achurch CONSULTING

INCIDENT RESPONSE PLAN TEMPLATE

Executive Summary

The goal of this document is to help the organization be more prepared in the event of a cybersecurity incident. By preparing a plan in advance, the organization will be better prepared to react when a cyber security incident occurs.

Roles and Responsibilities

Organizations need to identify people within their organizations to serve in specific roles in the event of a cybersecurity incident. Three recommended roles include:

- **Incident Response Mana**ger- This person will head the overall organization's response to the incident. In small organizations, this could be the COO or CEO, or a director level position in larger organizations.
- **Tech Lead** – This person may not necessarily be the person who can fix the issue, but can manage the containment, eradication, and recovery to successful conclusion.
- **Communication Manager** – This person is responsible for crafting communication to all parties as identified in the Communication Plan, or additional communication as necessary. In smaller organizations this is often the Incident Response Manager.

Incident Identification

Upon identification of an incident, the reporter on the incident (Customer Service, IT, Vendor) should notify the incident response manager with all information about the incident. It is essential to determine:

- What is the nature of the incident?
- What is the impact/effect on operations?
- How big is the impact?
- What is the cause of the incident?

Severity Definition

Every organization will define its own severity levels- this is just a sample. The severity will help to determine the appropriate response.

1) Incident results in Personal Identifiable Information (PII) for a sizable number of customers/members being released beyond the organization. Theft of over $ 10,000. Data taken from organization servers.
2) Incident results in systems being vulnerable for an extensive period, with possible release of PII, or theft of under $10,000
3) Systems were vulnerable for a period, with no evidence of a break in, limited amount of PII exposed.

Communication Plan

The communication plan may differ based on the cybersecurity incident; however, the real variable is the severity. Message template can be prepared in advance, leaving specifics to be filled in at the time of the incident.

Severity Level 1

- Notify property authorities / Insurance company
- Immediate Notification of the Board
- E-Mail notification to Organizations/Customer Base

Severity Level 2

- Immediate Notification of the Board or Executive Team and ask for direction
- Notify Authorities / Insurance if required by policy
- Email Notification of affected individual

Severity Level 3

- Notification of the Executive team
- Notification affective individuals

Containment, Eradication and Recovery Plan

Remediation plans can exist for different type of cybersecurity incidents, for example, the remediation for a successful phishing attempt (Training/testing) will differ from a hacker penetrating a firewall (patch/setting changes)

1. Technology Resource/ Vendor to clearly articulate issue details to Incident Response Manager/ Communications Manager
2. Technology Resource/ Vendor to stop/fix any technical issue that resulted in cyber security incident (password change/ security patch / firewall settings)
3. Technology Resource/Vendor to put in place corrective action to prevent repeat of cybersecurity incident

Retrospective

After the issue has been contained, eradicated, and recovery is under way, the organization should evaluate its reaction and determine where improvements can be made to reduce future risk of a cybersecurity incident and be better prepared in the event of an incident. The Incident Response Plan should be modified as appropriate.