Preserving Electronically Encoded Evidence

Robert E. Davis, CISA, CICA, is an independent management audit consultant, a Pleier Corp. author, and a Boson Software Inc. author and instructor. He has provided data security consulting and IS auditing services to the US Securities and Exchange Commission, the United States Enrichment Corp., Raytheon Company, the US Interstate Commerce Commission, Dow Jones & Company, and Fidelity/ First Fidelity (Wachovia) corporations. His workbook credits include *IT Auditing: An Adaptive Process, IT Auditing: Information Assets Protection, IT Auditing: Information Security Governance, IT Auditing: Irregular and Illegal Acts, IT Auditing: IT Governance, IT Auditing: IT Service Delivery and Support,* and *IT Auditing: The Process.* He has also written articles addressing IT issues for numerous journals and magazines.

Seeking to preserve electronically encoded evidence implies that an incident or event has occurred requiring fact extrapolation for presentation, as proof of an irregularity or illegal act. Whether target data are in transit or at rest, it is critical that measures be in place to prevent the sought information from being destroyed, corrupted or becoming unavailable for forensic investigation.

Anticipating this potential scenario requires information security management to proactively construct incident response and forensic investigation capabilities, considering legal imperatives. Evidence at rest or in transit requires adequate security procedures to ensure evidential nonrepudiation. Consequently, procedures addressing the infrastructure and processes for incident handling should exist within the security response documentation inventory.

INTERCEPTING DATA

To enable the demonstration of due care, extracting in-transit electronically encoded evidence should be sanctioned through approved authorization procedures. Legitimate in-transit data extraction is commonly known as lawful interception (LI). LI is generally recognized as the legally endorsed official right to access private communications. The means and authority for conducting LI are often recorded in governmental laws or regulations. Such mandates include, but are not limited to:

- US Communications Assistance for Law Enforcement Act (CALEA) of 1994
- The Netherlands' Act Aftappen Telecommunications Network and Public Services of 1998
- UK Regulation of Investigatory Powers Act (RIPA) of 2000
- Part XI Section 88 of Germany's Telecommunication Act of 2004

Regarding IT-related transmissions, LI supports information extraction activities when a network operator or service provider grants law enforcement officials accessibility to monitor, review, tag and/or capture communications of suspect private individuals or groups. For instance, LI can be utilized to capture an employee's inbound as well as outbound data packets to specifically identify delays and/or inconsistencies in transactional treatment.

Generally, as suggested in the Internet Engineering Task Force (IETF) informational request for comment (RFC) 3924, "Cisco Support for Lawful Intercept in IP Networks," management should ensure that the entity's personnel are unable to perform LI processes themselves. Furthermore, the deployed LI process should:

- Prevent detection by targeted parties
- Ensure that appropriate authorized personnel know about specific interceptions
- Disable the capability for separate agencies targeting a subject to detect each other during electronic evidence collection

Adherence to these constructs will normally aid in ensuring legal evidence admissibility.

EXTRACTING STORED DATA

Primarily, all potential electronically captured evidence should be protected (as soon as possible) from deletion, contamination, modification and inaccessibility. When dealing with stored data, prudent information security management dictates informing appropriate parties that evidence will be sought through electronic discovery from the target IT—establishing specific protocols that address preserving electronically encoded evidence and enforcing eradication restrictions for data residing within the target IT. In addition, when feasible, electronically captured evidence should be stabilized in the environment that existed during the suspected inappropriate activity.

Conditionally, if the target system is turned off, simply turning the technology on and permitting a "boot" can introduce content changes to files directly or indirectly connected through operating system procedures. Some files interacting with the IT boot process may not be of interest to an investigation. Nevertheless, IT boot configuration modifications can cause

previously deleted files—containing pertinent information—to become irretrievable.

When circumstances will not permit the maintenance of the embryonic operational state and site until law enforcement authorities arrive or when management accepts lawful extraction risks, data acquisition procedures may be invoked for evidence preservation. Data acquisition procedures involve the process of transferring encoded content into a controlled location, including electronic media types associated with an incident or event.

Upon commitment to this course of action, all earmarked hardware media, as well as the target content, should be protected during transference to another medium, through an approved methodology. However, capturing volatile data (such as open ports, open files, active processes, user logons and other random access memory information) is also critical in most situations where evidence integrity can become an issue. By definition, volatile data are transient electronic bits. Therefore, without adequate precautions, volatile data cease to exist when information technology is shut down.

> "…Simply turning the technology on and permitting a 'boot' can introduce content changes…"

Volatile data capture assists investigators in determining the system state during the incident or event.

IMAGING SOFTWARE

Creating evidential copies through routine backup procedures will permit replicating only specific files, while none of the files with delete indicators nor the designated "free space" between files is recovered. To remediate this limitation, task-oriented software should be used to obtain a forensic image. Appropriate forensic-imaging software reproduces an exact working copy of the original media's content. Technologically, media content imaging can be carried out without launching the computer's operating system, thereby avoiding tempering allegations, if acquired electronic evidence is utilized for prosecuting criminal misconduct. Functionally, applied imaging software should be capable of making an exact replication of every encoded bit contained on the target media.

Forensic-imaging software can capture residual data on targeted drives. Residual data include deleted files, fragments of deleted files and other data that still exist on the electronic media's recording surface. With appropriate tools, even data commonly considered destroyed can be recovered from a magnetized surface for forensic analysis. Effective imaging replicates a disk surface sector-by-sector, as opposed to reproduction file-by-file. Depending on the product, imaging software can also generate a log file recording of IT parameters, such as disk configuration, interface status and data checksums, that are critical for supportable conclusions regarding an incident or event.

Functionally sound imaging software and practices are essential to maintaining evidential continuity. Specifically, after creating at least two certifiable media images, one replication can be inserted as a target system substitute for the original media, while the second replication can be utilized for forensic analysis. Once facsimiled, the original media should be sealed in a sterilized container, labeled and stored as evidence in a secure area until required for judicial proceeding.

CONCLUSION

In summary, whether target data are in transit or at rest, it is critical that measures be in place to prevent the sought information from being destroyed, corrupted or becoming unavailable for forensic investigation. When evidence is at rest, adequate procedures should be followed to ensure evidential nonrepudiation. Volatile data capture assists investigators in determining the system state during the incident or event. Consequently, the utilization of functionally sound imaging software and practices is essential to maintaining evidential continuity.

REFERENCES

Baker, Fred; Bill Foster; Chip Sharp; *Cisco Support for Lawful Intercept in IP Networks*, USA, The Internet Society, October 2004, *www.ietf.org/rfc/rfc3924.txt?number=3924*

Sheldon, Andrew; "Forensic Auditing," *IT Audit*, 15 January 1999, *www.theiia.org/ITAuditArchive/index.cfm?act=ITAudit.archive&fid=108*

ISACA, *Information Systems Standards, Guidelines and Procedures for Auditing and Control Professionals*, USA, p. 137-42, *www.isaca.org/standards*