Cyber Crisis Management, Survival or Extinction?

Yoram Golandsky
CEO @ CybeRisk Security Solutions
ygolandsky@gmail.com

Abstract

'Cyber Incidents' are common in every domain where technology is prevalent. Recurring or sequential incidents are not unusual and are often manageable. Whilst more rare, the incidents that reach crisis levels have been shown to cause an unexpected amount of damage.

Companies need to remain prepared for such cyber crises. This entails not only building an Incident Response Team (IRT) and creating and testing an incident response plan, but mainly establishing the capability to properly manage business crisis triggered by cyber-attacks.

In today's highly interconnected global economy, a major breach can quickly explode into an extinction-level event for any company. We operate in a 24/7, multi-platform news environment which presents organizations with an entirely novel communications challenge. In the past, a crisis might have played out in the media of one country and, in time, spread internationally. Moreover, the cyber domain doesn't have geographical boundaries. Today, a negative story can go around the world in minutes, putting organizations under even more pressure to plan for reputational crises and respond quickly when problems arise.

Cyber Crisis involves additional levels and challenges compared to general crisis management, including the technical aspects, the fact that Cyber Crisis can be hard to detect in time, and the possible cascading effects. To a much greater degree than in cases of general crisis management, there is a vast amount of information that needs to be grasped and organized during instances of Cyber Crisis management.

Effective crisis management requires that managers understand both the sources of crisis events (i.e. cyber incidents) and the strategies and tactics needed to identify and plan for them.

A crisis event rarely occurs "out of the blue." Instead, it usually follows one or more warning signs. Typically, a series of precipitating events occur before a crisis can commence. These events lead to the "trigger event" that ultimately causes the crisis, and in the cyber domain they're typically identified in the SIEM (Security Information and Event Management).

> Adequate Crisis Management planning goes through the five key tasks or challenges that are involved in resolving cyber crisis situations. The tasks are[1], in rough chronological order: sense-making, meaning-making, decision-making, termination, and learning. These tasks can be (unevenly) separated into a loose before–during–after categorization, where the bulk of the actual crisis management happens during the actual crisis. A well-planned and efficiently executed cyber crisis management plan can be the differentiator between cyber breach survival and extinction.

Before a Crisis

Because we're dealing with Cyber Crisis Management, a significant portion of the preparation is focused on the systems that can provide us with prevention and early warning. These include but are certainly not limited to a broad portfolio of technical capabilities, such as, Threat Intelligence, Security Operations Centers (SOCs), Incident Response (IR) and digital forensics capabilities, Security Information and Event Management (SIEM) systems, behavioral analysis, sandboxing, honeypots and more. All of the abovementioned together with ancillary security and risk management capability should lead to the "Situational Awareness" which should be your goal. In short, Situational Awareness is knowing what's going on all around you at all times so you can figure out how best to react when conditions change.

Identify and anticipate the Cyber Crises - Through threat modelling or risk assessment the organization should identify, in advance, potential cyber crises. Threat scenarios should be examined, in addition to the threats you're anticipating it's also advisable to identify "known unknowns" (https://en.wikipedia.org/wiki/There_are_known_knowns) and to at least discuss them. This step is an absolute must otherwise the entire crisis management planning may completely miss the mark.

The Crisis Management Team (CMT) and the Crisis Management Plan (CMP) are the core of an organization's crises planning efforts. Once the CMT is in place, efforts can be made to construct the Crisis Management Plan. The CMP is a systematic way of thinking about organizational crises. Top management support is very important in the development of the CMP and in managing a crisis. Flexibility is favored over a rigid step-by-step procedure. When human, technical, and other unknown elements are integrated, some degree of improvisation is required to discern effectively and act on the situation accordingly.

Brainstorming and drafting a plan - In addition to the CMT gathering senior representatives from all potentially impacted internal functions (IT, security, sales, marketing, finance, ops, etc...) identified in the previous stage, supporting functions such as HR, Legal and most importantly the Crisis Communications Team (PR) should be included for intensive brainstorming sessions on all the potential crises that could occur at your organization. The exercise should include an analysis of the anticipated impact on the various organizational units, as well as the possible implications across legal, finance, operations, sales, marketing, customer care, and other internal and external shareholders.

The outcome from the brainstorming should be the basis for creating an integrated plan that addresses the potential crisis-causing threats identified in threat modeling/risk assessment phase. It should also detail (with flexibility) what each function should do at which stage for any of the scenarios identified, special emphasis should be given to coordination and unison.

[1] As per definition by ENISA

Identify and Train Spokespersons - The message and the person who delivers that message are two critical components. It should be ensured, via an appropriate policy and training, that only authorized spokespersons speak publicly. This shouldn't be "on the job" training!

Develop Holding Statements - In case of any cyber crisis, your stakeholders have the right to know what has happened and in some cases you also have a regulatory or legal mandate to make a full disclosure. A holding statement has to provide the media with an initial statement that sets forth the basic facts about the incident and lets people know that you are actively dealing with the situation. Of course you would need to adjust this to the particular circumstances of the incident and anticipate the implications of each one before you finalize it.

Assign Responsibility - A company needs a single person or function that oversees the technical and non-technical aspects of preparing for and responding to cyber crises. This person should understand how the technical aspects of a breach can impact the entire enterprise, including the follow-on 'risks' it could pose. They should direct the preparation and response in the context of mitigating enterprise risk. That person should also own the plan, be responsible for creating the plan, updating changes, exercising it and more importantly executing it on "D-day." Having it any other way would potentially lead to challenges with coordinating the different parties and poor (costly) execution during the cyber crisis.

Testing and Exercising - The CMT leads training in the area of crisis management. The best plans are worthless if they exist only on paper. Team training should occur at regular scheduled intervals. The CMT needs an exercise that focuses on collaboration with different actors and meaning-making in relation to the general public and investors' relationship. The security organization needs an exercise that focuses on Incident Response and on explaining to the CMT what the problem is. By far the best way to test the CMT and the CMP is War Gaming. War games are about resilience and how well the organization responds to realistically simulated cyber incidents. They help the organization to assess how suitable CMP is and under what conditions they are more likely to fail.

During a Crisis – Show Time!

The IRT has completed the triage and congratulations, you've been breached, what now?

Time to gather the Crisis Management Team (CMT) –

The first step in the formal response to a crisis is to convene the CMT. The length of time managers have to react to a crisis is related to its impact on the organization and its stakeholders. Having a formalized Crisis Management Plan, or protocol (CMP) makes it possible to think and act expediently during the first few hours of a crisis. The CMP is a key strategic organizational tool responsible for initiating the crisis decision-making process by helping to frame the problem, determine the parties responsible for implementing various actions, and develop justifications for the decisions that are made.

Assess the Crisis Situation (Meaning making)

The most important task for the CMT at this stage is to assess the situation so that decisions can be made to mitigate the crisis. Situational assessment refers to the information processing and knowledge creation aspects of crisis management. Some describe it as an awareness of knowing what is going on and then predicting how the crisis may evolve. Situational awareness is critical to understanding the crisis and identifying its dimensions and intensity.

The CMT should collect all relevant information: Learn as much as possible about the situation, including what happened, who was involved, where it took place, and the current status of the crisis. This step should not only occur during the situational assessment but also throughout the duration of the crisis, and should be repeated at set intervals.

Decision Making while continuing with Meaning Making

Assign tasks and continue fact finding. The crisis management team should delegate duties.

Damage Containment

It is important that the CMT does what is feasible to contain the damage inflicted on its internal & external stakeholders, the reputation of the organization, and its assets. This task is the bottom-line goal for all crisis managers.

Damage containment is the effort to keep the effects of a crisis from spreading and affecting other parts of the business. On the "technical side" crisis damage containment & eradication means to quickly stop the spread of the attack and prevent further damage. The CMT role is to allocate resources such as funds and human resources to help contain the damage.

Develop solution alternatives.

Identify possible solutions that can be implemented.

Mitigation Strategies

Once the situational analysis is completed, strategies for managing the crisis can be identified and implemented. Not all strategies will work initially, so care must be taken to reassess the situation on a regular basis. Flexibility must be maintained because a crisis situation can rapidly change. Care should be taken to address the crisis directly and restore confidence with the affected stakeholders.

Implement the chosen solution(s).

Implementation is often the most difficult part of the process. It requires competent people, time, and money. Allocation of sufficient resources is important.

Notification and Communication

Communicate with the media.

The organization should be proactive in meeting with the media and presenting its side of the story. If the organization does not communicate, the media will find the facts of the story elsewhere, a situation that takes control out of the hands of management.

While having pre-prepared statements as a starting point, the Crisis Communications Team must continue developing the crisis-specific messages required for any given situation. The team already knows, categorically, what type of information its stakeholders are looking for and what information should be made available.

Notifying Customers

Customer notification should be made as soon as the ‘Meaning Making’ process has confirmed the scope and nature of the attack, including whether customer information was involved in the crisis.

Notifying Law Enforcement

Based on the circumstances established through investigation, the organization must determine whether and when to notify law enforcement.

Notifying Governing bodies and Regulators

A legal analysis should be made in the preparation to crisis stage and the organization should know at this point which governing body/regulators should be notified, how they should be notified, and in which circumstances. After such notifications, the organization must coordinate with regulators to manage the relationship and repercussions. Listed companies are also responsible for evaluating cybersecurity risks and disclosing these risks to investors as appropriate.

Monitoring Systems.

The CMT must recognize the importance of monitoring the opinions and behaviors of its key stakeholders during a crisis and exercising its own influence when possible. It may be necessary to adjust the message being communicated, the stakeholders being addressed, and the manner in which the leader is communicating.

Intelligence gathering is an essential component of both crisis prevention and crisis response. Knowing what’s being said about you on social media, in traditional media, by your employees, customers, and other stakeholders often allows you to catch a negative “trend” that, if unchecked, can escalate the crisis.

Termination

The major goal at the beginning of a crisis is to minimize potential damage to the firm and its reputation. In some cases the objective may even be to turn any potential negatives associated with the crisis into positives for the organization.

The termination task is where decision makers decide that the crisis is finally over and that the CMT can be disbanded. This does not necessarily mean that every last detail of the crisis has been fully resolved, but rather that what remains can be handled using normal, non-crisis means and methods.

After a Crisis

Review what happened.

Evaluate the decisions that were made and the results that followed. What was learned, and how might such a crisis be handled differently in the future?

The evaluation process is not an activity that occurs only after the crisis ends. Evaluation is a process that begins when the crisis commences and continues throughout its duration. The more the CMT can understand what is and what is not working in the crisis response, the more easily they can adjust their plans in tackling the crisis. Because the evaluation process is so important, the following benchmark questions should be raised:

How has the crisis affected both internal and external stakeholders' behaviors and opinions?

To what extent normal business operations have been affected?

Which crisis response strategies and tactics were effective and which were not?

To sum it up, adequate Crisis Management planning goes through the five key tasks or challenges that are involved in resolving cyber crisis situations. The tasks are*, in rough chronological order: sense-making, meaning-making, decision-making, termination, and learning. These tasks can be (unevenly) separated into a loose before–during–after categorization, where the bulk of the actual crisis management happens during the actual crisis. A well-planned and efficiently executed cyber crisis management plan can be the differentiator between cyber breach survival and extinction.

References

http://www.itgovernance.co.uk/
Freshfields Bruckhaus Deringer llp, crisis communications professionals' survey 2013
https://en.wikipedia.org/wiki/There_are_known_knowns
https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/nis-cooperation-plans/ccc-management