incidents and ensure consistency of external communications | 1. Events should be reported consistent with established criteria<br>2. Information should be shared consistent with response plans<br>3. Voluntary information sharing should occur with external stakeholders to ensure transparency |

# Key insights – **During response (Cont.)**
# Matched to best practices

| Observation | Improvement desired | Industry best practice |
|---|---|---|
| 4. Communication management | 1. Consider correcting misinformation in media<br>2. Use consistent vocabulary (e.g. breach vs. hack) | 1. Information should be shared consistent with response plans<br>2. Voluntary information sharing should occur with external stakeholders to achieve broader cybersecurity awareness and to ensure transparency |
| 5. Cultural shift | 1. Place more focus on employee workload management | 1. Segregate roles to reduce the amount of administrative work that each member is responsible for |

# Key insights – **Post-incident**
# Matched to best practices

| Observation | Improvement desired | Industry best practice |
|---|---|---|
| 1. Step-by-step playbook | 1. Establish a process for getting breached assets online again (and determining which parts) | 1. Recovery protocols are prepared and executed after an event |
| 2. Threat assessment | 1. Design clearer documentation of conflicting rationales describing why decisions were made | 1. Incident response teams should immediately begin recording all facts in a logbook |
| 3. Defining security requirements | 1. Ensure right to audit clauses are included in vendor contracts | 1. Conduct regular supply chain protection activities including vendor audits |

# Key insights – **Post-incident (Cont.)**
# Matched to best practices

| Observation | Improvement desired | Industry best practice |
|---|---|---|
| 4. Communication management | 1. Develop clearer, breach-ready communication for other internal clients that may not know what happened | 1. Include provisions in incident response for notification of typical parties, including other internal stakeholders |
| 5. Cultural shift | 1. Risk should be top of mind and staff should consider impacts of potential incidents when dealing with sensitive data or technology | 1. A privacy awareness strategy should be implemented to promote a culture of privacy |

# Appendix I: List of interviewees

# Appendix I
# List of interviewees

The following personnel were interviewed throughout the course of this engagement:

| Name & Position |
| --- |
| Jeff Conrad, Deputy Minister |
| Sandra Cascadden, CIO & Associate Deputy Minister |
| Rob Samuel, ED, Cybersecurity and Risk Management |
| Maria Lasheras, Chief Information Access and Privacy Officer |
| Donna Chislett, Director, Communications |

# Appendix II: Cyber Incident Response Lifecycle (Literature for Future Consideration)

# Most common challenges faced by organizations
# Managing a breach throughout the lifecycle

Deloitte, through the facilitated session, introduced some leading practices and perspectives. However, none of these are to be viewed as direct recommendations or indications of the quality of the Province's management of the incident, but rather content for consideration during the facilitated workshop.

**Throughout the stages of the lifecycle**

- Telling an accurate and consistent story across a cascade of communications to multiple audiences, including what actually happened, who was affected, what you plan to do about it, and what progress you are making
- Responding to an overwhelming volume of information requests from citizens, journalists, business partners, vendors, law enforcement, etc.
- Managing requests from business partners to modify business arrangements, processes, and methods of sharing information
- Dealing with the impending threat of legal action, and determining what legal recourse, if any, are available to you
- Navigating the confusion created by changing and/or uncertain priorities, roles, and responsibilities
- Managing the gap and associated risks during the timeline between identification of remediation requirements and implementation of required changes

# Most common challenges faced by organizations
# Managing a breach throughout the lifecycle

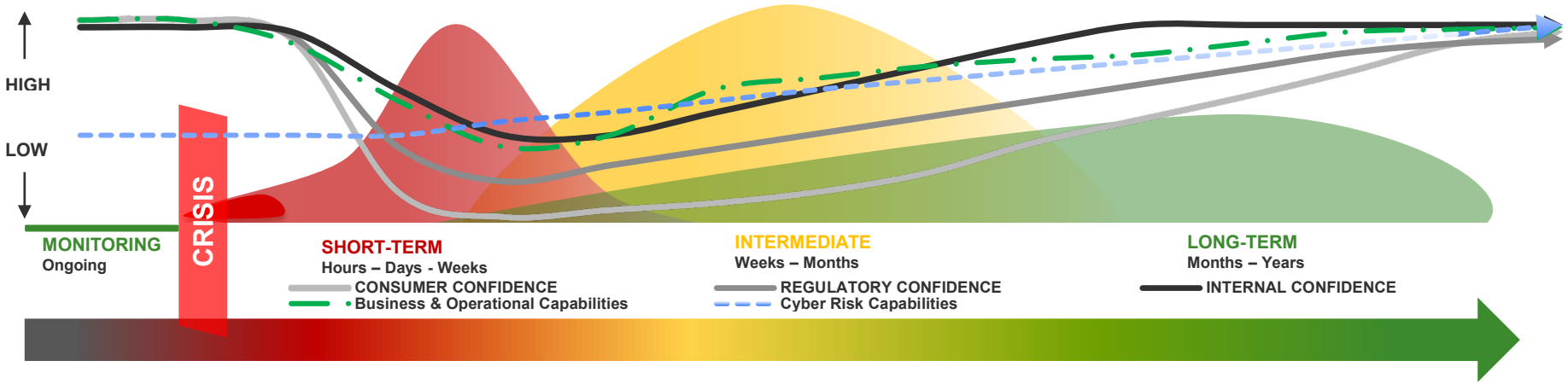
## Short term

- Management of the incident as a technology issue without the required integration points into the organizations and broader executive management decision making process
- Distinguishing good, actionable information from misinformation or partial information when making critical decisions and communicating with specific stakeholders
- Keeping the organization focused on operations at the same time you are planning and executing the recovery
- Managing potential periods of outage when the business is not able to access systems or complete normal daily operations, which leads to a lull in productivity

## Intermediate to long term

- Understanding capability gaps and communicating an achievable remediation plan to specific stakeholders
- Managing expectations with respect to deploying “throw away” solutions to address immediate gaps vs. establishing more strategic, more sustainable capabilities
- Balancing the organization’s inclination to secure information and assets with the strategic need to develop better vigilance and the practical necessity to prepare for another significant incident
- Prioritizing the influx of technology project requests and a substantially increased technology budget
- Identifying, tracking and managing the risks associated with work-arounds deployed across the organization during recovery
- Preparing for heightened scrutiny from stakeholders and a much more rigorous examination regimen, affecting almost all aspects of operations and technology
- Defending legal claims

# Cyber incident response lifecycle
# The interplay between capabilities and stakeholder confidence




At the most strategic level, recovering from a cyber incident involves an important balance between recovering or enhancing capabilities and restoring confidence among a broad spectrum of stakeholders. This lifecycle is for example purposes and represents that of a generic organization that has experienced a breach and isn't a specific reflection of the incident at the PNS.

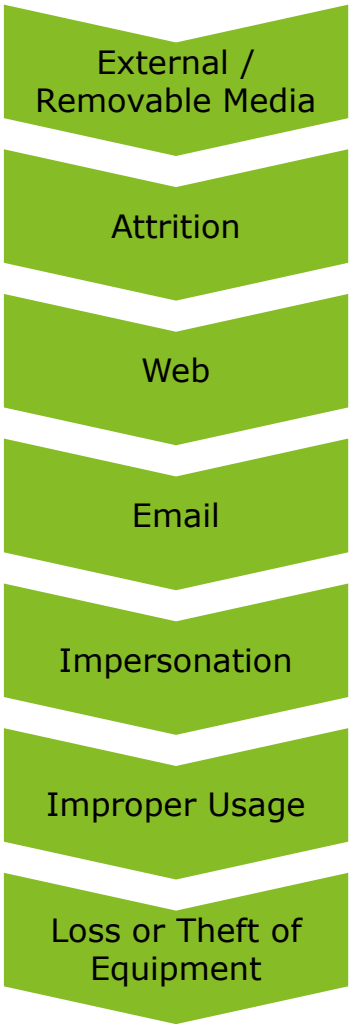
***Capabilities***

- ***Business and operational capabilities*** need to be restored in the case of disruptive or destructive attacks, which usually takes hours or days, but can extend for weeks or even months in severe cases.
- ***Cyber risk capabilities*** need to be enhanced to secure the environment, provide better visibility into ongoing threats, and reduce the impact of future attacks. Important progress can be made in the short term, but significant improvement usually takes months or years to achieve.

***Confidence***

- ***Citizens*** are most immediately concerned with direct personal damage from loss of data
- ***Employees*** can be overwhelmed by negative publicity and increased chaos in both their work and personal lives
- ***Business partners*** are concerned about the immediate threat of cross contamination and the longer-term integrity of business transactions

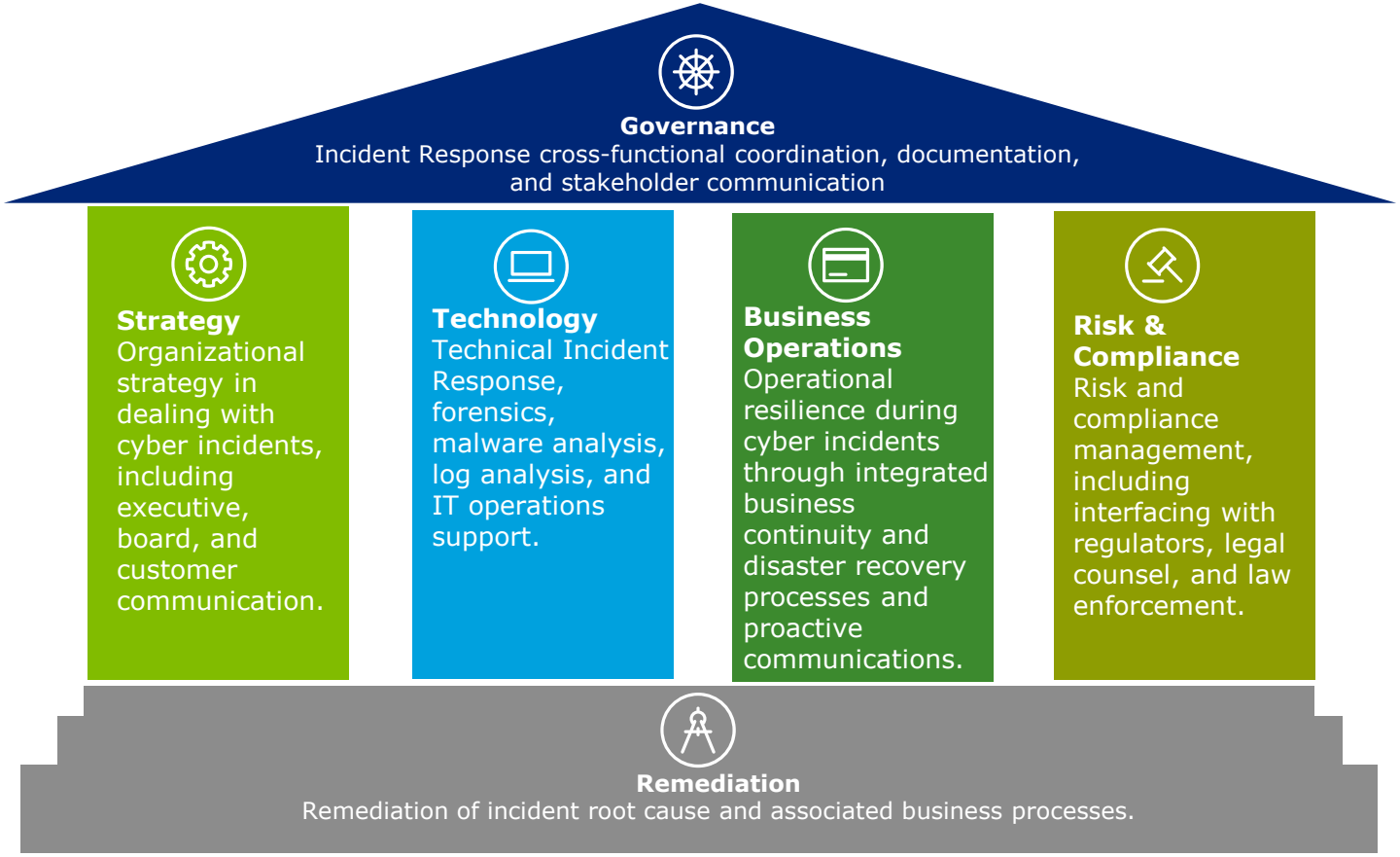
# Common attack vectors
# Different incidents merit different response strategies




- An attack executed from removable media or a peripheral device – for example, malicious code spreading onto a system from an infected USB flash drive
- An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services (e.g. a DDoS intended to impair or deny access to a service or applications; a brute force attack against an authentication mechanism, such as passwords, CAPTCHAS, or digital signatures)
- An attack executed from a website or web-based application – for example, a cross-site scripting attack used to steal credentials or a redirect to a site that exploits a browser vulnerability and installs malware
- An attack executed via an e-mail message or attachment – for example, exploit code disguised as an attached document or a link to a malicious website in the body of an e-mail message
- An attack involving replacement of something benign with something malicious – for example, spoofing, man in the middle attacks, rogue wireless access points, and SQL injection attacks all involve impersonation
- Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories; for example, a user installs file sharing software, leading to the loss of sensitive data; or a user performs illegal activities on a system
- The loss or theft of a computing device or media used by the organization, such as a laptop, smartphone, or authentication token

# Incident response requires executive leadership
# Incidents can quickly become critical business issues

To manage the challenges associated with incident response, and to appropriately balance rebuilding and enhancing confidence and capabilities, organizations should embrace an enterprise incident response approach. At the helm, a cross-functional executive level incident response team should drive decisions and lead the prioritization of restoration and enhancements.



# Guiding principles

## During an incident, the obvious is often overlooked or mismanaged

**Governance**

How you organize and manage your team

- Implement structured response team from initial response through to resumption of business as usual
- Account for segregation of duties:
  - Independent and parallel investigation team to help determine the root cause and determine necessary remediation steps
  - Strategy and decision process; Business Operations; and Recovery should be independent teams with established rhythm and flow
- Consider the role of counsel –they should be actively engaged but a business representative should lead the response team
- Define incident response and recovery lifecycle phases and decision framework with clear criteria outlining progression and success

**Strategy**

How you lead, prioritize and communicate

- Collective communications driven by executive leadership should articulate as simply and clearly as possible what happened and what they are doing to remediate and protect the affected individuals
- Create a communication cadence that provides continuous and planned updates based on the identified facts. Make that cadence known to your stakeholders
- Engagement with governmental affairs team is critical and can help stave off public statements by elected officials that might add fuel to negative media communications. This is absolutely critical in regulated industries.
- Define escalation and prioritization processes – during an incident, escalation will be needed to prioritize recovery and business as usual activities

# Guiding principles

## During an incident, the obvious is often overlooked or mismanaged

**Technology**

How you perform investigation and rebuild environments

- Don’t overestimate the importance of additional tools – Tools are an important component of building additional capabilities, but cyber risk should be managed as a business risk
- Be conscious of the constant tension between immediate needs and the long term solution. Throw away work is not uncommon and is often necessary to meet near term priorities.

**Business operations**

How you minimize business disruption

- When needed, implement out-of-band processes to replace those that are broken or have too many constraints during crisis. Developing out-of-band just in time processes often is the most efficient and effective during incident management.
- Plan for surge support
- Understand business limitations that may exist

**Risk & Compliance**

How you address regulatory compliance

- Anticipate requests from law enforcement and regulators. This may include requests for access to certain parts of your network and infrastructure, as well as requests to review the approach and details of response activity.
- Understand additional risks brought about by the ad-hoc processes, technology and work-arounds required during the crisis.

# The adversary: Advanced Persistent Threats
# APT's are present in virtually all organizations

Advanced Persistent Threats ("APTs") are initiated by **nation states** and **organized crime networks**

They generally target government and organizations with **high-value** information

APT groups **steal** information, **disrupt** the marketplace, and **damage** the victim's reputation

APTs are "**low and slow**", penetrating without detection and are impossible to identify with traditional methods

While the incident at PNS was not the result of an APT, this material is included for informational purposes, as APT related incidents continue to be more common.

It's not a question of **if** an organization has been compromised, but **when**. **Proactive** attempts at detection can **minimize** the risk associated with an APT.

# The adversary: Advanced Persistent Threats
## Understanding an APT: a typical attack progression

**Pre-compromise**

The APT group **identifies** an organization based on specific objectives, and attempts to gain initial access through a **targeted attack** (e.g. spear-phishing)

**Initial compromise**

The APT group **establishes** an entry point through which to begin **compromising**, usually a single system on the network at first


**Exfiltrate and hide**

Once further penetration is established, the APT group can **acquire** and **exfiltrate** data from the network without being detected. Then, the APT group will cover its tracks and **persist** within the network for future exploits.

**Further compromise**

Using the initial compromise, the attack will move l**aterally** across the internal network, gathering more intelligence to **further** its attack (e.g. administrative controls)

Deloitte.

About Deloitte

Deloitte provides audit & assurance, consulting, financial advisory, risk advisory, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights and service to address clients' most complex business challenges. To learn more about how Deloitte's approximately 264,000 professionals—9,400 of whom are based in Canada—make an impact that matters, please connect with us on LinkedIn, Twitter or Facebook.