CrowdStrike Solutions

CROWDSTRIKE

LESSONS LEARNED: HOW TO SURVIVE A BREACH

By Roxanne Austin

1. FOCUS ON ROR VS. ROI.

The risk of (and cost to repair) damage to the reputation of the enterprise trump the traditional ROI discussions we use to justify projects or investments. The time and money spent to repair the damage after a major incident (Return of Reputation) is staggering .

> **PRO TIP FROM ROXANNE**
>
> "Consider the legal, regulatory, customer, employee and financial impact — it adds up very quickly."

2. ANY WEAKNESS IS MAGNIFIED 10X+ DURING A CRISIS.

Any weakness in leadership, process, communication or crisis plan will be glaringly apparent and magnified during times of stress.

> **PRO TIP FROM ROXANNE**
>
> "Existing weaknesses in all these areas — some known and others that may not be apparent — will come to light when the breach unfolds. What you don't know CAN hurt you."

"Existing weaknesses in all these areas — some known and others that may not be apparent — will come to light when the breach unfolds. What you don't know CAN hurt you."

3. HAVE A COMPLETE CRISIS MANAGEMENT PLAN — NOT JUST A BUSINESS CONTINUATION PLAN.

Cyber is an enterprisewide risk, not an IT risk. A robust and complete Crisis Management Plan for a major cyber event should be prepared, tested and updated regularly. It should include all applicable functional areas and have deep engagement across the business.

> **PRO TIP FROM ROXANNE**
>
> "In my experience, our focus was too heavily weighted on business recovery and continuation, and we were caught flat-footed on the media response, customer communications, employee impact, etc. The plan needs to be tested and war-gamed beyond a perfunctory 'tabletop exercise.'"

4. FOCUS ON THE JUDGEMENT AREAS.

Buying tools and capabilities, or hiring third-party assistance, is only part of the story: The judgements made in setting up, establishing rules of engagement, and implementation are critical.

PRO TIP FROM ROXANNE

"Who determines the level of acceptable risk? It is often these judgments that kill you!"

Who determines the level of acceptable risk? It is often these judgments that kill you!

5. WHO, WHAT AND WHEN

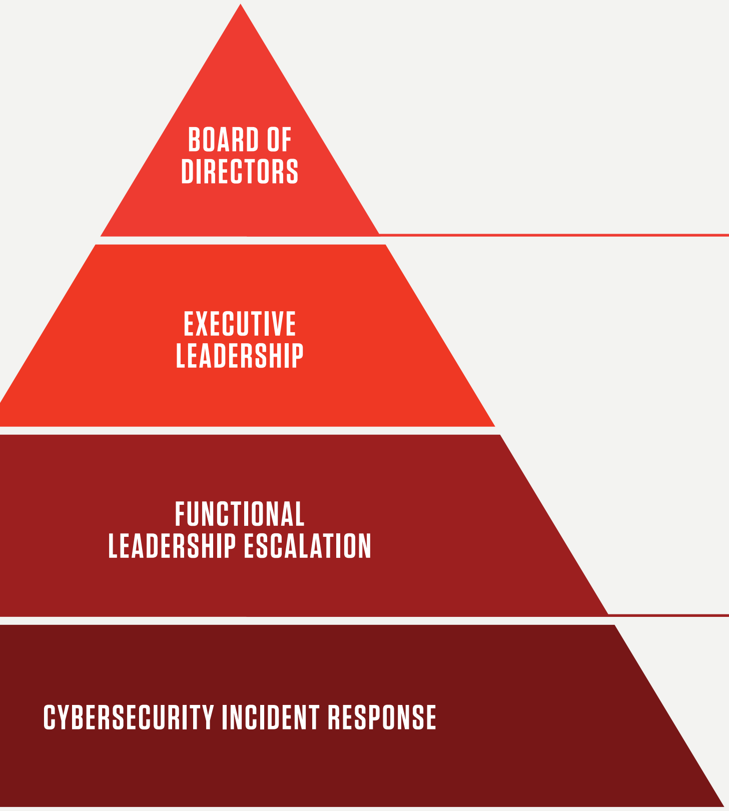
What is your incident governance and escalation process, and is it clearly defined? Is it known to all parties?

PRO TIP FROM ROXANNE

"It wasn’t, in our case. Below is an example of an Incident Escalation Pyramid that can help guide your governance and escalation priorities."

INCIDENT ESCALATION PROCEDURES ARE CLEARLY DEFINED ACROSS THE ORGANIZATION

SECURITY INCIDENT ESCALATION PYRAMID EXAMPLE



BOARD OF DIRECTORS

EXECUTIVE LEADERSHIP

FUNCTIONAL LEADERSHIP ESCALATION

CYBERSECURITY INCIDENT RESPONSE

LEVEL 3

- Final level of escalation for issues that may have a significant, material, operational, brand, or reputational impact

LEVEL 2

- Incidents with a potential broad impact are escalated to functional leadership and, if significant, the Executive Leadership Team
- Critical data identification and protection, crisis management exercises and vendor engagement occurs across all functions
- Key decisions and Information Security Program metrics are reviewed quarterly

LEVEL 1

- Incidents requiring investigation are escalated for action, containment and remediation

ROXANNE AUSTIN

President & CEO, **Austin Investment Advisors**
Audit Committee Chair, **CrowdStrike Board of Directors**

Roxanne Austin is President and CEO of Austin Investment Advisors, a private investment and consulting firm, and chairs the US Mid-Market Investment Advisory Committee of EQT Partners.

Ms. Austin serves on the Board of Directors of Target Corporation, Abbott Laboratories, AbbVie, and Teledyne Technologies and formerly, the Board of Ericsson.

She was named 2018 Director of The Year – Corporate Leadership and Service by the Forum for Corporate Directors, and one of the most influential directors in the boardroom by the National Association of Corporate Directors. She is co-chair of the annual corporate governance conference at Northwestern's Kellogg School of Management. She is a frequent speaker on matters of corporate governance and crisis management.

Previously, Ms. Austin was the President and CEO of Move Networks, an IP-based television delivery service. She has also served as the President and COO of DIRECTV, the world's leading provider of digital television entertainment services.

Prior to joining DIRECTV, Ms. Austin was the Executive Vice President and CFO of Hughes Electronics Corporation (then parent of DIRECTV). She was a partner of Deloitte and Touche before joining Hughes, and served as a firm designated specialist in mergers and acquisitions, and aerospace and defense.

ABOUT CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over two trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.