Deloitte.

# Focus on: The board's-eye view of cyber crisis management

## Forget about being an observer

The board's chief role in the organization may be oversight, but board members are increasingly being pulled from their elevated vantage point into the thick of cybersecurity issues. The possibility of being held personally liable in the event of a breach is one motivator to roll up their sleeves. Another is the ripple effect a cyber crisis can impose on the organization. A website going down is one thing; the company going down is another.

The fallout from many breaches often includes costly drawn-out litigation, distracting regulatory actions, trickle-down operational disruption, impaired strategy execution, and increased insurance liability, all of which diminish corporate value.

## Beyond business: This is personal

The reputational stakes for board members are high. Shareholders have responded to some cyber breaches by calling for removal of board members or filing derivative lawsuits against the directors and officers, alleging, for example, misconduct and breach of fiduciary duty, both before and after the cyber breach. Board members of companies involved in a cyber incident may see impacts to their reputation and effectiveness as scrutiny and attention continue to mount over cyber incidents.

Class action lawsuits have become more common on the heels of a cyber breach, often with more than one suit filed. Regardless of the outcome of a suit, external and internal legal fees nonetheless mount throughout the class proceedings, making class action lawsuits costly.

## Threats of operational impairment

Beyond the personal threat, board members must also contend with the ways a breach can trigger widespread disruption far beyond the initial point of attack, and in turn, greatly magnify losses.

Consider today's tightly integrated, demand-driven supply chains. The same cyber functionality that enables great efficiency along the chain—from raw materials procurement to production to inventory and distribution—also introduces vulnerability at every link. A hack that brings down a vital piece of equipment, sometimes for only a few hours, can start a chain reaction. Disruptions in procurement impede production, which can deplete inventories and result in the inability to fulfill orders. As each link in the chain is impaired, financial losses mount.

## Compromised growth

M&A and joint ventures can be particularly vulnerable to the fallout from cyber breaches. Cyber espionage in these deals has become all too common, with cyberattacks launched in hopes of gaining financial or operational intel to use as leverage in negotiations. Cyber breaches can also be used as a means to devalue a company on the grounds of weak defenses and failure to properly address risks.

## Relationship risks

The tight integration many companies have with their suppliers and vendors means their company is susceptible to third-party risks. A third-party breach could quickly jump inside the organization's four walls to compromise operations and create a liability issue. Viewed from a third-party's perspective, a breach or inadequate defenses in an organization could result in vital suppliers declining to do business with them, fearing the risk of disruption to their own organizations.

## Beyond litigation—insurance implications

Cyber breaches pose another danger that many boards fail to consider: the effect on insurance. Some companies and board members have taken comfort in having insurance to cover liabilities due to breaches. Data breach or cyber insurance policies are becoming an important part of a company's preparedness plans. In 2013, only 10 percent of survey respondents said their company purchased a policy. In 2014, the percentage more than doubled to 26 percent.[1] Insurance providers, however, have become increasingly focused on examining the root cause of such breaches. If companies are found to be negligent in their defenses or in following leading practices, their insurance payouts may be reduced or even declined.

## A three-pronged approach

The board plays an important role in helping the organization determine how to respond to the new cyber threat landscape. Boards should challenge management to assess the organization's cyber posture and critically review its cyber crisis management capabilities. Crisis management starts with identifying and preparing for the risks of a cyber incident that may turn into a crisis and also building a broad portfolio of capabilities, such as event monitoring, crisis simulation and planning,

### A world of crisis triggers

Crises can be malicious, accidental, or completely random. Most organizations are susceptible to threats from more than one of these potential triggers:

| Malevolence & cyber | Misdeeds & financial crime | Financial disruption | Technological & industrial | Confrontations | Other catastrophes |
|---|---|---|---|---|---|
| Cyberattacks, identity theft, or product tampering | Fraud or other criminal activity | Financial failures that threaten a company's existence | Complex systems failure, either through accident, mismanagement, or sabotage | Legal, commercial, geopolitical, military conflicts | Natural or manmade destructive events that broadly disrupt |

[1] "Is Your Company Ready for a Big Data Breach? The Second Annual Study on Data Breach Preparedness," Ponemon Institute, September 2014.

real-time response, and crisis communications. While the number of companies that have data breach response plans in place is growing, more than a quarter (27 percent) of companies still do not have a plan in place.[2]

Preparedness is more than checking a box or passing a test; it requires understanding where the organization's prized assets are and how criminals may try to compromise them. Cyber risk management begins with securing risk-sensitive assets. If the assets at the heart of your organization's mission are not properly protected, they are open to risks that can turn into major business-threatening crises. At this point, cyber *risk* management turns into cyber *crisis* management. In order to be prepared for a crisis, organizations must be **vigilant** in monitoring for threats against them and **resilient** in recovering from a breach as quickly as possible should an event occur.

To be **vigilant** means that an organization is in a better position to predict and prevent security incidents; it has a custom approach to cyber intelligence that identifies threats specific to the organization's environment and continuously evolves. Cyber threat intelligence and cybersecurity awareness should be emphasized at all levels of the organization. In fact, many cyber breaches enter through phishing emails that are opened by staff and inadvertently launch malicious code into the technology environment.

**Resilience** is key in the event of a breach; organizations should respond rapidly to contain the incident and prevent its spread. While resilience requires investment in traditional technology-based redundancy and disaster recovery capabilities, the bigger picture also includes a broad set of cyber crisis management capabilities. This is where plans are put to the test and immediate, on-the-ground incident response is used to analyze the breach, stop the damage, and mitigate any after-effects.

Boards must challenge management to confirm the organization is proactive, clearly understands the effectiveness of its cybersecurity program, and is focused on the right things:

- Know your crown jewels—not just what you want to protect, but what you need to protect.
- Know your friends—contractors, vendors, and suppliers can be security allies or liabilities.
- Make awareness a priority—within every internal department and among external partners.
- Fortify and monitor—diligently gather intelligence; develop situational awareness; build, maintain, and proactively monitor defenses.
- Prepare for the inevitable—test your incident management process.

## How to start

**Commit to evolving.** The board should hold management accountable for implementing a cyber crisis management plan and for building cyber resilience capabilities that address the unique risks to the organization. Furthermore, the plan should be regularly measured for effectiveness and should continually evolve over time. Cyberattacks are constantly evolving, and the board should confirm the organization can evolve as well.

**Test capabilities and learn from the results.** In order to be effective during a cyberattack, the board should ensure the organization's cyber incident response is tested and shown to be effective in a simulated attack. Results of simulations should be used to correct weaknesses in security, vigilance, and resilience.

**Don't try to go it alone.** The board should ensure that its organization is prepared with subject matter experts who can be on the ground as soon as security is compromised. An external team can organize the chaos and keep your management team focused on running the business. The team should include not only cyber specialists, but also public relations, legal, and other professionals to enable you to act quickly to address the aftershock of the breach. An emerging boardroom practice is for directors to invite cybersecurity subject matter experts to provide advice and perspective to the board.

## Cyber crisis management in action

### A top five priority

In an effort spearheaded by the board's concern about the potential for a security crisis, a global energy company adopted cybersecurity as one of its top five organizational priorities. Board members took it upon themselves to seek the counsel of a leading security adviser who outlined the specific threats to the organization. The board then queried executive leadership about the company's cyber strategy, which led to the development of a comprehensive and coordinated organization-wide approach. Cybersecurity requirements in each business unit are being aligned throughout the enterprise in accordance with leading industry standards and practices—but more importantly, in proportion to the actual threats facing them.

[2] Ibid.

## The Deloitte Center for Crisis Management

No one knows when a turn of events will demand the best your organization can deliver. No matter what form it takes—whether it's front-page news or a quiet struggle only you know about—crisis is a moment of truth that tests your readiness, resilience, and character.

Deloitte Advisory's Crisis Management Solutions team helps organizations prepare for, respond to, and emerge stronger from major crisis events. In addition to its access to a global team of experienced crisis management specialists, Deloitte Advisory has resources in every industry and discipline who can help bring experience and realism to crisis planning.

Deloitte Advisory's Cyber Risk Services can help transform your cyber defenses to become secure, vigilant, and resilient. Our goal is to help you get ahead of cyber risks so your business can keep moving forward.

Disruptive events bring not only danger, but also opportunity—the "unforeseen advantage" you can seize if you're prepared. To learn more, visit **www.deloitte.com/us/crisismanagement.**

*This paper is part of Deloitte Advisory's commitment to provide insights that help board members and senior executives navigate the crisis management life cycle, including readiness, response, and recovery.*

## Contacts


**Rhoda Woo**
Director | Deloitte Advisory
US Crisis Management Solutions Leader
Deloitte & Touche LLP
rwoo@deloitte.com
+1 212 436 3388

**Ed Powers**
Principal | Deloitte Advisory
US Managing Principal, Cyber Risk Services
Deloitte & Touche LLP
epowers@deloitte.com
+1 201 499 0605