**Cybercrime Policy for ABC Organization**

Contents

[Introduction 3](#_Toc165489045)

[Policy Background 3](#_Toc165489046)

[Policy Purpose 3](#_Toc165489047)

[Aim 4](#_Toc165489048)

[Objective 4](#_Toc165489049)

[Incident Response – Preparation 4](#_Toc165489050)

[Staffing 4](#_Toc165489051)

[Incident Response Team Composition 4](#_Toc165489052)

[Roles and Responsibilities 5](#_Toc165489053)

[Support from External Experts 6](#_Toc165489054)

[Training 6](#_Toc165489055)

[General Cybersecurity Awareness Training 6](#_Toc165489056)

[Specialized Training for Incident Response Team 7](#_Toc165489057)

[Role-Specific Training0 8](#_Toc165489058)

[Continuous Learning and Improvement 8](#_Toc165489059)

[Detection and Analysis 9](#_Toc165489060)

[Detection 9](#_Toc165489061)

[Analysis 10](#_Toc165489062)

[Incident Categories 10](#_Toc165489063)

[Incident Reporting 11](#_Toc165489064)

[Forensics Analysis tools 12](#_Toc165489065)

[What tool do we use in case of a cybercrime? 12](#_Toc165489066)

[Containment, Eradication, and recovery – Containment 12](#_Toc165489067)

[Containment 12](#_Toc165489068)

[Eradication 13](#_Toc165489069)

[Recovery 13](#_Toc165489070)

[Post-Incident Activity 13](#_Toc165489071)

[Escalation 14](#_Toc165489072)

[Risk Assessment 14](#_Toc165489073)

[Roles and Responsibility 14](#_Toc165489074)

[Policy Conclusion 15](#_Toc165489075)

[References 15](#_Toc165489076)

# Introduction

The ABC Organization is dedicated to maintaining the integrity and security of its data systems. Our business operations, client data, and intellectual property are all seriously threatened by cybercrime. Acknowledging this, ABC Organization has put in place a thorough cybercrime strategy to safeguard against harmful activity and guarantee the availability of its services.

## Policy Background

Because of our dependence on digital technology, ABC Organization must have a strong cybercrime policy in place to protect us from a variety of cyber threats. We created this policy in order to safeguard our operations, respect legal and ethical norms, and preserve stakeholder confidence in response to the rise in sophisticated cyberattacks. This adaptable strategy uses the most recent security techniques and technology to keep ahead of future threats. Our cybersecurity strategy is based on it, which guarantees a safe and reliable digital environment for our company's activities.

## Policy Purpose

By addressing the risks related to cyber attacks, ABC Organization's cybercrime policy aims to provide a strong framework that protects digital assets and maintains operational integrity. Protecting sensitive data and IT infrastructure, adhering to pertinent cybersecurity laws, setting up a strong incident response mechanism, managing cyber risks through ongoing risk assessment and control implementation, raising employee awareness of cybersecurity, and strengthening the organization's resilience to quickly recover from cyber incidents are all goals of this policy. The ABC Organization works to create a safe digital environment that meets its operational needs and strategic objectives by putting these principles into practice.

## Aim

To maintain the confidentiality, integrity, and availability of ABC Organization’s information assets against any form of cybercrime.

## Objective

* To define clear procedures and responsibilities for responding to cyber incidents.
* To minimize the impact of cyber incidents on operations and reputation.
* To ensure that all employees are aware of and comply with the cybercrime policy.

# Incident Response – Preparation

## Staffing

For ABC Organization to be able to respond to cyber incidents quickly and effectively, incident response personnel is essential. The following is how the company will arrange its workforce:

### Incident Response Team Composition

The person in charge of the incident response team is the chief information security officer (CISO). In addition to making sure cybersecurity regulations are followed, this position is in charge of managing the reaction to significant events and supervising the overall cybersecurity strategy.

Security analysts keep an eye out for security lapses in the organization's networks and systems and look into any unusual activity that may be noticed. They are essential to the incident response's early detection and analysis stages.

Network engineers are responsible for making sure that the network infrastructure is safe against intrusions. They are essential for putting into action modifications that segregate impacted systems in order to contain the event during it.

IT help Specialists: These members of the team guarantee minimum interruption to company operations by offering technical help. They support the implementation of containment tactics and aid in service restoration and recovery.

Legal Counsel: When handling the legal ramifications of cyberattacks, particularly those involving data breaches that might expose personal data, legal counsel is crucial. They make certain that the incident response complies with all applicable rules and legislation.

Officer of Communications: This position is in charge of overseeing both internal and external communications. The communications officer keeps the organization's security and reputation intact while making sure all relevant parties are informed about the occurrence and its effects.

Human Resources: HR officers help with employee communications and handle any personnel-related concerns that may come up. They also assist in making sure that staff members obtain sufficient cybersecurity training.

### Roles and Responsibilities

Coordination and Quick Reaction: Every team member has a pre-planned course of action for all kinds of situations. This guarantees a well-thought-out and prompt reaction to reduce harm.

Availability Around-the-Clock: The incident response team works in shifts to provide coverage around-the-clock. It is essential to always have qualified staff on hand due to the unpredictability of cyberattacks.

Ongoing Education: To remain current on the newest cyberthreats and countermeasures, team members of the incident response division participate in ongoing education. Participating in simulated cyberattack situations and doing routine exercises are part of this.

### Support from External Experts

The Incident Response Team may sometimes be augmented by outside specialists. These could consist of:

Digital forensic specialists are crucial when in-depth investigation is required to determine how a breach happened and how to stop it from happening again.

Cybersecurity Consultants: Consultants may help by reviewing and refining the organization's incident response plans or by offering further knowledge in certain fields.

ABC Organization can successfully manage and minimize the effects of cyber events by making sure the Incident Response Team is well-defined, well-composed, and adequately supported. The goal of this staffing approach is to preserve business continuity and safeguard the organization's information assets by using a variety of skills and competencies.

## Training

Effective preparation and management of cybersecurity crises heavily relies on training. The goal of ABC Organization's training program is to provide all staff members with the information and abilities they need to support the company's cybersecurity resilience, with specific training intended for individuals who deal directly with incident response. The following essential elements are included in the program:

### General Cybersecurity Awareness Training

**Objective:** To raise overall awareness about cybersecurity among all employees.

**Frequency:** Annually, with quarterly refreshers on specific topics or recent threats.

**Content:**

* Basics of cybersecurity: Understanding the importance of security in the digital workplace.
* Identifying phishing and social engineering attacks: How to recognize and report suspicious emails or messages.
* Password security and management: Best practices for creating and managing strong passwords.
* Secure browsing and email practices: Guidelines for safely navigating the web and handling email.
* Mobile device security: Best practices for securing personal and company-issued mobile devices.
* Data protection: Understanding the importance of protecting sensitive and personal information, both of customers and the organization.

### Specialized Training for Incident Response Team

**Objective:** To equip the IRT with the skills and knowledge needed to respond effectively to cyber incidents.

**Frequency:** Bi-annually, with additional sessions following significant changes in technology or processes.

**Content:**

* Advanced incident detection: Training on the latest tools and techniques for detecting breaches and security incidents.
* Incident analysis and decision making: How to analyze the scope and impact of an incident and make critical decisions under pressure.
* Hands-on simulations: Conducting mock drills that simulate various types of cyber incidents to provide practical experience in incident handling.
* Legal compliance: Training on relevant laws, regulations, and company policies regarding data breaches and cybersecurity.
* Communication strategies: Effective communication techniques during an incident, including internal communication with staff and external communication with media and stakeholders.

### Role-Specific Training0

**Objective:** To provide role-specific cybersecurity knowledge that enables employees to fulfill their specific responsibilities securely.

**Frequency:** Annually, or as new roles are introduced or significantly modified.

**Content:**

* IT staff: Advanced security measures, system monitoring, and endpoint protection.
* Human resources: Securing employee data and training on handling confidential information.
* Finance team: Best practices for securing financial transactions and protecting against fraud

### Continuous Learning and Improvement

**Objective:** To keep the training program and the organization's response capabilities up-to-date with the evolving cyber threat landscape.

**Method:**

* Regular updates to training content based on new threats, vulnerabilities, and incidents.
* Feedback loops from training sessions to identify areas for improvement and to adapt training methods and content.
* Subscription to cybersecurity newsletters, webinars, and participation in relevant conferences and workshops to stay informed about the latest in cybersecurity.

# Detection and Analysis

### Detection

**Objective:** To detect any unauthorized access, activity, or potential security incidents in real-time.

**Tools and Technologies:**

* **Intrusion Detection Systems (IDS):** Deploy IDS to monitor network traffic for suspicious activity and known threat patterns.
* **Security Information and Event Management (SIEM) Systems:** Use SIEM tools to collect and analyze logs from various sources within the organization's IT infrastructure, providing a holistic view of the security state and alerting on anomalies.
* **Endpoint Detection and Response (EDR):** Implement EDR solutions on all endpoints to detect, investigate, and respond to potential threats on individual devices.
* **Phishing Detection Tools:** Use specialized software to detect and quarantine phishing emails and other social engineering attempts.

**Procedures:**

* Continuously monitor all detection tools and respond to alerts promptly.
* Regularly update detection tools to recognize the latest malware and attack vectors.

### Analysis

**Objective:** To analyze detected incidents to understand their nature, scope, and potential impact.

**Approach:**

* **Initial Assessment:** Quickly determine the severity and credibility of the alert to prioritize response efforts.
* **Deep Dive Analysis:** Conduct a thorough investigation into the origin, method, and extent of the breach. This may involve analyzing network traffic, reviewing access logs, and examining affected systems.
* **Impact Assessment:** Evaluate the potential impact on data integrity, system availability, and overall business operations.

**Tools:**

* Forensic analysis tools like EnCase and FTK for in-depth examination.
* Log analysis tools integrated within SIEM systems.

### Incident Categories

Incidents are categorized to streamline the response process according to their nature and severity. Typical categories include:

* **Category 1 - Critical:** Includes major data breaches, ransomware attacks affecting core systems, or incidents impacting sensitive customer information.
* **Category 2 - High:** Involves unauthorized access to restricted areas, significant malware infections, or denial of service attacks that do not cripple critical systems.
* **Category 3 - Medium:** Encompasses incidents like virus infections that are quickly contained, phishing attempts without data loss, or minor policy violations.
* **Category 4 - Low:** Generally includes probing attempts or detected activities that are thwarted by standard defenses without any impact.

### Incident Reporting

**Objective:** To ensure that all incidents, regardless of size, are reported and documented in a timely and precise manner.

**Procedure:**

* **Immediate Reporting:** Employees are required to report any suspected security incidents immediately to the IT department or directly to the Incident Response Team.
* **Standardized Forms:** Use standardized forms for incident reporting to capture all relevant details such as the time of detection, systems affected, and initial impact assessment.
* **Documentation:** Maintain comprehensive records of the incident from detection to resolution as part of the organization's incident response log.

**Communication:**

* Ensure clear lines of communication are maintained during the reporting and subsequent handling of the incident. This includes internal notifications and, if necessary, communication with external stakeholders like clients, regulatory bodies, or the public.

# Forensics Analysis tools

Tools for forensic analysis are essential to the investigation of cyber events because they enable the in-depth review of digital data, which aids in determining the perpetrator and method of an attack. These instruments are also essential for guaranteeing the accuracy of the evidence in future court cases.

# What tool do we use in case of a cybercrime?

* Use EnCase for desktop and laptop analysis.
* Employ FTK for rapid data processing.
* Utilize Wireshark for network breach analysis.
* Turn to Cellebrite for mobile device forensics.
* Consider X-Ways for handling complex datasets.
* Utilize Autopsy for comprehensive hard drive analysis.

# Containment, Eradication, and recovery – Containment

## Containment

In the case of a cybercrime, the danger must be contained quickly. ABC Organization will quickly isolate impacted computers and use network segmentation to stop the assault from spreading. The hacked accounts and services will not be accessible, and suspicious traffic will be blocked by firewall rules. Stakeholders will be notified internally about containment strategies, guaranteeing a coordinated reaction to reduce further harm.

## Eradication

Eliminating the cyber threat requires determining its underlying source. The ABC Organization will identify compromised systems and assets via a comprehensive examination. We will use specialized technologies to eliminate malware and unapproved entry points. To stop future illegal access, vulnerabilities will be fixed and credentials reset. In order to strengthen defenses against such situations, security measures will also be strengthened.

## Recovery

The ABC Organization will concentrate on resuming activities when containment and eradication measures are completed. Backups will be used to restore data and services, and integrity checks will be performed to make sure no threats survive. Extensive testing will be carried out to verify functioning and resolve any remaining problems. We'll put continuous monitoring into place to find and address any new or emerging hazards. Finally, in order to find areas for improvement and update the cybercrime policy appropriately, a thorough assessment of the incident response procedure will be conducted.

# Post-Incident Activity

Following the prompt reaction to a cyber attack, ABC Organization will take part in post-event activities to make improvements to future responses and learn from the experience. This entails carrying out an exhaustive analysis of the occurrence, recording the lessons discovered, and revising policies and procedures as necessary. Furthermore, in order to ensure stakeholders of the steps taken to reduce future risks and to be transparent about the occurrence, ABC Organization will contact with them.

# Escalation

The ABC Organization will adhere to established escalation protocols in the case of a serious cyber incident to guarantee that it is dealt with effectively. Depending on the incident's gravity and possible consequences, this might include reporting it to top management, legal counsel, or outside authorities. Throughout the escalation process, open channels of communication shall be maintained to support prompt decision-making and coordination.

# Risk Assessment

ABC Organization will carry out a thorough risk assessment in the wake of a cyber event in order to determine possible vulnerabilities and analyze the incident's effect. The evaluation will take into account several aspects, including the kind of assault, the efficiency of current security protocols, and the possible repercussions for the company and its stakeholders. ABC Organization will put steps in place to reduce risks and improve its overall cybersecurity posture based on the results of the risk assessment.

# Roles and Responsibility

The cybercrime policy of ABC Organization will clearly outline roles and duties in order to guarantee efficient coordination and responsibility during cyber events. The Incident Response Team, which consists of representatives from the IT, legal, and PR departments, as well as specific persons in charge of communicating with external stakeholders, may play important roles. To enable a well-coordinated and effective response to cyber events, each function will have particular obligations delineated.

# Policy Conclusion

In summary, the cybercrime policy of ABC Organization is a flexible and dynamic structure created to defend against online threats and guarantee business continuity. ABC Organization is dedicated to protecting its digital assets and upholding the confidence of its stakeholders in the face of an increasingly complex threat landscape. To this end, the organization has established clear protocols for incident response, put in place strong security measures, and promoted a culture of cybersecurity awareness.

# References

Enhancing the effectiveness of cybercrime prevention through policy monitoring. (2019). Retrieved May 1, 2024, from Journal of Crime and Justice website: <https://www.tandfonline.com/doi/abs/10.1080/0735648X.2019.1691855>

Introduction: new directions in cybercrime research. (2019). Retrieved May 1, 2024, from Journal of Crime and Justice website: <https://www.tandfonline.com/doi/full/10.1080/0735648X.2019.1692426>

Cockcroft, T., Shan-A-Khuda, M., Z Cliffe Schreuders, & Trevorrow, P. (2018). Police Cybercrime Training: Perceptions, Pedagogy, and Policy. *Policing*, *15*(1), 15–33. <https://doi.org/10.1093/police/pay078>

Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Stefano Caneppele, & Aiken, M. (2022). Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. *Forensic Sciences*, *2*(2), 379–398. <https://doi.org/10.3390/forensicsci2020028>