DAVIS GILBERT

Breach Response and Ransomware

The consequences of a serious data breach range from inconvenient to catastrophic. In the event of such a breach, a call to our attorneys is often one of the first our clients make. In situations that are inevitably stressful for all involved, companies count on us to be a calming presence, mapping out a measured action plan calibrated to the level of threat both to their business and to their legal obligations. We help manage the response process and work with them to minimize any legal, financial and reputational repercussions.

Who Must Be Notified

In any security incident, we advise clients of their compliance obligations, especially consumer and regulatory notifications that are required by applicable security breach notification laws. As each state has its own unique set of notification requirements, that task can be remarkably complex. Beyond the legal obligations, there are parties that must be notified under existing contracts and others it is advisable to notify for business or personal reasons. Many of our clients delegate the entire notification process to us.

Courses of Action

Guided by industry best practices, we take a lead role in managing an incident and working toward remediation. We often engage specialized forensics firms to determine what happened and to develop a remediation plan. We coordinate efforts to assess the business risk of all available options and to help decide the best courses of action to pursue.

To Pay or Not

In a ransomware incident, many of our clients want us involved in deciding whether or not ransom should be paid, and we are adept at laying out the variables that drive that decision. Since paying ransom can be legally problematic in some jurisdictions, we help weigh the legal risk of paying against the business risk of not paying. In either case, we guide our client in any engagements or negotiations with law enforcement agencies.

Managing the Aftermath

Once the crisis has been contained, the damage assessed and remediation efforts underway, we are frequently asked to conduct post-incident analyses to locate any gaps in policies and procedures. We help identify points of vulnerability — in data systems, employee training, vendor practices or other aspects of operations — and work to plan a new and safer way forward for the business.

Representative Matters

- Managed and supervised a breach response action plan for a leading online entertainment service, including application of 50 separate state security breach notification laws to unique facts.
- Advised a large agency regarding a security breach that involved the exposure of thousands of employee W-2 records. Coordinated with law enforcement and the IRS regarding hundreds of unauthorized requests for tax refunds.

- Advising a high-end UK retailer regarding a ransomware attack that impacted the majority of the company's internal systems. Managing breach response obligations in the U.S. with breach response obligations in the EU.
- Advising a boutique financial services company regarding a security incident due to a lost laptop that contained personnel files.
- Advising a mid-size agency regarding a phishing scam that resulted in vendor payments being erroneously sent to a fraudster instead of the vendor. Representing our client in threatened litigation from the vendor.
- Advising a major consumer products company regarding inadvertent data disclosure by an employee who emailed personal information of hundreds of individuals to the wrong consumers.