

The SOX-HIPPA Impact on the Legal System: A Case Study of a Law Firm

Stan Lewis, The University of Southern Mississippi, 118 College Drive #5178, Hattiesburg, MS 39406, USA; E-mail: s.lewis@usm.edu

Ernest W. King, The University of Southern Mississippi, 118 College Drive #5178, Hattiesburg, MS 39406, USA

Scott Magruder, The University of Southern Mississippi, 118 College Drive #5178, Hattiesburg, MS 39406, USA

Eddy J. Burks, Troy University, USA; E-mail: eburks@troy.edu

ABSTRACT

Ongoing research was conducted on the impact of technology on a law firm handling tort (civil) cases in the U.S. legal system. The firm used in the study is heavily involved in mass tort litigation and was the subject of a study previously reported at the IRMA 2005 International Conference [1]. The current research is the third of several planned studies on individual law firms and the legal system usage of technology. Specifically this segment of the research is to determine the potential implications of the Sarbanes-Oxley Act of 2002 (SOX) and the Health Insurance Portability and Accountability Act (HIPPA) of 1996 regarding a law firm ensuring a security repository database for confidential client information that is subject to the sections of these two acts. All professional firms, especially law firms, have a legal and ethical obligation to protect clients' interests including documents. Both acts have increased the work (data) flow of professional firms due to increased need for the documentation of signed permission by individuals to access "sensitive" data from every source.

ORGANIZATION BACKGROUND

Research being conducted is limited to four areas of interest related to tort law within the category of civil law within the U.S. legal system: (1) to develop an initial descriptive technology-usage-and-trend benchmark for a single law firm handling tort (civil) cases in the U.S.; (2) to determine the costs and time currently known to provide existing professional services in the tort (civil) case area in the U.S. (cost versus benefit); (3) to use the findings in (1) and (2) as a basis in expanding the study into a study of representative, comparable firms with similar practices in the area of tort law; and (4) to collect and analyze data on the nature of the impact of technology on the U.S. legal system. The law firm in this study is identified only as the Professional Law Firm (PLF). It was chosen because it was accessible, and it is heavily involved in mass tort litigation which is one of the major health and litigation issues in the U.S. This phase is intended to develop insight into one illustrative intrusion issue that might have legal implications for a law firm as well as their clients.

REVIEW OF LITERATURE

In the May 2004 issue of *Government Technology*, the National Consortium for Justice Information and Statistics or SEARCH recommendations for nine milestones is presented. These milestones are: (1) Initiate the process and institutionalize a governance structure, (2) continue planning, (3) develop and use performance measures, (4) analyze information exchange, (5) adopt or develop standards, (6) create sound integration architecture, (7) develop the infrastructure, (8) improve agency and organization applications, and (9) establish interfaces [3].

The Dennis Kennedy.com web site that is immensely popular within the legal profession describes the complexity of issues facing the legal firm and justice system as a whole. Two quotes are worth repeating and allow the researchers to drill down through the justice system to the level of the law firm and the environment in which a firm operates. "The courts are very serious about moving to e-filing and judges want to get attorneys moved to electronic systems." "Computer forensics and electronic discovery tools have become standard tools for some of the best litigators. Increasingly, the evidence you may need exists in the form of e-mail or never was printed out onto paper." [4] Additionally, law firms and oth-

ers must ensure their IT efforts are compatible with their clients' efforts to meet the changing expectations regarding transparency and accountability in business processes and corporate accounting designed to improve public confidence in publicly regulated businesses. [5]

As part of the ongoing research to understand the impact of technology on legal firms and thus on the entire legal system we selected one intrusion tool for illustrative purposes that if not detected and protected against within the law firm's networked system that contains confidential privileged client information could compromise client corporations under the SOX and HIPPA acts. In short, the authors wanted to examine the issues related to protecting clients' interests (documents, access to documents, etc.) in a law firm that has a legal as well as ethical obligation to ensure that sensitive client data is well protected. No effort in this study was made to explore the potential legal implications to a law firm that fails to adequately protect sensitive data of its clients.

The intrusion tool examined in this segment of the study is the use of port knocking. The networked environment of today requires that information technology (IT) professionals utilize virus scanning tools, firewalls, network operating system features to manage the access to a given company's networked system. Most of the attention is focused on the use of well-known tools or procedures such as matching user names to passwords and the use of firewalls to reduce the intrusions by hackers.

This third phase of the ongoing study is an attempt to describe the technical issues and the related implications of several approaches (tools) available to those who wish to enter without authorization into a network and those that use such approaches for financial gain, illegal activities or for other reasons, areas with significant fraud prevention and detection implications – in short to compromise a law firm's client database. Intrusion tools which may be used by individuals engaged in fraudulent activities the authors describe how "port knocking" could be used as an intrusion tool to gain entry into a firm's network and thus allow someone to obtain (without authorization) corporate data (client, employee, financial, etc.) and/or be used by users (having authorized access) to the data electronically transfer classified or sensitive corporate data to others located internally and externally to the organization.

In simple terms port knocking refers to the technical interactions between two computers as one attempts to open a closed port and thus pass through the second's firewall. Managerial issues for the IT professional range from the routine management of the networked system including the firewall (good) to the use of the port knocking method to pass messages between computers (individuals) in a manner that bypasses or circumvents the normal network security features (bad). Port knocking as presented in the Linux Journal is a process for a remote user to connect to a server when the port (service) is closed and a firewall is in place. The remote user sends a sequence of requests to the server. All of the ports are closed and the firewall logs the attempts. Software is in place that monitors the firewall's logs. When a correct sequence of port attempts are detected by the software, then a given port will be opened and the remote user can then access the requested port. This is a form of "a stealthy method of authentication and information transfer to a networked machine that has no open ports". Port knocking also "...can be extended to transmit any type of information encoded in a port sequence." [6]

CASE DESCRIPTION

The law firm [PLF] used as the basis for this case study is considered a specialty firm that coordinates litigation efforts by legal firms located in thirty-five states that are involved in class action suits related to health care. The required legal documents (paperwork) and information change exponentially with the addition or deletion of new plaintiffs to existing litigation. A concurrent requirement is a database to permit the firm to manage the required coordination between separate suits in each separate legal jurisdiction. Thus, a law firm has a need to ensure that all client data held in repository for pending and past litigation is managed as if it was held in the client's own computer system.

Phase I: Strategic Considerations

The PLF at the beginning of the study phase reported that it was studying the potential that intrusion tools could have on its ability to provide a secure environment for its clients that find themselves under the guidelines of the sections of the Sarbanes-Oxley Act of 2002 and the privacy provided by the Health Insurance Portability and Accountability Act of 1996.

- Professional and non-professional staff (internal) access accountability
- Client and other non-firm parties (external) access accountability to reduce to a zero intrusion level to ensure confidential client data would not be compromised.

Phase II: Intrusion Effort Study

The researchers with the assistance of the law firm undertook an effort to demonstrate the electronic passing of text information between two networked machines using port knocking to bypass the network monitoring system in place for the law firm. This implementation did not require a firewall be used by the receiver. We illustrate this process with a sender (server) and client (receiver-law firm) software written in Perl. The server took the message, mapped the characters to predefined ports and sent the message to the client (external party). The client had the same port mapping information and decodes the message. One very important aspect is this process is meant to be "invisible" as possible, so the information was not sent all at once. Rather it was sent over (perhaps) a lengthy period of time. Thus, monitoring software at the sender's site will not detect a pattern of unusual behavior. At most, a stray packet here and there may be detected if the sender's organization uses a sniffer program as a component of its monitoring system since fraudulent activities can occur under the noses of those whose responsibility it is to prevent.

The PLF strategic planning was delayed due to aftermath of Hurricane Katrina but remains as a priority for the firm. The PLF has identified an initial set of issues since its recovery from the impact of Hurricane Katrina that must be included in the strategic planning and include the following areas of interest by the firm:

- Client data retention,
- Repository database management to ensure potential issues under SOX and HIPPA coverage for clients are met, and
- Increased intrusion detection

The partner in charge of operations management (POM) at the PLF currently has the IT staff developing a set of alternatives for consideration by the firm. These alternatives include, but are not limited to, the use of additional SOX and HIPPA compliant software guidelines and the development of an additional intrusion layer of security in the existing network firewall structure. Once the IT staff presents the alternatives including costing and capabilities to the POM the professional staff will be given an opportunity to provide input to the partners that will ultimately make the decision.

There is heightened awareness by the firm that as it moves past the recovery efforts related to Hurricane Katrina other issues will once again have significant ramifications on the decisions to be made by the firm. Since many of the court document repositories have been damaged or destroyed, the recovery effort undertaken by the courts for filing and maintaining records will shape the opportunities that exist to fundamentally change the legal system; this will, in turn, impact the direction individual firms will need to go regarding the filing and processing of tort litigation. An integral consideration is that of ensuring that law firm practices do not raise additional liability exposure issues for firm clients.

CONCLUSIONS

Currently the PLF is actively involved in strategic planning that is designed to allow the firm to address potential SOX and HIPPA issues concurrent to its representation of its clients. No specific time-frame was identified by the firm since the legal system in the area impacted by Hurricane Katrina is still addressing continuing recovery needs.

REFERENCES

- [1] Lewis, Stan; King, Ernest W.; Hsieh, Chang-Tseh; and Chen, Kuo-Lane; "Impact of Technology on the Legal System – An Initial study of a Law firm;" 2005 Information Resources Management Association International Conference Proceedings; San Diego, California; May 15-18, 2005; pages 922-923.
- [2] "Outline of the U.S. Legal System: The Civil Court Process," <http://usinfo.state.gov/products/pubs/legalotn/civil.htm>
- [3] Harris, Blake, "Building Blocks," Government Technology, Vol. 17, Issue 5, May 2004, 27-28.
- [4] Kennedy, Dennis, "2004 Legal Technology Trends: Do We Stand on the Threshold of the Next Legal Killer App?," <http://www.denniskennedy.com/pred2004.htm>.
- [5] Logan, Debra and Mogull, Rich, CIO, "Sarbanes-Oxley: Gartner on the Role of Technology," http://www.insidesarbanesoxley.com/sarbanes_oxley_articles, October 2006.
- [6] Krzywinski, <http://www.linuxjournal.com/article.php%3Fsid%3D6811>

0 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/proceeding-paper/sox-hippa-impact-legal-system/33264

Related Content

Sheaf Representation of an Information System

Pyla Vamsi Sagarand M. Phani Krishna Kishore (2019). *International Journal of Rough Sets and Data Analysis* (pp. 73-83).

www.irma-international.org/article/sheaf-representation-of-an-information-system/233599

Do We Mean Information Systems or Systems of Information?

Frank Stowell (2008). *International Journal of Information Technologies and Systems Approach* (pp. 25-36).

www.irma-international.org/article/mean-information-systems-systems-information/2531

Application of Improved Sparrow Search Algorithm in Electric Battery Swapping Station Switching Dispatching

Qingsheng Shiand Feifan Zhao (2023). *International Journal of Information Technologies and Systems Approach* (pp. 1-21).

www.irma-international.org/article/application-of-improved-sparrow-search-algorithm-in-electric-battery-swapping-station-switching-dispatching/330421

Interacting with Digital Information

Kamran Sedigand Paul Parsons (2015). *Encyclopedia of Information Science and Technology, Third Edition* (pp. 3762-3769).

www.irma-international.org/chapter/interacting-with-digital-information/112813

A Guide to Non-Disclosure Agreements for Researchers Using Public and Private Sector Sources

Paul D. Witman (2009). *Information Systems Research Methods, Epistemology, and Applications* (pp. 104-119).

www.irma-international.org/chapter/guide-non-disclosure-agreements-researchers/23471