Cyber Incident Response Plan

1st Edition

November 1, 2022

1. Incident Identification

For cyber insurance purposes, a Cyber Incident is a cyber event that is a: cyber security breach, cyber extortion threat, or data breach. These events together will serve as a robust guideline in identifying a Security Incident, although other types of events also may constitute a Security Incident.

A. Cyber Extortion Threat

A threat against a network to:

- Disrupt operations.
- Alter, damage, or destroy data stored on the network.
- Use the network to generate and transmit malware to third parties.
- Deface the website.
- Access personally identifiable information, protected health information, or confidential business information stored on the network made by a person or group, whether acting alone, or in collusion with others, demanding payment, or a series of payments in consideration for the elimination, mitigation, or removal of the threat.

B. Cyber Security Breach

Any unauthorized access to, use, or misuse of, modification to the network, and/or denial of network resources by attacks perpetuated through malware, viruses, worms, Trojan horses, spyware, adware, zero-day attack, hacker attack, or denial of service attack.

C. Data Breach

The actual or reasonably suspected theft, loss, unauthorized acquisition of, or unauthorized access to data that has or may compromise the security, confidentiality and/or integrity of personally identifiable information, protected health information, or confidential business information.

D. Other Cyber Events

Other cyber events include:

- Attempts from unauthorized sources to access systems or data.
- Unplanned disruption to a service or denial of a service.
- Unauthorized processing or storage of data.
- Unauthorized changes to system hardware, access rights, firmware, or software.
- Presence of a malicious application, such as ransomware, or a virus.
- Presence of unexpected/unusual programs.
- Non-malicious or non-unauthorized failures or mistakes of your data, applications, systems or network.

2. Designation of an Incident Response Manager

The organization shall designate an Incident Response Manager who is either a full- or part-time technology person working daily in your organization, or the highest-ranking administrative person employees would normally contact when having computer or technology problems. Ideally, this person should be readily available in the case of a cyber event.

A. Responsibilities

- The organization has designated an Incident Response Manager responsible for determining whether a cyber event is declared a Cyber Incident.
- The Incident Response Manager is responsible for ensuring this policy is followed.
- The Incident Response Manager is responsible for establishing an Incident Response Team to support the execution of this plan.
- The Incident Response Team is tasked with executing this plan in accordance with and at the direction of the Incident Response Manager.

- The highest-ranking administrative official in the organization is responsible for ensuring end-users have sufficient knowledge to recognize a potential Cyber Incident and report it in accordance with this plan.
- Employees are responsible to report potential Cyber Incidents in a timely manner and provide any requires support during plan execution.

3. Incident Response Team and Notification

Establish an Incident Response Team to quickly respond to Cyber Incidents, and a team broad enough to gather the needed resources and make the appropriate decisions to resolve the incident. Such team shall at least include the following:

Title / Position	Name	Telephone #
Highest-ranking Administrative Official		
Chief of Police		
General Counsel		
Human Resources Manager		
Incident Response Manager		
JIF Risk Management Consultant		
JIF Claims Administrator		
Technology Support Contact		
AXA XL Data Breach Hotline		855-566-4724

Please verify with your breach advisor/counsel that their firm will be handling the required breach notifications including, but potentially not limited to, those agencies listed below.

IC3	FBI Internet Crime Complaint Center: https://www.ic3.gov/
NJ Cybersecurity and Communications Integration Cell (NJCCIC)	Incident Reporting: https://www.cyber.nj.gov/report 609-963-6900x7865

4. Incident Response Phases

A. Detection, Reporting, & Analysis

1. If a user, employee, contractor, or vendor observes a potential Cyber Event they should notify the Incident Response Manager immediately. If the Incident Response Manager is not available, the events should be immediately reported to the highest-ranking administrative official.
2. The Incident Response Manager is responsible for communicating the Incident, its severity, and the action plan to the highest-ranking administrative official.
3. If the Incident Response Manager or the highest-ranking administrative official are not available, a user should isolate the affected devices from the network or internet by removing the network cable from the device. If operating via wireless, turn off the wireless connection. If isolating the machine from the network is not possible then unplug the machine from its power source.
4. If you have determined or suspect the Incident is a cyber security breach, cyber extortion threat, or data breach (*see Definitions Related to Cyber Liability Insurance – Section 4 of this document*) proceed to Step 5. If not, proceed to Step 6.
5. For a cyber security breach, please follow this process:

   If the AXA XL Data Breach Hotline does not answer, leave a message with your contact information. Do not delay in calling the Hotline. When they respond, follow their instructions.

They will refer the matter to a "breach advisor/counsel" (an attorney experienced in cybersecurity incidents) who will coordinate the response. The Breach Counsel will gather information about the Incident and work with you to determine an action plan.

The Incident Response Manager should follow the advice from the Breach Counsel until the issue is resolved.

6. If the Incident is determined not to be a *cyber security breach, cyber extortion threat, or data breach*, the Incident Response Manager should work with the Incident Response Team to assess the Incident, develop a plan to contain the Incident, and ensure the plan is communicated to and approved by the highest-ranking administrative official.
7. The Incident Response Manager should ensure all actions are documented as they are taken and that the highest-ranking administrative official, Incident Response Team, and outside support are regularly updated.

B. Containment, Eradication, & Recovery

Containment is the act of limiting the scope and magnitude of the attack as quickly as possible. Containment has two goals: preventing data of note from being exfiltrated and preventing the attacker from causing further damage.

Immediate triage:

1. Immediately contact technology expert to report the event and follow their instructions. It is now the responsibility of technology expert to notify management of the incident and to execute the security incident response plan.
2. If technology expert is not available, isolate the affected devices from the network or internet by removing the network cable from the device. If operating via wireless, turn off the wireless connection. DO NOT TURN OFF DEVICE OR REMOVE POWER SOURCE unless instructed by technology expert.
3. Incident response team assembles and assesses if the incident is a cyber security breach, cyber extortion threat, or data breach. If it is, or if there is any question the incident may or may not be one, management contacts their JIF Claims Administrator to advise them of the incident and management (or technology support) will call the Cyber Insurer Hotline. Work with the breach coach and the other partners they suggest to help resolve the incident.
4. Document all actions as they are taken.
5. Technology expert should compile the following:
    - List of IP addresses involved
    - Logs
    - User accounts compromised

Eradication is the removal of malicious code, accounts, or inappropriate access. Eradication also includes repairing vulnerabilities that may have been the root cause of the compromise. A complete reinstallation of the operating system (OS) and applications is preferred.

Recovery allows business processes affected by the Incident to recover and resume operations. It generally includes:

- Reinstall and patch the OS and applications.
- Change all user and system credentials.
- Restore data to the system.
- Return affected systems to an operationally ready state.
- Confirm that the affected systems are functioning normally.

C. Forensics

Security incidents of a significant magnitude may require that a forensics investigation take place. Once that need has been established all additional investigation/containment activities need to be directed and/or performed by a forensics specialist to ensure that the evidence and chain of custody is maintained. The highest-ranking administrative official, in consultation with the Incident Response Manager and/or the insurer will advise if engaging a forensics firm is required.

D. Post-Incident Review

To improve the Incident Response processes and identify recurring issues each Incident should be reviewed and formally reported on. The report should include:

- Information about the Incident type
- A description of how the Incident was discovered.
- Information about the systems that were affected.
- Information about who was responsible for the system and its data.
- A description of what caused the Incident.
- A description of the response to the Incident and whether it was effective.
- A timeline of events, from detection to Incident closure
- Recommendations to prevent future Incidents.
- A discussion of lessons learned that will improve future responses.

5. Periodic Review

This policy and associated subordinate procedures will be reviewed at least annually by the Incident Response Manager to adjust processes considering new risks and security best practices. Material changes in this policy should be approved by the highest-ranking administrative official and/or governing body of the organization.

6. Special Situations/Exceptions

Any personally owned devices, such as PDAs, phones, wireless devices, or other electronic devices which have been used to access organizational data and are determined to be relevant to an Incident, may be subject to retention until the Incident has been eradicated.