Before the Aftermath: How to Prepare Now for the Possibility of a Privacy Lapse or Data Security Breach

May 16, 2014

Despite a greater focus on prevention than ever before, privacy lapses and data security breaches continue to increase as a source of financial, legal, and reputational risk for a wide array of businesses. According to the Identity Theft Resource Center, a nonprofit group that tracks data security breach reports, there were 614 data security breaches reported in 2013, covering almost 92 million records.

The litany of recent breaches in the headlines includes names of venerable brands and fast-growing technology companies. If even large businesses with significant resources and tech-savvy companies cannot always prevent data security breaches, what are the odds your company will be 100% successful in avoiding a breach? It seems almost irresponsible these days to assume that you can stop every attack and prevent every oversight indefinitely. Instead, every business must face the reality that a breach is possible, and take steps now to address the possibility. This article will focus not on prevention, but upon preparing for an effective response.

Notice Requirements

In the event of a significant breach, approximately 46 states and the District of Columbia have laws that require a business suffering a breach to notify the affected customers, the state attorney general, and the consumer reporting bureaus.

One result of the notices required by these laws is that watchdog groups are better able to monitor breaches. However, this is not the entire picture. Breaches affecting a small number of persons may not be required to be reported and are, therefore, not included in the publicly-available statistics.

For example, under North Carolina’s Identity Theft Protection Act, only breaches affecting 1,000 or more individuals must be reported to the North Carolina Attorney General and consumer reporting bureaus. Many commentators believe that the majority of data breaches go unreported for this and other reasons.

A Costly Matter

Data security breaches can be very expensive. A study of insurance claims in 2013 conducted by the risk management firm NetDiligence showed that the average total reported cost of a security breach to a business was $954,253, with average legal fees of $574,000. The same study found that 29.3% of data breach-related insurance claims were made by businesses in the health care sector, with 15% in the financial services sector.

Preparing for the Possibility of a Breach

Given the immense financial and reputational risks of a privacy violation or data security breach, and the near impossibility of
absolute prevention, it is important for each business to prepare in advance for the possibility of a breach. Prudent breach preparation can help a business to more effectively respond to a breach, mitigate losses and liability, and demonstrate compliance with applicable laws. The following categories of measures are strongly suggested:

- **Conduct a Risk Assessment and Document It.** Although breach prevention measures are beyond the scope of this article, evidence of a reasonable risk assessment can be useful in the aftermath of a breach to document that commercially-reasonable steps were taken to identify vulnerabilities and weigh the costs of addressing them.

- **Implement Commercially-Reasonable Policies and Security Measures.** After identifying the categories of sensitive information held and the likely sources of risks, a business should then take and document reasonable measures to prevent them. This should include the adoption of effective technological standards and well-thought-out policies and procedures. The scope and rigor of the measures will depend upon the risk profile and resources of the business. Although primarily intended to prevent a breach, the existence and documentation of a reasonable prevention program can help to mitigate liability following a breach.

- **Review Policies and Procedures Periodically.** At regular intervals, policies and procedures should be re-evaluated to ensure they remain current or revised to reflect changes in the risk profile and landscape. Again, the scope and frequency of these reviews will depend upon the risk profile and resources of the business.

- **Prepare a Response Plan.** Just as every business should have a documented disaster recovery plan, every business that holds sensitive data should have a documented breach response plan ("Response Plan") ready (and tested) to guide the business's efforts in the hours and days following a breach. Assembling a Response Plan from scratch in the immediate aftermath of a breach wastes valuable time and risks overlooking important matters in the rush to handle an emergency.

  The Response Plan need not address every conceivable contingency, but should contain the basic, universal response protocols that will form the basis of the business's response. The Response Plan should be created with the input of security personnel, IT personnel, legal counsel, and senior management.

- **Select a Response Team.** Every business is comprised of individuals with unique strengths. In advance of a privacy or security incident, each business should determine who is best suited to perform each task addressed in the Response Plan. Those individuals should be assigned to a response team and trained to implement the Response Plan so that they will be able to "hit the ground running" when called upon to respond. The response team should include security, IT, communications/public relations, and legal experts, as well as senior management.

- **Perform Due Diligence on Third Parties.** Several recent major data security breaches have arisen from the actions of vendors who obtained customer information from another business. The vendor usually has no direct relationship with the customer, and the customers typically sue the business with which they have a relationship instead of, or in addition to, the vendor.

  Selecting third-party vendors to handle your customers' information should involve a commercially-reasonable due diligence process to ensure that only responsible vendors are deemed to be eligible to receive customer information. Knowing the right questions to ask is key.

- **Use Carefully-Crafted Contracts.** Some risks of liability and other losses arising from data security can be reduced through well-drafted contracts with third-party vendors. Many contracts presented to businesses by third-party vendors are woefully inadequate to protect the business if the vendor fails to prevent a breach of the business's customer data. A lawyer who understands the issues can potentially help a business save large sums in litigation fees and liability in the event of a subsequent breach.

- **Consider Cybersecurity Insurance.** A number of firms now offer insurance against losses arising from data security breaches. This category of coverage is available as an addition to directors and officers liability insurance coverage (better known as a "D&O" policy) or as stand-alone coverage. Coverage terms are not standardized in the way that, for example, homeowner's policies are, and there are usually significant exclusions from coverage. Therefore, it may be useful to have a proposed policy reviewed by legal counsel and technology professionals to ensure that the offered coverage is adequate and that the remaining risks are understood.
Prior Planning Prevents Poor Performance

A business should do all it reasonably can to prevent a privacy or information security breach, but must recognize that some risk of a breach inevitably remains. By taking a few responsible steps in advance, the losses associated with a breach can be mitigated efficiently and effectively. In addition to commercially-reasonable preventative measures, a solid and well-documented Response Plan can go a long way toward helping customers, employees, managers, shareholders, and other stakeholders sleep more soundly at night.

© 2019 Ward and Smith, P.A.

This article is not intended to give, and should not be relied upon for, legal advice in any particular circumstance or fact situation. No action should be taken in reliance upon the information contained in this article without obtaining the advice of an attorney.

We are your established legal network with offices in Asheville, Greenville, New Bern, Raleigh, and Wilmington, NC.