



# Cyber Incident Response Plan **CREATION AND IMPLEMENTATION TOOLKIT**



## Table of Contents

Introduction.....	3
Why Cyber Incident Response Plans Matter .....	4
The Benefits of a Cyber Incident Response Plan .....	4
Cyber Incident Response Plans: A Part of Larger Cyber Security Programs .....	6
1) Top-down Involvement .....	6
2) Training and Policies .....	8
3) IT Security .....	10
Cyber Security Programs: A Continual Process.....	10
5 Phases of Cyber Incident Response Plans.....	12
When to Escalate an Incident .....	18
Response Levels.....	18
Types of Incident Response .....	20
Regulatory Considerations .....	23
State Data Breach Notification Requirements.....	23
Payment Card Industry Compliance .....	23
Executing the Plan .....	25
Contain the Incident .....	25
Convene Your Cyber Incident Response Team .....	26
Analyze the Incident .....	28
Be Prepared, Remain Protected .....	29
APPENDICES.....	30

## Introduction

When a data breach or other cyber event occurs, the damages can be significant, often resulting in lawsuits, fines and serious financial losses. What's more, cyber exposures impact businesses of all kinds, regardless of their size, area of focus, or status as a private or public entity.

Even the most secure organizations are at risk of a data breach. It can often take days or even months for a company to notice its data has been compromised. And, when it comes to containing the damage caused by a data breach, having a response plan in place is crucial.

While cyber security programs help secure an organization's digital assets, cyber incident response plans provide clear steps for companies to follow when a cyber event occurs. Response plans allow organizations to notify impacted customers and partners quickly and efficiently, limiting financial and reputational damages.

Timely responses to breaches are increasingly important when you consider that, according to a recent report sponsored by IBM Security, organizations that contain a breach in less than 30 days save an average of \$1.79 million (\$4.88 million compared to \$6.67 million). However, on average, U.S. organizations took 206 days to identify a breach and 55 days to contain one. Failing to have a clear plan in place that ensures immediate action in the face of a breach could potentially cost an organization millions of dollars and shatter its reputation.

This guide provides organizations with a general overview of cyber incident response plans—what they are, their benefits, how to implement them and how they can help organizations meet the increasing demands of privacy laws. While organizations may approach cyber security differently depending on their unique exposures and the kind of data they store, this resource provides a number of best practices to keep in mind.

## Why Cyber Incident Response Plans Matter

Simply put, every organization that stores or handles data is at risk of a cyber attack. As technology advances, companies are collecting, storing and transferring more personal information about their customers and employees than ever before. This not only puts a target on an organization's back, but it also means that just one breach can affect thousands or even millions of individuals.

And, unfortunately for businesses, cyber incidents cost more than just data:

- **Data breaches are becoming increasingly expensive.** While cyber liability insurance can help offset the costs of a data breach and any subsequent litigation, just one breach can be financially devastating. According to a survey conducted by the Ponemon Institute, the average cost of a data breach was \$5.78 million, or \$255 per lost or stolen record.
- **Cyber incidents can lead to serious reputational damage, significantly impacting directors and officers.** Reputational damages can easily reach six figures. According to Kaspersky Lab, a global cyber security company, a single cyber incident caused brand damage of \$8,000 for small and medium-sized businesses and \$200,000 for larger organizations. When wide-scale breaches occur, a company's reputation can be tarnished, sometimes permanently. In addition, the public holds organizations accountable for major losses of personal data, and directors and officers are often the ones who take the blame.

## The Benefits of a Cyber Incident Response Plan

Most organizations have some form of data protection in place. While these protections are critical for minimizing the damages caused by a breach, they don't provide clear action steps following an attack. That's where cyber incident response plans can help.

Cyber incident response plans are written guides comprised of instructions, procedures and protocols that enable an organization to respond to and recover from various kinds of data security incidents. Cyber attacks are no longer a matter of if, but when, and reacting to an inevitable breach takes more than just threat neutralization.

Companies must have the ability to respond to and defend against evolving threats. Cyber incident response plans give organizations the tools they need to further enhance their data protection practices as well as help them:

1. Anticipate cyber security incidents before they occur.
2. Minimize the impact of cyber security incidents.
3. Mitigate threats and vulnerabilities while a cyber attack occurs.
4. Improve cyber security response overall, encouraging buy-in at a management level.
5. Reduce the direct and indirect costs caused by cyber security incidents.
6. Maintain business continuity in the face of major threats.
7. Prevent the loss of data critical to their business.

8. Improve the overall security of their organization.
9. Strengthen their reputation as a secure business, thus increasing partner and customer confidence.
10. Devote more time and resources to business improvements, innovation and growth.

Above all, cyber incident response plans can help organizations better understand the nature of an attack, which, in turn, promotes a fast and thorough response to threats. However, cyber incident response plans are typically created and implemented as part of larger cyber security programs. As such, it's important for businesses to have a basic understanding of what goes into creating an effective cyber security program.

## Cyber Incident Response Plans: A Part of Larger Cyber Security Programs

In a general sense, a cyber security program establishes a framework that allows businesses of all sizes to be proactive when it comes to cyber threats and attacks.

**Cyber security programs are a complete set of organizational resources—including policies, processes, practices and technologies—used to assess and mitigate cyber risks.**

Cyber incident response plans, however, are designed to be reactive and are just one component of cyber security programs. Response plans, in effect, provide guidance for an entire organization in the event of an incident, assigning accountabilities and promoting the containment of an incident.

While companies can have a cyber incident response plan without implementing an overall cyber security program, it's not advised. This is because cyber security programs are one of the best weapons companies have to focus on cyber security initiatives and limit the impact of data breaches.

Cyber security programs may vary from business to business, but they generally include the following features:

### 1) Top-down Involvement

Many wrongly assume that IT departments are solely responsible for managing data risks and ensuring cyber security across an organization. In order for businesses to protect themselves, management personnel must also play an active role. Not only does involvement from leadership improve cyber security, it can also reduce liability for directors and officers.

Asking thoughtful questions can help management better understand the strategies IT uses to prevent, detect and respond to data breaches. When it comes to cyber threats, organizations need to be diligent and thorough in their risk prevention tactics, and management can help move the cyber conversation in the right direction.

To help oversee their organization's cyber risk management tactics, management should ask the following questions:

1. **Does the organization utilize technology to prevent data breaches?** Every company must have robust cyber security tools and antivirus systems in place. These systems act as a first line of defense for detecting and preventing potentially debilitating breaches. While it may sound obvious, many organizations fail to take cyber threats seriously and implement even the simplest protections. Boards can help highlight the importance of cyber security, ensuring that basic, preventive measures are in place.



2. **Has the company's management team identified a senior member to be responsible for organizational cyber security preparedness?** Organizations that fail to create cyber-specific leadership roles could end up paying more for a data breach than organizations that do. This is because, in the event of a cyber incident, fast response and clear guidance is needed to contain a breach and limit any damages. When establishing a chief information security officer or similar cyber leadership role, management needs to be involved in the process. Cyber leaders should have a good mix of technical and business experience. This individual should also be able to explain cyber risks and mitigation tactics at a high level so they are easy to understand for those who are not well-versed in technical terminology. It should be noted that smaller organizations may not have an in-house cyber specialist. In these instances, organizations must still identify a qualified team member to help co-ordinate cyber initiatives and breach response practices.
3. **Has the organization discussed and formalized a cyber risk budget? How engaged is management in terms of providing guidance related to cyber exposures?** Both overpaying and underpaying for cyber security services can negatively affect an organization. Creating a budget based on informed decisions and research helps companies invest in the right tools. Management can help oversee investments and ensure that they are directed toward baseline security controls that address common threats. Management, with guidance from the chief security officer or a similar cyber leader, should also prioritize funding. That way, an organization's most vulnerable and important assets are protected.

---

## **Both overpaying and underpaying for cyber security services can negatively affect an organization.**

---

4. **Does the organization have a system in place for staying current on cyber trends, news and federal, provincial and international data security regulations?** Cyber-related legislation can change with little warning, often having a sprawling impact on the way organizations do business. If organizations do not keep up with federal, provincial, international and industry-specific data security regulations, they could face serious fines or other penalties.
5. **Has the organization conducted a thorough risk assessment? Has the organization purchased or considered purchasing cyber liability insurance?** Cyber liability insurance is specifically designed to address the risks that come with using modern technology—risks that other types of business liability coverage simply won't cover. The level of coverage your business needs is based on your individual operations and can vary depending on your range of exposure. As such, businesses need to conduct a cyber risk [assessment](#) and identify potential gaps. From there, organizations can work with their broker to customize a policy that meets their specific needs.

While it's important for management to provide adequate oversight, carrying out cyber security initiatives is ultimately up to a company's appointed leadership. Above all, management must make sure

that directors and officers clearly understand their roles and responsibilities. At a high level, directors and officers must ensure the following:

GENERAL RESPONSIBILITIES OF DIRECTORS AND OFFICERS	
Policies	<ul style="list-style-type: none"> <li>• Adopt written cyber security policies, procedures and internal controls.</li> <li>• Implement tools that detect cyber security events.</li> </ul>
Appointments	<ul style="list-style-type: none"> <li>• Discuss (at the management and board level) the hiring of a chief information officer, chief security officer or similar role. Hiring a chief information security officer or creating a new cyber leadership role is not practical for every business. In these instances, organizations should identify a qualified, in-house team member and roll cyber security responsibilities into their current job requirements.</li> </ul>
Reviews and Reports	<ul style="list-style-type: none"> <li>• Review budgets and IT security programs annually.</li> <li>• Receive and review reports on any data incidents.</li> <li>• Remain well-informed on cyber security trends that could impact the business.</li> <li>• Create and oversee a team of individuals who are responsible for cyber security oversight.</li> </ul>
Direction	<ul style="list-style-type: none"> <li>• Assess cyber security risks.</li> <li>• Determine which risks can be mitigated directly and which may be transferred using cyber liability insurance or other coverage.</li> </ul>

## 2) Training and Policies

Every cyber security program must address employee training and create cyber security policies. The content of these policies will differ depending on the size and type of the organization, but typically include similar elements. The checklists below identify questions organizations should ask in order to establish or adjust companywide policies regarding cyber security:

POLICIES	YES	NO	N/A
Does your organization have a cyber security policy in place?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Is your organization's cyber security policy enforced?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Does your organization's cyber security policy include an internet access policy?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Does your organization's cyber security policy include an email and communications policy?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



Does your organization's cyber security policy include a remote access policy?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Does your organization's cyber security policy include a "bring your own device" (BYOD) policy?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Does your organization's cyber security policy include an encryption policy?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Does your organization's cyber security policy include provisions regarding privacy?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PERSONNEL SECURITY	YES	NO	N/A
Does your organization have a system in place for checking the background of employees and contractors that have access to computer systems and sensitive data?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Are employees and contractors required to wear ID badges?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
After an employee or contractor is no longer authorized to conduct work on your organization's behalf, do you revoke access to your computer systems?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PHYSICAL SECURITY	YES	NO	N/A
Does your organization ensure the physical security of its computer systems?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Are personal computers inaccessible to unauthorized users?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Are there procedures in place to keep computers from remaining logged in for prolonged periods of time?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Does your organization have a process for notifying IT personnel if a device is misplaced or stolen?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

SECURITY AWARENESS AND EDUCATION	YES	NO	N/A
Is your staff informed regarding the importance of computer security?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Does your organization provide employees with cyber security training on a regular basis?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Are your staff members familiar with techniques they can use to prevent a security breach?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
In the event of a data breach, does your staff know how to respond?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Do your staff members know how to keep their passwords and hardware secure?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

A sample data breach response policy can be found [here](#). Again, you may need to amend this policy based on your organization and its exposures.

### 3) IT Security

One of the most important aspects of a cyber security program are IT defenses themselves. Above all, organizations want to invest in the right solutions—solutions that are adequate and up to date.

Organizations should install industry-standard antivirus and malware protections, documenting any and all updates. It's also important that your network is protected against internal and external attacks as much as possible.

You should secure wireless networks using firewalls, malware detection and similar protections. Conduct penetration testing regularly and make sure that technical solutions are in place to detect and block suspicious activities or access.

The checklist below outlines some general questions organizations should ask to promote thorough and comprehensive IT security:

IT PROCEDURES	YES	NO	N/A
Does your organization keep operating systems and antivirus software up to date?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Does your organization periodically perform vulnerability scans on servers and all the computers used in your organization?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Does your organization patch the software on all systems by following a regular schedule?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Are employees required to create strong passwords?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Does your organization encrypt sensitive data?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Does your organization have a process for retrieving backup and archival copies of critical data?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Does your organization have policies and procedures in place for handling credit card and other personal private information?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Does your organization have “secure send” procedures in place so it can receive and distribute client information safely?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

### Cyber Security Programs: A Continual Process

Creating a cyber security program is an involved process, and there is no one-size-fits-all solution. In fact, certain organizations may have more detailed programs depending on the scope of their IT infrastructure and the type of data they handle for customers, partners and employees.

While basic considerations are outlined above, organizations will want to perform regular [risk assessments](#) to help them determine what specific steps to take when crafting a cyber security program.

Qualified insurance brokers can help you understand your cyber risks and provide you with a list of key business areas to examine. Cyber security programs should evolve alongside the threat landscape, and you will need to update policies, IT protections and training information as needed.

---

**Having a general cyber security plan in place is a great way to boost the effectiveness of cyber incident response plans. And, once you understand the key elements of a cyber incident response plan, you will be able to develop an overall risk management strategy.**

---

## 5 Phases of Cyber Incident Response Plans

While cyber incident response plans will differ based on a company's size, assets and industry, they contain similar elements. All cyber incident response plans should be:

1. Prepared in advance
2. Detailed
3. Tested
4. Understood by those within the organization
5. Drafted with [industry best practices](#) in mind

Response plans help focus the efforts of many individuals following a cyber incident and should be the result of input from stakeholders across the company. When establishing a cyber incident response plan, it's best to think in phases.

### Phase 1: Plan and Prepare

PHASE 1: PLAN AND PREPARE	PHASE 2: DETECT AND REPORT	PHASE 3: ASSESS AND DECIDE	PHASE 4: RESPOND	PHASE 5: PERFORM POST-INCIDENT ACTIVITIES
<ul style="list-style-type: none"><li>• Form response team.</li><li>• Manage security awareness across the organization.</li><li>• Implement cyber safeguards.</li></ul>	<ul style="list-style-type: none"><li>• Monitor security systems.</li><li>• Detect cyber incidents.</li></ul>	<ul style="list-style-type: none"><li>• Assess the severity of the incident.</li><li>• Prioritize your response.</li></ul>	<ul style="list-style-type: none"><li>• Contain the incident.</li><li>• Neutralize any threats.</li><li>• Analyze.</li></ul>	<ul style="list-style-type: none"><li>• Document lessons learned.</li></ul>

The initial phase of cyber incident response plans is all about cyber incident response plan groundwork. In this phase, you will want to form a response team, manage security awareness across your organization and implement cyber safeguards.

Specifically, the following are key activities to engage in during Phase 1:

- **Obtain support from management personnel**, outlining the importance of cyber incident response plans.
- **Establish a cyber incident response plan and policy that:**
  - Describes which types of events should be considered incident

- Establishes the organizational structure for incident response
  - Defines roles and responsibilities
  - Defines regulatory requirements
- **Develop incident response procedures.** These procedures should be detailed and outline steps for responding to a variety of cyber incidents. They should also cover every phase of the cyber incident response plan and be based off an overall cyber incident management policy. While specific response procedures will differ from organization to organization, they should account for:
  - Identifying and containing a breach
  - Recording information on the breach
  - Notifying key stakeholders, including employees, partners and customers
  - Training employees
- **Inventory the data assets your organization controls.** Leadership should have an understanding of what kinds of losses would occur in the event of a breach. Identifying critical assets, quantifying potential losses and prioritizing data can go a long way toward securing buy-in from upper management. Data should be prioritized based on its sensitivity and how important it is for daily operations. Specifically, when inventorying data, you should specify:
  - Who owns a particular set of data
  - Where the data is stored
  - What controls you have in place to safeguard your data
- **Implement controls to safeguard your organization's information assets.** Possible controls include firewalls, patch management and vulnerability assessments.
- **Create a cyber incident response team.** Cyber incident response plans must identify key internal and external personnel who are responsible for addressing a breach. Your incident response plan should outline the roles and responsibilities of these individuals and identify the [procedures](#) they must follow after a data incident. Be sure to account for all aspects of a data incident response, including planning, detecting and reporting, assessing, responding and post-incident review.

The actual members of the team will vary depending upon the organization and the nature of the incident. For example, smaller organizations may combine several responsibilities into one job role or outsource cyber tasks altogether. In either case, the following areas must be accounted for when it comes to cyber incident response:

- Legal personnel
- Public relations professionals
- Customer care professionals

- Corporate security officers
  - IT specialists
- **Conduct training for team members.**
- **Develop a communications plan** and awareness training for the entire organization.
- **Provide easy reporting mechanisms.**
- **Deploy endpoint security controls** (e.g., anti-malware scanners) on information systems.
- **Ensure that anti-malware scanners and other endpoint controls are updated frequently.**  
Subscription-based security services should be renewed on a yearly basis. Once you let the subscription lapse, your information systems will immediately become vulnerable to cyber threats.
- **Establish relationships with governmental entities and law enforcement agencies.**
- **Practice your incident response capability.**
- **Involve legal counsel.** To ensure effective plans, you should involve legal counsel throughout the entire cyber incident response process. Additionally, response plans should be consistent with applicable laws in relevant jurisdictions (e.g., jurisdictions where your organization and customers are located).

Above all, you must make sure that your cyber security plan is actionable and practicable. Cyber incident response plans should be short, simple documents that:

- Specify tasks and outcomes.
- Assign accountability to specific incident response team members.
- Provide guidance and advice to help the incident response team make important technical, business and legal decisions in a timely manner.



## Phase 2: Detect and Report

PHASE 1: PLAN AND PREPARE	PHASE 2: DETECT AND REPORT	PHASE 3: ASSESS AND DECIDE	PHASE 4: RESPOND	PHASE 5: PERFORM POST-INCIDENT ACTIVITIES
<ul style="list-style-type: none"><li>• Form response team.</li><li>• Manage security awareness across the organization.</li><li>• Implement cyber safeguards.</li></ul>	<ul style="list-style-type: none"><li>• Monitor security systems.</li><li>• Detect cyber incidents.</li></ul>	<ul style="list-style-type: none"><li>• Assess the severity of the incident.</li><li>• Prioritize your response.</li></ul>	<ul style="list-style-type: none"><li>• Contain the incident.</li><li>• Neutralize any threats.</li><li>• Analyze.</li></ul>	<ul style="list-style-type: none"><li>• Document lessons learned.</li></ul>

Phase 2 of cyber incident response plans is dedicated to monitoring your organization's IT systems. When it comes to responding to a threat, the quicker you act, the better. According to a study conducted by the Ponemon Institute, it takes organizations an average of 206 days to identify a data breach and another 55 days to fully contain one.

With each day that passes after a cyber incident, organizations accumulate more financial and reputational damage, making active monitoring a must. Specifically, the following are key activities to engage in during Phase 2:

- **Create a method for employees and other partners to report suspicious activity.** Monitor these reports carefully.
- **Ensure your IT security systems are equipped with active monitoring protocols,** notifying you following the discovery of an issue. You should also establish a method for monitoring and responding to these notifications. Causes of cyber security incidents can vary, but are often the result of the following:
  - Attempts to gain unauthorized access to a system or its data
  - Attempts to disrupt an organization's service delivery
  - Unauthorized access to information systems
  - Unauthorized changes to information systems
  - Malware infections
  - Malicious employees

- Phishing emails and other spam
  - Infected USB flash drives
  - Malicious websites
  - The theft or loss of a laptop or smartphone
- **Monitor information on potential and current cyber threats shared by peers, law enforcement officials, vendors and organizations** who specialize in cyber security, like the FBI's Internet Crime Complaint Center (IC3).
- **Look for signs of abnormal network activity.** Signs that an IT infrastructure or system has been compromised can include, but are not limited to, the following:
  - Accounts or passwords no longer work
  - Company websites contain unauthorized changes
  - Computer systems run out of disk space or memory unexpectedly
  - You can no longer connect to your network
  - Computers crash constantly or reboot unexpectedly
  - Web browsers and other applications no longer function as expected
  - Your email contacts are receiving spam messages
  - Endpoint security controls, such as virus scanners, are no longer functioning
  - Your virus scanners or other security protocols inform you that an attempt has been made to compromise your network
  - System logs show suspicious activity
- **Gather relevant information, continue monitoring and detection practices,** and ensure reports are forwarded to your incident response team.

There are a variety of incident types, and your organization should have a system in place to detect these threats. The chart below outlines various types of incidents.

TYPE	DESCRIPTION
Unauthorized access or usage	An individual gains access to a network, system or data without permission.
Service interruption or denial of service	An attack prevents access to a service or otherwise affects normal operation.
Malicious code	Malicious software like viruses, worms and Trojans are installed.

<b>Network system failures (widespread)</b>	Any incident that negatively affects the confidentiality, integrity or availability of a network.
<b>Application system failures</b>	Any incident that negatively affects the confidentiality, integrity or availability of an application.
<b>Unauthorized disclosure or loss of information</b>	Any incident that negatively affects the confidentiality, integrity or availability of data.
<b>Privacy breach</b>	Any incident that involves the real or suspected loss of personal information.
<b>Information security/data breach</b>	Any incident that involves the real or suspected loss of sensitive information.
<b>Other</b>	Any other incident that affects networks, systems or data.

### Phase 3: Assess and Decide

PHASE 1: PLAN AND PREPARE	PHASE 2: DETECT AND REPORT	PHASE 3: ASSESS AND DECIDE	PHASE 4: RESPOND	PHASE 5: PERFORM POST-INCIDENT ACTIVITIES
<ul style="list-style-type: none"> <li>Form response team.</li> <li>Manage security awareness across the organization.</li> <li>Implement cyber safeguards.</li> </ul>	<ul style="list-style-type: none"> <li>Monitor security systems.</li> <li>Detect cyber incidents.</li> </ul>	<ul style="list-style-type: none"> <li>Assess the severity of the incident.</li> <li>Prioritize your response.</li> </ul>	<ul style="list-style-type: none"> <li>Contain the incident.</li> <li>Neutralize any threats.</li> <li>Analyze.</li> </ul>	<ul style="list-style-type: none"> <li>Document lessons learned.</li> </ul>

Suspicious network activity doesn't necessarily mean a cyber event has occurred. Phase 3 of cyber incident response involves assessing all cyber events and determining responses accordingly. This phase occurs when initial [signs](#) of a breach occur and the response team must determine the scope of the attack. Specifically, the following are key activities to engage in during Phase 3:

- Assign a person from your incident response team to oversee the assessment of events.

- Determine, with the help of IT and other professionals, whether an event is actually a cyber security concern or simply a false alarm. If you determine a cyber security incident has occurred, escalate the event to the rest of your response team.
- Find out what information, system or network is affected by the event. Analyze the impact in terms of data confidentiality, integrity and priority.
- Notify the appropriate officials.
- Find out if your business partners are affected.

### When to Escalate an Incident

It is important for your employees to know when and how to report suspicious activities. While it may seem like certain scenarios do not need to be escalated up to an organization's incident response team, employees should be trained to be overly cautious. At a minimum, employees should inform their manager or an IT team member of suspicious issues. The chart below outlines basic scenarios where issues should be reported:

EVENTS THAT <u>SHOULD</u> BE REPORTED TO INCIDENT RESPONSE TEAMS	
<ul style="list-style-type: none"> <li>• Suspicious emails with attachments or links</li> <li>• Data breaches</li> <li>• Theft or loss of your organization's electronic devices (e.g., laptops and smartphones)</li> <li>• Infections from viruses or other malicious software</li> <li>• Denial-of-service attacks</li> <li>• Suspicious or unauthorized network activity</li> <li>• Third-party system, service or network failure</li> <li>• The defacement or compromise of your organization's online presence</li> </ul>	

### Response Levels

In terms of responding to cyber incidents, it's a good idea to organize threats in levels. These response levels will provide general guidance on the level of co-ordination required to respond to any given event. Please note, these levels may differ depending on the complexity of your operations and the data you store.

—	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4
No cyber security incidents have occurred.  Critical and non-critical business functions are	No critical business functions are processed through the affected system.	A small number of the organization's critical business functions are processed	The majority of the organization's critical business functions are processed	All of the organization's critical business functions are processed

operating as normal.	Malware (or some other malicious software) causes <b>very little or no disruption</b> in service delivery.	through the affected system.  Malware (or some other malicious software) causes a <b>minor disruption</b> in service delivery depending on the system(s) impacted.	through affected system.  Malware (or some other malicious software) causes a <b>major disruption</b> in service delivery depending on the system(s) impacted.	through the affected system.  Malware (or some other malicious software) causes a <b>data breach or data destruction.</b>
----------------------	--	--	--	---

## Phase 4: Respond

PHASE 1: PLAN AND PREPARE	PHASE 2: DETECT AND REPORT	PHASE 3: ASSESS AND DECIDE	PHASE 4: RESPOND	PHASE 5: PERFORM POST-INCIDENT ACTIVITIES
<ul style="list-style-type: none"> <li>Form response team.</li> <li>Manage security awareness across the organization.</li> <li>Implement cyber safeguards.</li> </ul>	<ul style="list-style-type: none"> <li>Monitor security systems.</li> <li>Detect cyber incidents.</li> </ul>	<ul style="list-style-type: none"> <li>Assess the severity of the incident.</li> <li>Prioritize your response.</li> </ul>	<ul style="list-style-type: none"> <li>Contain the incident.</li> <li>Neutralize any threats.</li> <li>Analyze.</li> </ul>	<ul style="list-style-type: none"> <li>Document lessons learned.</li> </ul>

Once you have determined the presence and severity of a threat, your organization must respond accordingly. Response procedures allow organizations to contain a breach, investigate it and resolve the threat. While specific activities will differ depending on the type of attack, the following are key activities to engage in during Phase 4:

- Identify internal and external resources to help your organization respond to the incident.
- Contain the problem, for example, by shutting down the system. For more specifics on containing incidents, click [here](#).

- Remove the malicious components of the incident. For example, you could delete malware or disable a breached account.
- Recover from the incident by restoring systems to normal operation and fixing the vulnerabilities to prevent similar incidents.
- Conduct a forensic analysis of the incident, if applicable. To learn more about this step, click [here](#).

### Types of Incident Response

Responding to a cyber incident can be a complex process—one that involves members from across your organization. During Phase 4, consider the following types of responses to a cyber incident:

1. **Technical response**—The technical response side of Phase 4 focuses on the actions of IT and other cyber security personnel. Specifically, technical response teams are the individuals needed to resolve a specific cyber threat. Technical response may involve several groups or departments, as containing, resolving, mitigating and repairing threats can be complex. Following a data breach, technical response is critical for restoring your systems to a healthy state. Whether your company has an in-house, technical-response capability or outsources it completely, your team should take proactive steps to protect your IT infrastructure.
2. **Management response**—Management response is any activity that requires high-level intervention, notification, interaction, escalation or approval. This can include things like coordinating internal and external communications, handling finances, ordering audits and overseeing regulatory compliance. For smaller organizations, management personnel are tasked with coordinating with third parties to ensure cyber incident response initiatives are carried out properly.
3. **Communications response**—Communicating cyber security incidents effectively can make a major difference when minimizing reputational harm. These activities should involve senior leadership, cyber security officers or IT professionals, legal personnel, marketing and your cyber incident response team. Most importantly, every organization should have a predetermined point of contact with the media, like a public relations expert trained on developing precise and impactful press releases. Your public relations expert should have communication templates ready to address different breach scenarios. Above all, communications response staff will need to balance the company's business interests with public transparency.
4. **Legal response**—When it comes to cyber incident response, you should involve legal counsel whenever possible. These individuals can provide advice and work with outside regulators, third parties and other stakeholders to manage any litigation concerns. In addition, you may want legal input for any external communications to guarantee compliance with company policies and regulatory requirements. Legal personnel should effectively act as quality control, reviewing everything from your mission statement to the response plan itself. Overall, legal experts ensure your firm exercises due care at all times, particularly when it comes to handling confidential information, evidence and documentation. In doing so, they proactively defend the organization against liabilities.



## Phase 5: Perform Post-incident Activities

PHASE 1: PLAN AND PREPARE	PHASE 2: DETECT AND REPORT	PHASE 3: ASSESS AND DECIDE	PHASE 4: RESPOND	PHASE 5: PERFORM POST-INCIDENT ACTIVITIES
<ul style="list-style-type: none"> <li>Form response team.</li> <li>Manage security awareness across the organization.</li> <li>Implement cyber safeguards.</li> </ul>	<ul style="list-style-type: none"> <li>Monitor security systems.</li> <li>Detect cyber incidents.</li> </ul>	<ul style="list-style-type: none"> <li>Assess the severity of the incident.</li> <li>Prioritize your response.</li> </ul>	<ul style="list-style-type: none"> <li>Contain the incident.</li> <li>Neutralize any threats.</li> <li>Analyze.</li> </ul>	<ul style="list-style-type: none"> <li>Document lessons learned.</li> </ul>

Phase 5 outlines post-incident activities your organization must complete following an incident. Again, this will differ based on the location of the organization, the scope of the incident and the type of data affected by the breach. Phase 5 helps organizations learn from specific incidents and make key changes to improve cyber security and the response process.

Specifically, the following are key activities to engage in during Phase 5:

- Identify the lessons learned from the cyber security incident.
- Identify and make improvements to the organization's security architecture.
- Review how effectively the incident response plan was executed during the cyber security incident.

To aid in the recovery process of future incidents, organizations must evaluate the issues that caused the breach, how quickly they responded and how long the incident lasted. Effectively, during post-incident analysis, you must review and document everything that went well and poorly. The following are general questions to ask when evaluating incidents and your company's response practices:

- What happened and at what time?
- Was the incident found in a reasonable amount of time?
- Was the system down longer than expected?
- Were the right personnel available to respond? How well did staff and management perform in dealing with the incident?
- Did recovery and restoration happen as quickly as expected?
- Were backup files available and as up to date as possible?

7. Were documented procedures followed?
8. Were any steps or actions taken that might have inhibited the recovery?
9. What would staff and management do differently the next time a similar incident occurs?
10. What corrective actions can prevent similar incidents in the future? What additional tools or resources are needed to detect, analyze and mitigate future incidents?

After your assessment is complete, update and enhance your incident response plan. Auditing your plan helps make sure you're carrying out future response practices based on accurate and current information. In addition, assessing your plan helps you identify potential issues in advance and, should a future breach occur, ensures smoother response processes.

## Regulatory Considerations

A major consideration to keep in mind throughout all phases of your cyber incident response plan is regulatory compliance. Depending on where your business is located and what industry you operate in, a variety of specific data breach notification and reporting requirements may apply. Complicating the issue, it's an organization's job to be informed on these different requirements. While regulatory bodies can provide general guidance, it's ultimately up to the business to implement compliance practices.

For U.S. organizations, there are two major compliance considerations to remember:

1. State data breach notification requirements
2. Payment card industry compliance

## **Employers have a responsibility to know what reporting laws affect them.**

### State Data Breach Notification Requirements

Employers have a responsibility to know what reporting laws affect them. Depending on where you do business, there are a variety of compliance considerations to keep in mind. Every state has enacted security breach notification laws that require businesses to notify consumers if their personal information has been compromised.

This is particularly true for companies that operate overseas, as several countries—like Europe, Australia, India and the United States—have their own set of data breach regulations. To ensure you compliant, work with your legal team to identify and mediate regulatory exposures.

### Payment Card Industry Compliance

To help protect customers, it's critical that any organization that accepts payment cards understands the payment card industry's (PCI) Data Security Standards (DSS). The PCI DSS is a set of requirements designed to ensure that all entities that process, store or transmit credit card information maintain a secure environment. In essence, the PCI DSS establishes a minimum set of requirements for protecting the account information of cardholders. Regardless of whether a merchant processes one credit card a year or 1 million, they must adhere to the PCI DSS.

There are four major steps to compliance, as outlined by the PCI Security Standards Council. If followed closely, these steps can help merchants of any size integrate PCI DSS into their businesses. Those steps include the following:

1. **Determine merchant level**—This step involves determining which merchant level applies to your organization as determined by the payment card brands you accept.

2. **Assess**—This process involves identifying vulnerabilities in your IT assets and payment card processing systems.
3. **Remediate**—After you have assessed all PCI DSS issues, you must fix any security vulnerabilities you have found.
4. **Report**—Once you have assessed and remediated vulnerabilities, you must document your compliance efforts and submit them to the acquirers and payment card companies you are working with.

Navigating the PCI DSS can be taxing for the average merchant, as an overview of PCI DSS compliance specifics and best practices are rarely found under one, all-encompassing source. Moreover, the PCI DSS itself is over 100 pages and is filled with acronyms and terminology that can be confusing. PCI DSS compliance is not something that can be easily addressed on your own—especially if you are a merchant with limited resources. Contact [B\_Officialname] for a general guide to PCI DSS compliance.

## Executing the Plan

While having an understanding of the mechanics of a cyber incident response plan is important, knowing how to effectively execute the plan is critical. When a cyber attack occurs, it can be chaotic. Understanding how to use your incident response plan can minimize the impact of an incident.

## Contain the Incident

As part of Phase 4 of your incident response plan, containing threats quickly and thoroughly is essential for recovering from a breach. Following every incident, whether it's a data breach or the loss of physical assets (e.g., company laptops), you will need to make split-second decisions on how best to act.

Immediately after the detection of an incident, consider the following:

1. **Discovery**—Record the date, time, location and duration of the breach. You will want to note whether this was a one-off incident or an attack that has been persistent for months. In addition, document who discovered the breach and how.
2. **Breach**—Document specifics regarding the breach. This can include details on:
  - a. Point of entry
  - b. Method of intrusion
  - c. The systems affected
  - d. What information was accessed, deleted, modified or taken
3. **Data**—Catalogue details regarding the data, including who was affected, where the affected individuals are located, what type of information was compromised and how many records were impacted.

To help you contain an incident, the following checklist outlines considerations to keep in mind:

CONTAINING THE INCIDENT	YES	NO	N/A
Have you limited employee and public access to the affected area? Have you changed locks, access card permissions and passwords?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Have you notified law enforcement or other officials?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Have you conducted an internal or external investigation? If so, have you identified any employee misconduct and notified HR?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Have you determined what assets have been lost or affected?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Did you record the date, time, location and duration of the breach? Did you record who discovered the breach and how?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Did you determine whether this was a one-off incident or persistent event?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Did you document details on point of entry, method of intrusion, the systems affected and what information was accessed, deleted, modified or taken?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Did you catalogue details regarding the data, including who was affected, where the affected initials are located, what type of information was compromised and how many records were impacted?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## Convene Your Cyber Incident Response Team

Once you have determined a cyber event [should be reported](#) to your response team, you will have to escalate the incident and convene the team itself.

Team members should be assembled and briefed. If possible, communications between team members should be done by phone only to avoid using potentially compromised email systems. The actual members of the team will vary depending upon the organization and the nature of the incident. However, team member responsibilities generally cover the following areas:



LEGAL/COMPLIANCE	PUBLIC RELATIONS/MARKETING	CUSTOMER CARE DEPARTMENT	HUMAN RESOURCES	CORPORATE SECURITY AND IT
<ul style="list-style-type: none"> <li>• Implements a privilege protocol</li> <li>• Determines how to notify affected individuals, the media, law enforcement, government regulators and other third parties</li> <li>• Establishes and manages relationships with outside counsel before an incident</li> <li>• Manages communications with privacy commissioners and regulators</li> <li>• Ensures internal documents and reports are generated at the counsel's direction</li> <li>• Issues and monitors a litigation hold</li> <li>• Reviews all outgoing communications, filings, reports, etc.</li> </ul>	<ul style="list-style-type: none"> <li>• Identifies key media and crisis-response strategies</li> <li>• Executes an internal communication plan that addresses confidentiality and appropriate employee actions</li> <li>• Tracks and analyzes media coverage, responding to negative coverage if necessary</li> </ul>	<ul style="list-style-type: none"> <li>• Determines whether incident inquiries will be dealt with internally or whether a call center will be utilized</li> <li>• Sets up a call center and consumer protection program to handle customer complaints</li> </ul>	<ul style="list-style-type: none"> <li>• Manages employees during the incident, shifting employee resources as required</li> <li>• Handles internal investigations, disciplinary actions and terminations if the incident is the result of employee wrongdoing</li> </ul>	<ul style="list-style-type: none"> <li>• Communicates with law enforcement (alongside the legal team)</li> <li>• Manages incident risks as well as the isolation of affected areas</li> <li>• Works alongside external IT forensics professionals to identify and remove any malicious code or other remnants of a data incident</li> <li>• Assists with evidence gathering and litigation efforts</li> </ul>

## Analyze the Incident

The moment an incident is identified, you should begin gathering and analyzing the information available. Notably, any information you gather is subject to a comprehensive litigation hold. Therefore, this data must be preserved, collected and analyzed at the direction of counsel (and provided to law enforcement if required/appropriate). Your legal team can help you review any information gathered to determine if it is relevant.

Following a data breach or other incident, your organization has a very short window to collect key evidence. While your IT team will essentially act as a first responder, they may not have the necessary training to conduct data recovery and analysis procedures. Because of this, outside IT forensics teams specializing in data breach response should be retained.

These firms should be able to:

- Identify and neutralize threats.
- Preserve and manage evidence using data recovery tools and processes.
- Work across various operating systems and devices.
- Manage forensic practices in a way that respects employee sensitivities and workplace culture.
- Identify individuals who can provide testimony and appear as confident witnesses in court.
- Understand privilege issues, litigation holds and the role their firm plays in regulatory and court proceedings.

Organizations should establish relationships with experienced forensics firms long before a breach ever occurs.

## Be Prepared, Remain Protected

While organizations may take every necessary precaution, they are seldom prepared for a major cyber security event. These events can put a serious strain on finances, resources, technology and reputations, particularly if you fail to create an effective cyber incident response plan.

These plans, alongside cyber security programs and cyber liability insurance, decrease the likelihood that your organization will close as the result of an attack. It should be noted that there is no agreed-upon format for cyber incident response plans, but many do share commonalities. To review a sample plan and begin the process of creating one of your own, click [here](#).

To learn more about basic cyber security protections and coverage options, contact an experienced broker at [B\_Officialname] today. We will be able to assist you with all of your cyber risk management needs, providing insight into the steps you need to take to better protect your business.

The background is a complex, abstract network diagram. It features numerous nodes, some labeled 'NODE 01' through 'NODE 06' and 'BLOCK 01'. These nodes are connected by a dense web of lines in various colors (blue, orange, yellow, green). The overall aesthetic is futuristic and digital, with a light blue and white color palette. The text 'APPENDIX A: CYBER EXPOSURE SCORECARD' is centered over this background.

# APPENDIX A: CYBER EXPOSURE SCORECARD

# CYBER RISK EXPOSURE SCORECARD

In recent years, cyber attacks have emerged as one of the most significant threats facing organizations of all sizes. The internet and other network operations have created risks that were unheard of less than a decade ago. When cyber attacks (such as data breaches and hacks) occur, they can result in devastating damage, such as business disruptions, revenue loss, legal fees, forensic analysis, and customer or employee notifications. It is important to remember that no organization is immune to the impact of cyber crime. As a result, cyber liability insurance has become an essential component to any risk management program.

**INSTRUCTIONS:** Begin by answering the questions below. Each response will be given a numerical value depending on the answer:

- **YES:** 5 points
- **UNSURE:** 5 points
- **NO:** 0 points

After completing all of the questions, total your score to determine your organization's level of cyber risk using the scale below.

EXPOSURE	YES	NO	UNSURE	SCORE
1. Does your organization have a wireless network, or do employees or customers access your internal systems from remote locations?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
2. Does anyone in your organization take company-owned mobile devices (e.g., laptops, smartphones and USB drives) with them, either home or when travelling?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
3. Does your organization use cloud-based software or storage?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
4. Does your organization have a "bring your own device" (BYOD) policy that allows employees to use personal devices for business use or on a company network?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
5. Are any employees allowed access to administrative privileges on your network or computers?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
6. Does your organization have critical operational systems connected to a public network?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
7. Does anyone in your organization use computers to access bank accounts or initiate money transfers?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
8. Does your organization store sensitive information (e.g., financial reports, trade secrets, intellectual property and product designs) that could potentially compromise your organization if stolen?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
9. Does your organization digitally store the personally identifiable information (PII) of employees or customers? This can include government-issued ID numbers and financial information.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
10. Is your organization part of a supply chain, or do you have supply chain partners?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
11. Does your organization conduct business in foreign countries, either physically or online?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
12. Has your organization ever failed to enforce policies around the acceptable use of computers, email, the internet, etc.?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
13. Can the general public access your organization's building without the use of an ID card?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
14. Is network security training for employees optional at your organization?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
15. Can employees use their computers or company-issued devices indefinitely without updating passwords?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
16. Has your IT department ever failed to install anti-virus software or perform regular vulnerability checks?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
17. Can employees dispose of sensitive information in unsecured bins?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
18. Would your organization lose critical information in the event of a system failure or other network disaster?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
19. Can employees easily see what co-workers are doing on their computers?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
20. Has your organization neglected to review its data security or cyber security policies and procedures within the last year?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<b>TOTAL SCORE:</b>				

**Low risk.** Review cyber policy and procedures, and contact us with questions: 0-10

**High risk.** Contact us today: 30-50

**Moderate risk.** Contact us for assistance: 15-25

**Escalated risk.** Contact us now: 55-100



The background is a complex, abstract illustration of a network or data system. It features numerous nodes, represented by small circles and larger rectangular blocks, connected by a dense web of colorful lines (red, blue, yellow, green). Some nodes are labeled with text such as 'NODE 01', 'NODE 02', 'NODE 04', 'NODE 05', 'NODE 06', 'BLOCK 01', and 'BLOCK 02'. The overall aesthetic is futuristic and technological, with a soft, glowing light effect.

## APPENDIX B: DATA BREACH RESPONSE POLICY



# Data Breach Response Policy

Location:

Effective Date: [Effective\_Date]

Revision Number:1

[C\_Officialname]

## Purpose

This policy establishes how [C\_Officialname] will respond in the event of a data breach. In addition, it outlines an action plan that will be used to investigate potential breaches and mitigate damage if a breach occurs. This policy is in place to minimize potential damages that could result from a data breach and ensure that parties affected by a data breach are properly informed of how to protect themselves.

## Scope

This policy applies to all incidents where a breach of customer's or employee's personal identifying information is suspected or confirmed.

## DEFINITIONS

- **Personal identifying information (PII)**—Information that can be used to distinguish or trace an individual's identity. PII includes, but is not limited to, any of the following:
  - Social security numbers
  - Credit card information
  - Business number registration information
  - Biometric records (fingerprints, DNA or retinal patterns, and other measurements of physical characteristics for use in verifying the identity of individuals)
  - Payroll information (paychecks and paystubs)
  - Medical information of any employee or customer (doctor names and claims, prescriptions and any related personal medical information)
  - Other personal information of a customer, employee or contractor (dates of birth, addresses, phone numbers, maiden names, names or customer numbers)
- **Breach**—Any situation where PII is accessed by someone other than an authorized user, for anything other than an authorized purpose.

## POLICY GUIDELINES

### Upon Learning of a Breach

A breach or a suspected breach of PII must be immediately investigated. Since all PII is of a highly confidential nature, only personnel necessary for the data breach investigation will be informed of the breach. The following information must be reported to appropriate management personnel:

- When (date and time) did the breach happen?
- How did the breach happen?
- What types of PII were obtained?
- How many customers were affected?

Management will then make a record of events and people involved, as well as any discoveries made over the course of the investigation and determine whether or not a breach has occurred.

### **Perform a Risk Assessment**

Once a breach has been verified and contained, perform a risk assessment that rates the:

- Sensitivity of the PII lost (customer contact information alone may present much less of a threat than financial information)
- Amount of PII lost and number of individuals affected
- Likelihood PII is usable or may cause harm
- Likelihood the PII was intentionally targeted (increases chance for fraudulent use)
- Strength and effectiveness of security technologies protecting PII (e.g., encrypted PII on a stolen laptop. Technically stolen PII but with a greatly decreased chance of access.)
- Ability of [C\_Officialname] to mitigate the risk of harm

All information collected during the risk assessment must then be compiled into one report and analyzed. The risk assessment must then be provided to appropriate [C\_Officialname] personnel in charge of data breach response management.

### **Notifying Affected Parties**

Notification responsibility is based both on the number of individuals affected and the nature of the PII that was accessed. Any information found in the initial risk assessment will be turned over to the legal counsel of [C\_Officialname] who will review the situation to determine if, and to what extent, notification is required. Notification should occur in a manner that ensures the affected individuals will receive actual notice of the incident. Notification will be made in a timely manner, but not so soon as to unnecessarily compound the initial incident with incomplete facts or to make identity theft more likely through the notice.

In the case that notification must be made:

- Only those that are legally required to be notified will be informed of the breach. Notifying a broad base when it is not required could raise unnecessary concern in those who have not been affected.
- A physical copy will always be mailed to the affected parties no matter what other notification methods are used (e.g., phone or email).
- A help line will be established as a resource for those who have additional questions about how the breach will affect them.

The notification letter will include:

- A brief description of the incident, including the nature of the breach and the approximate date it occurred.
- A description of the types of PII that were involved in the breach. (The general types of PII, not an individual's specific information.)
- Explanation of what [C\_Officialname] is doing to investigate the breach, mitigate its negative effects and prevent future incidents.
- Steps the individual can take to mitigate any potential side effects from the breach.
- Contact information for a [C\_Officialname] representative who can answer additional questions.

### **Mitigating Risks**

Based off the findings of the risk assessment, a plan will be developed to mitigate risk involved with the breach. The exact course of action will be based on the type of PII that was involved in the data breach. The course of action will aim to minimize the effect of the initial breach and to prevent similar breaches from taking place.

- Affected individuals will be notified as soon as possible so they can take their own steps to mitigate potential risk.
- If there is a substantial concern for fraudulent use of PII, [C\_Officialname] will offer affected individuals free access to a credit monitoring service.

[C\_Officialname] will also provide steps to mitigate risks that can be taken by affected individuals. The steps provided to affected individuals will depend on the nature of the data breach. If the breach has created a high risk for fraudulent use of financial information, customers may be advised to:

- Monitor their financial accounts and immediately report any suspicious or fraudulent activity.
- Contact the two major credit bureaus and place an initial fraud alert on their credit reports. This can be extremely helpful in situations where PII can be used to open new accounts, such as if social security numbers have been taken.
- Avoid attempts from criminals that may see the breach as an opportunity to pose as [C\_Officialname] employees in an attempt to deceive affected individuals into divulging personal information.
- File a report with local police or in the community where the breach took place.

Instructions on what steps a customer can take to reduce their risk will be included in the notification letter. In addition to the information listed above, appropriate [C\_Officialname] personnel, when possible, will provide additional information tailored to the individual breach.

The background of the page is a complex, abstract digital network. It features numerous nodes, represented by small circles and larger pill-shaped labels, connected by a dense web of colorful lines in shades of blue, orange, yellow, and purple. Some of the visible labels include 'NODE 01', 'NODE 04', 'NODE 05', 'NODE 02', 'BLOCK 01', and 'NODE 03'. The overall aesthetic is futuristic and technological, suggesting a cyber environment.

# APPENDIX C: CYBER INCIDENT RESPONSE PLAN BEST PRACTICES CHECKLIST

# CHECKLIST | CYBER INCIDENT RESPONSE PLAN BEST PRACTICES


Presented by [B\_Officialname]

While cyber security programs help secure an organization's digital assets, cyber incident response plans provide clear steps for companies to follow when a cyber event occurs. Response plans allow organizations to notify impacted customers and partners quickly and efficiently, limiting financial and reputational damages.

The following checklist is a set of general recommendations organizations should keep in mind when creating a cyber incident response plan.

ITEM	YES	NO
Your plan is part of a larger cyber security program that identifies tools and resources for incident handling. This program helps prevent incidents from occurring by ensuring that networks, systems and applications are sufficiently secure.	<input type="checkbox"/>	<input type="checkbox"/>
Your plan establishes mechanisms that outside parties can use to report incidents.	<input type="checkbox"/>	<input type="checkbox"/>
Your plan takes into account the periodic auditing of critical IT systems.	<input type="checkbox"/>	<input type="checkbox"/>
Your employees understand what normal network, system and application behavior looks like. They are trained to report any suspicious activity.	<input type="checkbox"/>	<input type="checkbox"/>
Your plan accounts for data retention and allows you to create and store information about any and all breaches.	<input type="checkbox"/>	<input type="checkbox"/>
Your plan allows you to record and track information regarding a breach the moment one occurs.	<input type="checkbox"/>	<input type="checkbox"/>
Your plan allows you to quickly assess cyber incidents and prioritize them accordingly.	<input type="checkbox"/>	<input type="checkbox"/>
Your plan establish strategies and procedures for containing incidents.	<input type="checkbox"/>	<input type="checkbox"/>
Your plan provides specific steps to restore system and network integrity.	<input type="checkbox"/>	<input type="checkbox"/>
Your plan accounts for privacy and payment card industry compliance. Legal counsel is involved in the creation and management of your plan.	<input type="checkbox"/>	<input type="checkbox"/>
Your plan includes a cyber incident analysis phase that allows you to evaluate the success of your response plan.	<input type="checkbox"/>	<input type="checkbox"/>
Your plan establishes an incident response team with clearly defined and documented responsibilities. These individuals are properly trained and understand their roles following a cyber security event.	<input type="checkbox"/>	<input type="checkbox"/>
Your plan establishes a method for facilitating communications, internally and externally.	<input type="checkbox"/>	<input type="checkbox"/>
Your plan is practicable.	<input type="checkbox"/>	<input type="checkbox"/>

Your plan is regularly updated.	<input type="checkbox"/>	<input type="checkbox"/>
Your plan makes note of safeguards, including cyber liability insurance.	<input type="checkbox"/>	<input type="checkbox"/>
Your plan provides information on who to contact following a breach, including law enforcement and government officials.	<input type="checkbox"/>	<input type="checkbox"/>

The background is a complex, abstract network diagram. It features numerous nodes, represented by small circles and larger pill-shaped labels, connected by a dense web of thin, multi-colored lines (blue, green, yellow, red). The labels include 'NODE 01', 'NODE 02', 'NODE 04', 'NODE 05', 'NODE 06', 'BLOCK 01', and 'BLOCK 02'. The overall aesthetic is futuristic and digital, with a soft, glowing light effect.

## APPENDIX D: SAMPLE PLAN

## FORM

# Cyber Incident Response Plan

[C\_Officialname]

Organization name:

Review cycle: Annually

Address:

Plan prepared by:

Date:

This cyber incident response plan ensures that [C\_Officialname] is prepared to respond to a variety of threats in an effective and efficient manner. Working alongside [C\_Officialname]'s Data Breach Response Policy, this plan documents the roles, responsibilities and steps that will be followed to identify, contain, eradicate and recover from cyber security incidents. By having a plan, a team and conducting exercises, organizations will be better prepared for inevitable incidents and will be able to contain the damage and mitigate further risk to the organization.

This plan applies to all [C\_Officialname] networks, systems and data as well as employees, contractors and vendors that access these systems.

## Revision History

This Cyber Incident Response Plan has been modified as follows:

DATE	VERSION	DESCRIPTION OF THE MODIFICATION	MODIFIER

## Roles and Responsibilities

INTERNAL CONTACTS				
TITLE	NAME	RESPONSIBILITIES	PHONE	EMAIL
CEO or other company leader				
Chief information officer or other high-				

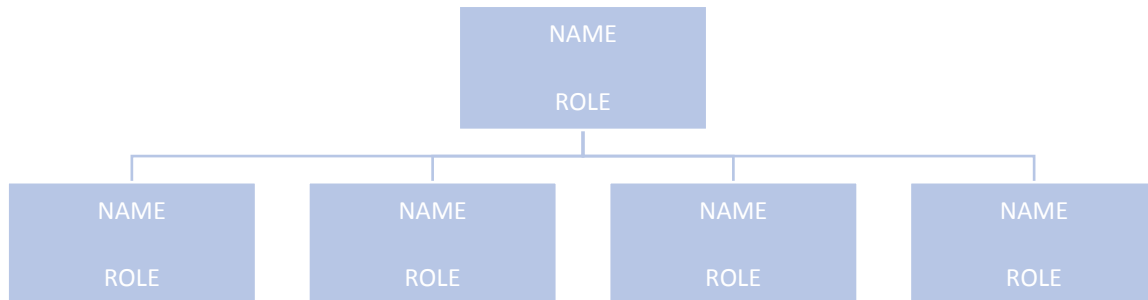
Prepared by [B\_Officialname]



ranking IT professional				
Human resources manager				
Customer care manager				
Marketing and public relations manager				
Legal representative				

EXTERNAL CONTACTS				
TYPE	ROLE	COMPANY NAME	PHONE	EMAIL
Vendor	Service provider			
Vendor	Forensics team on retainer			
Vendor	Technology vendor			
Connected organization	Peer			

## Incident Response Team Structure\*



*\*To add more roles to this flow chart, click into the image, then double-click on a specific box. From there, use the “subordinate” and “assistant” buttons located at the far left of the document ribbon.*

## Incident Types and Escalation

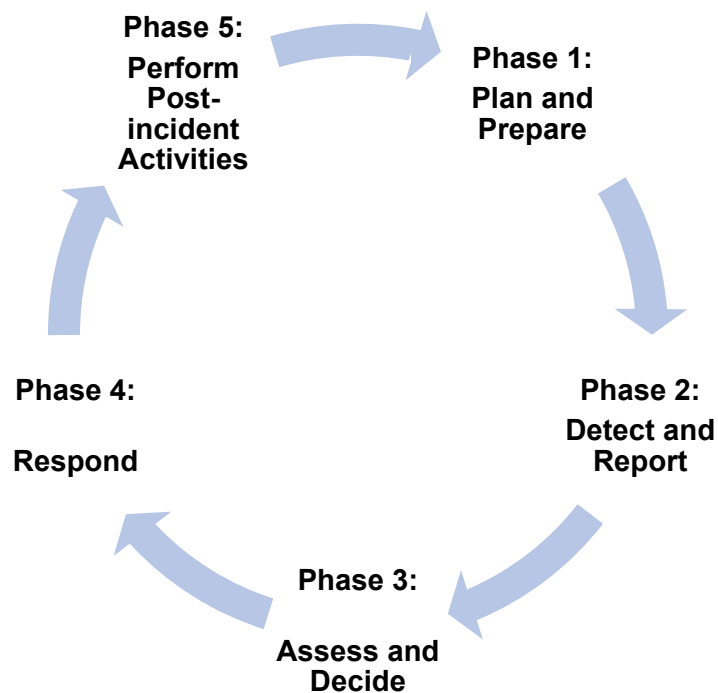
One of the major roles of the incident response team is to assess the various incidents reported to them by employees or antivirus software and similar protections. If an incident is determined to be a threat, the team will prioritize the response process based on the escalation level.

The charts below outline common incident types and various threat levels.

TYPE	DESCRIPTION
Unauthorized access or usage	An individual gains access to a network, system or data without permission.
Service interruption or denial of service	An attack prevents access to a service or otherwise affects normal operation.
Malicious code	Malicious software like viruses, worms and Trojans are installed.
Network system failures (widespread)	Any incident that negatively affects the confidentiality, integrity or availability of a network.
Application system failures	Any incident that negatively affects the confidentiality, integrity or availability of an application.
Unauthorized disclosure or loss of information	Any incident that negatively affects the confidentiality, integrity or availability of data.
Privacy breach	Any incident that involves the real or suspected loss of personal information.
Information security/data breach	Any incident that involves the real or suspected loss of sensitive information.
Other	Any other incident that affects networks, systems or data.

—	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4
<p>No cyber security incidents have occurred.</p> <p>Critical and non-critical business functions are operating as normal.</p>	<p>No critical business functions are processed through the affected system.</p> <p>Malware (or some other malicious software) causes very little or no disruption in service delivery.</p>	<p>A small number of the organization's critical business functions are processed through the affected system.</p> <p>Malware (or some other malicious software) causes a minor disruption in service delivery depending on the system(s) impacted.</p>	<p>The majority of the organization's critical business functions are processed through affected system.</p> <p>Malware (or some other malicious software) causes a major disruption in service delivery depending on the system(s) impacted.</p>	<p>All of the organization's critical business functions are processed through the affected system.</p> <p>Malware (or some other malicious software) causes a data breach or data destruction.</p>

## Incident Handling



PHASE 1: PLAN AND PREPARE	PHASE 2: DETECT AND REPORT	PHASE 3: ASSESS AND DECIDE	PHASE 4: RESPOND	PHASE 5: PERFORM POST-INCIDENT ACTIVITIES
<ul style="list-style-type: none"> <li>Form response team.</li> <li>Manage security awareness across the organization.</li> <li>Implement cyber safeguards.</li> </ul>	<ul style="list-style-type: none"> <li>Monitor security systems.</li> <li>Detect cyber incidents.</li> </ul>	<ul style="list-style-type: none"> <li>Assess the severity of the incident.</li> <li>Prioritize your response.</li> </ul>	<ul style="list-style-type: none"> <li>Contain the incident.</li> <li>Neutralize any threats.</li> <li>Analyze.</li> </ul>	<ul style="list-style-type: none"> <li>Document lessons learned.</li> </ul>

## Plan and Prepare

ITEM	
Obtain support from board members or other executives, outlining the importance of cyber incident response plans.	<input type="checkbox"/>
Establish a cyber incident management policy that: <ul style="list-style-type: none"> <li>Describes which types of events should be considered incident</li> <li>Establishes the organizational structure for incident response</li> <li>Defines roles and responsibilities</li> <li>Defines regulatory requirements</li> </ul>	<input type="checkbox"/>
Develop incident response procedures. These procedures should be detailed and outline steps for responding to a variety of cyber incidents. They should also cover every phase of the cyber incident response plan and be based off an overall cyber incident management policy. While specific response procedures will differ from organization to organization, they should account for: <ul style="list-style-type: none"> <li>Identifying and containing a breach</li> <li>Recording information on the breach</li> <li>Notifying key stakeholders, including employees, partners and customers</li> <li>Training employees</li> </ul>	<input type="checkbox"/>
Inventory the data assets your organization is responsible for. Leadership should have an understanding of what kinds of losses would occur in the event of a breach. Identifying critical assets, quantifying potential losses and prioritizing data can go a long way toward securing buy-in from upper management and a cyber security budget. This data should be prioritized based on its	<input type="checkbox"/>

<p>sensitivity and how important it is for daily operations. Specifically, when inventorying data, you should specify:</p> <ul style="list-style-type: none"> <li>• Who owns a particular set of data</li> <li>• Where the data is stored</li> <li>• What controls you have in place to safeguard your data</li> </ul>	
<p>Implement controls to safeguard your organization's information assets. Possible controls include firewalls, patch management and vulnerability assessments.</p>	<input type="checkbox"/>
<p>Create a cyber incident response team. Cyber incident response plans must identify key internal and external personnel who are responsible for addressing a breach. Your incident response plan should outline the roles and responsibilities of these individuals and outline the procedures they must follow after a data incident. Be sure to account for all aspects of a data incident response, including planning, detecting and reporting, assessing, responding and post-incident review. The actual members of the team will vary depending upon the organization and the nature of the incident, but generally account for the following areas:</p> <ul style="list-style-type: none"> <li>• Legal personnel</li> <li>• Public relations professionals</li> <li>• Customer care professionals</li> <li>• Corporate security officers</li> <li>• IT specialists</li> </ul>	<input type="checkbox"/>
<p>Conduct training for team members.</p>	<input type="checkbox"/>
<p>Develop a communications plan and awareness training for the entire organization.</p>	<input type="checkbox"/>
<p>Provide easy reporting mechanisms.</p>	<input type="checkbox"/>
<p>Deploy endpoint security controls (e.g., anti-malware scanners) on information systems.</p>	<input type="checkbox"/>
<p>Ensure that anti-malware scanners and other endpoint controls have their databases updated frequently. Subscription-based security services, such as anti-malware software, typically must be renewed on a yearly basis. Once you let the subscription lapse, your information systems will immediately become vulnerable to cyber threats.</p>	<input type="checkbox"/>
<p>Establish relationships with law enforcement agencies.</p>	<input type="checkbox"/>
<p>Practice your incident response plan.</p>	<input type="checkbox"/>
<p>Involve legal counsel. To ensure effective plans, you should involve legal counsel throughout the entire cyber incident response process. Additionally, response plans should be consistent with applicable laws in relevant jurisdictions.</p>	<input type="checkbox"/>

## Detect and Report

ITEM	
Create a method for employees and other partners to report suspicious activity. Monitor these reports carefully.	<input type="checkbox"/>
Ensure your IT security systems are equipped with active monitoring protocols, notifying you following the discovery of an issue. You should also establish a method for monitoring and responding to these notifications.	<input type="checkbox"/>
Monitor information on potential and current cyber threats shared by peers, law enforcement officials, vendors and organizations who specialize in cyber security, like the Internet Crime Complaint Center.	<input type="checkbox"/>
Look for signs of abnormal network activity.	<input type="checkbox"/>
Gather relevant information, continue monitoring and detection practices, and send reports to your incident response team.	<input type="checkbox"/>

## Assess and Decide

ITEM	
Assign a person from your incident response team to oversee the assessment of a particular event.	<input type="checkbox"/>
Determine, with the help of IT and other professionals, whether an event is actually a cyber security concern or simply a false alarm. If you determine a cyber security incident has occurred, escalate the event to the rest of your response team.	<input type="checkbox"/>
Find out what information, system or network is affected by the event. Analyze the impact in terms of data confidentiality, integrity and priority.	<input type="checkbox"/>
Notify the appropriate officials.	<input type="checkbox"/>
Find out if your business partners are affected.	<input type="checkbox"/>
Use your incident identification and escalation charts to prioritize any incidents.	<input type="checkbox"/>

## Respond

ITEM	
------	--

Identify internal and external resources to help your organization respond to the incident.	<input type="checkbox"/>
Contain the problem, for example, by shutting down the system.	<input type="checkbox"/>
Remove the malicious components of the incident. As an example, you could delete malware or disable a breached account.	<input type="checkbox"/>
Recover from the incident by restoring systems to normal operation and fixing the vulnerabilities to prevent similar incidents.	<input type="checkbox"/>
Conduct a forensic analysis of the incident, if applicable.	<input type="checkbox"/>

## Perform Post-incident Activities

ITEM	
Identify the lessons learned from the cyber security incident.	<input type="checkbox"/>
Identify and make improvements to the organization's security architecture.	<input type="checkbox"/>
Review how effectively the incident response plan was executed during the cyber security incident.	<input type="checkbox"/>