Expert Q&A on Avoiding Common Mistakes in Data Breach Prevention and Response

As data breaches continue to plague large and small organizations across a wide variety of industry sectors, often exploiting well-known vulnerabilities, many companies are struggling to keep their technical security controls current. Increasingly, companies must take active steps to prevent and respond to data breaches, and specifically address crucial organizational and communications issues. Practical Law asked Douglas Meal and Seth Harrington of Ropes & Gray LLP to share their insights on common mistakes companies make before and after data breaches occur, and highlight actions companies can take to avoid costly errors and manage litigation risk.

Given the prevalence of data breaches, should companies focus their efforts on preventing these incidents or planning for them?

Ultimately, this is not an “either/or” question, but rather a “both/and” approach. While a company cannot afford to completely focus on one at the expense of the other, it also will not have unlimited resources to devote to both. Striking the right balance is key.

Ideally, a company should:

- **Implement reasonable and appropriate security measures to protect the data it collects.** Failing to create and maintain a solid information security program and allowing an otherwise preventable data breach to occur can create legal exposure, not only from the breach itself, but also from any applicable contractual or regulatory obligations.

- **Develop and regularly test its incident response plan.** A robust incident response plan provides effective risk management because an entity’s response to a data breach can reduce, or at least avoid increasing, legal exposure. The unfortunate reality is that no organization, no matter what security measures it adopts, is immune to suffering some type of data security incident. As then-FBI director Robert Mueller...
said in 2012, “There are only two types of companies: those that have been hacked, and those that will be.” That still holds true today.

**What are some common mistakes companies make with their incident response plans?**

The most obvious mistake in response planning is having no plan at all. More often, however, companies have an ineffective response plan in place that essentially provides the same amount of readiness as having no plan at all. Some mistakes that can result in an ineffective response plan include:

- **Adopting an overly rigid and detailed approach.** This type of plan might not provide much help in an actual data breach, because it is unlikely to anticipate every possible scenario. Instead, companies should implement a flexible plan that:
  - clearly identifies the responsible contacts; and
  - defines a general process that guides a company’s actions in any situation.

- **Not having external resources lined up in advance of a data breach.** Companies should have their third-party vendors and outside counsel in place and available to respond quickly in the event of a breach. Companies should structure these engagements so that counsel retains and directs any third-party vendors. This maximizes the privilege protections over the work performed.

- **Failing to regularly test the plan for effectiveness.** Companies should routinely assess their plans by running fire drill type exercises, which can help:
  - identify any limitations or oversights; and
  - ingrain the procedures and lessons learned into personnel as second nature.

**How can companies improve their approach to information security governance and reduce their vulnerability to data breaches?**

One of the common mistakes companies make is treating the information security function as subordinate to the overall IT function. Instead, companies should grant independence to information security and provide it with a direct reporting chain to executive leadership within the corporate governance structure. IT groups often have competing priorities. Empowering information security with the autonomy to prioritize and take needed actions helps companies to avoid overlooking security deficiencies that opportunistic hackers can exploit.

Additionally, companies can help prevent human error through a “defense in depth” approach to staffing. This entails hiring sufficient personnel with appropriate technical expertise, and making sure no one individual or group is solely responsible for any function that impacts information security without being checked, or even double-checked, by others.

Finally, one of the most common organizational security weaknesses that hackers exploit is the failure to manage third-party service provider risk. Companies can limit their exposure to these third-party conduits by:

- Implementing an appropriate due diligence and monitoring program.
- Clearly defining shared responsibilities for information security in service contracts.

**What steps should companies take immediately after a data breach?**

From a company’s perspective, a data breach event begins at the time of discovery. A breach may be self-identified or, more commonly, companies may receive notification from third parties, such as customers, law enforcement, or others. What follows in the hours and days after discovery can have a significant impact on a company’s legal exposure. Going into denial and failing to take timely, appropriate action can have a negative impact on a company’s potential legal liability and public relations.

Once it has confirmed that a breach has occurred, a company should act quickly and make responsive decisions, which can be complex. For example, because a data breach means that a company could likely face litigation or a regulatory investigation, at the outset, the company should:

- Take steps to preserve forensic evidence and other potentially relevant information.
- Bring in third-party vendors, such as experienced outside counsel, assisted by forensic investigators working at their direction, to:
• advise on the company’s legal obligations; and
• maximize privilege protections over the investigation.

Additionally, the company should promptly assess its potential legal liabilities. For instance:

- A company may be obligated to notify consumers, regulators, or both under the various breach notification statutes (for more information, search Breach Notification and Data Breach Notification Laws: State Q&A Tool on Practical Law).
- A public company may be obligated to make market disclosures.
- A company may have contractual obligations to provide notice about and take other steps in response to a breach.
- A company may be obligated to provide notice of a claim or a notice of circumstances under an applicable insurance policy.

**Consumers, regulators, and the media demand transparency when a data breach occurs. How can a company’s best efforts backfire?**

As discussed further below, recent case law suggests that what a company says about a data breach can mean the difference between succeeding or failing at the motion to dismiss stage in subsequent litigation. Potential plaintiffs can use public statements against the company, even if the underlying breach turns out to be less serious than originally presumed.

**How can companies better prepare for media interactions and limit their risk without being seen as evasive?**

The best approach is to stick to just the facts. Companies should:

- Disclose only what they can confirm with reasonable certainty, and avoid offering details before facts have been verified, speculating, or promising whether or when additional information may be provided.
- Back up statements to the media with their own thorough investigations to provide satisfactory answers to major questions, such as:
  - What happened?
  - How did it happen?
  - What is the company doing to prevent it from happening again?

To avoid generating uncertainty and concerns by making multiple statements and corrections to the public, ideally, companies should deliver a statement once, providing the most accurate information available.

**Recent case law suggests that what a company says about a data breach can mean the difference between succeeding or failing at the motion to dismiss stage in subsequent litigation.**

Everything a company publicizes about a data breach must be accurate and comply with relevant breach notification statutes, contractual obligations, or other requirements. There is much pressure to err on the safe side by over-complying with notice obligations and identifying more individuals who may be affected by a breach. But a company cannot “unring” the bell if it later turns out that less information was at risk or there was no data breach at all.

While companies should make legally required notifications, there often is little that can be said with certainty early on after a data breach occurs. Identifying the scope, causes, and consequences of a breach can be a complicated and time-consuming (and, in many cases, ultimately unsuccessful) effort. Even if the company has some initial understanding of the breach, facts can change quickly and dramatically in the days and weeks following discovery.

**When should a company contact law enforcement, and what issues does this raise?**

Many data breaches are the result of crime. When that is the case, the company that suffers the breach is a victim, and it should contact law enforcement as early as possible. Notification to individuals may potentially be postponed based on a request from law enforcement (depending on the jurisdiction). In some instances, law enforcement may be able to share information regarding similar incidents to assist in the company’s investigation. Also, consumer notification obligations may be delayed to aid in the investigation, if directed by law enforcement. However, it is important to remember that information shared with law enforcement is not privileged. Companies must balance assisting in any criminal investigation with avoiding disclosure of information that may be otherwise protected.
How have class action litigation trends impacted data breach response?

In a large, highly publicized incident, class action litigation on behalf of consumers is nearly inevitable. Complaints often are filed on the same day as the public announcement of a data breach. The threat of defending against these claims, which are costly even when early dismissal is obtained (and that is becoming less likely), is obviously a driver in how an organization prepares its response. This is especially true given that public disclosures can form the basis of claims.

For example, in In re Zappos.com, Inc., Zappos allegedly communicated to shoppers on its e-commerce site that “shopping on Zappos.com is safe and secure — guaranteed.” After Zappos experienced a data breach incident, consumer plaintiffs relied on this alleged statement to assert that the company negligently misrepresented the safety of the plaintiffs’ financial information and violated California’s unfair competition statute. The court found the statement sufficient to form the basis for both counts at the motion to dismiss stage. (2013 WL 4830497, at *4-5 (D. Nev. Sept. 9, 2013); Consol. Am. Class Action Compl., No. 12-00182 (Mar. 12, 2012).)

Similarly, in Remijas v. Neiman Marcus Group, LLC, Neiman Marcus posted statements on its website to keep customers abreast of the data breach it had suffered. The statements included acknowledging that 350,000 payment cards were potentially exposed, and 9,200 of those cards had experienced fraud. Neiman Marcus argued in its motion to dismiss that the consumer plaintiffs did not face an actual or imminent risk of harm sufficient for Article III standing. The Seventh Circuit found the offer “telling,” reasoning that “it is unlikely that” Neiman Marcus made the offer “because the risk [to the plaintiffs] is so ephemeral that it can safely be disregarded.” (794 F.3d at 692-94.)

These cases demonstrate that companies should regularly review the statements they make on their websites, including their privacy policies, and in marketing materials. Additionally, as discussed, post-breach statements should stick to confirmed facts.

What is the one takeaway that every company should know about information security and data breaches?

Many companies focus on the large-scale data breaches that dominate the news media, review their risk profiles, and then dismiss the possibility of exposure from a data breach as too remote. But any entity that has a computer network and human employees, and handles confidential information of any kind, is at risk of suffering some kind of data breach — that means just about every company.

The key takeaway is that information security is an ongoing struggle, a never-ending war against a constantly evolving adversary. It is a rare type of risk where there is a thinking opponent working to undermine everything you do, so commitment and constant vigilance are critical.