MANDIANT
NOW PART OF Google Cloud

THREAT INTELLIGENCE
WHITE PAPER

4 Phases of Cybersecurity Crisis Communications

The content in this document was originally published in The Defender's Advantage Cyber Snapshot Issue 4.

Communicating during a crisis is tough for even the savviest and most well-prepared organizations. The unique attributes of a cyber attack, and the increasing use of the public domain by threat actors, mean how a victim organization communicates with their stakeholders during an incident can impact their brand long after the technical remediation is wrapped up.

To further complicate the response, the process of managing communications can compete for the time and attention of the crisis responders and executive leaders as the organization works to quickly restore business operations and remediate networks during a cyber incident. Moreover, there is often confusion on the scope of Cybersecurity Crisis Communications. While media relations is a very visible part of the communication strategic response, it is only one audience. In practice, organizations should develop a comprehensive communications strategy that informs all of its internal and external stakeholders.

To avoid communication missteps, particularly at a stressful time when every second counts, it helps to have seasoned cybersecurity crisis communications experts providing advice and expertise to help organizations and their governing boards respond appropriately. As the threat landscape evolves and threat actors incorporate new techniques, Mandiant now offers cybersecurity crisis communications specialists alongside its incident response team to help customers navigate incidents, evaluate stakeholder engagement, and strategize for the associated cascading communications.

What is Cybersecurity Crisis Communications?

Cybersecurity-specific Crisis Communications is a combination of incident response and crisis management operations, where tailored messaging is developed for a variety of stakeholders and channels, with intricately timed delivery. During a crisis, the communications strategy should consider several factors beyond impact to business operations, risk appetite, and the potential for brand or reputation damage. For example, threat actor behavior and intelligence trends are important considerations in deciding how, what, and when to communicate. Sometimes a "strategic non-response" is the best response as certain messaging may tip off the threat actor, causing them to change their tactics, techniques, and procedures.

Trust and brand resilience are notably tested during a cyber incident - and the middle of an incident is not the time to start building trust. Rather, an organization's approach to crisis communications and failure to provide information and be transparent can further erode trust. Communication missteps compound the overall loss and impact to business operations. Therefore, it is imperative to have a strong understanding of what crisis communications is, best practices for response during times of crisis, and how to prepare and plan for game day.

What leads to the best Cybersecurity Crisis Communications response?

From Mandiant's experience, success starts well before day one of a breach or incident. Rather, it is a continual cycle of review, analysis, and refinement of the organization's incident response and business continuity plans. With specific attention to crisis communications, we will share lessons learned from our specialists' first-hand experience addressing cybersecurity crisis communications planning. The cycle of these activities is grouped into four phases — strategic readiness, assurance, response, and post-incident review.

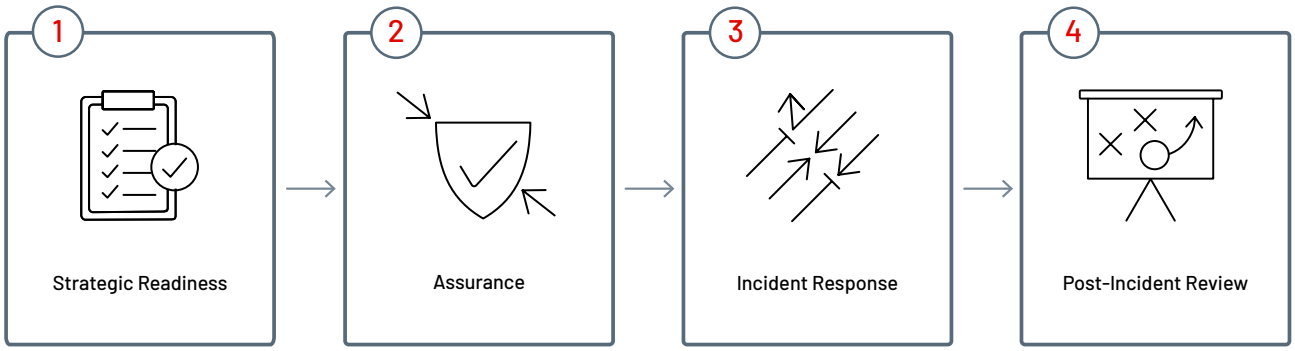
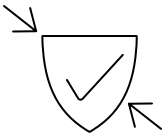


FIGURE 1: Cybersecurity Crisis Communications Phases

Phase 1: Strategic Readiness

First in the cycle is the pre-breach "Strategic Readiness" phase or simply stated, the planning phase. This phase is a foundational and essential activity for all organizations, regardless of size, sector, or location. The approach should be customized to the organization, providing a written and repeatable plan with clearly defined roles and responsibilities, a governance structure with formal decision authority levels, and a framework for response. Like many athletic coaches, for responders it is our playbook and is based on potential activities. This should also be thought of and serve as a living breathing document that is regularly reviewed and shared with those individuals that will be part of the response team during an incident.

It is important to have the right team in the room with clearly defined roles and responsibilities. This team should include representation from across the organization (including HR, Procurement, Communications, Legal, Logistics, and Operations to name a few). You can't anticipate what you'll need, especially when it comes to provisioning hardware, getting out cascading communications, and conducting insightful data impact assessments. The team should also implement a governance and management model, with specific working groups aligned to functional responsibilities. One of the deliverables developed during the planning phase is a Crisis Communications annex to the Incident Response Playbook. This playbook should be specific to the organization and include sections on incident and crisis response, key messaging based on hypothetical scenarios, and stakeholder identification and channel mapping. One additional consideration is the importance of having alternative communication mechanisms, commonly referred to as "out of band" communications, in the event your primary way of communication is compromised. In data breach and cybersecurity incidents, a threat actor may have persistence in the network, requiring leaders and responders to use these alternative communication methods.

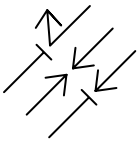


Phase 2: Assurance

The second phase, also part of the proactive and pre-breach response, is the "Assurance" or exercise phase. During this phase, companies should exercise their team's response based on real-world attacks and scenarios. Some states are even moving to mandate this as part of the board response[1]. It certainly helps to bring in well-trained specialists to develop and facilitate exercises based on tailored, realistic scenarios. During these exercises, the team can practice their plan, test their playbook, and identify gaps for remediation. The team members also develop muscle memory in a safe and less stressful environment. Come game time, the consequence of a mistake is more significant and more likely under the higher-pressure situation. It is much easier to stay calm and respond clear-headed when you can anticipate what is next in your expected delivery and execution.

It is also imperative as part of the assurance phase for teams to be receptive to advice and feedback. This phase should also be a recurring activity, and not a "check the box" exercise, with individuals from across the organization, in various job roles and levels, well beyond the executive leadership team and the board. Lastly, the exercise should include the "reinforcement" or surge team, and this should be a deep bench of talent. Response team planning should account for sustained efforts covering at least the first 30 days, with shifts of personnel. The initial response will likely require 24/7 coverage — and to prevent burnout and exhaustion—it helps to have a ready relief roster trained and set for response. It is important to ensure your organization has a communications annex or section in the organization's Business Continuity Plan, the Disaster Recovery Plan, and the Incident Response Plan.

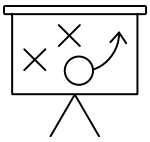
1. New York State Department of Financial Services, DFS SUPERINTENDENT ADRIENNE A. HARRIS ANNOUNCES UPDATED CYBERSECURITY REGULATION, November 2022



Phase 3: Incident Response

The third phase is the reactive phase of "Incident Response." Response execution will be defined by the priority and attention you put into the first two phases. The adage that is you should spend 80% of your time planning, and 20% on execution is certainly true. When the day comes, it is imperative that companies are able to quickly spin up their teams for response. They will know their roles and responsibilities and have a working governance structure to respond. They will be able to organize the requisite information exchange sessions and track the action items and tasks. They will have already mapped their stakeholders and communication channels and be able to quickly assess channel readiness.

The smoothest and most-effective responders are usually those who are well-trained, well-equipped, and have pre-staged the requisite tools ahead of time. They respond with dignity, respect for the team, and consideration for pace — recognizing that it is a marathon not a sprint. They closely collaborate and share information prior to making decisions, but they also don't get into analysis paralysis. Organizations that fail or stumble are typically those not open to advice or feedback, don't recognize their performance failures, or are poorly organized and coordinated in their response and communications.



Phase 4: Post-Incident Review

Managing a breach is hard, both from an emotional and an operational standpoint and many people never want to talk about the incident again. However, as difficult as it may be, it's important to move to the final phase, the Post-Mortem Assessment. This phase starts just as the dust settles —the investigation is complete, the remediation activities restored business operations, and notifications have been made to regulators or victims. Some may also call this the "After Action" or "Lessons Learned" phase and second to planning, it is one of the most important phases to be thorough. Specialists can work alongside clients to identify gaps and solutions to mitigate the impact of future incidents.

Some of the best practices garnered from Mandiant's client cases surfaced during Post-Mortem Assessments. Each incident and each response is different – some have false starts and recover well; others are shining examples of industry best practices. What is important is to share lessons learned for the benefit of others. As Winston Churchill famously said, "those that fail to learn from history are doomed to repeat it."

Read more articles from **The Defender's Advantage Cyber Snapshot**.

Mandiant
11951 Freedom Dr, 6th Fl, Reston, VA 20190
(703) 935-1700
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant
Mandiant is a recognized leader in dynamic cyber defense, threat intelligence and incident response services. By scaling decades of frontline experience, Mandiant helps organizations to be confident in their readiness to defend against and respond to cyber threats. Mandiant is now part of Google Cloud.

MANDIANT
NOW PART OF Google Cloud