Data Protection and Retention

By Brian A. Nettleingham

News coverage of significant data breaches continues to fill broadcasts and newspapers. Most recently, it appears that a foreign government may have hacked federal government computers, gaining access to incredibly sensitive information. Now, more than ever, companies must take steps to ensure that adequate data protection measures are in place.

What measures are adequate? We counsel clients to require, as part of any data hosting or similar agreement, representations and warranties regarding the specifications of the electronic data protection measures being used. But organizations cannot simply depend on electronic protections.

Physical measures also need to be implemented. For example, do your employees tape written lists of passwords and usernames under keyboards, inside drawers, or other “secret” locations? If an email, appearing to come from your IT department, asked your employees to forward their current passwords and usernames, how many would comply? Data thieves frequently use these methods to gain access to systems rather than forcibly hack through firewalls and other security measures.

In short, a comprehensive data protection policy will address physical and electronic security. Such policies should be included in employee handbooks and rigorously enforced. Failure to do so can yield severe consequences.

For example, if your company handles sensitive corporate data from customers, such as specifications for parts manufacturing, failure to protect that data properly could result in a breach of contract claim and significant damages, both in terms of a lawsuit and damage to the customer relationship. If your company handles consumer data, such as health, financial, or other non-public personal information, a breach will result in tremendous costs, both in terms of the cost of responding and curing the breach and damage to your company’s reputation.

A complete solution involves a comprehensive review of service provider

contracts, organizational policies and procedures, and cyber risk insurance to best mitigate the risk of any breach.

Data Retention

The more data an organization retains, the broader its exposure. Therefore, a key theme in any data retention policy should be mitigation of risk by keeping only the data that is required.

If your company is a regulated entity (financial institution, accounting firm, health care provider, etc.), you may be subject to specific data retention requirements for certain types of data. For companies operating in less regulated contexts, a clear Data Retention Policy (“DRP”) is still recommended.

A key reason for limiting the data you retain is the potential cost of managing that data if litigation should arise. Once litigation becomes likely, it is too late to suddenly start deleting the terabytes of data needlessly stored on individual hard drives and servers. The volume of that unnecessarily retained data will suddenly become a tremendous cost burden, as it has to be reviewed for potential production in any lawsuit. On the other hand, a reasonable DRP implemented and followed as a regular business practice can help mitigate that cost.

Maddin Hauser regularly assists clients with data security and retention efforts, including drafting policies and procedures, reviewing service provider contracts, and helping coordinate insurance coverage for cyber liability risk.