Schnader
ATTORNEYS AT LAW

Schnader Harrison Segal & Lewis LLP

CALIFORNIA DELAWARE JAKARTA* NEW JERSEY NEW YORK PENNSYLVANIA WASHINGTON, D.C.

PRIVACY AND DATA SECURITY

ALERT

JANUARY 2015

# SAFEGUARDING YOUR INFORMATION ASSETS: ARE YOU PREPARED?

*By Stephenie W. Yeung*

In view of the well-publicized data breaches in 2014 and the current renewed federal legislative focus on privacy and data security issues, we are providing this Alert to highlight some action items to safeguard your company's information assets, and reduce exposure to liability in the event of a breach. Data security is good business. A Ponemon Institute and IBM study estimated that in 2014, organizations paid an average of $5.9 million to respond to one data breach incident, and the cost to the organization in lost revenue, reputational harm, and diminished good will average at about $3.2 million.

***Know What You Have***

The first step in protecting information assets is to conduct a data asset inventory to determine:

- What type of data is collected and retained?
- From what sources is the data collected?
- How and where is the data stored and for how long?
- With whom is the data shared?
- What processes use the data?
- Who has access to the data?
- Who needs to have access to the data?

The data should then be classified according to sensitivity and confidentiality. Public Data is information that is otherwise publicly available and does not create exposure if it is obtained. An example is telephone directory information. Restricted Data is the personally identifiable information such as health data or social security numbers that could expose the organization to liability if released without authorization. Private Data is the information between Public Data and Restricted Data.

***How are You Protecting the Data Now?***

The next step is to determine the organization's current physical, administrative and technical safeguards for protecting its information assets. Some questions to explore include:

- Are authentication, firewalls, anti-malware systems in place?
- Are there requirements to ensure that "strong" passwords are used, and that they are required to be periodically changed?
- Are intrusion detection or prevention systems being used?
- What kind of employee access control is in place?
- If your company allows employees to bring their own mobile devices, are they encrypted?
- What kind of system log information is gathered for your company's network? What is the retention period of the logs?

- What are your company's data retention policy and procedures?

Security options range from lock-and-key for physical files to sophisticated intrusion and detection systems. The National Institute of Standards and Technology (NIST) has developed a voluntary cybersecurity framework that is useful for organizations to consider. Organizations should be aware that the Federal Trade Commission has brought lawsuits following a data breach, asserting that the defendants' security measures were insufficient.

Consult the organization's chief information or technology officer concerning encryption. Statutes in many states exempt organizations from the obligation to report a data breach if the exposed data has been encrypted. The benefits of encryption should be weighed against the sensitivity of the types of personal information held by the organization and its effects on the organization's IT infrastructure.

***Get Your Policies in Order***

Every organization should conduct periodic reviews of its customer-facing privacy notices to make sure that its procedures match its public promises regarding the use of private information. Discrepancies could expose the company to unfair trade practices claims by the FTC or a state attorney general.

Similarly, the organization's contracts with business partners and vendors should have provisions that address and clearly define responsibility, accountability, and liability for privacy and data protection issues. Third-party vendors should treat personal information at least as securely as the organization does. Periodic reviews of these contract provisions to ensure that they reflect current practices are likewise necessary.

***Don't Keep Data Longer Than is Necessary***

Design and implement a timely data destruction plan. Data hoarding is risky business. The benefit of keeping data to meet legitimate business needs and to comply with statutory or regulatory requirements should be assessed against the risks and costs of keeping data beyond its useful life. Many states now have data destruction laws that mandate the time and manner of destruction or erasure of data. Data relating to anticipated or ongoing litigation must be preserved in any event.

***Assemble a Data Breach Response Team***

A data breach is a crisis incident that requires the organization to respond quickly to a host of legal, regulatory, compliance, and crisis communication issues. State data breach laws typically require that organizations notify law enforcement agencies almost immediately after detection of the breach, and, depending on the number of individuals affected, to notify credit reporting agencies and potentially affected consumers without unreasonable delay. If a data breach is discovered, the organization will not have time to prepare a response plan for the first time. It is critical that the organization has prepared an incident response plan in advance of a data breach event. Typically, representatives from legal, information technology, operations, human resources, and marketing/customer relations are involved in preparation of the response plan.

Moreover, it is important to appoint a "head coach" to lead the response effort and to act as a centralized driving force for the data breach incident response team. Insurance carriers consider data breach coaches to be an indispensable part of the team. Outside counsel who has worked with the organization's data breach response team to design the incident response plan is well-suited to serve this function. The use of counsel has the benefit of protecting confidential attorney-client communications from disclosure.

***Practice…Practice…Practice***

Annual mock trials of the incident response plan—table top exercises—provide an opportunity for the data breach response team to address different issues arising in a breach so the response team can refine the plan. If unanticipated vulnerabilities are discovered, they can be addressed in advance of an actual breach.

***Consider Cyber Insurance***

More insurance companies are offering Cyber or Data Security coverage. Selection of the policy should be made in consultation with your insurance broker and outside counsel.

***Train Your Employees***

One of the leading root causes of many data breach incidents is human error, a category that includes weak passwords, lost devices, and misplaced documents. Employee training on the organization's policies and procedures is a critical part of

safeguarding your customers' privacy and data security.

Implementing some or all of these steps will better prepare your company to address privacy and data security issues, including responding to a data breach, which will limit its exposure to a variety of risks. ◆

*This summary of legal issues is published for informational purposes only. It does not dispense legal advice or create an attorney-client relationship with those who read it. Readers should obtain professional legal advice before taking any legal action.*

*For more information, please contact one of Schnader's legal professionals.*

*Anne E. Kane*
*Partner*
*215-751-2397*
*akane@schnader.com*

*Stephenie W. Yeung, CIPP/US*
*Associate*
*215-751-2277*
*syeung@schnader.com*