IBM X-Force cyber crisis management services

A whole-of-business response to crisis-level cyberattacks that threaten your entire organization

Assesses and enhances your cyber crisis management program

Develops an integrative, cross-organizational cyber crisis management plan

Targets and tests response functions with playbooks and tabletop exercises

Validates your plans with a cyber range simulation drill

Organizations of all types and sizes face cybersecurity threats and attacks nearly every day. While most attacks remain contained within an organization's IT and security teams, some attacks can escalate rapidly beyond being simply a security problem to become a *crisis* for the business itself. A crisis-level cyberattack of this nature 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 its worst, such an attack can cripple an organization permanently.

The cyber crisis management services capability available within IBM® X-Force® helps organizations prepare for and respond to crisis-level cyberattacks with confidence. These X-Force cyber crisis management services provide several key capabilities to keep your business safe and secure.

Assess and enhance your cyber crisis management program

This proactive preparation helps your organization review its existing cyber crisis management program to assess maturity and growth areas. Cyber crisis experts work hand in hand with your teams to conduct in-depth document reviews, interview key stakeholders and analyze existing plans and procedures for incident and crisis response. You'll receive a detailed roadmap that identifies gaps and the actions needed to improve your cyber crisis management program, with specific recommendations on how to get there.

Develop an integrative cyber crisis management plan and playbooks

For organizations that require building out a full plan, 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. You'll come away with a customized, carefully considered and integrated plan developed to ensure that your organization's cyber crisis response capabilities are adequate—*before* a crisis occurs.

Having a playbook in place provides the ability 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.

Test and refine your response with tabletop exercises

Once plans are in place and stakeholders can rely on them in case of emergency, next comes the testing phase. We start with 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, tabletop exercises enable your organization to test business processes, procedures and responses; help stakeholders communicate more openly; and build relationships that break silos. This type of exercise helps expose gaps in established processes and technologies, and enhance cyberawareness, readiness and coordination.

Validate your plans with our capstone drill: IBM X-Force Cyber Range
Simulating an attack at a detailed, granular level is the next best thing to a real-life experience. Pilots use simulations, and you've likely practiced administering first aid if you've taken any CPR-certification courses. Although committing theory to paper is good practice, sometimes, what looks great on paper can crumble when enough pressure is applied.

Without regularly using and honing skills, muscle memory weakens, and it might 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 an actual security crisis.

X-Force Cyber Range experiences create an immersive environment designed to help your organization validate and refine cyber crisis management plans and playbooks. Skilled instructors facilitate and guide your security teams through realistic cyber crisis scenarios in an immersive, highly gamified environment that simulates real-world experience. Your teams come away from this experience with enhanced awareness of how an attack can impact their judgement and decision-making when they're stressed and many things are happening at once. It helps them identify where breakdowns might be happening that can be addressed and prevented in real-life attacks.

In today's dynamic threat landscape, cyber crisis management services within X-Force help your organization prepare for crisis-level attacks. Our expert-led services enable customization of crisis plans, creation of attack playbooks, tabletop exercises and simulated attacks. Investing in these services can minimize reputational damage, financial loss and operational disruption, helping ensure swift recovery. Cyber crisis management is not just a line item in your IT spend, but a critical investment in organizational resilience and success.

IBM X-Force can help you through all aspects of a threat. X-Force hackers adopt the mindset of threat actors, X-Force incident responders help detect and counter threats and X-Force analysts research and examine threats. X-Force is an industry leader in cybersecurity, supported by expert professionals with decades of experience in incident management, vulnerability management and threat intelligence. The X-Force team has assisted organizations with many of the world's largest breach investigations across 17 industries in the public and private sectors, with over 20,000 security professionals participating in X-Force Cyber Range experiences.

To learn more about cyber crisis management services within X-Force, contact your IBM representative, schedule a briefing or inquire about a cyber range experience.

Explore X-Force →

This document is current as of the initial date of publication and may be changed by IBM at any time.

Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

No IT system or product should be considered completely secure, and no single product, service or security measure can be completely effective in preventing improper use or access. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.