CrowdStrike Services

CROWDSTRIKE

Incident Response Executive Preparation Checklist

How to Use This Template

CrowdStrike's Incident Response Executive Preparation Checklist provides a starting point. It identifies many of the common crisis management activities that business leaders and executives should consider when responding to a cybersecurity incident. It should be updated to focus on the activities that are most important to your organization and to identify the parties responsible for doing them. You may also consider developing checklists specific to each key leadership role to focus on their responsibilities and clarify who does what.

Read our accompanying blog post:

CrowdStrike Services Offers Incident Response Executive Preparation Checklist

Overview

Executives tend to be adept, experienced crisis managers. Navigating a severe cybersecurity incident requires applying those same skills and processes. However, cyber-generated crises also pose unique challenges. To be prepared, executives must understand cyber-specific decisions, the factors that inform them and the consequences they can lead to. This checklist provides guidance for executives to prepare for and manage cybersecurity crises.

Before an Incident

□ **Maintain Executive Readiness: Train and Test**

Your Information Security and Legal teams should coordinate with executive stakeholders to manage a list of cyber crisis response documents, where to find them and how to use them. Organizations should hold tabletop exercises annually with executive, management and technical-level staff to pressure-test their response plans in a simulated environment.

Responsible Party: ______________________________

□ **Implement Out-of-Band Communications**

Your Information Security and Legal teams should identify communications channels to use if normal channels are down or teams suspect an attacker has compromised them. The solution should allow for notifications, conference bridges and document sharing separate from the organization's network.

Responsible Party: ______________________________

□ **Evaluate Cyber Insurance Coverage**

Your Legal and Risk teams should review any relevant cyber insurance policy to understand what response efforts, cyber impacts and third-party support are covered. Legal should review exclusion clauses in detail to confirm they will not affect coverage for different types of incidents or threat actors.

Responsible Party: ______________________________

□ **Review Regulatory and Contractual Requirements**

Your Information Security, Legal and Operations teams should periodically review regulatory and contractual requirements for responding to and disclosing cybersecurity incidents. These may be government requirements, customer requirements or partner requirements.

Responsible Party: ______________________________

□ **Retain Third-Party Support**

Your Information Security and Legal teams should confirm they have identified vendors to cover at least external legal counsel, crisis communications and digital forensics and incident response support. Some organizations also wish to identify ransom negotiation firms or eDiscovery firms for data breaches. Keeping vendors on retainer can increase assurance through guaranteed response times.

Responsible Party: ______________________________

During an Incident

□ **Review the Incident's Severity and Scope**

Your Information Security, Legal and Operations teams must determine a cybersecurity incident's potential or realized impact. For significant incidents, executives should review this assessment, identify any additional effects and assess how long the business can sustain operations, given the impacts to affected systems. Executives should be a key part of an ongoing review to determine the incident's materiality to the organization.

Responsible Party: ______________________________

□ **Invoke Attorney-Client Privilege as Relevant**

Your Legal team should determine whether and how to invoke attorney-client privilege for internal actions as well as with third parties or vendors, if relevant. Legal should provide guidance on document markings, preferred methods of communications, evidence retention and requirements to limit participants in the investigation.

Responsible Party: ______________________________

□ **Set Operational Priorities**

Leadership must communicate operational priorities based on the business impact of the incident. This can include financial, legal, reputational and other company or industry-specific forms of impact.

Responsible Party: ______________________________

□ **Draft and Review Internal and External Communications**

Your Communications, Information Security, Human Resources and Legal teams should draft and review communications regarding the incident. This includes communications for internal and external audiences (e.g., employees, partners, the general public, media, customers and shareholders). Communications teams should templatize and receive pre-approval for cyber-specific holding statements that can be easily updated during an incident.

Responsible Party: ______________________________

□ **Activate Third-Party Support**

Your Information Security and Legal teams should activate third-party support as necessary. This may include external counsel, eDiscovery firms, third-party incident response providers and ransom negotiators.

Responsible Party: ______________________________

□ **Communicate with the Board of Directors**

Executives may need to notify the Board of Directors of a cybersecurity incident and, depending on the severity, provide additional information or seek the Board's guidance in certain decisions. Read CrowdStrike's perspective on how to engage the Board in cybersecurity.

Responsible Party: ______________________________

□ **Oversee Regulatory and Contractual Compliance**

Your Legal and Compliance teams should confirm that any actions taken during the incident satisfy regulatory or contractual requirements (e.g., notifications to impacted parties). This should include reviewing any information that is shared with outside parties.

Responsible Party: ______________________________

□ **Determine Whether to File an Insurance Claim**

Your Information Security, Legal and Finance teams should consult relevant stakeholders to review insurance coverage, decide whether and when to file a claim, and facilitate notification of the insurer. Multiple types of coverage may apply, depending on the incident. Your insurer may also connect you with a breach coach or recommend external counsel.

Responsible Party: ______________________________

□ **Determine Whether to Involve Law Enforcement**

Your Information Security and Legal teams should decide whether to proactively involve law enforcement and, when necessary or useful, respond to inquiries and notifications from law enforcement agencies.

Responsible Party: ______________________________

□ **Revisit the Incident Severity and Scope**
As new information becomes available, reassess each of the preceding tasks.
Responsible Party: ______________________________

After an Incident

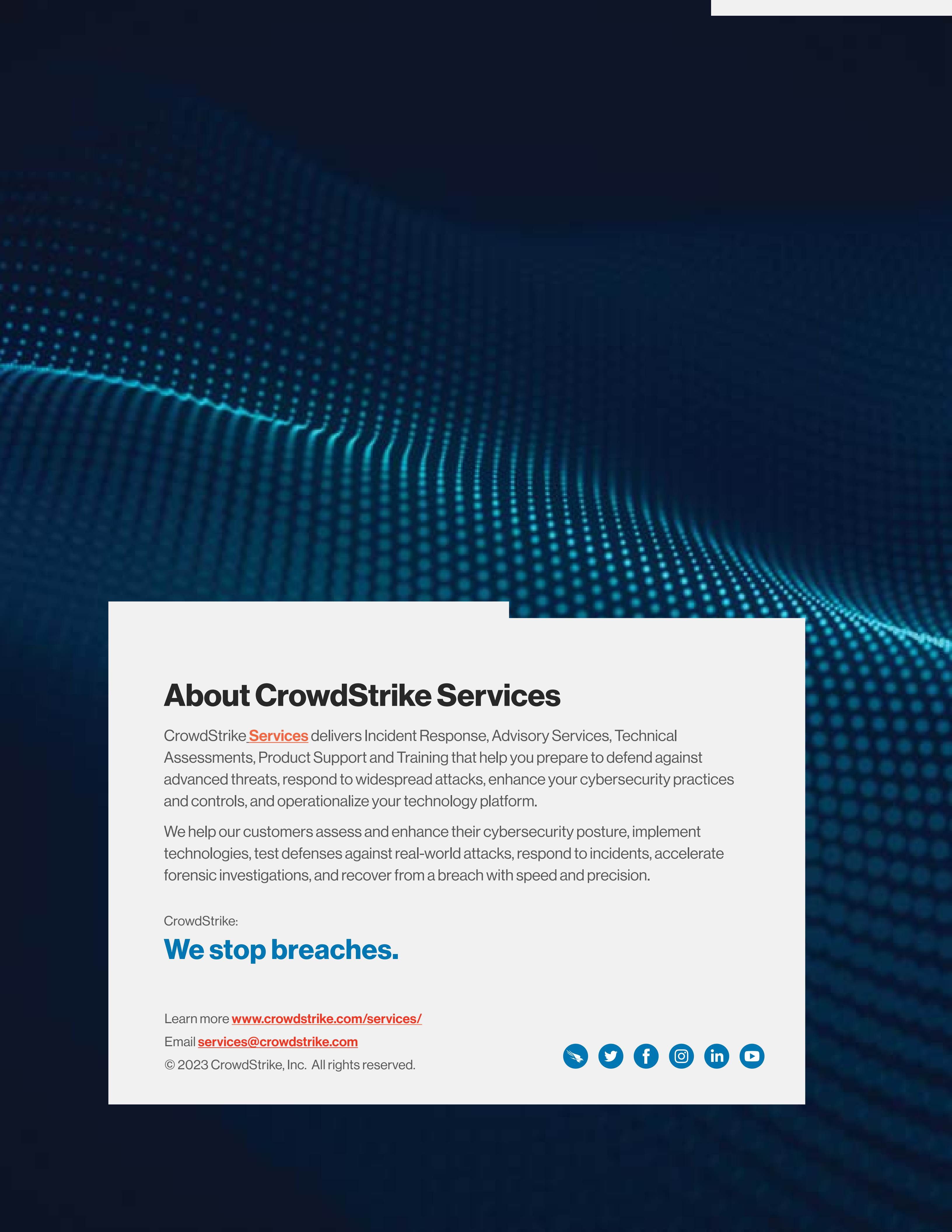
□ **Review Regulatory and Contractual Requirements**
After the investigation is complete, your Legal and Compliance teams should manage fulfillment of any regulatory and contractual obligations.
Responsible Party: ______________________________

□ **Participate in After-Action Reviews (AAR)**
Executive stakeholders should join an AAR to evaluate the response process and identify any necessary improvements or lessons learned. Executives should play a key role in overseeing action items from the review.
Responsible Party: ______________________________

□ **Address Post-Incident Fallout**
Cyber incidents can have lasting effects. Executive leadership may be required to restore customer confidence, rehabilitate the public image, or address legal and regulatory liabilities.
Responsible Party: ______________________________

□ **Review Remediation Plans**
Executive stakeholders should review and approve remediation plans for their respective areas of responsibility to validate that appropriate personnel address underlying issues in a timely manner.
Responsible Party: ______________________________

Discover more about CrowdStrike Services Tabletop Exercises to prepare your executives and Board of Directors for cybersecurity incidents.



About CrowdStrike Services

CrowdStrike Services delivers Incident Response, Advisory Services, Technical Assessments, Product Support and Training that help you prepare to defend against advanced threats, respond to widespread attacks, enhance your cybersecurity practices and controls, and operationalize your technology platform.

We help our customers assess and enhance their cybersecurity posture, implement technologies, test defenses against real-world attacks, respond to incidents, accelerate forensic investigations, and recover from a breach with speed and precision.

CrowdStrike:

We stop breaches.

Learn more www.crowdstrike.com/services/

Email services@crowdstrike.com