ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

4 Steps In-house Counsel Must Use to Prepare for a Breach

Information Governance

Technology, Privacy, and eCommerce

The state of corporate cybersecurity is in trouble. After years of increasing threats, 2020 was a turning point that influenced major cybercrime activity — and so far this year, things aren't looking any better.

Ransomware attempts, phishing strikes, hacking attempts, and accidental employee breach of information are all higher year over year, according to a recent data breach report by Verizon. The report investigated more than 5,200 confirmed breaches, and found that social engineering and basic web application attacks caused a majority of new breaches, with human actions contributing to about 85 percent of the aforementioned attack types.

Ransomware attacks also continued to grow, with 10 percent of the breaches studied also involving ransomware — double the prior year's figures. Attackers seem to be focusing more on obtaining external cloud and email credentials rather than the computers of remote workers.

This is all troubling (but perhaps unsurprising) news. With breaches becoming more common, many business leaders understand that it's not a question of "if" an organization will suffer a breach, but "when?"

The problem facing in-house legal teams is that, while most companies have some sort of incident response plan, there are often breakdowns in process when the plan gets dusted off and executed. Many legal teams and their outside counsel use manual, ad hoc processes involving spreadsheets and potentially out of date research or information to execute the response plan, which impedes their ability to make critical decisions regarding reporting and breach notification.

Legal is in the best position to understand regulatory processes that must be followed during a breach — and best suited to establish processes that courts and regulators find defensible. This

expertise can help deter some of the financial and reputational risk that often comes with a data breach. Here are four major considerations for law departments, and how they can help mitigate the legal impacts of data breaches.

1. Have a plan in place (and follow it)

While companies often have some kind of incident response plan, it may be incomplete, outdated, or unfamiliar to those who must act on it. Employee change, like losing long-term workers who managed or understood the process, can affect organizational knowledge and make the response less efficient.

At a minimum, organizational breach response plans should seek to uncover the following information, and ensure that there are processes in place to act on related legal and regulatory requirements:

- The scope of the breach
- How the breach occurred
- The severity of the breach
- Which business data was affected
- Whether any personal data was affected
- Where the individuals' whose data was affected reside
- Which regulatory authorities must be notified and by when
- Which third parties must be notified and by when

Ensuring that a plan was in place and properly followed are critical to helping prove that your organization was acting prudently following an incident.

2. Align teams and stakeholders

Most organizations store vast amounts of data that stretches across siloed departments — and breaches can affect business data in different areas of the enterprise, requiring the cooperation of several stakeholders. Further, due to increasingly complex regulations surrounding breach reporting requirements, timelines are often tight, meaning department heads must work together to ensure requirements are met. Because the legal department understands these requirements, they are often best suited to lead the entire process to create a smooth flow of information.

Added to this are the breadth of responsibilities for other tangential departments, like compliance, HR, IT, cybersecurity, as well as operational leadership and executive teams. The best way to mitigate against the technical, financial, operational, and reputational fallout of a breach is to ensure that every major stakeholder within the business is in alignment — and communicating both internally and externally. Jurisdictional considerations must be taken into account as well.

3. Automate and maintain the response process

The process area is where most inadequacies tend to exist. However, this is also the area that can have the most influence on breach response without the need for additional budget — meaning critical dollars can be spent elsewhere, like on technology to improve efficiencies.

Due to the speed at which regulations are changing, and the ever-increasing complexity of ensuring regulatory compliance across jurisdictions, many organizations lack efficient, automated processes

and workflows to help respond to new data challenges. These ad hoc manual tasks are inefficient, tedious, and soon to be obsolete.

Companies must continually review their breach management and response processes and update them. It’s important to do this every six months if possible, along with employee drills to help ensure that stakeholders are ready to act should a real breach occur.

4. Maintaining privilege and defensibility

Ultimately, the goal of your incident response is to coordinate it so that it contains financial, market, technical, operational, and reputational, damage and limits an organization’s potential legal liability. The communications throughout the response process — including all the steps, information, and decisions — should be regarded as potentially relevant in a lawsuit. There must be a secure, reliable, controlled means of communication. This creates the opportunity to assert privilege over that communication if warranted.

It’s important to design your breach response process so that it maintains privilege. There is no surefire way to ensure this, but maintaining privilege is a top priority when working with outside counsel to create pre-incident activities involving cybersecurity or other IT assessments. Documentation of the incident by employees is also important, as are secure communication portals to disclose information to outside counsel.

Preparedness and process automation can help your defense

There are never any guarantees regarding cyberattacks and the resulting legal and repetitional fallout of a data breach. However, it’s clear that regulators and courts will generally look more positively at organizations that have done all the right things during a breach — particularly if they’ve shown preparedness and follow consistent, repeatable, and automated processes.

Only an orchestrated incident response process and a centralized workflow system can consolidate the interdepartmental and multilocation effort to present a consistent message to stakeholders inside and outside the company. An optimized workflow will also create the best possible conditions to limit the incident’s impact, enabling law enforcement to track down the perpetrators. It is the best tool to streamline a stressful event into a manageable set of tasks.

Daniel Sholler

Product Marketing Manager

Exterro

Dan Sholler is a software industry veteran who has been building integrated platforms and working on the hard problems around data management, privacy compliance, and metadata for his entire career. He spent many years as a Gartner analyst, and has worked throughout the industry building and delivering data solutions and strategies. He is currently at Exterro, contributing to their Legal GRC solutions. Sholler is an avid sailor, likes to ski, and enjoys trying to repair mechanical things, at which he sometimes succeeds.