

Compliance White Paper

September 1, 2005

Steven Richardson

srichardson@techpathways.com

www.TechPathways.com

Technology
Pathways

Compliance and Computer Forensics

Information security compliance requires the precise enforcement of policies and controls. Digital investigations utilizing computer forensics are an essential part of this enforcement. This white paper reviews key information security laws and regulations that mandate computer forensics for compliance.

Information Security Compliance Landscape

THE BIG “4”

There are four laws and regulations that clearly indicate the need for digital investigations: Sarbanes Oxley, California SB 1386, Gramm Leach Bliley and HIPAA. These laws/regulations specify investigation and response to security breaches or policy violations. In our opinion, without computer forensics, it is not possible to meet these requirements.

The “Big 4” were selected for this paper as they have the broadest implications for commercial organizations. They affect organizations that are publicly traded, store financial or medical information, or do business with a California resident. These broad criteria affect most medium to large businesses domestically as well as international companies that do business in the United States.

This paper will examine the “Big 4” and the role of computer forensics in achieving compliance to them.

Sarbanes Oxley

The Sarbanes Oxley Act was enacted to fight corporate fraud. Massive financial fraud at Enron, Worldcom, Global Crossing and Arthur Anderson led to the passing of this legislation in 2002. The SEC is responsible for enforcement of Sarbanes Oxley and all publicly traded companies must report yearly on the effectiveness of their financial controls. Corporate Governance has become a critical operational focus of organizations to ensure that they have the proper controls and audit processes in place to prevent and detect fraud.

The legislation has serious consequences for non-compliance. This includes civil and criminal penalties. In fact, Section 302 specifies that CEOs and CFOs are directly responsible for the accuracy of their company’s financial reports.

Much of the focus on Sarbanes Oxley has been regarding Section 404. Section 404 requires management to specify their responsibility for financial controls and report on the adequacy and shortcoming of the controls. Many companies offer products and services to help companies achieve Section 404 compliance.

Sarbanes Oxley has other provisions that have not received the same attention from technology and service providers. For example, Section 301 provides for the handling of fraud complaints and investigations while Sections 806 and 1107 mandates that companies must support and protect whistleblowers.

Section 802 is another important element in Sarbanes Oxley that forbids the intentional destruction, altering or falsification of financial or related operational records.

Many companies recognize the need for computer forensics as part of normal business operations and controls and it therefore indirectly supports Section 404 compliance. For Section 301, case law has established that computer forensics is required to properly investigate fraud. In addition, computer forensics is widely accepted as the only precise and reliable method to determine if digital records have been deleted and/or altered; therefore computer forensics is needed to maintain compliance with Section 802.

Computer forensics has proven itself in battling wrongful termination litigation, HR investigations, theft of intellectual property and e-Discovery management; all of these issues enhance the accuracy of financial reporting; thus supporting Section 404.

Section 301 and 802 compliance will require the use computer forensics as established by case law and by best practices. Organizations should have computer forensics capability anywhere and anytime in their organizations to ensure compliance with Sarbanes Oxley.

California SB 1386

Enacted on July 1, 2003, California SB 1386 requires organizations doing business in California to report security breaches that result in the unauthorized disclosure of a resident's private or financial information. The intent of this legislation is to thwart identity theft and consumer fraud.

Given the size of California and its economy, this law affects most domestic and international companies. Disclosure is required if an individual's name and either a driver license number, Social Security number or the combination of a financial account number and password is accessed. Notification is not required if the information disclosed was encrypted.

The law allows for civil actions to be brought against non-complying businesses or they may be enjoined by the court. The key for any business is to conduct a thorough investigation to determine if they "reasonably" believe that information has been compromised or not.

The legislation does not clearly define a 'reasonable' investigation of a security breach. However, current incident response processes have been documented by security organizations and government agencies. The National Institute of Standards and Technology (NIST) has provided clear guidance for government and commercial organizations to investigate security incidents.

NIST published the "Computer Security Incident Handling Guide", which specifically outlines incident investigation and the role of computer forensics to properly acquire and analyze the incident. NIST also clearly identifies "unauthorized access" as a type of security breach that their process addresses.

The Information Systems Audit and Control Association (ISACA) is an association of information technology auditors who utilize audit and control standards to improve their organizations' information security, compliance and governance.

ISACA has developed a checklist for incident response planning and implementation. This checklist specifically calls for computer forensics to determine if data has been compromised, altered or deleted.

In a nutshell, the NIST Guidelines provide practitioners with processes using computer forensics to investigate cyber crime. The ISACA checklist provides the planning and implementation criteria for creating an enterprise computer forensics infrastructure.

There are numerous other resources including the FIRST organization. FIRST (Forum of Incident Response and Security Teams) is an association of private and government CIRTs (Computer Incident

Response Teams). These CIRTs use FIRST to share information about incident response and the utilization of incident response tools (including computer forensics). The FIRST organization has a marquee membership of prominent commercial and government organizations.

With the potential liability of CA SB 1386 non-compliance, organizations must have immediate access to computer forensics capability. The decision criteria for deploying that capability internally or through outsourcing will be covered in the “Best Practices” section of this paper.

Gramm-Leach Bliley (GLB)

Gramm-Leach Bliley or The Financial Modernization Act of 1999 or simply GLB, has a broad spectrum of qualifications, requirements and regulating parties. Eight agencies and the states are charged with managing and enforcing the regulations.

GLB applies to financial organizations or any organization that collects or transfers private financial information for the purpose of doing business or providing a service to its customers.

The two regulations of GLB are the Financial Privacy Rule and the Safeguards Rule. The Financial Privacy Rule addresses the collection and dissemination of customers’ information while the Safeguard Rule governs the processes and controls in an organization to protect customers’ financial data.

The Safeguard Rule is enforced by the Federal Trade Commission. In addition to the public embarrassment of non-compliance, organizations may be fined thousands of dollars a day while they are non-compliant.

The Safeguard Rule of GLB calls for financial institutions to:

1. Ensure the security and confidentiality of customer information;
2. Protect against any anticipated threats or hazards to the security or integrity of such information; and
3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

As previously discussed in this paper, computer forensics is an integral part of investigating and auditing all of the above GLB Safeguard Rule elements. For response to incidents, GLB guidelines requires:

“Response programs that specify actions to be taken when the bank suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies;”

Technical guidelines that support GLB call for extensive Intrusion Detection System (IDS) response utilizing computer forensic investigations.

From the guidelines for security controls and the guidelines for incident response, we believe that GLB compliance requires the utilization of computer forensics both proactively and for incident response to ensure the privacy of client information and to exhibit due diligence in GLB compliant efforts.

HIPAA

HIPAA is the acronym for the Health Insurance Portability and Accountability Act of 1996. A primary goal of HIPAA is for healthcare providers to improve the privacy and security of their clients’ medical information.

Health care providers, records clearinghouses and health plans must comply with HIPAA. Trading partner organizations that handle medical records electronically would fall under HIPAA rules.

Several HIPAA rules have been finalized including information security which encompasses incident response. HIPAA defines a security incident as "... the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system."

HIPAA specifies thorough analysis and reporting of security incidents. The guidelines do not provide specific information on incident response policies, so organizations must consider their incident response policies carefully.

As previously outlined in this paper, NIST and ISACA specify computer forensic software as part of any reasonable incident response policy to clearly understand the scope of the incident. Determining, with forensic precision, what information has been compromised, when the compromise took place, what systems were affected, and if malware or backdoors that are invisible to non-forensic tools are still present, are examples of the types of investigations that are essential to having an effective incident response program.

In addition to security incidents, computer forensics plays a natural role in supporting overall information security by providing the investigation of any anomalies that could indicate policy or use violations that could jeopardize HIPAA privacy rules.

Computer Forensics Best Practice for Compliance

The review of the key investigation provisions of Sarbanes Oxley, Gramm Leach Bliley, CA SB 1386 and HIPAA clearly suggest a prominent role for computer forensics in achieving information security compliance. Implementing an enterprise-wide computer forensics capability for compliance support requires consideration of several issues to ensure that the organization is utilizing best practices in achieving compliance. These are critical criteria for overall organization risk and liability.

Traditional Forensics Versus Remote Forensics

Computer forensics requires accessing system data in a least-intrusive manner. Traditionally, this has meant removing the hard drive from the suspect computer and connecting it to a forensic workstation using a write blocker. This allows the forensic investigator to examine the data on disk without alteration. This methodology has several drawbacks. First, it is costly and slow to physically remove the disk from a server, and of course this means downtime and user dissatisfaction. Additionally, while no data is altered, important volatile data is lost because the system must be powered down to remove the disk. While the investigator may utilize system tools and freeware to access this data before the system is shut down, the data gathered is suspect as it may be compromised by malware running in the server.

These issues have given rise to a new generation of computer forensic tools that can examine a live system through your corporate network. By placing a small read-only agent on the server, disk data and volatile system data can be accessed and imaged via the network. This methodology, though new, has been successfully utilized in court. With the new generation of network enabled computer forensics, the investigations can be done quickly and at a lower overall cost than traditional computer forensics.

In-house Versus Outsource

Given the need for computer forensics capability to meet compliance requirements, the decision must be made as to whether to develop the capability to do computer forensics in-house or to outsource this capability. There are many competent computer forensics consultants available to provide this capability. This decision is based on several key factors.

- **Cost:** Outsourcing will initially minimize costs such as software and training. However, recurring service fees can easily exceed software purchase and training costs.
- **Headcount:** Outsourcing will allow an organization to not assign headcount to computer forensics but also requires a total reliance on the service provider. Computer forensics will typically not require full, dedicated headcount as skilled computer security personnel may be trained to perform computer forensics as needed.
- **Response time:** Utilizing in-house capability allows for immediate response to any incidents that are compliance relevant. With a service provider, there will typically be several hours before the investigator can respond to your needs. During this time, valuable IP may be stolen and data critical to the investigation may be lost or altered by the malware to cover its tracks.
- **Scope of forensic utilization:** With an in-house capability, the technology can be applied whenever needed. Given the high costs of utilizing a service provider, companies may be hesitant to investigate all incidents. Also, with an in-house capability, computer forensics may be applied in a proactive manner to forensically audit key applications and files for structural and policy integrity.
- **Court presentation:** Outsource services provide experienced investigators who typically have a law enforcement background. This is potentially an important element of an investigation and most internal IT personnel do not have an appropriate background.

Recommendation: Based on the key factors from above, it is our belief that a ‘hybrid’ strategy is best practice for most organizations. The hybrid strategy consists of having an in-house computer forensics capability to support compliance plus an established relationship with an outside service provider. Internal personnel should be trained to provide investigation services utilizing industry accepted tools and methods and handle the majority of cases. The service provider is then utilized for two scenarios. First is a situation where there is suspicion of insider involvement in illegal activities. Utilizing a service provider will eliminate any possibility of a cover up and will be able to support a court presentation of the investigation evidence if necessary. Second is a situation that exceeds the capacity of your inside forensic team such as a massive break-in requiring the investigation of hundreds of systems or answering a large eDiscovery request.

Conclusions and Summary

Compliance efforts require computer forensic investigation capabilities to investigate privacy and security incidents and whistleblower complaints that are received by management.

The reach of computer forensics must be enterprise wide and the response time must be immediate to demonstrate that the organization is utilizing best practices in managing and controlling their information security compliance. Our recommendation to achieve this best practice is with a hybrid approach with in-house capability supplemented with an outsource provider.

Information Resources:

CA SB 1386

http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html

<http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf>

SARBANES OXLEY

<http://www.sec.gov/about/laws.shtml#sox2002>

<http://www.sec.gov/about/laws/soa2002.pdf>

<http://www.sarbanes-oxley-101.com/sarbanes-oxley-TOC.htm>

<http://www.soqlaw.com/index.htm>

GRAMM LEACH BLILEY

<http://www.ftc.gov/privacy/glbact/>

<http://www.ftc.gov/os/2002/05/67fr36585.pdf>

http://www.ffiec.gov/exam/InfoBase/documents/02-joi-safeguard_customer_info_final_rule-010201.pdf

http://www.ffiec.gov/ffiecinfbase/booklets/information_security/information_security.pdf

HIPAA

<http://www.hhs.gov/ocr/combinedregtext.pdf>

<http://aspe.hhs.gov/admsimp/pl104191.htm>