Mandiant

DATASHEET

Cyber Crisis Communication Planning and Response Services

Build an effective incident communications approach that protects stakeholders, minimizes risk, and preserves brand reputation

The steps an organization takes to inform, engage and safeguard their stakeholders during a cyber incident significantly impacts a successful business recovery and long term brand reputation. The stakes are rising for victim organizations from threat actors employing non-technical offensive techniques using the public domain—magnifying awareness of the incident and engaging more stakeholders. This approach helps adversaries achieve their mission by increasing reputational risk and applying more pressure upon the victim organization.

Mandiant offers crisis communication services for before, during and after an incident—including multifaceted extortion and ransomware attacks. We deliver program assessments and customized plans that improve crisis communication processes and actions surrounding the non-technical, strategic response elements of a cyber attack.

The following services provide program evaluation, actionable preparedness, and improved response. Each service can be delivered separately or in any combination.

Incident Response

Align communication plans with technical response activities to anticipate key business decisions, mitigate reputational risk, and inform stakeholders.

- Create a crisis communications strategy based on evolving, real-time forensic findings from the technical investigation guided by Mandiant responders
- Perform audience and communication channel mapping to ensure relevant stakeholders are informed during an incident
- Develop communication content that maintains a consistent message tailored to meet the needs of each affected audience
- Support media relations and agency involvement to help prepare for down-stream impact

Strategic Readiness

Develop comprehensive playbooks to guide your incident communication workflows and ensure effective response measures.

- Identify all target audiences, stakeholders, and their specific communication channels
- Establish best practices for a crisis communication team's response working group and define roles, responsibilities, and decision-making processes
- Build new or enhance existing cyber crisis communication response plans and actionable playbooks
- Engage C-suite and Board members during an incident with key decision points tailored to various response scenarios for their specific organization

Real-World Testing

Evaluate existing cyber crisis communication processes, tools, and staff competencies to effectively respond to modern day attacks.

- Conduct executive-level and risk-based tabletop exercises with a focus on non-technical attacker escalation techniques based on real-world scenarios, not hypothetical situations
- Realize crisis communication capability gaps and process conflict points across an existing program
- Receive recommendations to refine existing cyber crisis communication response capabilities

Google Cloud

For more information visit cloud.google.com

M-EXT-DS-EN-US-000493-03