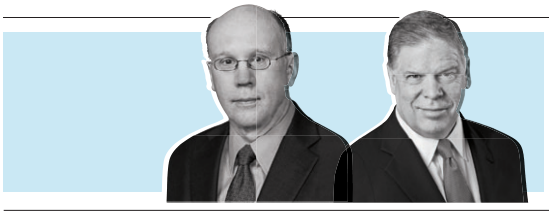

LIABLE FOR A DATA BREACH?

Taking reasonable preventive care is a must to prevail in court

The Anthem data breach has triggered over 90 lawsuits and scrutiny from numerous state insurance commissioners, law enforcement officials and the National Association of Insurance Commissioners. Other significant data breaches have occurred in the healthcare industry, and substantial litigation has ensued.

In the past, most data breach cases were settled or dismissed, because courts concluded that the plaintiffs' injuries were too speculative to support a lawsuit, dismissing the cases either for failure to establish standing or to plead a legally compensable injury. However, a few courts in consumer class actions recently have concluded that the alleged injuries arising from a data breach are sufficiently certain to allow the cases to go forward, allowing plaintiffs to take discovery on how the breach occurred and what the defendant did or failed to do before the breach to prevent it. At the same time, regulators are increasing scrutiny of companies that suffer data breaches. Ultimately, the defendants in these cases and regulatory investigations will have to prove that they took reasonable steps to prevent the data breach before it occurred.

Proving Reasonableness

These developments point to the importance of a company conducting and documenting "an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information held by the covered entity" ("Risk Assessment") and determining and documenting the "security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level" ("Written Information Security Plan" or "WISP"). The Risk Assessment and WISP, if properly prepared, can be a company's strongest evidence in defending against data breach claims.

Since the Risk Assessment and WISP may become evidence in a legal proceeding, it is important to obtain legal advice in preparing these documents, as well as technical advice from an IT security expert. All emails, expert reports and drafts prepared in the process of preparing a Risk Assessment and WISP can also become evidence in a legal proceeding, so care must be taken in preparing these preliminary materials as well. Retaining legal counsel to work with the technical expert to provide legal advice regarding the company's legal obligations may protect the confidentiality of the preliminary documents under the attorney client privilege.

In addition, legal counsel can provide input regarding frameworks of potential security controls to consider in formulating a plan. Various organizations have published standards listing potential controls, and there are pros and cons from a legal perspective to selecting each set of standards as a starting point for the analysis. It is important to select industry standards that will have credibility in a court room but, at the same time, are practical. Also, legal counsel can provide input regarding what controls have been the focus of regulatory actions and class action settlements.

Legal counsel can also help structure the process to be consistent with applicable law. For example, IT experts should be asked to identify potential security controls to be discussed with the company. The company, after receiving input from the expert and legal counsel, is responsible for deciding which controls are reasonable from a cost/benefit standpoint. Those decisions should then be implemented and documented in the WISP.

Bottom line: Since a Risk Assessment and WISP and the preliminary documents leading up to them may become evidence in a legal proceeding, legal input is critical in making sure that this evidence will support the company's position and not be used against it. ■

ABOUT THE AUTHORS

Robert Kriss is a partner in Mayer Brown's Privacy & Security group in Chicago, Illinois. James R. Woods is co-leader of Mayer Brown's global Insurance Industry Group based in New York, New York and Palo Alto, California.