Bloomberg BNA

Digital Discovery & e-Evidence®

DATA SECURITY

The discovery process can expose corporate organizations and the third parties they work with, to a heightened risk of breach by disturbing the data and taking it outside the protected corporate environment. Deloitte's Steve Shebest explains that although breach is an industry-agnostic risk, it presents several key opportunities that discovery participants can and should plan for.

High Risk Data: Have a Plan!

BY STEVE SHEBEST

Recent updates to the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) highlight the importance of protecting at-risk data in the context of the discovery process. The updates added some teeth to previous versions of the laws, expanding breach notification requirements for unsecured Personal Health Information (PHI) and Personally Identifiable Information (PII).

In addition, the HIPAA Security Rule now applies directly to business associates, rather than just covered entities. Finally, civil penalties for violations now range up to $1.5 million per calendar year[1].

But responsibility for high-risk data is not limited to the health care industry. A recent study by the Ponemon Institute[2] shows at-risk data is ubiquitous across the financial, commercial, transportation and industrial sectors, as well as numerous others.

Regulations providing penalties for disclosure, breach or other mishandling of data—such as the International Traffic in Arms Regulations (ITAR), the Export Administration Regulations (EAR) and those under HITECH—present both risk and challenge to organizations, particularly within the discovery arena.

The cost of a breach is very real for organizations, averaging $5.4 million for the "typical" breach of one hundred thousand records or less[3].

In addition to direct costs such as credit monitoring and providing discounts to existing customers to retain business, companies face indirect costs including abnormal customer churn, reputational loss, diminished goodwill and increased customer acquisition cost.

Worse yet, the Ponemon study found fully 40 percent of data breaches were caused by third parties, such as vendors or business partners, and those third-party errors can amplify the cost of managing a data incident. This doesn't take into account the regulatory penalties: Between 2012 and 2013, the published negotiated settlements and civil monetary penalties levied by the Department of Health and Human Services for viola-

Steve Shebest is a director in Deloitte Transactions and Business Analytics LLP, an affiliate of Deloitte Financial Advisory Services. Shebest is based in Washington, D.C., and focused on supporting corporations and counsel in their unique electronic discovery needs.

[1] Department of Health and Human Services, 45 CFR Part 160, January 25, 2013.

[2] Ponemon Institute, "2013 Cost of Data Breach Study: United States," May 2013.

[3] Ponemon Institute, *Ibid*, at 2.

tions of HITECH averaged more than $1 million per incident[4].

Enron Data. A particularly good example of the risk can be found in the Enron data set, long used as a body of sample data within the Discovery industry.

Recognition of the at-risk data in the Enron set resulted in the full data set being taken down from the Amazon Web Services site where it was hosted. Efforts to clean the data set and re-post it have met with mixed success.[5] No matter how you approach discovery requirements for data that may contain protected information, it's crucial to have a plan in place to mitigate the associated risk.

Understand the Weak Points

Understanding the weak points of the discovery data process and proactively implementing a plan, both internally and with business partners, is critical to mitigating the risk of data breach.

From a data security standpoint, three key weak points in the process could benefit from acknowledgement and, in some instances, action: the point of collection, the point of data transfer and the handling of data by your partners outside the corporate firewall.

The Point of Collection. From a discovery standpoint, an old maxim provides wisdom: If you do not collect it, you cannot expose it.

Do you have the opportunity to target the collection to avoid at-risk data in the first instance? For structured data, consider de-identification or anonymizing what is collected by using unique identifiers for protected data points that are not relevant to the matter.

For unstructured data, it may be unrealistic to collect only unprotected data, but consider whether at-risk data can be identified, either by custodian or resident file paths, for downstream risk mitigation through specialized workflows.

Data Transfer. One often-overlooked area of risk involves the transfer of data between parties. During a discovery matter, data can be transferred via myriad methods including physical collection, shipping, e-mail, secure file transfer protocol (SFTP) and so forth.

Because there are so many means to easily transfer electronically stored information, it pays to build and enforce structure around data transfers between parties. Some or all of the means previously named may be appropriate for your matter.

One of the primary risk mitigation strategies in this area involves encrypting data in transit. If collections are being performed, the collection kit should ideally include an encrypted laptop as well as encrypted target drives on which to write the collected data. To that end, whatever your target media for physical transfer of at-risk data, encryption through hardware or software is advised.

Likewise, if transferring data electronically via SFTP or e-mail, consider utilizing software encryption to protect it. Requests to either e-mail documents to counsel/client/expert or upload documents attached to an e-mail to the review platform are common in the course of a matter. Encrypting an e-mail or its attachments is easily done if you find this means of transfer otherwise acceptable.

"In response to this incident . . . [Company] has installed encryption software on all employee computers . . . strengthened access controls including passwords, reviewed and updated security policies and procedures, and updated its risk assessment. In addition, all employees received additional security training."

THE UNITED STATES DEPARTMENT OF HEALTH & HUMAN SERVICES BREACH NOTIFICATION WEBSITE

Managing Your Partners

The examples discussed above deal with the hand-off from you to your business partners, but what happens to the data once it is in the hands of your partner, counsel or vendor? Data residing outside the corporate environment can be exposed to risk at a number of points in the typical discovery process.

Understand and plan for the way your partners approach risk mitigation while your data is under their control. Have a conversation with your partners that specifically addresses potential weak points such as:

- *The point of processing and hosting*. How secure are the machines performing the processing and hosting? Are the USB and print capabilities disabled? The Ponemon study attributed 27 percent of data breach risk to systems glitches.[6]

- *The point of review*. Are precautions being taken to ensure at-risk data cannot be accidently or purposefully off-loaded? Are e-mails rendered in such a way that the local instance of Outlook won't trigger inadvertent transmission when being reviewed natively? Are the review stations configured to disable USB ports and printing? Do reviewers understand the rules regarding the at-risk data? Are they empowered to identify it? Is there a special workstream for identified at-risk data?

- The Ponemon study indicated fully one-third of data breaches are the result of human error (not including malicious attack)[7].

- *The point of production*. Again we are dealing with data in transit that could benefit from encryption.

---

[4] US Department of Health & Human Services, retrieved from HHS Web site: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html

[5] See, for example, http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202601452412&Enron_Sandbox_Stirs_Up_Private_Data_Again&slreturn=20130818122022, http://www.ediscoverydaily.com/2013/05/some-additional-perspective-on-the-edrm-enron-data-set-controversy-ediscovery-trends.html

[6] Ponemon Institute, *Ibid*, at 8.

[7] Ponemon Institute, *Ibid*, at pg 3.

  DDEE ISSN 1941-3882

How is the production being transferred? Whether by physical media or SFTP, one should check to ensure encryption is being utilized.

■ *The organizational culture.* Are your partners fostering an organizational culture aimed at protecting at-risk data and can they point you to indicia of that culture? For example, are employees required to undergo regular training to facilitate understanding and mitigation of the risk? Do they have a documented program in place devoted to handling at-risk data? Are there administrative, technical and physical safeguards in place? Is a data loss prevention tool leveraged at weak points of access, for example, with the review or case team?

Why Wait for a Breach?

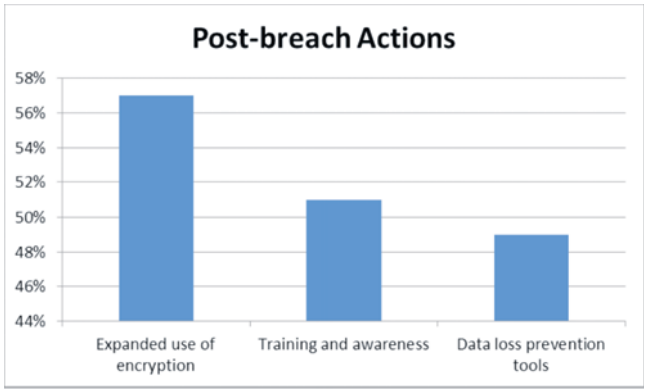
The actions corporate organizations typically take in response to a breach are the same actions the discovery industry should take proactively, at the outset of an engagement, to reduce the risk of breach in the first instance. The top three actions taken by organizations post-breach are:

1) expanding use of encryption,
2) providing training and awareness programs and
3) implementing data loss prevention tools.[8]

Each of these aspects of a high-risk data security program can be established proactively to reduce the risk of breach—rather than reactively following a breach—both within your partner environments and within the corporate firewall. Given the documented costs of a data breach, it behooves our industry to stand up and take notice.

Have a Plan!

The discovery process can expose corporate organizations, and the third parties they work with, to a heightened risk of breach by disturbing the data and taking it outside the protected corporate environment. Whatever the source of regulatory protection for data, breach is an industry-agnostic risk that presents several key opportunities for which discovery participants can and should plan.



Ponemon Institute: "2013 Cost of Data Breach Study: United States", May 2013

First, analyze how you are collecting data and look for ways to anonymize structured data or drive at-risk unstructured data into a more regimented workflow with your partners.

Second, review how you and your partners are transferring data and look to enforce encryption for data in motion.

Finally, your discovery-related data is exposed to a host of parties including outside counsel, experts, and vendors, any of which could be a weak point from a breach perspective and all of which should be able to speak to the physical, administrative and technological safeguards they have in place with respect to you data.

Understanding the path your data travels during the discovery process and having a plan in place for at-risk data with those that are exposed to it can pay dividends down the road.

[8] Ponemon Institute, *Ibid*, at 15.