

BCDR Scenario Analysis

A ransomware attack encrypted SolveTech’s servers, which caused a full operational shutdown affecting all 150 employees. Clients’ data, proprietary code, and operation systems are not accessible. Using the PrOACT framework (Hammond, Keeney & Raiffa, 1999) and decision analysis principles (Skinner, 2009), this report structures the key impacts and risk factors facing leadership.

Operational Impacts

Domain	Immediate Effect	Downstream Risk
Operational	Full system shutdown; all projects halted	Missed deadlines; SLA breaches
Financial	Revenue loss; ransom demand; IR costs	Legal liability; regulatory fines
Reputational	Mandatory client notification triggered	Clients churn; brand damage
Data Integrity	PII and source code encrypted/exfiltrated	GDPR/CCPA violations; IP loss

Primary Risk Factors

- Client data breach - consequence uncertainty is high; full scope though is unknown.

Skinner's framework requires assigning probabilities across outcome ranges before selecting a response strategy.

- Ransom payment dilemma - a direct risk-tolerance trade-off (Hammond et al., Ch. 8): paying may restore access faster but carries legal, ethical, and recurrence risks; refusing may prolong downtime.
- Backup integrity - the viability of backups is the critical uncertainty node determining the entire decision tree. If backups are compromised, all recovery alternatives and their consequences change.
- Regulatory non-compliance - an objective conflict: rapid disclosure satisfies legal obligations but may accelerate reputational harm, requiring explicit trade-off analysis across stakeholder groups.

Framework Summary

Applying PrOACT shows that the problem is not merely technical recovery but selecting the path that best balances speed, cost, legal compliance, and stakeholder trust. Objectives conflict like should we do rapid restoration vs. forensic integrity; cost minimization vs. full disclosure.

No alternative is without consequence, and as Hammond et al. emphasize, leaders must

"confront uncertainty, judging the likelihood of different outcomes and assessing their possible impacts" rather than defaulting to intuition under pressure.

Business Impact Analysis (BIA) Summary

Where the risk assessment starts from the threat side, the BIA starts from the business-process side: it identifies which functions are critical to SolveTech's ongoing operations and quantifies the impact of their disruption (Snedaker, 2013, Ch. 5). Per the Business Continuity Institutes's four objectives, the goal is to understand what the most critical objectives is and the timeframes for their resumption, establish the maximum tolerable downtime (MTD) for each function, identify recovery resource requirements, and map internal/external dependencies (Snedaker, 2013).

Recovery timing is expressed using four standard measures: Maximum Tolerable Downtime (MTD), the longest function can be unavailable before serious harm occurs. Recovery Time Objective (RTO), the target time to bring systems back online. Work Recovery Time (WRT), the time needed after systems are restored to re-synchronize data and clear backlogs ($MTD = RTO + WRT$). Recovery Point Objective (RPO), the maximum tolerable data loss, driven by backup frequency (Snedaker, 2013, Ch. 5). Using basketball as an analogy. In basketball MTD is the shot clock. It is the absolute limit of time a business can function before the organization suffers. Just like in basketball, if a shot is not put up/turnover then the shot clock will be done letting the other team attack. RTO is a time out; this is the system recovery time and when the players can take a breather. It is the target time to assess what is going on, what can improve, what do we have to repair, and reconfigure the strategies. WRT is like the warmup for the players, just because a player is on the court does not mean they are 100% yet. WRT is the warm-up phase where players shoot around and get their rhythms back. RPO is the like when in 2018 MVP James Harden and how they played against him. Harden was so good from the step back three, but he was even better at drawing fouls. After 6 fouls a player cannot play anymore, so drawing fouls is

a strategy that can see success. Due to this play style teams were tasked with a huge defensive problem, how do you guard a person who is good at deep and close. Some teams had their players defend without their hands so they would not foul. Others played behind him so he could not step back. These teams would sacrifice a guarantee of 2 points in order to keep their players in the game, and for Harden not to get a 3.

Critical Business Functions and Dependencies

Business Function	Criticality Tier	Key Dependencies	Target RTO / RPO	Potential Loss if Disrupted
Client-facing production applications (SaaS hosting)	Tier 1 – Mission Critical	Cloud infrastructure, network/DNS, authentication services, on-call engineering staff	RTO $\leq$ 4 hrs RPO $\leq$ 1 hr	SLA penalty payouts; client contract termination; direct revenue loss (~150 staff idle)
Client data & databases (PII, records)	Tier 1 – Mission Critical	Database servers, encryption/key management, backup infrastructure	RTO $\leq$ 4 hrs RPO $\leq$ 1 hr	Regulatory fines (GDPR/CCPA); breach-notification costs; loss of client trust
Proprietary source code repositories	Tier 1 – Mission Critical	Version control system, offsite/offline backup copies, developer access	RTO $\leq$ 8 hrs RPO $\leq$ 24 hrs	Loss of IP; competitive disadvantage; project rebuild costs
Development & QA environments	Tier 2 – Vital	Source code repos, CI/CD pipeline, cloud compute	RTO $\leq$ 24 hrs RPO $\leq$ 24 hrs	Delayed releases; missed project deadlines
Billing & financial systems	Tier 2 – Vital	ERP/accounting software, banking interfaces, finance staff	RTO $\leq$ 48 hrs RPO $\leq$ 24 hrs	Delayed invoicing/collections; cash-flow disruption
Internal communication & collaboration (email, chat)	Tier 2 – Vital	Cloud email/collaboration provider, network access	RTO $\leq$ 24 hrs RPO $\leq$ 1 hr	Coordination breakdown across 150 staff and multiple locations

Business Function	Criticality Tier	Key Dependencies	Target RTO / RPO	Potential Loss if Disrupted
HR & payroll	Tier 3 – Non-Critical	Payroll processor, HR information system	RTO $\leq$ 5 days RPO $\leq$ 24 hrs	Employee dissatisfaction if payroll delayed beyond one cycle

Interdependency and Impact Observations

Tier 1 functions are tightly coupled, client-facing applications cannot be restored until the underlying databases are restored. Also, the source code integrity must be confirmed before redeployment. Restoring one function in isolation provides limited operational value (Snedaker, 2013). The BIA confirms that IT recovery priority should follow business criticality, no technical convenience. Tier 1 systems must be recovered first even if Tier 2 or Tier 3 systems are technically easier to restore. Because the ransomware event has already occurred, current backup RPO must be validated immediately: if the last clean backup predates the encryption event by more than the stated RPO target, data loss will exceed tolerance and work-recovery time (WRT) will extend substantially. Another note is that financial impact compounds daily: with all 150 employees affected, idle labor cost, SLA penalties, and incident-response/legal fees accrue continuously until Tier 1 functions are restored.

Risk Assessment and Mitigation Strategies

Risk assessment evaluates threat sources with the equation, Risk = Threat + (Likelihood + Vulnerability) + Impact (Snedaker, 2013, Ch 4). The ransomware event is a human caused, technology centered threat; the risks below are drawn from that source acting on the Tier 1/2 functions identified in the BIA above. Mitigation strategies are organized using Snedaker's four standard options. Which is acceptance, avoidance, limitation, and transferences and are all separated into preventive and post even actions (Snedaker, 2013, Ch. 6).

Primary Risks and Impact on Critical Functions

Risk	Likelihood	Impact on Critical Function (from BIA)	Mitigation Category
Encryption of production servers/databases	High (realized)	Client-facing apps and client data (Tier 1) fully unavailable	Limitation
Compromised or unavailable backups	Medium	Extends RTO/WRT for all Tier 1 functions; may force MTD breach	Limitation / Avoidance
Data exfiltration of client PII / source code	Medium-High	Client data and IP (Tier 1); triggers legal/regulatory exposure	Transference / Limitation
Downtime exceeding MTD for Tier 1 functions	High	SLA breaches, revenue loss, client churn	Limitation
Regulatory non-compliance (breach notification)	Medium	Client data function; legal/financial exposure	Transference

Risk	Likelihood	Impact on Critical Function (from BIA)	Mitigation Category
Ransom payment without adequate review	Medium	Financial and legal risk; no guarantee of recovery	Acceptance (of alternative cost) / Avoidance

Mitigations Strategies: Pre Event and Post Event

Pre Event:

- Offline/Air gapped backups for Tier 1 databases and source code repositories, which are tested regularly to validate their RPO (Snedaker, 2013, Ch. 6). This is a strategy that directly addresses the risk surrounding the backup's integrity.
- Network Segmentation, endpoint detection and response, least privilege access and to the extreme a Zero Trust policy, to reduce the vulnerability component of the risk equation.
- Cyber-insurance coverage and have a third party incident response, which shifts financial and expertise burden off SolveTech.
- A documented and tested incident response and BC/DR plan (with detailed MTD/RTO/RPO per function) and regular tabletop exercises, so that recovery sequences follow the BIA priority order under pressure rather than on the fly.

Post Event

- Contain and isolate the affected systems to prevent further spread.
- Activate the incident response team and engage outside forensics before deciding on anything drastic. For example, ransom, payment, restoration order.
- Verify that the backups are clean before restoration, Restoration from a compromised backup will reintroduce the threat and reset the recovery timeline.
- Restore the function in BIA priority order, Tier 1 first followed by Tier 2 and Tier 3.
- Conduct a post-incident review to update the risk assessment and BIA once operations are restored, closing the loop on any control gaps the event revealed.

Business Continuity and Recovery Plan (BC/DR)

With critical functions, dependencies and mitigation strategies already established through the BIA and risk assessment. This section will translate the analysis into an operational plan. It follows the plan-development structure in Snedaker (2013, Ch. 7): defining the phases of activation, recovery, and business continuity; assigning teams and key personnel; and sequencing the emergency response and IT recovery tasks needed to restore SolveTech's Tier 1 functions first (Snedaker, 2013, Ch. 8).

Plan Activation

Snedaker recommends defining three disruption levels, minor, intermediate and major (Snedaker 2013, Ch 7). This is in order for the response to be proportional to the event and does not activate the full plan for every glitch. A minor event is isolated to a single system or component, and normal operations continue largely uninterrupted. An intermediate even impacts one or more but not all mission critical functions. A major event disrupts all or most business operation because all or a majority of the systems have failed/are inaccessible (Snedaker, 2013, Ch. 7). The ransomware attack against SolveTech meets the major disruption definition to the tea. With the production databases, source code, and operational systems are all encrypted and the entire IT infrastructure is inaccessible, so full plan activation is appropriate rather than a wait-and-see approach.

Disruption Level	Definition	Trigger for SolveTech	Response
Minor	Single system/component affected; normal operations continue	Isolated workstation or non-critical service outage	Handled by IT team through normal operations; no plan activation
Intermediate	One or more, but not all, critical functions impacted	A single Tier 2/3 system (e.g., billing) down but Tier 1 unaffected	Partial plan activation; damage assessment and IT team engaged

Disruption Level	Definition	Trigger for SolveTech	Response
Major (this event)	All or most operations disrupted; majority of systems inaccessible	Tier 1 databases, source code, and client-facing apps all encrypted	Full plan activation; CMT convened; all BC/DR teams engaged

The SolveTech event is already a major disruption; the activation trigger is retroactive rather than predictive. The Crisis Management Team should formally declare the event and activate the plan the moment ransomware and when the system accessibility was taken were confirmed. This is better than waiting for a lengthier assessment window (Snedaker, 2013, Ch. 7).

BC/DR Teams and Key Personnel

It is better to define teams by role rather than by named individuals so the plan survives staff turnover and for smaller organizations one person may fill more than one role (Snedaker, 2013, Ch. 7). At 150 employees, SolveTech does not need every single team besides the core ones, scaled down to SolveTech size and cover the roles most relevant to a ransomware attack.

Team	Composition	Primary Responsibility
Crisis Management Team (CMT)	CEO/COO, IT Director, Legal counsel	Declares activation; has ultimate authority over restore order, the ransom decision, and disclosure timing (Snedaker, 2013, Ch. 7, 8)
Damage Assessment / IT Recovery Team	IT Director, systems/DB engineers, on-call staff	Scopes the encryption, verifies backup integrity, executes technical restoration in BIA priority order
Legal and Compliance	General counsel, outside privacy counsel	Determines GDPR/CCPA notification obligations and timelines; coordinates with law enforcement and forensics
Crisis Communications	Marketing/comms lead	Single point of contact for media and client-facing messaging; withholds cause statements until legal clears them (Snedaker, 2013, Ch. 8)
Human Resources	HR lead	Communicates with the 150 affected staff, manages idle-labor logistics, coordinates remote/alternate work
Administrative Support	Office manager	Vendor coordination, expense tracking, logistics for the duration of the response

Recovery Phase: Emergency Response and IT Recovery

The recovery phase begins once the immediate cause has been contained and covers the emergency response and technical restoration work. For SolveTech, this sequence builds on post event mitigation steps identified earlier in the report:

- Contain and isolate affected systems to stop further encryption or exfiltration and preserve evidence for forensics and any law-enforcement involvement.
- Convene the CMT and IT Recovery Team; notify Legal so breach-notification clocks and evidentiary requirements are tracked from the outset.
- Verify backup integrity before any restoration begins. Snedaker (2013, Ch. 8) stresses that restoring from a compromised backup reintroduces the threat and resets the recovery timeline, so this is a hard gate, not a formality, given that backup integrity was already flagged as the critical uncertainty node in the risk assessment above.

Once backups are confirmed clean, IT recovery proceeds in the same priority order established in the BIA, because restoring systems in whatever order is technically easiest, rather than by business criticality (Snedaker, 2103, Ch. 8)

- Network and infrastructure restoration first, since every other recovery task depends on connectivity being back in place.
- Tier 1 functions next: client databases and source code repositories are restored and integrity-checked before client-facing SaaS applications are brought back online, since the applications cannot serve clients on unverified data (Snedaker, 2013, Ch. 8). Tier 2 functions follow once Tier 1 is stable. Tier 3's are restored last.

Business Continuity Phase

The business continuity phase begins once the recovery work is done and addresses how SolveTech resumes normal operations rather than emergency operations (Snedaker, 2013, Ch. 7). In practice this means standing up clean cloud instances of client-facing applications from verified backups while the primary environment is rebuilt, using manual or reduced-functionality workarounds for Tier 2 systems such as billing, and re-synchronizing any data generated during the interim. Communications during this phase has to reach several audiences, each with a different message and legal tolerance:

- Employees: status updates through an alternate channel, since email and internal chat may themselves be down; guidance on remote work or alternate reporting locations.
- Clients: direct notification by contractual SLA terms and, where applicable, regulatory breach-notification deadlines (GDPR/CCPA).
- Media: a single designated spokesperson who does not speculate on cause until Legal has cleared the statement (Snedaker, 2013, Ch. 8).
- Regulators: formal notification within the applicable statutory window, coordinated by Legal and Compliance.

Maintenance and Review

Once operations have stabilized, SolveTech should conduct the post-incident review already identified in the mitigation strategy above, close any control gaps the event revealed, and update the risk assessment, BIA, and this plan accordingly (Snedaker, 2013, Ch. 7 and 10). The incident timeline, decisions, and recovery actions should be logged in an event log for legal, insurance, and audit purposes, and any change to systems made during recovery, such as a new cloud

configuration adopted as a permanent fix, should trigger a formal change-control review of the BC/DR plan itself (Snedaker, 2013, Ch. 7).

Implementation, Testing, and Training

There are four testing emthods that trade off disruption to the business against how accurately the test reflects a real event. SolveTech does not need to use all four at the same time, but it is best practice to go over it (Snedaker, 2013, Ch.9).

Method	What It Tests	Disruption / Accuracy	Recommended Frequency
Paper walk-through (tabletop)	Full plan, scenario-based discussion with CMT and team leads	Lowest disruption; lowest accuracy, but still the most commonly used and useful baseline (Snedaker, 2013, Ch. 9)	Annually, using the ransomware scenario as the primary walk-through
Functional exercise	A subset of the plan, e.g., restoring a database from off-site backup, using a scripted 2–3-hour scenario	Moderate disruption; higher accuracy than a walk-through	Semi-annually, rotating across Tier 1 functions
Field exercise	Realistic, hands-on scenario, e.g., isolating a compromised network segment	High disruption; high accuracy	As resources allow; optional given company size
Full interruption test	Activates the entire plan and alternate site for all mission-critical functions	Highest disruption; highest accuracy	Not practical company-wide; consider for one isolated Tier 1 system only

Snedaker (2013, Ch. 9) also notes that regulators generally allow documented recovery from an actual incident to satisfy a testing requirement. SolveTech should formally document the recovery from this ransomware event, what worked, what didn't, and how long each phase actually took, and use it in place of a scheduled test for this cycle, feeding the findings directly back into the plan and the training program below.

Training Program

Training starts with a needs assessment, a gap analysis between the skills a role requires under the plan and the skills that role currently has (Snedaker, 2013, Ch. 9). For SolveTech, this means confirming that IT engineers can actually execute an off-site backup restoration under the written procedure, that Legal knows the breach-notification deadlines, and that CMT members know how to declare and communicate activation without hesitating over authority.

Training itself should have clear, measurable outcomes rather than general awareness goals, for instance, "an on-call engineer can restore the Tier 1 client database from the offline backup within the 4-hour RTO using the written procedure" which either happens or it doesn't (Snedaker, 2013, Ch. 9). Given SolveTech's 150 employees across multiple locations, delivery should combine a short online awareness module for all staff (what the plan is, who to contact, where to find status updates) with live or virtual tabletop sessions for the CMT, IT Recovery Team, Legal, and Communications leads, since those roles need hands-on rehearsal rather than passive awareness.

Monitoring should track two things on an ongoing basis: whether the required staff actually completed training, and whether personnel changes have left a role uncovered. Both the testing schedule and the training program should run on the same cycle so that gaps found in a walk-through or functional exercise feed directly into the next round of training, closing the loop between the BIA, the risk assessment, the plan itself, and the people who have to execute it.

References

Hammond, J. S., Keeney, R. L., & Raiffa, H. (1999/2015). Smart choices: A practical guide to making better decisions. HBR Press.

Skinner, D. C. (2009). Introduction to decision analysis (3rd ed.). Probabilistic Publishing.

Snedaker, S. (2013). Business continuity and disaster recovery planning for IT professionals (2nd ed.). Syngress.