Cyber Crisis Response

A service of Cyber Security Training Company Limited

Cyber Crisis Response Plan Development: Critical Success Factors

By Jeffrey Crump

Today's organizations are faced with a constant barrage of attacks from external threat actors hoping to find a vulnerability in the company's people, processes or technologies. Once found, the threat actors exploit the weakness for a variety of reasons ranging from causing disruptions to business operations to data exfiltration for financial, political or competitive gain.

Defense in depth or layered defense are often used to describe the recommended approach to reducing cyber risk. This requires a combination of people, processes and technologies to remain resilient prior to, during and after an attack. Despite the best intentions – and a sizable investment – we hear stories on a near daily basis about companies being breached. It's cliché but it continues to hold true; it's not if, but when a company will fall prey to an attack and subsequent media-driven persecution.

As such, it's imperative organizations take the time to plan now for how they will respond to a major cyber crisis. With this in mind, I offer the following non-exhaustive list of critical success factors for developing a cyber crisis response plan.

Understand the Differences

For our purposes, a traditional incident response plan details the activities a functional group – typically limited to information technology (IT) – performs during an incident, whereas, a cyber crisis response plan provides an overarching response plan that integrates the functional incident response plans from across an organization (e.g. IT, privacy, corporate communications, general counsel, etc.) to ensure a coordinated response during a major cyber incident.

It's a Collaborative Effort

Developing a cyber crisis response plan requires cooperation and collaboration from different organizational groups. Due to its cross-organizational impact, a qualified project manager should be assigned to lead the plan's development. As with many projects there will be people who will resist and do what they can to cause problems. Having an experienced project manager with the appropriate level of authority and senior management support is critical to breaking down these and other barriers the project will undoubtedly face.

The core strengths an organization should look for in their CCRP project manager are:

- Accountable – for their performance, the performance of their team members and the overall project's performance (e.g. on-time, on-budget, goals achieved)
- Effective Communicator – able to effectively interact with project leadership, key stakeholders, project team members, and business unit leaders
- Creative Thinker – who can help project team members think outside the box to ensure an appropriate level of scenarios are considered while building activity plans
- Thought Leader – with a broad understanding of incident response, crisis management, business operations, risk management, security and information technology

Teams, Teams and More Teams

To ensure the right people are working on the right work at the right time it's ideal to establish a variety of teams that will either be directly involved in the cyber crisis response effort or will be called upon in an ad-hoc manner to support the response teams.

At the top of a response structure we have the company's Board. Reporting into the Board we should have a Cyber Crisis Executive Team. A Senior Executive-in-Charge and an Executive-in-Charge comprise the Cyber Crisis Management team, who reports to the Cyber Crisis Executive Team and oversees the activities of the Cyber Crisis Response Team, the Technical Response Team, and the Cyber Incident Support Team.

Various Working Groups should be established proactively that have responsibility for ensuring ad-hoc requests during the cyber crisis are executed in an expedited manner. These may include technical and non-technical activities.

Templates and Checklists

To save time, reduce stress and minimize chaos it's recommended a variety of templates and checklists be developed and included in the plan. During a cyber crisis these may or may not be used exactly as they were developed but they will nonetheless provide a great place to begin customization in the fog of battle.

Examples include:

- Incident Information Form, which is used by the Lead Incident Handler to convey details about the incident to the Executive-in-Charge (EIC). The EIC verifies the information, cross-references it with pre-defined escalation criteria/thresholds, and uses it to make the decision (or not) to trigger the cyber crisis response plan.
- Cyber Crisis Notification Email Template, which is used by the Executive-in-Charge (EIC) to initially notify the Cyber Crisis Response Team (C^2RT) members that a high severity incident has been confirmed and notify them of the impending initial C^2RT meeting.

Segment the Plan

Given the various elements recommended be included within a CCRP the size of the document may become large. The size of the CCRP may cause a visceral reaction to some employees who may try to dismiss the plan as unusable. However, upon further inspection they would soon realize the majority of the content is supporting information such as templates and checklists contained in appendices and that the core part of the plan is often just a few pages long.

This highlights two important sub-factors: the need to tell the reader how to use the CCRP; and the need to train the appropriate staff on the use of the CCRP.

Tell Them What They Need to Know

A CCRP should include a How to Use This Document section. In this section tell the reader which section(s) of the CCRP they should read based upon their role. This helps the reader by pointing them to the specific information that is most important to them. This is particularly useful if the CCRP is long.

Examples:

Senior Executive-in-Charge (SEIC)

- Section 1 (Cyber Crisis Response Overview), Section 2 (Response Structure) and Section 3 (Response Process Flow graphic only)
- Incident Severity & Lifecycle
- Anatomies of a Cyber Attack and Response

Primary & Backup Functional Incident Response Lead (IRL)

- Section 1 (Cyber Crisis Response Overview), Section 2 (Response Structure) and Section 3 (Response Process Flow)
- Incident Response Plans (Your group's and those groups you work closely with)
- For Reference:
  - CCRP Response Teams Roles, Responsibilities & Contacts
  - CCRP Working Groups
  - Incident Severity & Lifecycle
  - Anatomies of a Cyber Attack and Response

Educate, Test, and Refine

Throughout the project there will be a high degree of collaboration with various functional groups. These groups will have limited exposure to the overall plan while it is in development so it's very important to plan training for the appropriate cyber crisis response team members once the plan is baselined.

Once the plan is baselined tabletop exercises should be conducted with subsets of the functional teams. These exercises will allow the team to validate the activities they initially developed are indeed what is needed. Changes to the CCRP and the individual functional response plans should be expected. This testing is integral part of completing a CCRP.