Managing the Data Risk

By Brian A. Nettleingham

Every modern business creates, collects, and stores electronic information. Managing that data has become a crucial aspect of managing operational risk. The following questions are just a sample of some of the areas in which Maddin Hauser helps its clients proactively manage these issues to minimize unnecessary risk and expense.

1. ***Do you have an appropriate data retention policy?***

   Current technology allows companies to store data in quantities that would not have been possible in a non-digital world. Many businesses assume it is easier to accumulate data than create a system that calls for information to be regularly purged.

   The absence of an appropriate data retention policy, however, may be one of the most expensive mistakes a company could make. In the unfortunate event that you face litigation, the sheer volume of potential data that may need to be processed by your attorneys as part of the discovery process could explode the expense of the litigation.

   An appropriate data retention policy insures that only essential data is retained and is properly organized to minimize cost and disruption if it needs to be reviewed and produced. The policy needs to be implemented before any dispute. Afterwards is too late.

2. ***Do you have the ability to quickly enact a "litigation hold" if necessary?***

   Organizations need to be able to implement "litigation holds" in the event that a legal dispute arises. Are you able to secure and preserve potentially relevant information in a way that imposes minimal cost and disruption on your operations? Failure to do so can result in serious consequences. Courts can impose financial penalties and – in extreme cases – default parties who fail to properly preserve electronic information.

3. ***What is your mobile device policy?***

   Mobile devices can store and transmit information that may not be stored anywhere else. Do you have a policy that manages the amount and type of information that may be available on your company's mobile devices? Do you have an inventory of the devices used for your business?

   Companies should also have a clear policy in place regarding who owns the data stored on devices used by employees.
4. ***Do you have a written policy regarding your employees' use of email and your company's systems?***

   Email is essential to any business. But clear guidelines need to be created regarding how this essential tool is used by employees.

   For example, if your employees regularly negotiate sales via email, do those emails contain disclaimers that make it clear that – unless otherwise expressly stated – the email exchange does not create or amend any contract being discussed?

   Are your email use, storage and retention policies clear? For example, are your employees using private email addresses (such iCloud or Gmail) to conduct business? Many clients are surprised to learn that their employees regularly use personal accounts, sometimes simply as a matter of convenience, rather than their official company email. This situation creates several problems, including data gathering in the event of litigation and controlling communications with customers if an employee is terminated.
5. ***Do you monitor social media posts by your employees? Do you have a policy governing such postings?***

   Do you have a policy regarding your employees' posts on social media sites such as Twitter, LinkedIn, and Facebook? For certain regulated industries – such as consumer finance and securities – posts by employees may be deemed "advertisements" or "offers" on behalf of the entire company. Depending on the content of the posting, it may violate state or federal law regulating such advertisements.
6. ***Do you have a process for entering into contracts "electronically" that will allow you to easily demonstrate which version of an***

agreement is authentic?

Today it is common to sign and return documents electronically. Companies need to implement policies that leave no room for doubt as to whether a document is the final, executed, and unaltered version of any agreement that may be at issue.

7. ***Do you collect and/or store sensitive consumer information on your systems?***

   If you collect and/or store sensitive information, you must take steps to insure that it is properly secured. For example, the collection and storage of certain personal financial and health information, is regulated by statute, and additional protections and disclosures are usually required.

   If sensitive personal data is compromised, most states have enacted laws that require you to undertake a series of steps to investigate the breach and notify affected individuals in a timely fashion. Advance planning for a potential breach – including evaluating your insurance policies for coverage – can significantly reduce the cost and risk.

   In the business-to-business environment, you may be receiving and storing information from a customer that must be treated as "confidential" under whatever contract governs the relationship. Failure to do so may constitute a breach of that agreement.

At Maddin Hauser, we help our clients efficiently assess and address these issues to reduce the potential disruption and costs related to the creation, retention, and storage of electronic information. If you would like more information on an assessment of your company's risk, please contact me at either 248.359.7503 or bnettleingham@maddinhauser.com for more information.