



IBM Security X-Force Cyber Crisis Management Services

A whole-of-business response to a crisis-level cyberattack that escalates beyond traditional incident response and threatens the entirety of your organization

Organizations of all types and sizes face cybersecurity threats and attacks nearly every day. While most attacks remain contained within the IT and security teams, some attacks can expand rapidly beyond being simply a security problem and escalate to becoming a crisis for the business itself. A **crisis-level cyberattack** involves the entirety of an organization. It can damage reputation and brand, disrupt or halt delivery of products and services, and expose customer and employee private information. At their worst, these attacks can cripple an organization permanently.

Successful remediation of a crisis-level cyberattack requires not only adept security technical prowess but a nimble "whole-of-business" response that allows an organization and its executive team to respond effectively, lead the charge, and work in unison—not in silos. Advanced preparation is critical and must include senior management, as planning and testing that encompasses identified members from multiple functions across the organization. This approach ensures that leadership and teams outside of the IT/security functions understand they have important roles to perform, know how to accomplish them, and how their participation

Highlights

- Provides clients a framework to prepare for and respond to crisis-level cyberattacks
- Includes a “whole-of-business” plan that enables distinct business functions to act in unison during a crisis
- Helps preserve reputation, brand and customer loyalty
- Fortifies an organization’s business continuity



can help the entire organization respond to and recover from a crisis-level cyberattack.

With crisis management quickly becoming a required standard, organizations are looking to partner with a leader that can help them build, deploy, and execute a cyber crisis management program.

IBM Security X-Force Cyber Crisis Management Services

IBM Security X-Force Cyber Crisis Management (CCM) Services can help to improve your organization's cyber resiliency to better respond to crisis-level cyberattacks. These services provide industry experts who consult your teams as a trusted partner to build and practice a cyber crisis management plan across your organization, guide them during an actual cyberattack, and create post-attack lessons learned.

X-Force CCM delivers five offering components:

Cyber Crisis Management Program Maturity Assessment

This proactive preparation helps your organization review and enhance its existing cyber crisis management program to assess maturity and growth areas. Cyber crisis experts work hand-in-hand with your teams by conducting best practice reviews, interviewing key stakeholders, and analyzing existing incident response and crisis response plans and procedures. You will receive a detailed roadmap that identifies actions needed to improve your cyber crisis management program and specific recommendations on how to get there.



Cyber Crisis Management Plan Development

For organizations that require building out a full plan, IBM Security X-Force cyber crisis experts work with your organization to develop a cyber crisis management plan that helps your business leaders quickly identify and respond to crisis-level cyberattacks. Clients come away with a customized, carefully considered, and integrated plan developed to ensure that an organization's cyber crisis response capabilities are adequate before a crisis occurs.

Cyber Crisis Management Playbooks

A Ponemon survey, sponsored by IBM Security, found that respondents' security response efforts were hindered by a lack of specific playbooks for common attack types. Most reported that even their technical response plans are either ad-hoc, applied inconsistently, or that they have no plans at all. This lack of planning can impact the duration and cost of security incidents.

Having a playbook in place is being able to fall back on an agreed-upon process for handling a security incident. It distills the knowledge and experience of your most seasoned leaders into a solid, repeatable process that can be followed to the letter by even the greenest of new recruits.

X-Force Cyber Crisis Management playbooks are a proactive preparation that provides prescriptive playbooks *for the executive team* that can enable individual business functions to act in unison to swiftly, and adeptly, resolve a cyber crisis.



Cyber Crisis Management Tabletop Exercises

Once plans are in place and stakeholders can rely on them in case of emergency, the next phase is the testing phase. We start by a dry-run type of exercise known as the Tabletop exercise. Participants will practice their response to crisis-level cyberattacks with skilled facilitator guidance. Based on actual life events, the tabletop exercises will enable your organization to test business processes, procedures, and response; help stakeholders communicate more openly and build relationships across silos. This exercise helps expose gaps in established processes and technologies, and enhance cyber awareness, readiness, and coordination.

Our Capstone Drill: IBM Security Cyber Ranges

Cyber Range Experiences

Simulating an attack down to every detail is the next best thing to a real-life experience. Pilots use simulations, and you likely practiced first if you took CPR courses. While theory on paper is good, sometimes, what might look great on paper, tends to crumble when enough pressure is applied.

Without regularly using and honing skills, muscle memory weakens, and it would be harder to produce a timely response. Executives need to understand more than crisis-response theory. They need to practice their responses, so they know what to anticipate during actual security crisis.

IBM Security Cyber Range experiences are an immersive environment designed to help your organization validate and refine cyber crisis management plans and playbooks. Skilled instructors facilitate and guide customer teams through realistic cyber crisis scenarios in an immersive, highly gamified environment that simulates real-world experience. Clients come away from this



experience with enhanced awareness to how an attack can impact their judgement and decision making when they are stressed, and many things happen at once. It helps them identify where breakdowns might be happening that can be addressed and prevented in real life attacks.



Why IBM Security?

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM Security X-Force® research, provides security solutions to help organizations drive security into the fabric of their business so they can thrive in the face of uncertainty.

IBM operates one of the broadest and deepest security research, development and delivery organizations. Monitoring more than one trillion events per month in more than 130 countries, IBM holds over 3,000 security patents. To learn more, visit [ibm.com/security](https://www.ibm.com/security).

© Copyright IBM Corporation 2022.

IBM, the IBM logo, and [ibm.com](https://www.ibm.com) are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at <https://www.ibm.com/legal/us/en/copytrade.shtml>, and select third party trademarks that might be referenced in this document is available at https://www.ibm.com/legal/us/en/copytrade.shtml#section_4.

This document contains information pertaining to the following IBM products which are trademarks and/or registered trademarks of IBM Corporation:



All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice and represent goals and objectives only.

For more information

To learn more about IBM Security Cyber Crisis Management, please contact your IBM representative or IBM Business Partner, or visit the following website:

<https://www.ibm.com/security/services/incident-response-services>