Deloitte.

Digital Forensics in the Mobile, BYOD, and Cloud Era

A company suspected that one of its employees had started a competing enterprise and was transferring clients and assets to that business. An experienced digital forensics team was directed to gain access to the compromised company's information technology (IT) systems to collect evidence, including data from e-mail boxes in a cloud-computing environment. The forensics team accessed and analyzed the shadow accounting system that was a key to the investigation, and suspended potentially hostile users' access to the compromised company's systems. The forensics team provided the analysis results to the company's legal counsel in real time to support the filing of a temporary restraining order against the competing company[1].

In the story above, the early use of digital forensics proved invaluable in a company's investigation and legal pursuit of a renegade employee, helping avert potential large business losses. However, such effective outcomes can be challenging to achieve due to constant technology advancement. Today, vital evidence may lie in someone's smartphone, tablet, or as happened in this story, a cloud-computing environment. Finding, accessing, and securing data from such disparate sources can be a significant challenge, especially with the number of remote or contract workers that many companies employ today, the pervasiveness of outsourced IT services, and the increasing pervasiveness of bring-your-own-device (BYOD) environments.

Yet quick, decisive action is often crucial to determining the facts and protecting an organization's interests, whether the impetus is suspected fraud, a whistleblower claim, a lawsuit, or a regulatory inquiry. Organizations can strengthen their ability to address this diverse array of risks by establishing digital forensics as a standard procedure very early in internal investigations and making sure investigations encompass all possible data sources, while avoiding some potential pitfalls in forensics application.

A growing urgency

Digital forensics involves the collection, recovery, preservation, and analysis of data from digital devices. Its purpose is twofold: secure and safeguard the data, and provide the capability to search the preserved data as part of an investigatory or litigation process. (see "What is digital forensics?")

Not so long ago, gathering digital data for an investigation involved tapping into servers, rounding up laptops, and retrieving backup tapes. And today, it still does. But now the process can also involve retrieving data from, in extreme cases, potentially thousands of smartphones and tablets, both company-issued and employee-owned in businesses that allow BYOD. Add to device counts the increasing number of cloud storage and computing environments, and these disparate sources can require forensic specialists to deal with not only vastly more data, but also various operating systems and data formats. Such widely distributed environments can heighten the risk of data spoliation due to, for example, inadvertent overwriting of data.

[1] Deloitte client engagement experience.

Along with a plethora of data sources, the formidable and growing array of regulatory and legal risks facing businesses further increases the challenge and importance of digital forensics. Whistleblower provisions of the Dodd-Frank Act provide additional protection and incentives to employees to report suspicious activities to the U.S. Securities and Exchange Commission (SEC). Increased SEC investment in forensics capabilities is compelling many companies to proactively collect and preserve data in order to know what potentially may be found.[2]

Investigation and enforcement actions by the Financial Industry Regulatory Authority (FINRA) further demonstrate the need for the proper identification and preservation of digital data. FINRA recently sanctioned a company and one of its principals for failing to comply with guidelines for preserving business-related e-mails in both "firm" and "non-firm" email accounts.[3] Because such email accounts – especially non-firm accounts maintained by third-party service providers – are often cloud-based now, the implication is that financial institutions need to be much more vigilant about their internal written supervisory procedures and the actual review of samples of e-mails. The latter activity, in particular, can be more complex when e-mail accounts are maintained in the cloud and by third-party providers.

Beyond the federal government, other jurisdictions including states are working to embed digital forensics into law. For example, a bill proposed in Georgia regulating e-discovery includes rules for preserving electronic records and retaining documents, as well as sanctions for noncompliance.[4]

Facing such growing risks, organizations and their external counsel should consider the life cycle of a typical investigation and carefully assess their ability to act quickly in the earliest stages of an investigation with digital forensics capabilities scaled to meet potential challenges of their environment.

What is digital forensics?

Digital forensics is a multifaceted process for streamlining and simplifying discovery to uncover issues and increase investigation, litigation, and regulatory readiness. It can include a number of steps and impact various stages of an investigation, including:

- Data collection
- Data processing
- Maintaining chain of custody records
- Hosting
- Review
- Production
- E-mail analytics
- Social networking and timeline analysis

3 potential pitfalls in digital forensics

As noted earlier, it is important to regard digital forensics as a standard procedure and scope it in as early as possible in an internal investigation. Organizations can benefit from being alert to three potential missteps in that process:

Not having an up-to-date plan for identifying new or expanded digital data sources or procedures for preserving that data.

Many companies with processes in place for digital data management and preservation may not have reviewed and updated them for some time. With rapid technology evolution and expanding compliance demands, it can be valuable to promptly begin updating those processes and continue doing so on a regular basis.

[2] Aruna Viswanatha, "Defense lawyers balk as SEC makes play for hard drives," Reuters, January 16, 2013, http://www.reuters.com/article/2013/01/16/us-sec-enforcement-forensics-idUSBRE90F1EI20130116, accessed May 21, 2014.

[3] "Disciplinary and Other FINRA Actions, Financial Industry Regulatory Authority, January 2014, http://www.finra.org/web/groups/industry/@ip/@enf/@da/documents/disciplinaryactions/p428878.pdf, accessed May 21, 2014.

[4] Kathleen Joyner, Georgia Moves Closer to Regulating E-Discovery, Law and Technology News, January 21, 2014, http://www.lawtechnologynews.com/id=1202639221672/Georgia-Moves-Closer-to-Regulating-E-Discovery, accessed May 21, 2014.

Early assessment of data mapping can contribute to more efficient investigations, providing an accessible reference to sources of data and potential evidence. For example, this process can identify often-overlooked data custodians, such as administrative assistants with e-mail or file access to relevant information. Identifying media types not usually considered, such as mobile devices and backups, e-mail journaling vaults, and legacy systems, can help provide a solid foundation to support investigation procedures and transparency for outside review of company policies.

Also, understanding and addressing various regulations can help overcome red tape and legal ramifications of collecting data from foreign subsidiaries or overseas locations. *For one company, an early assessment identified a data gap and improper procedures for collecting and transferring digital personally identifiable information and Health Insurance Portability and Accountability Act (HIPAA) data across borders to the company's U.S. headquarters. This assessment and subsequent remediation helped the company proactively demonstrate information security and potentially reduced the risk of investigations or litigation.*[5]

Not involving a qualified forensics team early enough in the process.

Early collection of digital forensics by a qualified forensics team can help address technology issues at the outset of an investigation by identifying systems and data that may require additional time and effort to be extracted or converted. Also, preserving relevant data early can help reduce the risk of spoliation and the loss of information potentially critical to investigations or subsequent litigations.

In a recent FCPA investigation of a company's operations in Latin America, an early assessment of electronically stored information identified that e-mailboxes from departing employees were purged from the e-mail server after 14 days and were not backed up to tape. Also, the hard drives of departing executives were not archived or backed up, and the machines were wiped clean and issued to the next incoming employee. This discovery, by an external forensics team, prompted a recommendation to preserve the laptop data and e-mails of departing employees, keep their mailboxes active for a year, and then archive the data to tape for seven more years.[6]

At another company, network monitoring prompted suspicions of keystroke logging and led to an early investigation involving external forensics specialists. Affected computers were taken offline, and file analysis confirmed a false positive and no keylogging had occurred. By investigating early, the company was able to lay to rest concerns and avoid the unnecessary cost of imaging and analyzing a large number of computers.[7]

Planning for too narrow of a scope in collections

Casting a wide net early on in terms of the number of possible data sources and early identification and collection of more inclusive digital information can help reduce unexpected scope changes later into the investigation process.

In an investigation at one company, an external forensics team collected a wide scope of data at the outset, but only that which was necessary to meet investigator requirements was processed. As the investigation continued, government authorities requested additional data. The forensics team was able to process and provide the requested data more efficiently than if it had needed to conduct further collection, earning plaudits from the government. Broader collection practices allowed the company to conduct deeper analysis into certain custodian collections to determine the causes of missing e-mails. Had a narrower scope of collection been conducted, "e-mail only" for instance, the company likely would not have been able to respond to the government's subsequent enlarged requests, nor investigate the missing e-mail claims.[8]

[5] Deloitte client engagement experience.
[6] Deloitte client engagement experience.
[7] Deloitte client engagement experience.
[8] Deloitte client engagement experience.

An invaluable, timely tool

Many organizations that have employed digital forensics in both internal investigations and in responding to outside queries recognize the crucial role it can play in uncovering facts and protecting enterprise finances, operations, and reputation. However, as organizations adopt new technologies and as their approaches to the deployment of those technologies change, they should continually evolve their digital forensics practices to keep pace. Having an up-to-date plan for identifying and preserving critical data, employing a qualified forensics team early on in the process, and properly scoping the collection of digital information can help organizations conduct more in-depth and productive investigations.

Telling signs

Internal counsel, external counsel, internal auditors, compliance personnel, or others engaged in compliance activities should watch for any of the following terms that might appear in government information requests.[9] These terms may indicate the need for involvement by experienced digital forensics specialists:

- Electronically stored information (ESI)
- Evidentiary documents
- Electronic documents
- Preserve or Preservation of data
- Electronic production
- Document production
- Data compilations
- Electronic media hardware
- Imaging

[9] SEC Enforcement Manual, October 9, 2013, http://www.sec.gov/divisions/enforce/enforcementmanual.pdf, accessed May 21, 2014.

For more information, contact:

Kerry Francis
Partner
Deloitte Financial Advisory Services LLP
+1 415 783 4274
kfrancis@deloitte.com

Matt Larson
Principal
Deloitte Transactions and Business Analytics LLP
+1 404 220 1637
malarson@deloitte.com