Incident Recovery Plan

TEMPLATE

For Business: ______________________________

Introduction

Purpose & Scope

The purpose of this document to have a single source of truth for the business when managing cyber incidents that cause service outages or impact the business operation. It will help to coordinate responses and efforts of teams across the business.

The intended audience for this document includes leadership, managers, technical SMEs, and IT admins. All members of the team can use this as a reference during an incident so the business will be aligned for response.

Goals of this document include:

- Role clarity and who to notify within the team
- Response plan for incidents
- Documents and backups prepared for incidents
- Assessing situation regarding incidents
- Prioritization of response activities
- Which individuals to notify about incidents
- Lessons learned for future incidents
- Support recovery of the business operations to completion
- Limit potential damages to the business

This is a living document and needs to be reviewed and updated regularly. The document is an amalgamation of multiple standards (including CIS, NIST), industry best practices, and experience from supporting organizations through incident recovery.

Authorization

Incident Recovery Plan is endorsed by the [CEO] and managed by [IT Director] who is responsible for ensuring that [Organization] has a dependable and tested program

Review

The Incident Recovery plan is reviewed [monthly, quarterly, or annually] cadence [annually/quarterly/monthly] to ensure the organization is prepared to respond to cyber incidents.

Review Date	Reviewed By	Changes

Recovery Objectives

The following are priority for recovery objectives:

- An organized approach to responding to cyber incidents
- Reduce the downtime of the business operation and limit the impact
- Selecting the right response path to unplanned incidents and reduce errors caused by not planning and making in the moment decisions
- Ensuring the legal requirements of privacy regulations and contracts are met during a cyber incident
- The internal and external stakeholders are properly notified in the correct manner, this includes partners, customers, investors
- Reduce financial loss through taking the correct steps
- To reduce the potential of a reinfection by assessing the probability and making informed decisions based on risk

Additional objectives specific to the organization:

Incident Assumptions

This document primarily focuses on handling and recovery of severe cyber incident(s), it is assumed there is a certain level of business interruption and impact to the core functioning of the organization.
This would include a partial or complete loss of access to systems/servers/data and scenarios listed below.

The list of outages that the business is concerned about are as follows:

- Loss of access to the networks (internet, local network)
- Loss of data (files are encrypted, deleted, modified, missing)
- Loss of systems or services (servers or services are offline or not functioning)
- Loss of VOIP (phone lines are down)

Additionally, we have incidents that are excluded from this document:

- Minor cyber incidents such as a phishing email that was not clicked

Parts of this incident recovery plan can be used for minor cyber incidents and some other events, choosing which parts will be left to your discretion.

Confidentiality

It is the responsibility of all employees and contractors to keep all information recorded herein confidential.

Cyber Incidents

Event List

In this section we compile a list of events that are cyber incidents the team needs to be aware of. These will need to be maintained as the cyber landscape continues to change.

- virus or malware found on a hard drive
- unauthorized access to a system
- antivirus or EDR has been disabled by a bad actor
- Denial of Service (DoS) attack that affects service availability
- data is compromised (sensitive, confidential)
- email accounts are compromised
- Network(s) are compromised
- servers are compromised

What are severe impact cyber incidents for your organization?

Multiple days to recover critical servers and data. The entire organization will be impacted by these events

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.

What are medium impact cyber incidents for your organization?

1-2 days to recover workstations, servers, some data. Some of the organization might feel the impacts of these events, it will be compacted into certain areas but not affect all

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.

What are low cyber incidents to your organization?

The business won't feel the impact of these events, only a couple employees might be impacted

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.

Roles and responsibilities

Organization Role Assignment List

Role	Responsibilities	Team	Assigned To	Contact Info
Security Manager	Management role to manage the team of analysts, Gauge the business impact and severity, Notify IMT if necessary and relay the findings	DMT		
Security Analyst	Investigate digital forensics, Write a rapid report on the findings that could be sent to Security Manager, IMT and SET.	DMT		
Incident Commander	Leads the entire engagement, when to switch between phases, priority, the incident commander will take on all of the responsibility for ensuring the incident management and recovery is handled properly, and efficiently. During a severe incident the Incident Commander communicates directly with the Senior Executive Team (SET) and the CEO/President.	IMT		
Backup and Recovery Manager	Planning and operations of all backups, agents, backup servers, backup storage, and recovery. Provide Technical Advice	IMT		
Investigation Manager	Planning and operations, Provide Technical Advice	IMT		

Backup and Recovery Operations		IMT		
Investigation Operations		IMT		
Digital Forensics	Recovery, investigation, examination, and analysis of material found in digital devices	IMT		
Communications and Reputation	Handling internal communications, client communications, vendor discussions, and handling public relations (communicating with stakeholders)	IMT		
Decision Makers	Primary, Secondary, and Tertiary decision makers that will provide guidance in an incident	SET	Primary: 1. 2. Secondary: 1. 2. Tertiary: 1. 2.	
Legal Counsel	Internal or outsourced	SET		
Emergency budgeting and expenses	Typically, CFO or Finance	SET		
Staff Welfare	Ensure staff are taken care of during cyber incident (Meals, drinks, sleep, exercise)	SET – Human Resources		
Insurance Broker	Emergency contact information	Partners		

Cyber Incident Recovery Preparation

Based on the input from various sections of the program, this needs to be filled out prior to an incident.

Recovery Preparation List

1. **[Assets]** Inventory all the assets - servers, workstations, laptops, mobile devices, data (sensitive, confidential, corporate/client), on-prem/cloud, networking equipment, miscellaneous
2. **[Backups]** Inventory what is being backed up - record all of the assets being backed up, include the date backups where verified, the date recovery was tested on that asset group, if something is not being backed up, include a reason why, and the name of the technician who did these checks, and the manager who signed off on each line item. Include the name of the backup software being used and the backup strategy, backup schedule, backup retention, backup locations.
3. **[Configurations]** Inventory configuration files - these are backups of the network configurations, and other configuration files that can help recover the good configuration of a device or service quickly. (Cisco routers/switches, WIFI, software services configurations)
4. **[Diagrams]** Inventory the architecture diagrams (on-prem and cloud infrastructure / system design), network diagrams (subnets, VLAN, ports, protocols), data and backup architecture, security documentation (security tooling and security architecture decisions, GPO's, security policies, compliance frameworks)
5. **[Compliance]** Inventory the compliance and regulation requirements and reports - include any documentation that is relevant to maintaining compliance with each required privacy regulation
6. **[Contacts]** Inventory of staff, management and executives including contact information - at a minimum the department leads and managers for a larger organization so each department can be reached. Include personal phone number / email address, corporate email address so staff can be reached outside of regular work hours for emergencies.
7. **[Store the Inventory]** Cloud or offline storage of the inventoried documents and information so they are readily accessible during a severe cyber incident
8. **[Secure Communication Checklist]** Secure communications procedure and checklist

For each of the items above we go into detail below.

Assets

Inventory all assets in your organization in this section including servers, virtual machines, workstations/Laptops, mobile devices, networking equipment, cloud and data assets (sensitive, confidential, corporate/financial/accounting, client data).

When an item in these asset tables changes, the table entry must be updated. If an employee leaves and hands in their laptop during off-boarding, the owner field should be cleared and replaced with "extra" or "backup". The assets will still exist for the organization, but the assets list will identify it has not been in use. If the asset is used, the asset table must be updated to reflect the owner of the device, the employee or contractor using the device. These tables can be updated to reflect check-out dates, to retain an audit trail if necessary, but the objective of the cyber incident recovery plan, this document must track all of the organization assets, their current locations, the ip addresses if applicable to communicate with the devices or analyze security even logs post-mortem. Your team can add additional fields to these tables for added capability.

Servers

Asset	Date Checked In	Owner	Location	Hardware	IP Address
Van-ESXi-01.org.local	Aug 2020	IT Team	Van Office	Dell R750	10.10.10.10
Bur-ESXi-02.org.local	Aug 2020	IT Team	Burnaby Office	Dell R750	10.20.20.20

Virtual Machines

Asset	Date Checked In	Owner	Location	IP Address
Van-DC01.org.local	Sept 2020	IT Team	Van-ESXi-01.org.local	10.10.100.100
Van-DC02.org.local	Sept 2020	IT Team	Bur-ESXi-02.org.local	10.20.200.200

Workstations / Laptops

Asset	Date Checked In	Owner	Location	Hardware
Lap-05.org.local	June 2020	Judy E.	Van Office	Dell XPS13
Lap-08.org.local	July 2020	Jason E.	Burnaby Office	Lenovo X1 Carbon

Mobile Devices

Asset	Date Checked In	Owner	Location	Hardware
Cell #10	June 2020	Judy E.	Van Office	iPhone 12
Tablet #09	July 2020	Jason E.	Burnaby Office	iPad Mini 4

Network Equipment

Asset	Date Checked In	Owner	Location	Hardware
Van-Firewall01	July 2020	IT Team	Van Office	Cisco ASA5525
Van-Switch01	July 2020	IT Team	Van Office	Cisco WS-C3850

Cloud

Asset	Date Checked In	Owner	Location	IP Address
Corp.s3bucket.aws.amazon.com	Sept 2020	Dev Team1	AWS US-East	50.252.25.25
Corp.ec2.us-east.aws.amazon.com	Sept 2020	Dev Team1	AWS US-East	50.252.30.30

Data

Asset	Date Checked In	Owner	Location	IP Address	Classification
postgres.org.local	Sept 2020	Dev Team1	AWS US-East	50.252.25.25	Sensitive Client Data
MySqlDB.rds.us-east.aws.amazon.com	Sept 2020	Dev Team1	AWS US-East	50.252.30.30	Classified Financial Database (Corporate)

Backups

Inventory all the assets being backed up. Maintain records of the assets being backed up, include the date when the backups where verified, the date recovery was tested on that asset group, if something is not being backed up, include a reason why, and the name of the technician who did these checks, and the manager who signed off on each line item. Include the name of the backup software being used and the backup strategy, backup schedule, backup retention, backup locations.

Asset	**Backup Software**	**Backup Locations (Primary Data, Offsite/Cloud, Replication)**	**Verification Date**	**Verifier Name**	**Manager Sign Off**	**Backup Schedule**	**Backup Strategy**	**Backup Retention**	**RPO / RTO**
Van-DC01.org.local	Veeam	Veeam Repo (On Prem), Veeam Cloud, Veeam Cloud Replication	June 12 2022	Mark D.	Jane D.	GFS (Bi-Monthly, Weekly, Daily)	3-2-2 (OnPrem, Cloud, Cloud)	12 Months	RPO = 24-48 Hours RTO = 4-24 Hours

Configurations

Inventory configuration files - these are backups of the network configurations, and other configuration files that can help recover the good configuration of a device or service quickly. (Cisco routers/switches, WIFI, software services configurations)

Asset	Location	Owner	Date
Van-Switch01.org.local	https://securestorage /.../van-switch01.txt	IT Team	June 20, 2021

Diagrams

Inventory the architecture diagrams (including on-prem and cloud infrastructure, system design), network diagrams (including subnets, vlans, ports, protocols), data and backup architecture, security documentation (including security tooling and security architecture decisions, GPO's, security policies, compliance frameworks)

Asset	Location	Owner	Date
Van Office Infrastructure Diagrams	https://securestorage /.../van-office-infras.drawio	IT Team	October 10, 2021
AWS Cloud Infrastructure (US-East)	https://securestorage /.../aws-infras-r&d.drawio	IT Team	October 11, 2021

Compliance

Inventory the compliance and regulation requirements and reports - include any documentation that is relevant to maintaining compliance with each required privacy regulation

Asset	Location	Owner	Date
CIS for AWS	https://securestorage /.../org-CIS-for-AWS.docx	IT Team	October 14, 2021
Sox2	https://securestorage /.../org-sox2.docx	IT Team	October 18, 2021

Contacts

Inventory of staff, management and executives including contact information - at a minimum the department leads and managers for a larger organization so each department can be reached. Include personal phone number / email address, corporate email address so staff can be reached outside of regular work hours for emergencies.

Corporate Contact List

Name	Title	Email (Work / Personal)	Phone (Work / Personal)
Jane D.	CEO	jane.d@org.com / jane.d@gmail.com	555-555-5525 / 555-555-5526

Corporate Services

Name	Description	Email (Work / Personal)	Phone (Work / Personal)
Law Firm			
Insurance			
Cyber Security			
Brand / Reputation			
Notifications / Communications			

Vendors

Name	Description	Email (Work / Personal)	Phone (Work / Personal)
Server Hardware			
Network			
Cloud			

Inventory Storage

Cloud or offline storage of the inventoried documents and information so they are readily accessible during a severe cyber incident. This is the location of this document and any relevant documentation.

Asset	Location	Owner	Date
IRP Document Bundle	https://securestorage /.../irp-bundle.zip	IT Team	October 02, 2022
IRP Document Bundle Backup	https://securebackup/.../irp-bundle.zip	IT Team	October 02, 2022

Secure Communication List

This is the process of handling secure and encrypted communications with internal and external parties during a cyber incident.

Informing stakeholders that a cyber incident has taken place, discussing the severity of the incident and working on the incident all require proper communication channels. Communications depend on pre-planning of roles and responsibilities, but also the information required to reach each stakeholder and employee if the entire infrastructure is inaccessible (emails, work phones, etc.)

1. **Invites:** Only have a few dedicated admins for the Signal group, do not grant every member the ability to invite users. This might seem quicker but if the wrong person is invited, all your conversations and information shared through the Signal group are no longer safe.
2. **Last Minute Invites:** Have the admin of the Signal group invite only trusted phone numbers, if there is a request to add additional phone numbers to the group chat then call or facetime to ensure it is the correct employee and not an adversary trying to infiltrate the safe and encrypted group chat.
3. **Privileged:** Invite your lawyer into the chat for privileged conversations. The lawyer needs to be invited before the chat begins to retain privilege. This lawyer should be your corporation's independent lawyer, not the lawyer provided to you by an insurance company, the insurance lawyer should not be invited into these secure communications channels.

Chat App	Group	Members	Purpose
Signal	Incident Management Team (IMT)	John D. Mike E.	Discuss discovery and response efforts
Signal	Senior Executive Team (SET)	Jane D. Lucy M.	Discuss business decisions, financial, budget, resourcing

Incident Response Actions List

1. **[Detection]** Identify if an incident has occurred or is occurring - what are common detection methodologies. precursors (current news, threats toward the company - they are rare), indicators / monitoring (EDR or event/security logs), accidental (too late, saw a ransomware note once files are encrypted, data was leaked, contacted by a hacker that they have access to your network). tools that can help identify adversaries like EDR solutions. can include unusual or suspicious activity.
2. **[Analysis]** Identify the scope, impact and severity of the incident and classify it. Review logs and security alerts to identify suspicious behaviour.
   Standard Operating Procedures (SOP) for reviewing different systems, services, devices for intrusion (Windows/Linux/Network Equipment/Active Directory/Email/SaaS Products/Data and Files). Consult with knowledgeable experts if needed (can the unusual or suspicious activity or files be explained as legitimate or does it lead your team to believe an intrusion has taken place).
   Research the potential intrusion, security alerts, log files, file names, or system/network activity that seems suspicious (IP addresses, files, etc), look through search engines, security alert platforms for indicators of compromise (AlienVault open threat exchange), upload and check suspicious files or scripts on virus total (if it is not confidential or personal or private data). Google scripts names, or functionality or even variable names to identify if they are used in adversary Tactics Techniques and Procedures (PowerShell, bash, python, etc.).
   CAUTION - if there is a suspicious IP address do not try to connect to it directly. If it is a server own by an adversary it could alert them to your awareness of their presence on the network (that could force them to deploy ransomware immediately, etc).
3. **[Classification]** Now with the knowledge at hand classify the intrusion or cyber incident and rate it on a severity level. We gauge cyber incidents by severity levels that has a matrix of impact
   a. from no reduced function to critical function impacted,
   b. data from none to personal/sensitive or classified/proprietary data,
   c. reputation impact from negligible to severe,
   d. and financial costs from negligible to severe.

   This matrix can be used to classify the potential impact of the cyber incident at this time.
4. **[Contact IT and Executive Teams]** Contact the incident team and depending on the severity and classification, inform the senior executive team if needed. The senior executive team should be contacted if there is a severe cyber incident or one that could have a business impact. Minor cyber incidents like finding a virus on a computer might not be serious enough to alert the entire incident team or senior executive team.
5. **[Contact Internal Stakeholders]** Contact internal stakeholders that could be impacted by the cyber incident - send out notifications, call the mangers/leads. At this point only internal stakeholders should be contacted as part of the communication and discovery phase. This conversation should also seek to obtain information from stakeholders on suspicious activity or unusual changes to their systems, computers, services, files, data, because it is possible their departments have also been breached but they may not be certain so they may not have mentioned any unusual or suspicious activity yet.
   CAUTION – Before any outside correspondence occurs your legal counsel should be contacted.
6. **[Documentation]** Document everything discovered up until this point and continue documenting throughout the entire process. The documentation should include each of the previous steps include who was contacted or notified, retain records of what was sent. At this point only internal communication and notifications, nobody outside of the company (except stakeholder contractors) should be notified.
   Insurance can cover services like reputation and brand repair, but also communications services for your clients, partners, investors - to ensure they are handled appropriately, and your business is not damaged. Those notifications could have a 24-72 hour timeline depending on your privacy regulation requirements or contracts, so they don't need to be notified in a hurry, the communication messaging can be sent out when more information has been gathered and worded with the help of a professional service.

For Severe Cyber Attacks

1. **[Legal]** Contact the organizations legal counsel and seek legal advice - list of things to obtain legal counsel for instance how to make an insurance claim, regulatory authority notification, when to contact impacted third parties such as partnerships, customers, vendors, and to check on any contractual obligations.
2. **[Insurance]** Contact the insurer following the advice of the legal counsel on making the claim - ideally, they will provide the green light to use one of their panel vendors for cyber security investigation immediately or to receive written authorization to hire your own that has been previously approved by them. They should also have a list of other services you can start using immediately.
3. **[Police / Gov Agency (FBI, CSIS)]** You may be asked to contact the police or an agency to disclose a breach has occurred, this is usually for more severe incidents. You will want to take your lawyers advice on what information to provide, and if you should contact them. The insurer may also have requirements on complying with the police or government agencies like the FBI or CSIS, ensure that you are well informed of the requirements and legalities prior to contacting any of them. Your lawyer might recommend they call on your behalf and provide certain information. This step is incredibly important to take your lawyers advice on because the police do not work for your business, and any information that is released to them is not considered privileged, it becomes part of a case file and can be later used against your business in a lawsuit by a third party. Follow your lawyer's advice on disclosure.
4. **[Cyber Security Team]** Contact the cyber security team that will provide the investigation and digital forensics - confirm that they begin work immediately and that they are aware you are waiting for the systems and servers to recover your business operation.
5. **[External Notifications]** Identify the stakeholders affected by the incident and prepare communications notices to inform them - this might be done by a communications service provided by the insurer. Ensure that your legal counsel over sees the communication notifications and verifies every notice that is sent outside of the company. You will want your independent legal counsel to review it, as well as any lawyer that has been provided to you by the insurer. The messaging in these notices is incredibly important to get right and could protect you from further reputation damage, fines or law suits.
6. **[Check Backups]** With the other teams in full swing, your IT team will need to check the backup systems as some of them may have been affected by the incident. Verify if local backups are available for recovery, or begin the download process for the cloud backups, as that could take some time to complete.
7. **[Catch and Release]** Communicate with the cyber security team to identify which systems are safe to go through the recovery process - they will release selected systems intermittently to your IT staff that can be recovered. Be sure to speak with your cyber security team and make sure they know you are waiting for them to release each system back to you as they finish with them, so they can be recovered. Ensure that the cyber security team is aware that you will be wiping every system that they return to you, unless you get a stamp of approval from them that there is no chance of a compromise on a specific system.
8. **[Safe Network]** Build the green zone network to house the recovered systems and services - If the cyber incident is severe enough to require this
9. **[Recovery Priority]** Determine the priority of the recovery - You will want to prioritize the core business functionality first, to regain minimal business operation. This list of servers and services need to be recovered first in order to start functioning as a business again.
10. **[Recovery Process]** Work through the incident recovery process to eradicate malware and compromised systems and services and recover them in the green zone network- This is going to be your IT staff working with the cyber security team,
11. **[IMT Disengage]** Disengage the senior executive team and the incident management team when the recovery requirements have been met and the business is operational
12. **[Review]** Post incident review - what worked, what didn't and document
13. **[Update]** Update the incident recovery plan

Detection

Identify if an incident has occurred or is in the process of occurring using common detection methodologies.

#	Item	Description	Response
1	Time and Date	Of the first detection	
2	Contact	Who identified it	
3	Type of Incident	Is this an attack indication like malware attack, phishing attack, ransomware attack? Or is this a precursor to an attack like EDR agent disabled, or multiple user account locked up?	
4	Details of Incident	Details about what happened? Include: filenames, scripts, malware, ransomware note, email.	
5	How was the incident detected?	Explain how the incident was detected.	
6	System or Device	What is the name and IP of the system or device the incident was detected on. (If multiple, include them all)	
7	System / Device location?	Is it on-prem in an office or Wearhouse, or off-prem at a datacenter or the Cloud?	

Analysis

The digital forensics and investigation will be performed by an authorized investigator (this could be an IT administrator, cyber security team member, or a member of the CSIRT team). They will use forensic techniques like reviewing system and event logs, EDR alerts and logs, reviewing files and scripts found on the system, looking through emails their headers and attachments. In addition, the investigator will interview witnesses and the targeted persons or employees to discover useful information about the incident. The questions that need to be answered are what happened, how it happened, why it happened, who did it, and what does it effect?

Primary Analyses Checklist

#	Item	Description	Response
1	System Criticality	Is the system or service affected used for a critical business function? (Can the business operate without this system or service?)	

2	What is the severity of the impact to the system?	Can the system(s) continue to function, does it have to be taken offline and for how long?	
3	What is the estimated impact to the business	Explain which parts of the business could be affected by this incident. (exclude financial or resourcing here)	
4	Digital Forensics	Will digital forensics and investigation be conducted on the system or service?	
5	DFIR Responder	Who is providing the digital forensics and investigation for this incident?	
6	Time spent on investigation	This is the initial investigation time; it could be 15 minutes or an hour to gather relevant pieces of information and conduct the interviews with the employees	

System/Service Checklist (Copy this table for every system/service/device)

#	Item	Description	Response
1	System / Service Details	Include name of the system, operating system, version and patch number if applicable, IP address, & location	
2	Incident Information	Include any relevant incident details for this specific system/service. Include the date and time	
3	Origin information	Include the origin IP address or domain, and any additional information on the origin of the attack. This could be an email that was sent (back up the email, retain the headers and attachment), or a file or script that was located on device (make a copy).	
4	Entry Point	What is the initial entry point into this system/service/device?	
5	Should the device be powered down immediately?	Is this believed to be a critical attack on the system, should the system be powered off immediately and left for the cyber security team to conduct digital forensics?	

Digital Forensics

#	Item	Description	Response
1	Is the incident real?	During the initial investigation does the incident appear to be real?	
2	Is the incident in progress?	During the investigation does the incident appear to have completed or is the attack still in progress? (Is it attempting to spread to other systems?)	
3	Other risks	What other systems / services and data are at risk? (Describe the risk to other systems/services and if they should be investigated)	
4	What type of impact could this attack have on the business?	Explain in more detail as the investigation is conducted what impact this incident could have on the business and its operations	
5	Is the incident inside of the local network?	Is there reason to believe the incident has provided access to an adversary inside of your trusted networks? (Explain in detail how and why)	
6	Does the response need to be escalated?	Does the Incident Management Team (IMT) need to be activated? And does this team believe a cyber security team should be contacted for digital forensics and investigation?	
7	Can this incident be contained?	Can this incident be easily and quickly contained? (Wipe and recover the system or service – remember to preserve all evidence if doing this)	
8	Will response to this incident alert an adversary?	Is it a C2 agent, or a backdoor that was found, that if removed could alert the intruder?	
9	Initial Foothold	What is the initial foothold of this cyber incident? This is the first place the attackers gained access inside of your environment before spreading out to the remainder.	

Severity Classification

The severity of the attack will need to be defined when creating a support ticket and reporting the incident to management. The severity levels are a measurement of impact an incident has on the business. In this section, define your company's response to different severity incidents.

Severity is not a prioritization but based on the current impact of an incident. The severity level will be adjusted according to the current situation and not the estimated situation.

[Include the date and time, and the reason the severity number was chosen for this incident.]

Severity	Description	Examples	Response
1	A critical incident with a very high business impact	Customer data loss, security breach, client facing service is offline. A critical business system or service is not functioning (The business cannot operate without it). This will affect SLA.	
2	A major incident with significant impact	A business system or service is partially functioning and only effecting a subset of operations (The business can somewhat operate). This will affect some SLA.	
3	A minor incident with low impact	All critical business systems and services are functioning but there is an inconvenience caused. This will not directly affect SLA but could be annoying for the business operation or customers.	
4	A support request that is irritating a customer	This could be a bug, a connectivity issue.	

(*These severity descriptions are referenced from and aligned with Atlassian)

Contact IMT and Senior Executive Teams

SEV-1 or SEV-2 classified incidents should activate the IMT. SEV-3 incidents may not need to activate the IMT.

Internal Stakeholders Notifications

The only time external parties are to be notified is after senior executives authorize it, and legal counsel has provided guidance on notifying those contacts.

#	Item	Description	Response
1	Critical business function recovery priority	Acceptable downtime for critical business systems: 2 hours, 4 hours, 8 hours, 12 hours, 24 hours, or more. (Include the critical business systems that need to be recovered, the acceptable downtime, and the teams that are working on fixing it, and their priorities for fixing critical systems in which order.	
2	Do not use ….	List all of the systems and services the staff needs to stop using. If systems have to be powered down ensure that communications are clear, and that the staff responds back to you when the system or service is powered down. Include the staff members name, date and time of communication, date and time of powering down confirmation, and the reason that it was powered down.	
3	Encrypted Communications	For a severe breach, let the teams know through private channels (Personal mobile phones, personal emails, do not use corporate emails for these communications. (In the response mark it as Yes all notifications where done through encrypted channels in private, or No – all notifications where sent through corporate email/chat/phones).	

What to Document

The team should document everything that has been discovered up until this point and continue documenting throughout the remainder of the process. In addition to the discovery and analysis the following should be documented as well.

#	Item	Description	Response
1	Dates and Times	Retain dates and times of all communications and notifications	
2	Internal stakeholder notifications	Names/Emails of stakeholders who received notifications of the incident	
3	Retain copies of notifications sent	What information was provided to each stakeholder?	
4	IMT	Was the Incident Management Team (IMT) activated or engaged? (Who contacted the IMT, and which members of the IMT where contacted, and did the IMT respond?)	
5	SET	Was the Senior Executive Team (SET) activated or engaged? (Who contacted the SET, and which members of the SET where contacted, and did the SET respond?)	
6	Duration of the incident	When did the incident begin, and when did it end. (This is the time that hacking has stopped. This includes automated scripts or malware left behind by the adversaries, when did the incident end. This does not include your recovery time)	
7	Duration of response and discovery	How long did the response and discovery take? (Include the resources used, and the efforts in hours for each team member, include their names and their effort provided to the response and discovery)	
8	Duration of recovery	How long did the recovery take? Include the systems/services, and how they where recovered (which backups, and what backup date was used, location of the backups used)	
9	MISC	What additional resources or efforts went into response/discovery/recovery? Describe in details additional resources, unforeseen circumstances and scenarios	
10	Areas of the business that where impacted?	Which areas of the business where impacted, and on a scale of 1-10 for each one on severity. Include production, marketing/sales, services, client facing services, manufacturing?	

11	Special business issues?	Things that could arise from this incident that are special to your business. This could be lost contracts that where about to close / onboarding new staff, partnerships that where effected, etc.	
12	List of assets that are compromised	Retain a list of assets that where compromised, the date and time, what affected them, how they where compromised, filenames or scripts, and any point of entry.	
13	List of assets presumed to be compromised	List of assets that could potentially be compromised. What your team believed could have happened and why, retain all of the evidence as listed in the analysis and discovery tables.	
14	List of equipment that is available to build a new infrastructure	In the scenario of a critical breach or SEV-1 or serious SEV-2 that requires a green zone network, what equipment is available to build the new infrastructure with? List all of the hardware here.	

Check Backups

Are any of the backups functioning or not functioning? Make a list....

#	Item	Description	Response
1	Available Backups	Check if any of the backups have been affected by the breach. Make a list of the backups that are available	
2	Unavailable Backups	Make a list of the backups that are not functioning. Include the software tool, the storage location or repository that are not available.	
3	Test the backups	Have an IT member test the backups from different locations. Make a list and verify the backups that work. (This could be 1 image per backup location)	
4			
5			
6			

SEV-1 / SEV-2 Cyber Incident or Breach

The following sections are for severe cyber incidents or breaches. This will involve the senior executive team, legal counsel, regulatory authorities, insurance, police, cyber security team, external notifications to customers and partners and more advanced recovery efforts.

Legal

Contact your corporate legal counsel and seek legal advice on the incident and breach. Have the earlier sections of this document filled out and on hand when discussing the specifics.

(Discuss the following and obtain advice from your legal counsel. The senior executive team should be having these conversations, your technical management/staff may be included to relay the analysis and discovery details of the breach)

#	Item	Description	Response
1	Regulatory Authority Commissioners	Discuss which regulatory authorities your organization is required to comply with, discuss what types of data and data sources have been breached and are potentially breached. If there is reason to believe they exfiltrated the data and holding it at ransom.	
2	Business Contracts, Customers, Partners and Board Members.	Discuss if the cyber incident is severe enough or impactful to your contracts, customers and/or partners and which ones are required to be notified. Discuss if the board members should be involved and what information should be communicated to the board. Ensure your Senior Executive Team knows what information to relay to each one of them, discuss this with the legal counsel.	
3	Insurance Claim	Discuss what type of information to put	

		together for the insurance claim, and what details will be communicated to the insurance at this time.	
4	Policy / Federal Agencies	Discuss if the cyber incident should be reported to the police or a federal agency.	
5	Ransomware	Discuss if a ransomware attack took place, the name of the group, and the known details of the incident. Discuss with your legal counsel the ransomware extortion fees.	

Cyber Security Team

Contact the cyber security team that will provide the investigation and digital forensic services. Ensure they begin working immediately on the highest priority systems/services and that they are aware you are waiting for those systems/services to recover the business operations.
(Ensure the cyber security company signs an NDA with your company, to retain all of this information confidential. You will want to include your lawyer in all communications with them for privilege, and include the lawyer in all reports, attachments, and file/information sharing as well)

#	Item	Description	Response
1	Contact time and date	The time and date the cyber security team is contacted, include who you spoke with, the names of the individuals that will be working on your incident, their expected start time. Include full names of all individuals at the cyber security company (salesperson, project manager, technical team lead, and technical team members)	
2	Start time and date	What time did they start, include full names and contact information for their staff. Did any of the team members change from the first contact conversation?	
3	Priority	Ensure the system/service priority list is shared with the cyber security team	

		to complete the critical business functioning systems/services first, so your IT staff can recover them.	
4	Communication	Plan out your communication touch points with the cyber security team. EXAMPLE: For the first X hours, you will have a touch point with their PM for 10 minutes once per hour, and after that 10-minute touch point every 3 hours. And in addition to that you will have a major touch point once every 3 hours to update about the findings, which will replace the 10-minute meeting for that hour.	
5	Data Recovery	If your IT staff cannot recover certain data from backups, or the cloud, or the replication and need to recover data from an infected device, this needs to be communicated to the Cyber Security Team early on. Let them know which devices you need the data recovered from and cleaned.	

External Stakeholder Notifications

In the legal step above, your Senior Executive Team along with your legal counsel will identify which external stakeholders are required to be contacted, but you may also decide which of them as a precaution should be contacted anyway. Especially when dealing with certain types of contracts, or data privacy regulations, it could be on the side of caution to include specific stakeholders in the external notifications.

This is the time to contact and notify those external parties.

[External Stakeholders Contact List]

#	Name	Contact Information	Description

Catch and Release

Communicate with the cyber security team to identify which systems are safe to go through the recovery process - they will release selected systems intermittently to your IT staff that can be recovered. Be sure to speak with your cyber security team and make sure they know you are waiting for them to release each system back to you as they finish with them, so they can be recovered. Ensure that the cyber security team has retained evidence and is aware that you will be wiping every system that they return to you, unless you get a stamp of approval from them that there is no chance of a compromise on a specific system.

Maintain a list of all servers/services that have been approved by the cyber security team and record the name of the security member that authorizes each one.

Item	Description (IP Address, Hardware, Purpose)	Critical?	Date	Authorized By

Create the Green Zone Network

If the cyber incident is severe enough to warrant the use of a green zone network, build it now. Record the type of hardware available, a description of what it is used for, and the location of where it is stored.

This could be a list of additional network equipment, servers and laptops for the IT Admins that are clean and waiting to be used to recover the business operation.

[A list of available hardware for the green zone network]

Hardware	Description	Location
Cisco Router		Vancouver Office
Cisco Switch		Vancouver Office
Dell R750 server		Burnaby Office

Recovery Priority

Define the priority of the recovery and prioritize the core business functionality first, to regain minimal business operation. This list of servers and services need to be recovered first to start functioning as a business again.

The critical level is on a scale of 1-10, where 10 is extremely important for the business to function.

#	Item	Description	Critical Level	Response
1	Active Directory #1	The primary domain controller for the business	10	
2	Exchange / O365	The email server / services	10	
3	Sharepoint	File Share	6	

Wrapping it up

IMT Disengage

When the incident recovery is concluded, disengage the Senior Executive Team and the Incident Management Team when the recovery requirements have been met and the business is operational.

Review & Retrospective

Review the entire process your organization just experience, reflect on the wins, and losses of the incident recovery and the lessons learned. Have each member record their perspectives and comments and bring the entire team together for a retrospective meeting. Share your thoughts and ideas on improvements with one another to ensure everyone is understood and heard.

The executives and management should congratulate their team for a job well done, and working through the hardship of a cyber incident, remember you went through this as a team and stuck together to win.

We suggest dinner and drinks post-retro.

Update

Collect the information from each team member during the review and retrospective and update this document. Ensure that it is adapted to your business needs specifically and fine tune it to make the experience even better for the next time a cyber incident comes your way.