Cyber Crisis Leadership: Sounding the Alarm

An Executive Education Primer Series

The Red Button

In *Cyber Crisis Management Planning: How to reduce cyber risk and increase organizational resilience* we highlight that as the cyber crisis executive-in-charge (EIC) it's your decision whether to declare a cyber crisis and trigger the use of the cyber crisis management plan (CCMP). Few events in a crisis leader's professional career will so clearly bring back childhood memories of the Aesop Fable *The Boy Who Cried Wolf*, which teaches us the consequences of repeatedly sounding a false alarm. As an expert on the organization's CCMP, a cyber crisis leader has great appreciation for the activities and visibility caused by pressing the alarm button. A cyber crisis leader should also have an appreciation for the business and professional ramifications if you incorrectly choose *not* to press the alarm button.

Objective Input

The assigned lead incident handler (LIH) is tasked with collecting information about the incident, documenting it (e.g. cyber crisis information form), and sending it to the EIC for decisioning whether to declare a cyber crisis and trigger the CCMP. The foundational information is based on hard facts and provides the EIC the initial objective input about the incident.

The EIC should receive the who, what, when, where, and how of the incident in order to gain some context. Information regarding the nature of the incident (e.g. compromised asset, data breach, data destruction, etc.), the indicators of compromise, and the known impact (e.g. financial, operational, brand, reputation, impacted record count, and third-parties involved/impacted) should be included. A summary of the information technology response should also be addressed in the initial communication with EIC.

This objective information holds immense value, however, it's not enough for the EIC to make a decision.

Subjective Input

The EIC, as a cyber crisis leadership executive, is relied up by their organization and teams to use the objective information to initiate some quick discussions with key internal partners and stakeholders in order to round out situational awareness. An organization's internal and/or external legal counsel should be involved in the initial crisis declaration decision and the decision documented.

Very few cyber crises are exempt from legal and/or regulatory risks. The rapid growth of the cyber insurance industry is enough evidence to prove customers and governments are taking the concept of data protection, due care, and due diligence very seriously. Information security professionals too are not immune from litigation.

In our post, Cyber Crisis Leadership: Decision Making, we address the need for cyber crisis leaders to ensure situational awareness during a cyber crisis. Given the fluid nature of a cyber crisis a cyber crisis leader must avoid analysis paralysis and decide whether to trigger the CCMP based on the objective and subjective information known at the time of decisioning.

Fear, uncertainty, and doubt are overused rhetoric during the cyber security product and services sales life cycle; however, a cyber crisis leader's intuition is a powerful trait that should not be suppressed by cognitive biases during the decision-making process.

Decisioning

The good news is that if a cyber crisis is declared and your organization has a CCMP—and have regularly exercised it—the cyber crisis response will enjoy the confidence its structure provides. As noted previously, if a cyber crisis is not declared it's important to document this decision. Also, keep in mind that as the incident evolves a leader's initial decision to not declare a cyber crisis may change. This is perfectly fine; however, exert caution against using this option as a stalling tactic.

Summary

Cyber Crisis Response, a service of Cyber Security Training and Consulting LLC is poised as a thought leader in the field of cyber crisis management. Our book, *Cyber Crisis Management Planning: How to reduce cyber risk and increase organizational resilience* provides a prescriptive, step-by-step approach to developing a CCMP. Our research-backed innovative and unique services are designed to help organizations and its leaders prepare for a major cyber incident.