Ransomware Response Playbook

This document has been designed at the request of the Canadian Investment Regulatory Organization. This document is to guide response to a ransomware attack that can have a material impact on the continuity of business operations. It outlines the actions required to ensure that these incidents are addressed in a coordinated and repeatable manner. Procedures should be tested and reviewed periodically via scenario-based exercises.

DATE OF ISSUE: August 22, 2023
AUTHOR: Juno Risk Solutions

juno risk solutions

CIRO · OCRI
Canadian Investment Regulatory Organization
Organisme canadien de réglementation des investissements

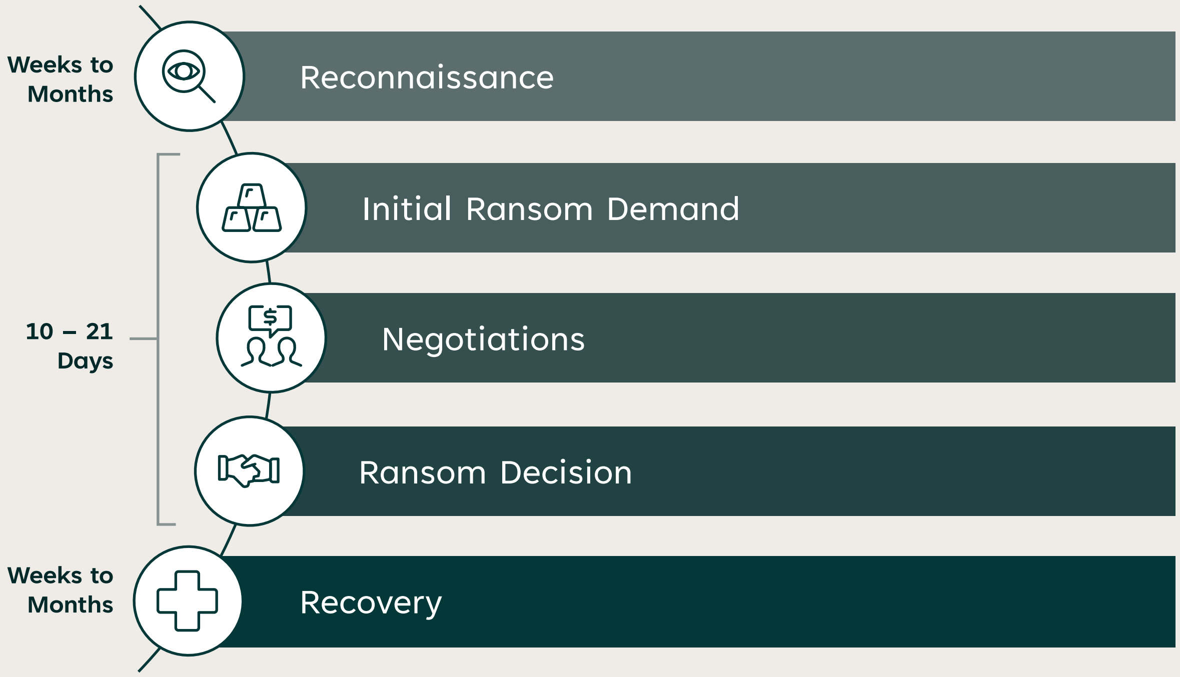
Ransomware Attack Overview

Cyber incidents are becoming increasingly prevalent and pose an existential threat to Canadian Investment Dealers and Mutual Fund Dealers, their investors, employees, and stakeholders. Without exaggeration, cyber incidents present a wide array of potential losses that could threaten these organizations and their stakeholders. Thus, timely, collective, and effective response to an array of cyber attacks from all facets of the company is essential to protect Canadian Investment Dealers and Mutual Fund Dealers, investors, employees, and stakeholders. In recent years, high-profile ransomware attacks have affected the Canadian financial industry impacting organizations such as credit unions, insurance companies, and accounting firms. These attacks have resulted in significant financial losses and caused considerable reputational damage.

Ransomware

The basic concept of a ransomware attack is to introduce malware onto the target's computer systems, to lock out those systems, often after exfiltrating sensitive data, and extorting a ransom in exchange for a decryption key and the promise to not release stolen data to third parties. The organized criminal groups that conduct ransomware attacks intend to create a range of impacts – financial, operational, reputational, legal, regulatory – upon their target so that they are compelled to pay the ransom. Ransomware attacks present an enterprise-wide series of risks. The related impacts occur simultaneously with the effect of overwhelming the target company's ability to react and manage the crisis. Figure 1 emphasizes the stages of a ransomware attack illustrating how recovering from an incident can extend from weeks to several months.

Figure 1 – Ransomware Attack Phases



Ransomware Related Risks

Ransomware attacks present more than an IT problem posing significant, interrelated business challenges. Table 1 highlights the range of impacts organizations likely experience in the event of a ransomware attack. It also includes corresponding industry-standard protections and safeguards that are commonly deployed to address each of these risks. It is the primary responsibility of leadership to address the risks in a timely and coordinated fashion.

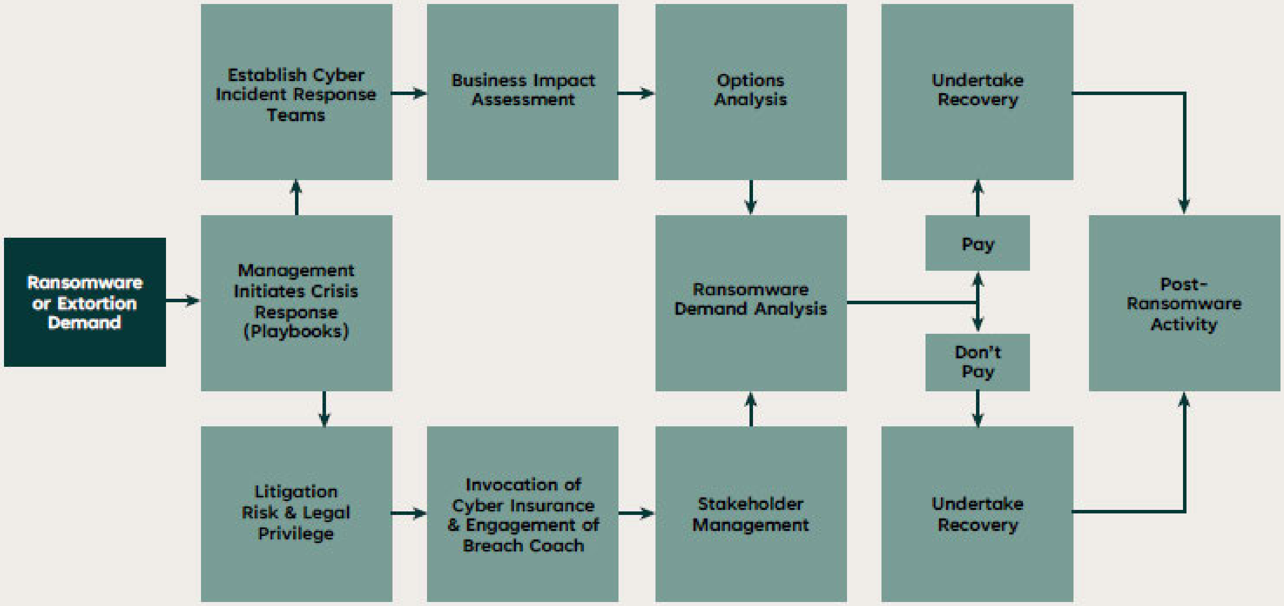
The task for an organization's Executive Team, Business Continuity Team (as part of an in-place Business Continuity Plan), IT Incident Response Team (as part of an organization's Disaster Recovery Plan), staff, and Board of Directors, is to react quickly and in a coordinated fashion. The main effort here will be to minimize the range of impacts presented by an attack on business, investors, and stakeholders.

Table 1 – Cyber Incident-related Risks

Risks	Impacts	Responses
Financial Risk	Ransom Demand Penalties / Fines Loss of Revenue / Incurred Costs	Financial reserves Cyber Insurance Debt Issuance
Operational Risk	Disrupted Services Systems Disruptions Including Website / Online Applications	Third Party Service Providers Incident Response Plans Cyber Insurance Manual Workarounds
Market Risk	Disruption to Operations Exposure of Personal Information Client Experience	Crisis Communications Plan Cyber Insurance Breach Reporting Procedures
Reputation Risk	Media Exposure Customer Flight	Crisis Communications Plan Cyber Insurance
Regulatory Risk	Breach Reporting – Including Canadian and United States Multi-Jurisdictional Reporting Regulations / Sanctions	Breach Reporting Procedures Crisis Communications Plan
Legal Risk	Litigation Breach of Confidentiality Contract Notification Requirements	Legal Privilege Protocol Vendor Management Cyber Insurance
Human Capital Risk	Employee Burnout Reduced Employee Retention Higher Turnover Inability to Attract and Recruit Talent	Employee Assistance Programs Workplace Culture Competitive Salaries Competitive Compensation & Benefits Package

Ransomware Attack Phases

Figure 2 – Cyber Incident Response Teams


Ransomware or Extortion Demand
Management Initiates Crisis Response (Playbooks)
Establish Cyber Incident Response Teams
Business Impact Assessment
Options Analysis
Undertake Recovery
Ransomware Demand Analysis
Pay
Don't Pay
Post-Ransomware Activity
Litigation Risk & Legal Privilege
Invocation of Cyber Insurance & Engagement of Breach Coach
Stakeholder Management
Undertake Recovery

Immediate Actions Upon Discovery of a Cyber Incident

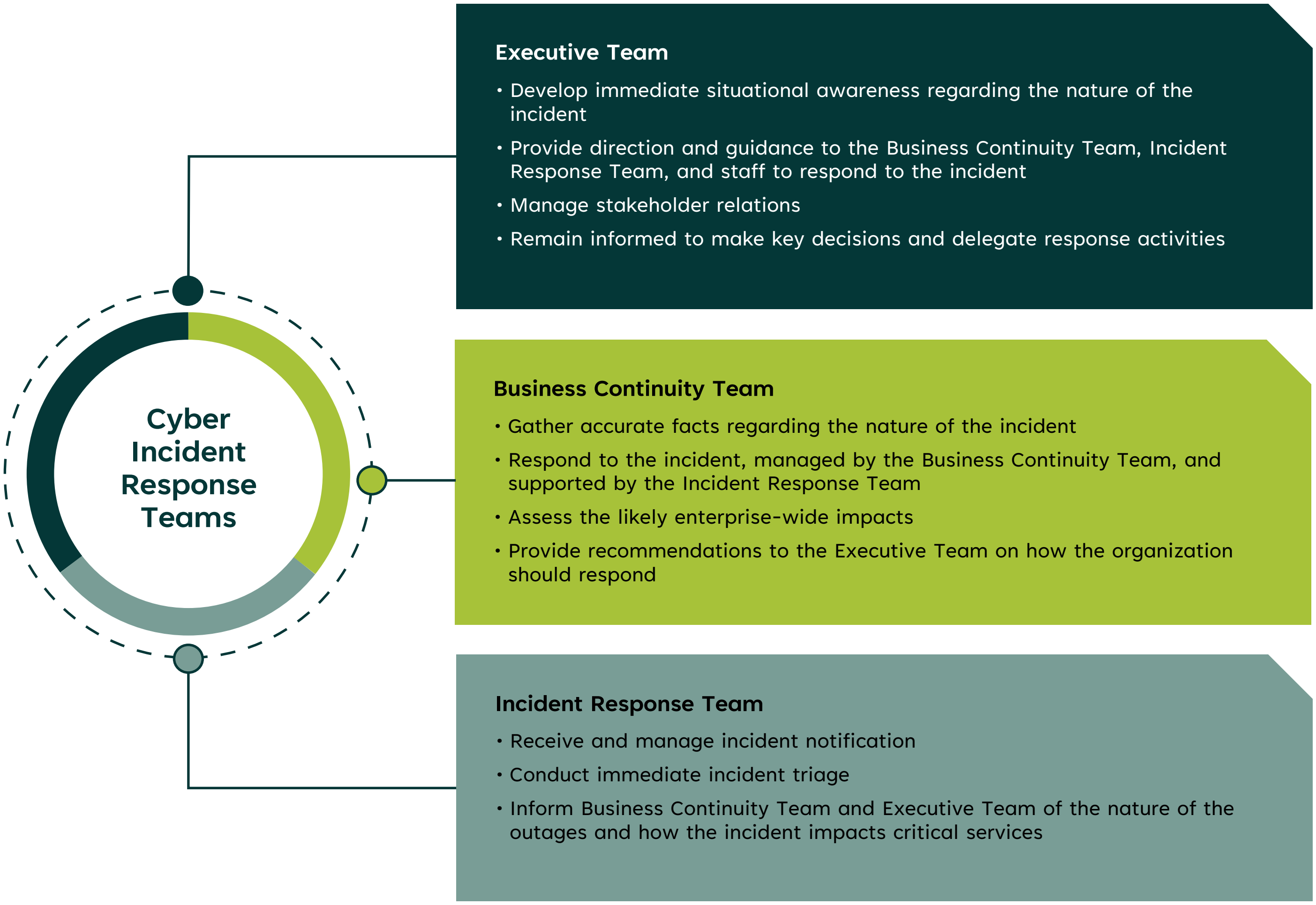
Establish Cyber Incident Response Teams

The role of the Executive Team during a ransomware attack is to act as the highest-level coordinating body, with the authority to make decisions on behalf of the company. Supported by the Business Continuity Team and Incident Response Team who conduct an initial incident triage, gather and evaluate information, and implement Executive Team direction, the Executive Team will make policy decisions on behalf of the company and direct efforts to address the incident. Even the smallest firms have these functions, the responsibility for which may sit with just one or two individuals within an organization.

The first manifestation of a ransomware attack is likely to be some form of IT systems outage. The initial response to this event will be under the direction of the Incident Response Team. The Incident Response Team will include an escalation of the event to the Business Continuity Team for initial triage to determine if the systems outage introduces impacts that require a broader enterprise-wide assessment.

Upon discovery of a suspected ransomware attack, both the Executive Team and the Business Continuity Team will convene. The Business Continuity Team will present its incident triage and an initial assessment of the impacts of the incident to the Executive Team.

Figure 3 – Cyber Incident Response Teams



Cyber Incident Response Teams

Executive Team

- Develop immediate situational awareness regarding the nature of the incident
- Provide direction and guidance to the Business Continuity Team, Incident Response Team, and staff to respond to the incident
- Manage stakeholder relations
- Remain informed to make key decisions and delegate response activities

Business Continuity Team

- Gather accurate facts regarding the nature of the incident
- Respond to the incident, managed by the Business Continuity Team, and supported by the Incident Response Team
- Assess the likely enterprise-wide impacts
- Provide recommendations to the Executive Team on how the organization should respond

Incident Response Team

- Receive and manage incident notification
- Conduct immediate incident triage
- Inform Business Continuity Team and Executive Team of the nature of the outages and how the incident impacts critical services

Litigation Risk and Legal Privilege

Any major disruption of services should first be evaluated to determine if the event introduces the possibility of legal action. Not all incidents present this risk. However, every ransomware or data breach-related incident does present the risk of litigation. During the initial incident triage by the Business Continuity Team, the organization's legal counsel will determine if the incident presents a risk of legal action. If the legal counsel determines that a risk of litigation exists, it will direct that the incident be managed under the cloak of legal privilege.

Legal privilege allows an organization to communicate freely with its lawyers about a cyber incident to obtain candid legal advice, without fear that these communications and related documents will be disclosed to others, including in litigation. It also allows an organization's lawyers to take steps to defend the organization in litigation or in anticipation of litigation, without fear that their "lawyer's brief" might be disclosed to others and used against their client. Managing incident response through the General Counsel under "the cloak of legal privilege" is a critical step to protect the organization in the event of legal action.

Invocation of Cyber Insurance & Engagement of Cyber Breach Coach

If an organization experiences an actual or reasonably suspected ransomware attack, it should immediately notify its cyber insurance provider or insurance broker if the organization maintains cyber insurance. Cyber insurance generally offers coverage for breach response that provides access to a panel of expert breach response service providers. This includes a Breach Coach who is an expert specialized in handling cyber incidents and provides valuable legal guidance and assistance in managing response efforts. The role of the Breach Coach is to act essentially as a specialist project manager for a cyber incident. The Breach Coach will engage crisis response vendors provided through the cyber policy and provide those resources under a cloak of legal privilege.

Business Impact Assessment

As businesses increasingly rely on technology, it is critical that organizations adopt a comprehensive approach to risk management. This is especially true with respect to ransomware attacks, as they not only threaten impacts to technology, but will carry business-wide impacts, as well. To help the Executive Team facilitate an enterprise-level understanding of the broad impacts caused by a cyber incident, Table 2 presents a high-level risk-based impact assessment framework. With this framework, the objective is to capture the range of potential and real-time impacts that the organization may face during a cyber incident, including disruptions to key lines of business, financial impacts, and reputational impacts.

Table 2 - Risk Based Impact Assessment Framework

	Day 1	Day 7	Day 14	Day 21	Day 28
Financial Impact					
Revenue Impact					
Lost or Deferred Revenue					
Incurred Expenses or Opportunity Costs					
Key Account Risk					
Incurred Costs					
Response Costs					
Recovery Costs					
Litigation Risk					
Data Breach					
Ransom Demand					
Ransom					
Operational Impact					
Delayed Services					
Disrupted Transactions					
Reputational Impact					
Traditional & Social Media					
Stakeholders					
Legal Action					
Leadership Embarrassment					
Mandate					

This risk-based assessment framework should be owned by the organization's Business Continuity Team and supported by the Incident Response Team, who provide an analysis of the financial, operational, and reputational impacts presented by a cyber incident in real time, as well as projections into future weeks. This assessment is used to provide the Executive Team with the situational awareness required to make informed decisions. When reviewing the risk-based assessment framework, the Executive Team must carefully consider which impacts presented by the cyber event warrant the greatest prioritization of response efforts.

This framework enables the Executive Team to consider the range of impacts to the business and thus make an informed business decision whether to pay the ransom or not.

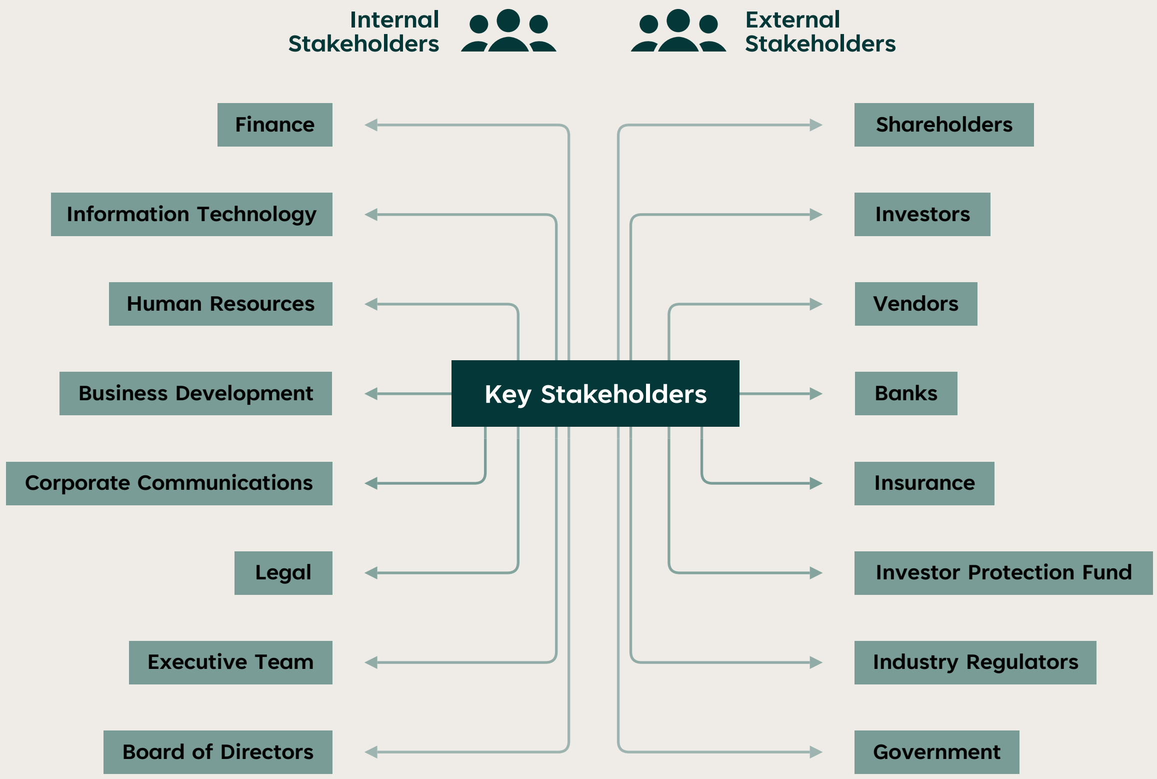
Stakeholder Management

Figure 4 highlights key stakeholders for Investment Fund Dealers or Mutual Fund Dealers. It is critical that communications are managed carefully for both internal and external stakeholders.

A ransomware attack will create twin opposing tensions for an organization:

- The need to inform clients and other stakeholders who are directly affected immediately with accurate and appropriate messages; and
- The obligation to protect confidential information regarding incident response from inadvertent release thereby increasing potential litigation risks.

Figure 4 – Key Stakeholders

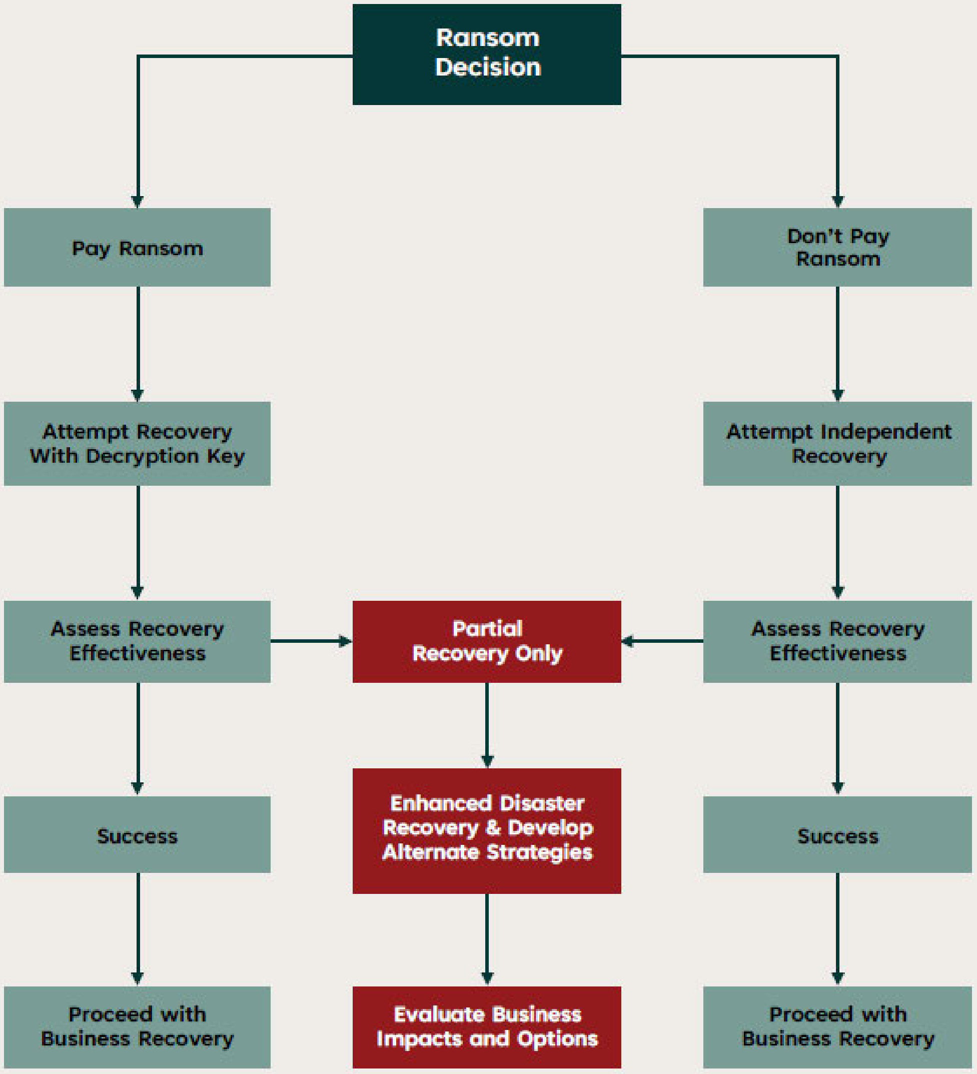


Options Analysis

A ransomware attack presents the Executive Team with a series of options at various stages of the crisis. Figure 5 highlights Executive Team decision points with respect to a cyber incident and emphasizes that the Executive Team needs to be well informed by the Business Continuity Team and Incident Response Team to facilitate decisions.

Each decision point requires consideration of the range of options presented to the Executive Team regarding how well the organization can weather the crisis, if there is sufficient confidence in recovery abilities, and the urgency with which to make these decisions.

Figure 5 – Options Analysis Model


Ransom Decision
Pay Ransom
Don't Pay Ransom
Attempt Recovery With Decryption Key
Attempt Independent Recovery
Assess Recovery Effectiveness
Partial Recovery Only
Assess Recovery Effectiveness
Success
Enhanced Disaster Recovery & Develop Alternate Strategies
Success
Proceed with Business Recovery
Evaluate Business Impacts and Options
Proceed with Business Recovery

Ransom Demand Analysis

Risk Impact Considerations

Reaching a decision to pay a ransom to a criminal actor is challenging. It raises emotional issues regarding the possibility of paying a ransom that ultimately rewards criminals. However, a ransomware attack presents a range of business risks to an organization, all of which need to be considered when deciding on how to respond to a ransom demand.

As the Business Continuity Team and Incident Response Team continue the invocation of their respective incident response plans, the Executive Team must develop and implement strategies to eradicate the cyber threat. The Executive Team should consider the range of impacts the cyber incident has had on the organization. Table 3 outlines general considerations across a range of impact vectors.

Table 3 – Risk Impact Considerations

Financial	• Is the financial impact upon the company resulting from the cyber incident sustainable? • At what point may the financial burden exceed the ransom demand? • Does the Executive Team have authority to facilitate a ransom payment?
Operational	• How are service level standards being managed? • How great is the backlog of unprocessed transactions and how long will it take to recover those transactions and return the business to a normal operational tempo?
Regulatory	• In the event of a data breach, does the organization have an obligation to take steps to protect breached personal identifiable information (PII) from further disclosure? • Would the payment of a ransom in exchange for its return/destruction better fulfill that duty?
Reputation	• What is the reputation impact upon the organization based upon the continued disruption to operations? • What is the reputation impact of a full or partial disclosure of stolen company data? • What is the reputation impact should the organization decide to pay the ransom and this information become public?
Sanctions	• Is the threat actor known to the Breach Coach and their team? • Is the threat actor that has conducted the cyber attack under sanctions in Canada or another jurisdiction that presents regulatory risk if the threat actor is paid?
Impact on Staff	• What is the nature of the human capital risk from the crisis? • What will be the reaction of the staff should the company decide to pay or not pay the ransom? • How long can the organization continue to effectively manage the stress upon staff and management?
Return to Operations	• How imperative is it that the organization return to operations quickly? • Do the assessed business risks provide the organization time to continue to either negotiate or attempt to recover independently without paying the ransom?

Business Recovery

Recovery Process Evaluation

How well the organization can respond to, manage, and recover from an incident can significantly reduce financial, operational, and reputational losses. The Executive Team, Business Continuity Team, and Incident Response Team have levers - highlighted throughout this Playbook and included in incident response plans - that can directly influence incident outcomes. Leveraging these tools can lead to positive incident outcomes, while limited utilization can result in negative consequences.

Recovery Process Monitoring

The priority in recovering from a cyber event is to resolve the immediate issues impacting systems, data, and operations that facilitate critical services. The Executive Team must direct the Business Continuity Team and Incident Response Team to take necessary steps to recover critical services and continuously monitor recovery efforts until the crisis can be de-invoked. Figure 6 provides a high-level recovery scorecard to provide necessary oversight of response activities.

Once the immediate crisis impacts are resolved, the Executive Team must ensure that the organization returns to business as normal. Many organizations that experience a cyber incident never recover fully. Once the organization de-invokes the crisis response by managing immediate short-term priorities the emphasis of recovery is lost and the organization fails to recover to pre-incident levels.

It is important that as the organization continues recovering critical services through the recovery of systems, data, and operability, the focus shifts to financial recovery, stakeholder confidence management, and reputational recovery. These attributes are more challenging to measure but have the greatest long-term impact on the organization.

Figure 6 – Recovery Monitoring Scorecard

Recovery of:	Week			
	1	2	3	4
Systems	🟨 *Key criteria and objectives & KPI(s)*	🟢	🟢	🟢
Data	🟨	🟢	🟩	🟩
Operations	🟧	🟨	🟨	🟢
Stakeholder Confidence	🟧	🟧	🟨	🟨
Financial	🟨	🟧	🟥	🟥

Legend	Exceeding Target	On Target	At Risk	Unacceptable	Very Unacceptable
	🟩	🟢	🟨	🟧	🟥

Post-Incident Activity

Post Crisis Analysis

Following the incident, organizations should seize the opportunity to investigate the cause of the crisis, looking for and acting on evidence of wider cultural problems that may have caused it, and identifying opportunities for change to gain competitive advantage and greater resilience.

Strengthened Defenses - Following the conclusion of the event, the organization should immediately begin steps to minimize the likelihood of a reoccurrence. Many of those companies that reported a cyber attack between 2021-2022 also reported that they experienced more than one attack. Given the publicity that accompanies a cyber attack, the organization can be assumed to have some form of vulnerability that allowed the initial attack. Failure to address that original vulnerability can lead to a follow-on attack.

Regulatory Reporting - Regulatory reporting including breach reporting may be required. In certain jurisdictions, in the case where a ransomware attacker exfiltrated data and claimed to have destroyed it as part of the ransom negotiations, a company may still need to make a breach report if there is no concrete evidence that the data was destroyed.

After Action Report - Document how the organization responded to the crisis and how best to improve the responses for future events. This process should also be directed by the General Counsel under legal privilege.

Client Management - Engage with key clients and third parties to manage relations to prevent client flight and long-term reputational damage.

Crisis Plans - Review crisis plans, processes and competencies to determine:

- Did processes work and did information flow well?
- Was communication with stakeholders adequate and timely?
- Were plans adequately prepared pre-crisis to assist in its management?
- Were regulatory requirements addressed accurately and in a timely fashion?

Lessons Learned - The Executive Team should ensure that the Business Continuity Team and Incident Response Team undertake a post-crisis lessons learned investigation led by an appropriately experienced senior executive. Key areas of focus for this process should include an evaluation of the nature of the threat the organization faces, the effectiveness of the organization's incident response measures, and an assessment of the Board's role in crisis response.