ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Tabletop Exercises and Cyber Insurance: Key to Navigating Ransomware Attacks

Compliance and Ethics

Law Department Management

Technology, Privacy, and eCommerce

Banner artwork by Bits And Splits / *Shutterstock.com*

When a ransomware incident strikes, the entire in-house legal department must swiftly mobilize to defend its organization, which is under siege by outside cybercriminals. The legal department's role in this process is crucial, as they are responsible for working closely with IT to manage the legal aspects of the incident, such as regulatory notifications, contractual obligations, and potential litigation. Ransomware gangs wreak havoc by encrypting systems and stealing data to sell on the dark web. The chaotic nature of cybersecurity incidents presents legal departments with a range of unique and complex challenges, from technical to purely legal, that simultaneously demand immediate attention. In our experience guiding organizations through these difficult incidents, the most effective way to prepare a legal department for a ransomware event is to start with training — specifically tabletop exercises — well before the situation.

For the unfamiliar, a tabletop exercise is just what it sounds like: a cross-functional team gathers around a table to discuss how the organization would respond to a hypothetical cybersecurity incident. How will we manage communications? Who will make the final decision regarding whether a ransom will be paid? Do we have key business partners with contracts requiring our organization to give notice in a tight timeframe? Do regulators need to be notified? What about an 8-K? Who is our spokesperson if the media is alerted to the incident? These conversations are ideally conducted regularly — perhaps annually — as part of a robust cybersecurity plan.

Organizations with large legal departments should consider two variations of a tabletop exercise: a training session for the in-house legal team on how it will respond to support the company and a second training session that includes the executive leadership team — and potentially, the organization's board of directors — to discuss their involvement and responsibilities.

Here are key considerations when developing tabletop exercises for your organization:

Maintaining privilege in an incident is paramount

Privilege plays a crucial role in incident response. Outside cyber insurance carriers appoint breach counsel to protect privilege as an incident unfolds. Incident response involves a range of outside technical experts, from forensic teams to crisis public relations teams.

Understanding the nuances of the privileges involved and how to exercise them is critical to incident response. The entire organization must be aware of the potential risks, such as waiving privilege with a rogue email to the wrong person. Focusing on the basics of attorney-client privilege and work product doctrine is crucial in an effective tabletop exercise so everyone understands the ground rules well before the incident strikes.

> Understanding the nuances of the privileges involved and how to exercise them is critical to incident response

Regular review of incident response plans by the legal team

An outdated incident response plan can create a host of issues when an incident arises. Further, with the prevalence of cybersecurity litigation (see, for example, the SolarWinds litigation brought by the Securities Exchange Commission), the wording around incidents and how they are categorized can be cited back to an organization later.

Cybersecurity professionals, such as chief information security officers (CISOs), often maintain incident response plans. Working in tandem with the CISO is critical to a legal department's success. Bringing the technical and legal teams together to review the plan on a regular basis ensures that the written plan has accounted for changes to the organization's processes and systems, as well as changes in the external thread landscape.

> Working in tandem with the CISO is critical to a legal department's success

ACC Members: Download the **ACC Cybersecurity Toolkit for In-house Lawyers**

Familiarity with the process and the plan brings efficiency

The value of any tabletop exercise is the teams' familiarity with executing the incident response plan well. By bringing relevant professionals from across the organization together and talking through the nitty gritty of a hypothetical incident, an organization is better served if the dreaded day comes and a ransomware event occurs. This familiarity breeds confidence and competence.

Cybersecurity is an ever-evolving threat landscape, with advances in artificial intelligence making it even more unpredictable. Preparation gives an organization the best chance of responding effectively to a ransomware event. Tabletop exercises should be as mandatory and regular as any other critical training at your organization (think HR and other compliance training).

> Preparation gives an organization the best chance of responding effectively to a ransomware event.

Understanding your organization's cyber insurance and the provider's coverage

Finally, if your organization has cyber insurance, become familiar with the terms of those policies. Understanding what may be covered — and what may fall outside of coverage — in the quiet before an incident hits can save headaches later. Many times, cyber insurance requires the use of specific "panel" providers who have negotiated agreements with the carrier. Know who those providers are and develop a relationship with them to speed up the response process, establish rapport, and hit the ground running. Equally important, identify the resources your organization may require that are not covered under the cyber insurance policy and determine how you will engage with them in a way that still preserves privilege. This understanding will provide a sense of security and preparedness.

Join ACC for more cybersecurity insights!

Beth Waller

Principal and Chair of the Cybersecurity & Data Privacy Practice

Beth Waller chairs the Cybersecurity & Data Privacy Practice at Woods Rogers, a nationally recognized team best known for its work in critical infrastructure and other high-stakes environments vulnerable to cyber incidents. She leverages her extensive experience in technology to advise clients on cybersecurity risk management, incident response, and privacy laws. Waller is a certified Privacy Law Specialist by the International Association of Privacy Professionals (IAPP), accredited by the American Bar Association. In addition, she is a Certified Information Privacy Professional with expertise in both U.S. and European law (CIPP/US & CIPP/E) and a Certified Information Privacy Manager (CIPM), also from the IAPP.

Adam Yost

Corporate Counsel and Global Data Privacy Officer

Indivior

Adam Yost is Corporate Counsel at global pharmaceutical manufacturer Indivior. He oversees global data privacy compliance and provides counsel to commercial leadership on legal and compliance issues. He is a former assistant attorney general and government investigations lawyer in private practice. He is a graduate of the University of Virginia School of Law and the University of Illinois Urbana-Champaign. He lives in Charlottesville, Virginia.