Cyber Security

Crisis Management Template

For Small to Medium Businesses

RBC® Be Cyber Aware

rbc.com/cyber/business

RBC®

Preamble:

Since most Small to Medium Sized Businesses (SMB's) have difficulty implementing proper security practices – either due to a lack of funds or resources – they are highly targeted as victims of cyber-attacks. Often a single cyber event can be damaging to an SMB by creating irreparable reputational/monetary loss, or even leading to disbandment. This documentation is intended to help close the gap between adequate cyber security practices and SMB's by offering the foundations to proper crisis management and the steps to recovery if a cyber-attack were to occur.

Disclaimer:

The information contained in this document is for general guidance and informational purposes only and it may not be accurate or complete, nor does it constitute legal or other professional advice. This template describes common practices and suggestions which may not be relevant or appropriate in every case. Readers should not consider any advice or guidance contained within this template as comprehensive and/or all encompassing. The contents are not meant as a substitute for legal, cyber security or other professional advice, and should not be relied upon as a complete analysis of the subject matter discussed. Readers seeking further guidance should consult a cybersecurity professional for specific advice about their cybersecurity program and its cyber security incident management plans. All risks related to the cyber security of information technology systems are the responsibility of system owners. No responsibility or liability is or will be accepted by RBC or its affiliates as to or in relation to the accuracy or completeness of the information contained in this document. All rights reserved.

Incident Response: Crisis Management Planning

Considering the possibility of a **cyber event: where an organization's assets or information systems are exploited, tampered with,** or **left inaccessible**, it's critical for SMB's to have a structured plan of action in order to respond as efficiently as possible. To ensure preparedness for a cyber event, SMB's should look to create a **Crisis Management Standard, an index of policies for approaching cyber events,** by following the procedures described below:

Foundations & Pre-Planning Policies for Crisis Management

Cyber Event Categorization

The only way for an organization to handle a cyber event is to adequately prepare ahead of time. SMB's should consider what events might have an impact on their organization and their level of harm if acted upon. The below is provided as an insight for how cyber events are categorized; this form should be adapted to fit the unique cyber events that the organization implementing a crisis management standard could face. The severity level that a cyber event could pose to a SMB is subjective and could differ from the severity levels identified below. Make sure you tailor the Cyber Event Categorization chart to your specific SMB.

Incident Types Examples:

Indication of Cyber Event	Example	Engagement Procedure	Severity Level
Lost Device	Employee loses laptop or mobile device or token		Low
Target of Malpractices: online or by phone	The organization is the target of a phishing or vishing campaign		Medium
System Disruption	Disruption of Organizational Systems (Denial of Service Attack)		High
Credentials Compromised	Executive Credentials are compromised with access to sensitive information or payment authorities		High
Inability to access Information (Ransomware)	Important organizational information is left inaccessible due to encryption malware		Critical
Data Breach	Organizational records and information are found outside of the organization		Critical

Communication with Stakeholders

A **Stakeholder is any entity that is affected by an event, either by impact or provided service.** Stakeholder communication is a critical area of crisis management that bolsters an organization’s ability to respond to a cyber event. Below is a template designed to help guide the process of identifying stakeholders within an organization to best define proper contact, method of contact and the organization's fast response in the possibility of a cyber event.

IT Stakeholders:

Position	Name	Primary Contact Info.	Department

Note: IT Stakeholders should account for key technology-based contacts that work within or to service the organization. (**Examples:** CTO, Service Vendors, IT Department, etc.)

Non-IT Stakeholders:

Role	Name	Primary Contact Info.	Department

Note: Non-IT Stakeholders are internal employees, governing bodies and key points of internal contact, as well as third party points of contact that provide a service to the organization. (**Examples:** Legal, Accounting, Human Resources, Public Affairs, etc.)

Constructing an Engagement Procedure

The engagement procedure is the centerpiece to any crisis management template, detailing how the organization wishes to deal with cyber events of a specific nature and clearly defining goals, strategy and scope of the procedure. Organizations should work to expand upon the pillars of the below engagement procedure to better fit the requirements for a proper response.

Mission Statement: What is the goal?	**Example:** Mitigating Loss of Organizational Hardware Containing Business information (Lost Device.)
Scope of Plan: What areas of the organization are impacted?	**Example:** Employee Line of Business (L.O.B) and any corresponding parties.
Organizational Strategy: How is the organization intending to return to normal business functionality?	**Example:** - Temporarily disable employee account access and require credential changes. - Address possible information loss following organization data loss policies & procedure.
Communications: How do we address impacted parties?	**Example:** Follow Communication Policies and standards to impacted parties.

Note: SMB's should take into consideration the resources they have, their function and assets to provide a plan that meets the unique requirements for response to a cyber event.

Communications Template

Addressing impacted parties, stakeholders and key users for awareness is an important step to crisis management. To best advise these groups, it's recommended that SMB's provide an adequate level of information to end-users without compromising the specifics of a cyber event. At a certain point, to be determined by each SMB, it may become necessary to fully communicate the happenings of a cyber event. The timing of communications and the amount of information disclosed, including notification to any governing bodies, should be thought out in advance and pre-planned.

General Alerting:

- **Current Date & Time**
- **Services effected:** What function of the organization is currently out of operation and who is impacted
- **Nature of the Outage:** Brief description of cause (eg. System X is down, Data XYZ cannot be accessed). You do not need to refer to the specific cyber event itself in this general alert
- **Time/date of service restoration:** Estimated time to regain business operation

Crisis Management Policies – Pulling it All Together

By following the completion of the above templates as the foundation of crisis management, the organization can create effective management policies based on:

- **Cyber Event Categorization:** A prioritized list of possible cyber events unique to the organization.
- **Key Stakeholder Identification:** Key contact information, both technical and non-technical persons in the event their services or contact is needed.
- **Engagement Procedure:** The organization's plan in response to a cyber event, detailing how events will be handled and communicated.
- **Communications Template**: A communications template used to address impacted parties.

SMB's should employ the above documentation relative to the perceived cyber event in order to answer the following prompts:

- **What happened?**
- **What is the impact?**
- **What is our plan?**
- **How are we communicating?**

These questions broadly detail each step to handling a cyber event from initial recognition to resolution. Policy creators should position themselves from the perspective of an employee trying to utilize a crisis management plan, to ensure the needs from the policy are being met. Below is an example of how these questions, paired with the above documentation can be employed to provide an effective plan of response.

Example Documentation of a Crisis Management Policy

Crisis Management – Lost Organizational Device *LOW*

IT Stakeholders

Position	Name	Primary Contact Info.	Department
Access Manager	John Doe	(555) 555-1234	Access Management
Device Provisioner	Jane Doe	(555) 555-9876	Device Provisioning

Non-IT Stakeholders

Position	Name	Primary Contact Info.	Department
Human Resources Consultant	Joan Doe	(555) 555-4334	Human Resources
Communications Lead	Joanne Doe	(555) 555-2317	Communications
Employee L.O.B	*Please Specify*	*Please Specify*	*Please Specify*

Engagement Procedure

Mission Statement:	Mitigating Loss of Organizational Hardware Containing Business information (Lost Device)
Scope of Plan:	Employee Line of Business (L.O.B) and any corresponding parties.
Organizational Strategy:	• Temporarily disable employee account access and require credential changes. • Address possible information loss following organization data loss policies & procedure.
Communications:	Follow communication policies and standards to impacted parties

Communications Strategy:

Contacts**:** Access Management, Employee L.O.B, Impacted Parties

Communications Standard:

- **Priority:** Low
- **Subject:** “Message to Impacted Parties: Lost Device”
- **Body of Message:** An organizational device has been reported missing**,** please follow organization standards to prevent further data loss.
- **Contact Names:**
  - **HR Consultant:** Joan Doe - (555) 555-4334
  - **Access Manager:** John Doe – (555) 555-1234
- **Reminder of Privacy, including Social Media:** *Privacy reminder*