PROJECT CYBERSAFE™

In Partnership With

fellsway group®

Executive Crisis Management & Incident Response Playbook

Version 0.5

CONFIDENTIALITY NOTICE

This document is the property of Fellsway Group (Fellsway Group). This document contains information that is confidential and proprietary to Fellsway Group. In consideration of receipt of this document, the recipient agrees to maintain this information in confidence and not to reproduce or otherwise disclose this information to any person without prior written approval from Fellsway Group. Fellsway Group reserves the right to, upon request, receive back any printed copies of this document or to request confirmation that any electronic copies have been destroyed.

Contents

Executive Cyber Crisis Management & Incident Response Playbook

Purpose

This playbook provides guidance on responding to significant cyber incidents that may disrupt normal operations at the company. It outlines a flexible, standardized approach for coordinated incident management.

Summary

The Cyber Crisis Management & Incident Response Playbook is designed to help the company respond to significant cyber incidents with the potential for severe, negative impacts. It provides a standardized core mechanism for coordinated and collaborative incident management, ensuring effective coordination using common processes and systems.

The playbook includes five key components: Core Team Model, Decision Responsibility, Key Actions, Information, and Communication.

It also details daily operations, roles, and responsibilities for various teams, including Legal, Technology & Security, Customer Relations, and Other Teams.

Structure

Cyber Crisis Management consists of five key components:

1. **Core Team (CT) Model:** Identifies who is involved in the response.
2. **Decision Responsibility:** Defines the questions and decisions each Core Team member is responsible for.
3. **Key Actions:** Specifies when decisions should be made during the response cycle.
4. **Information:** Details the information available to Core Team members to inform decisions.
5. **Communication:** Guides to whom and when actions should be communicated.

Daily Operations:

- The Incident Coordinator (IC) leads daily Core Team meetings to evaluate facts, raise risks, approve decisions, and identify actions.
- Core Team meetings conclude with actions for each member and their support teams.
- Progress is recorded, risks/issues/impacts identified, and items for decision are escalated for the next meeting.
- Information flows bi-directionally from the Core Team to the CEO and Other Teams.

Roles and Responsibilities

Core Team

Legal

This role will weigh the legal, privacy, and compliance implications of all decisions and recommended actions.

- **Key Prompts & Decisions:**
  - Do we need to engage outside Counsel and/or Cyber Insurance?
  - Did the incident violate any laws or regulatory standards?
  - Who are we legally obligated to notify?
  - What evidence preservation approach will we take?
  - What do we need to consider if there is an insider involved?
  - How do we want to approach law enforcement?
  - Do we need customer NDA or BAAs?
- **Information to Support Decision-Making:**
  - Progress updates on technical incident response
  - Privacy impact per regulations
  - Availability of emergency funding
  - Impact assessments on investments
  - Recommendations for engaging law enforcement
  - Recommendations on privilege status of the investigation
  - Recommendations of privilege status on remediation activities
- **Actions to Take:**
  - Contact Legal
  - Validate scope and timing of notifications – required and voluntary
  - Assess whether data compromised is protected or regulated data
  - Assess what employee, client, and other notifications are required
  - Coordinate regulatory response with Compliance, Office of Civil Rights (OCR) and Overseers
  - Oversee adherence to privacy standards

Technology & Security

This role will assess the impact of technical decisions on overall strategic business risk.

- **Key Prompts & Decisions:**
  - What business operation requires remediation efforts?
  - Should we disconnect or shut down impacted connected components?
  - What strategic considerations exist that may bear on how we respond to this incident?
  - Do we need to engage external technical resources to investigate or respond to the incident?

  - Do we need any additional technology resources to contain or remediate the incident?
  - Should we implement any immediate technology upgrades to improve our security posture?
  - Do we need out-of-band communications?
- **Information to Support Decision-Making:**
  - Progress updates on technical incident response
  - Business impacts due to technical events
  - Impact assessment on specific systems/network resulting from the incident
  - Assessment of estimated recovery time
  - Assessment of recovery costs
  - Exposure quantification
  - Hardening and reinforcement requirements
- **Actions to Take:**
  - Establish/confirm expectations for Core Team operating cadence
  - Evaluate the impact of technical decisions on the customers and operational connected components
  - Assess the risk information from the technical response teams
  - Weigh technical information against Legal and customer considerations
  - Provide periodic updates to CEO
  - Determine whether to bring in external resources

Customer Relations

This role will facilitate decision-making and communications that may directly impact customers and employees.

- **Key Prompts & Decisions:**
  - Are our customers and employees at risk?
  - Should we externally notify customers?
  - Do we need to provide support to customers?
  - Does the incident involve a customer? If so, who else do we need to engage?
  - What information do we need to provide, and how frequently should we update customers?
  - Are we engaging our customers in a way that encourages them to support us?
  - Do we have any obligations to third party vendors?
  - Should we activate our relationships with third party mass-communications vendors for Customer Service support?
- **Information to Support Decision-Making:**
  - Impact assessment of employee safety resulting from the incident
  - Quantifiable impact on employees and customers
  - Employee sentiment and morale throughout the response

  - Assessment and updates of on-the-ground situations for incidents involving data centers or other facilities
- **Actions to Take:**
  - Evaluate and approve messaging to employees and customers
  - Assess the employee and customer impact of the initial incident and the response
  - Review internal and external communications for consistency in messaging
  - Identify who should engage with the media
  - Evaluate the communications impact on employees and customers

Incident Reporting

Incident reporting is a critical component of effective cyber crisis management. The following steps outline the approach to reporting incidents:

1. **Initial Reporting:** Immediately report any suspected or confirmed cyber incidents to the Incident Coordinator (IC). Provide a brief description of the incident, including the date, time, and nature of the event.
2. **Detailed Reporting:** Once the initial report is made, gather detailed information about the incident (see “Information to Support Decision-Making”). This includes technical details, affected systems, potential impact, and any actions taken to mitigate the incident.
3. **Documentation:** Document all aspects of the incident, including the initial report, detailed information, and any actions taken. Ensure that all documentation is accurate and complete. This is where using a Situation Report (or “SitRep”) would be useful.
4. **Communication:** Communicate the incident to relevant stakeholders, including the Core Team, CEO, and Support Teams. Provide regular updates as new information becomes available. This is where you can follow any documented Escalation Procedure.
5. **Follow-Up:** Conduct a thorough review of the incident after it has been resolved. Identify any lessons learned and implement improvements to prevent future incidents.

Post-Incident Review

A post-incident review is essential for understanding the effectiveness of the response and identifying areas for improvement. The following steps outline the approach to conducting a post-incident review:

1. **Review Meeting:** Schedule regular meetings with the Core Team and relevant stakeholders to review the incident and response actions.
2. **Incident Analysis:** Analyze the incident, including the cause, impact, and response actions. Identify any gaps or weaknesses in the response.
3. **Lessons Learned:** Document the lessons learned from the incident. This includes identifying successful strategies and areas for improvement.
4. **Action Plan:** Develop an action plan to address the identified gaps and weaknesses. Implement improvements to enhance the organization's cyber crisis management capabilities.

5. **Reporting:** Prepare a report summarizing the post-incident review findings and action plan. Share the report with relevant stakeholders to ensure transparency and accountability. Follow legal guidance on what is reported and where this report should go.

Training

Training is a vital component of effective cyber crisis management. The following steps outline the approach to training:

1. **Training Programs:** Develop and implement training programs for all Core Team members and relevant stakeholders. These programs should cover incident response procedures, roles and responsibilities, and communication protocols.
2. **Regular Drills:** Conduct regular drills and simulations to test the effectiveness of the training programs. These drills should mimic real-world cyber incidents and provide opportunities for team members to practice their response actions.
3. **Continuous Improvement:** Continuously update and improve the training programs based on feedback from drills and actual incidents. Incorporate lessons learned and best practices to enhance the effectiveness of the training.
4. **Documentation:** Maintain comprehensive documentation of all training programs, drills, and simulations. Ensure that all team members have access to this documentation for reference and review.
5. **Evaluation:** Regularly evaluate the effectiveness of the training programs. Use metrics and feedback to assess the performance of team members and identify areas for improvement.

Appendices

Core & Support Team Contact Sheet

Role and contact information for each team member.

Core Team

ROLE	NAME	EMAIL	OFFICE #	OOB Email	CELL #
Legal					
Technology & Security					
Customer Relations					
Incident Coordinator					

Other Roles

ROLE	NAME	EMAIL	OFFICE #	OOB Email	CELL #
Privacy & Compliance					
Human Resources					
External Counsel					
Information Security					
Cyber Insurance					
Forensics					
Business Units					
Finance					
External Communications					