Beyond the Breach: A General Counsel's Guide to Managing Cyber Incident Risk

Sep 28, 2026

Categories:

Publications

Authors:

John T. Wolak
Ricardo Solano, Jr.
Megan Linares
Julia E. Browning

What often begins with something that appears routine — a locked account, an unavailable system, a suspicious email, or a call from the security team saying "something doesn't look right" — can quickly escalate into a significant cyber incident with far-reaching legal, regulatory, operational, and reputational consequences and, in some cases, even criminal exposure.

In those critical first hours, the facts are incomplete, business leaders are demanding answers, systems may be disrupted, and customers and employees may already be affected. Decisions made during this period can have lasting consequences, shaping not only the organization's response to the incident but also how regulators, law enforcement, and future litigants evaluate its actions.

So, what should organizations do when the crisis begins?

They should have a plan in place, create a "circle of trust," control the narrative, and stay calm. The organizations that navigate cyber incidents best prepare for an incident beforehand, establish a chain of command when it begins, and preserve credibility by communicating only what the facts support. This article explores best practices for having a plan and controlling the narrative when an incident begins, in order to minimize liability from potential legal and regulatory investigations in the future.

Establish a Chain of Command and Incident Response Plan in Advance

The time to decide who is in charge is not when the systems go down. Organizations should assume that a significant cyber incident will occur and build a response model before the first alert appears that answers practical questions, such as:

- Who is a part of the response team?

FBT Gibbons

- Who makes operational decisions?
- Who advises on legal and regulatory issues?
- Who owns communications?
- Who contacts insurers, vendors, and outside specialists?

The answer is not whoever is available. Rather, organizations should put meaningful thought into who is going to be a part of the "circle of trust" during a cyber incident. The "circle of trust" refers to those who are essential for incident response, decision-making, legal or regulatory obligations, business continuity, and executive oversight. This is the core group of individuals, usually from legal, information security, human resources, marketing/communications, and business leadership, who are authorized to receive and discuss sensitive information related to a cyber incident and ultimately make key decisions about the organization's response. Establishing a circle of trust before an incident occurs removes uncertainty and is critical to preserving privilege and managing communications about the incident. In addition to engaging an in-house team, alerting outside counsel early in an incident is crucial to aligning investigative efforts, preserving privilege, and serving as a shield for the company with law enforcement, regulators, and other stakeholders.

Critically, having a consistent and open line of communication among these individuals is essential to prevent siloed decision making and control the flow of information both upstream to the C-suite and downstream to employees and customers.

It is also important to remember that during an incident, communications and internet access are either unavailable or compromised and should not be used. So, once there is a final list of individuals that are part of the circle of trust during an incident and a final incident response plan, organizations should ensure the plan is printed out and everyone has a copy. Additionally, organizations should create a contact list with everyone in the circle of trust, including their personal cell phone numbers and email addresses so they have a way to communicate even if systems are down. This will save valuable time in trying to track down contact information and allow your organization to quickly spring into action.

FBT Gibbons

Consistent Communication Is Key

The initial period after discovery of an incident is the most unpredictable phase because the facts are incomplete, but disclosures to the C-cuite, employees, customers, and regulatory bodies may be necessary. Organizations must be prepared to speak with a single voice across all channels and only communicate what is known at the time. This is where counsel and having a circle of trust is critical.

Whether the organization is a public or private company, counsel can and should craft consistent statements that are based only on the facts known at the time. This is particularly critical for public companies, which are subject to regulatory scrutiny. For example, the organization may be required to make a public materiality disclosure before the Securities and Exchange Commission (SEC). But what if the organization gives more details to employees than to the SEC, or vice versa? Not only does this undermine the organization's credibility, but it also opens the organization up to regulatory inquiries and liability. As a rule of thumb, the organization can always add more facts as information becomes available, but it cannot walk back statements already made.

Another critical consideration when communicating about a cyber incident is that early statements often become key evidence in subsequent criminal, civil, and regulatory proceedings. As a result, organizations should carefully balance the need for timely disclosure with the importance of factual accuracy. For example, if an organization states in an SEC filing during the early stages of an investigation that no data has been compromised but later notifies consumers that their personal information was accessed, those seemingly inconsistent statements may invite scrutiny from prosecutors, regulators, and the plaintiffs' bar. While facts frequently evolve as a forensic investigation progresses, inconsistent messaging can raise questions about the organization's investigation, disclosures, and overall credibility. Ensuring that communications are accurate, appropriately qualified, and coordinated across legal, compliance, communications, and forensic teams is therefore essential.

FBT Gibbons

Four Principles to Mitigate Legal Risk

To minimize unnecessary legal exposure and reduce the risk of becoming the subject of a criminal, regulatory, or civil investigation, every communication should strike the appropriate balance between transparency and legal protection. As a practical framework, each statement should be grounded in four core principles:

- **What we know:** Clearly communicate the facts that have been verified.
- **What we have done:** Describe the steps the organization has taken to contain the incident, investigate the issue, and protect affected systems or individuals.
- **What we are still investigating:** Acknowledge where the facts remain under review and avoid speculation or premature conclusions.
- **Where stakeholders can obtain updates:** Direct customers, employees, regulators, and other affected parties to a reliable source for accurate and timely information as the investigation progresses.

This disciplined approach promotes credibility, preserves flexibility as new facts emerge, and helps ensure that the organization's communications remain accurate, consistent, and defensible throughout any parallel criminal, regulatory, or civil proceedings. Accuracy does not require silence. Rather, staying in communication with stakeholders will increase the organization's credibility.

Using these tips can also help an organization navigate a cyber incident that evolves into a parallel criminal, regulatory, and/or civil investigation. In those situations, every internal email, interview, forensic report, public statement, regulatory submission, and communication has the potential to become evidence that may be securitized by law enforcement or other regulatory bodies. From day one, organizations should engage experienced counsel, preserve evidence, maintain privilege where appropriate, and coordinate closely with forensic investigators. Organizations should

be prepared to develop a strategy that not only considers the company's business interests in restoring normal operations and remediating impacted systems but that also weighs the implications for potential regulatory and law enforcement activities. Critical to this strategy is to avoid making speculative public statements, waiving privilege without careful consideration, or conducting uncoordinated internal interviews that may later create inconsistencies or credibility issues. The goal is not simply to survive the immediate crisis but to position the organization to navigate every parallel proceeding with consistency, credibility, and strategic foresight.

Key Takeaways

It is no secret that cyber incidents are increasingly common, leaving general counsels and organizations with no choice but to be prepared to navigate an incident when it occurs. To strengthen resilience and improve outcomes, organizations should: (1) develop an incident response plan before an incident happens; (2) establish a clearly defined circle of trust and maintain printed copies of critical response procedures and contact information in the event systems become unavailable; and (3) preserve credibility by resisting the pressure to provide information to stakeholders before facts have been verified and are ready to be communicated.

Taking these steps will enable organizations to respond in a coordinated and disciplined manner, maintain stakeholder trust, make informed decisions under pressure, and ultimately reduce legal, regulatory, operational, and reputational risk throughout the lifecycle of a cyber incident. For help assessing an organization's cyber readiness, developing a disciplined response strategy, or navigating an active incident or parallel proceeding, please contact the authors or any attorney with the firm's White Collar & Investigations and Data Security & Privacy teams.

FBT Gibbons