5 Steps to Avoid a Cyber Incident and Save Your Company Millions

Most security professionals cite cybersecurity as a primary concern but don't necessarily have the tools to prioritize it and effectively protect their companies. Implementing these five steps will help to avoid significant disruption of service and reputational damage, while saving your organization millions of dollars.

The average cost of a data breach is **$4.35 million**

By 2025, a lack of talent or human failure will be responsible for over half of significant cyber incidents.

STEP 1
Set a cybersecurity budget

The goal of cybersecurity is not to achieve perfect protection, but to mitigate risk and minimize the impact of a successful attack.

INVEST IN:

- Cyber defense tools
- Incident response and digital forensics teams
- Proactive measures and services (red team and tabletop exercises)
- Cyber insurance

Conducting due diligence in evaluating your incident response team is critical and can make a difference between saving your company or losing it in a significant cyber incident.

STEP 2
Assess your incident response team's capabilities

The first priority in any incident response program is assessing your team's response capabilities.

THE ASSESSMENT SHOULD INCLUDE:

- Incident detection and identification
- Containment and eradication
- Recovery and restoration
- Post-incident analysis and reporting

STEP 3
Define your incident response plan

REPORT — Disclose the incident to the appropriate authorities, such as law enforcement, regulatory agencies, etc.

RESPOND — Restore systems, recover data, and implement additional security measures.

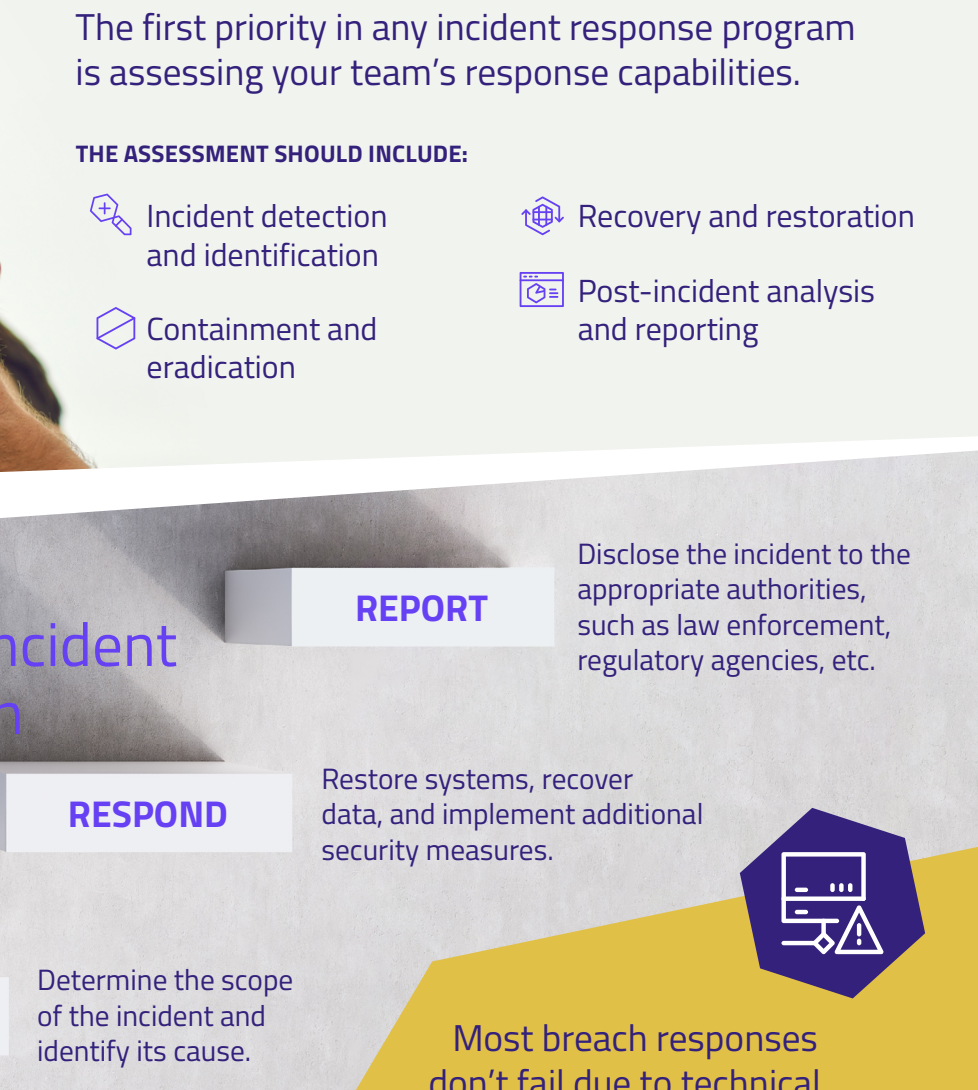
INVESTIGATE — Determine the scope of the incident and identify its cause.

STEPS TO TAKE WHEN RESPONDING TO A CYBER INCIDENT:

CONTAIN — Isolate the affected systems to prevent the incident from spreading.

Most breach responses don't fail due to technical reasons or knowledge gaps, but due to undefined or untested incident response plans (IRPs).

STEP 4
Evaluate your cyber insurance policy



STEP 5
Consider implementing proactive services

Actionable steps to test your security controls, strengthen your cybersecurity posture, and mature your incident response plan:

- Penetration Tests
- Vulnerability Management
- Tabletop Exercises
- Red Team
- Security Assessments
- Threat Hunting
- External Risk Analysis
- Threat Intelligence
- Cyber Awareness Training

SecurityScorecard's Cyber Resilience Services

SecurityScorecard Cyber Resilience Services help organizations build, defend, and strengthen cyber security and third-party risk management programs. Our Cyber Resilience Services team brings 100+ years of collective experience in cybersecurity investigations across government and private sectors with specialties in Digital Forensics, Incident Response, Penetration Testing, Red Teaming, Tabletop Exercises, and Third-Party Risk Development.

To increase your organization's cyber resilience, talk to an expert:

GET STARTED

Security Scorecard