BLUE LANCE

Applying LT Auditor+ to Address Regulatory Compliance Issues

An Executive White Paper

By

BLUE LANCE, Inc.

In today's business environments, computers and information systems have become critical tools in conducting business. The trustworthiness of these systems that a business depends on is vital and will increasingly be of interest to regulators. Relevant regulatory pressures depend on a number of factors, including industry type, size of the business, the degree of non-public information that the business processes, and the criticality of the business to the economic well being of the United States.

This paper explores the regulatory landscape that influences the demand for information security and specifically focuses on the role of security event monitoring within an information security practice.

Surveying the Legal and Regulatory Landscape

Let's consider some of the more influential laws and regulations that are helping to drive the demand for information security:

HIPAA

If a company is in the health care industry or is a business partner processing data for a company in the health care industry, the Health Insurance Portability and Accountability Act (HIPAA) requires the protection of certain health related information, protection that can only be reasonably achieved through implemented security controls (in accordance with security standards defined by the Health and Human Services Agency). All covered entities (i.e.; companies subject to the regulation) must comply with applicable security standards no later than April 2006, with the majority of entities obligated to achieve compliance by April 2005.

The information security related provision within HIPAA is Subtitle F –Administrative Simplification. Applicable security standards are defined in Code of Federal Regulations (CFR) 45 (parts 160, 162, and 164) -- the "Security Rule").

GLBA

The Gramm-Leach-Bliley act of 1999, known simply as GLBA, includes a provision that requires a company processing customer financial data to maintain the confidentiality of the data. Companies subject to this regulation include all Banks, financial service organizations, as well as many other types of businesses that have access to customer financial data.

BLUE LANCE

410 Pierce Street
Suite 300
Houston, TX 77002

www.BlueLance.com

The information security related provision within GLBA is Title V – Privacy. Applicable security standards are defined by various agencies assuming regulatory powers to enforce GLBA, including the Office of the Controller of the Currency (12 CFR Part 30), the National Credit Union Administration (12 CFR Part 748), the Federal Trade Commission (16 CFR Part 314), and the Securities and Exchange Commission (17 CFR Part 248).

Sarbanes-Oxley Act of 2002

The Sarbanes-Oxley Act of 2002 includes a provision that requires a CEO and CFO of a public company to sign off on the quality of internal control over the information used in the construction of financial reports. Weak security-related controls will need to be considered, since weaknesses can result in the integrity of the financial information becoming compromised. In addition, a company's public accounting firm is required to certify the effectiveness of internal controls, similar to the way a public accounting firm certifies the quality of financial reports. Stiff civil and criminal penalties directed against a CEO or CFO are stipulated for certain forms of non-compliance.

The main provisions within the Sarbanes-Oxley Act of 2002 that pertain to information security practices and controls are sections 302 and 404.

SB 1386

California's Senate Bill 1386 requires any company, regardless of where it is domiciled, to publicly disclose security breaches that "may" have led to an unauthorized disclosure of unencrypted data belonging to a California citizen and where the compromised data can used by a criminal to commit an act of identity theft. Data that is considered covered by this legislation includes social security numbers, credit card numbers, and driver's license numbers. SB 1386 is motivating companies to beef up the implementation of controls to prevent breaches, as well as increase use of detective controls, to enable a timely response to contain breaches and to demonstrate that "covered data" of California citizens has not been compromised (eliminating the need for a public disclosure).

USA Patriot Act of 2001

The USA Patriot Act includes provisions that require companies doing business in the United States to be prepared to provide information to law enforcement, if the company's records are perceived as valuable to combat terrorism. The powers granted through the Patriot Act are rather broad and normal legal requirements to support evidence discovery/ search and seizure have clearly been relaxed. Records that could be of interest to law enforcement include computer records and event logs that can be used to explain computer usage. Any company needs to be prepared to submit computer records to law enforcement in

BLUE LANCE

410 Pierce Street
Suite 300
Houston, TX 77002

www.BlueLance.com

accordance with law enforcement activity sanctioned by the Patriot Act.

The relevant provision within the USA Patriot Act, that can lead to requests from the FBI to access a company's computer security event logs, is Section 215, Access to Records and Other Items Under the Foreign Intelligence Surveillance Act.

Federal Information Security Management Act of 2002

The Federal Information Security Management Act of 2002, also known as FISMA, applies to all departments and agencies in the Federal Government, as well as to external businesses/contractors that process data belonging to the Federal Government. FISMA mandates the protection of information processed by the Government and requires all departments and agencies to implement an appropriate information security practice and to apply applicable baseline security standards. For most departments and agencies, the baseline security standards include detailed security event monitoring as defined by the National Institute of Standards and Technology (NIST).

The relevant provisions in FISMA, authorizing NIST to set security standards for the Federal Government, are sections 302 and 303. NIST has provided appropriate guidance through a number of documents, including the Special Publication 800 series covering various aspects of computer security.

FDA Modernization Act of 1997 -- 21 CFR Part 11

The 21 CFR Part 11 regulation was implemented by the Food and Drug Administration (FDA) to provide detailed rules related to new information processing requirements associated with the FDA Modernization Act of 1997. This regulation applies to any company requiring Food and Drug Administration (FDA) approval and mandates the protection of information that is electronically submitted to the FDA. The regulation specifically defines security event monitoring as a minimum requirement.

European Union Privacy Directive on Data Protection

The European Union Privacy Directive (EUPD) on Data Protection, a.k.a. Directive 95/46/EC, was intended to impose a requirement on any company outside of the European Union to protect personal data that flows from a country in the European Union into a county outside of the European Union. To ensure that data is adequately protected, the EUPD requires the implementation of appropriate technical and organizational measures to protect personal data against destruction, loss, alteration, or unauthorized disclosure or access. Many companies in the United States have applied for Safe Harbor treatment, offered by the Federal Trade Commission (FTC), to coordinate compliance with the EUPD.

BLUE LANCE
410 Pierce Street
Suite 300
Houston, TX 77002

www.BlueLance.com

The main information security related provision within the EUPD is Article 17.

Section 5(a) of the Federal Trade Commission Act

Section 5(a) provides consumers broad protection against any company doing business in the United States that is engaging in unfair or deceptive business practices. The FTC has used this act as the basis for enforcement actions against companies that have failed to respect their published privacy policies. Eli Lilly (http://www.ftc.gov/os/2002/01/lillycmp.pdf) and Microsoft (http://www.ftc.gov/os/2002/08/microsoftcmp.pdf) have both been the subject of the enforcement actions related to a Section 5(a) violation complaint within the last three years, and in both cases, the FTC enforcement action required the implementation of a comprehensive security practice.

Basel II – the new capital accord

One of the newest regulations came out of the Bank for International Settlements (BIS) last year and will have an international impact. The Basel II accord will require central banks using the services of the BIS to impose new capital reserve requirements on Banks operating within their countries. Basel II requires that "operational risks", in addition to other risk factors (credit and market risks), be factored into determining capital reserve requirements. Information-security related risks are a component of operational risks. This is the first time information-security related risks will be a factor in determining how much capital a Bank must place in reserve. Capital in reserve does not generate any revenue. The maturity of a Bank's information security practices, including the maturity of the practices of outside service providers that process a Bank's data, will be factored into a quantitative assessment of operational risk. Banks that have less mature information security practices or are dependent on outside service providers with immature practices will be penalized financially through the requirement to maintain higher capital reserves. The central banks need to refine guidelines to ensure that capital reserves adequately factor in operational risks. In the meantime, many Banks, and their outside service providers, will be motivated to improve their information security practices to be best prepared for the forthcoming changes in capital reserve requirements.

Broad guidance covering how operational risks will be factored into determining capital reserve requirements is provided in Section V, Operational Risk within the third consultative document entitled The New Basel Capital Accord, published on April 29, 2003 by the Basel Committee on Banking Supervision.

BLUE LANCE

410 Pierce Street
Suite 300
Houston, TX 77002

www.BlueLance.com

The Importance of Security Event Monitoring in Achieving Regulatory Compliance

A common element to the above laws and regulations is the need for regulated businesses to put in place comprehensive information security practices. Some of the laws, such as HIPAA, FISMA and the FDA Modernization Act, have resulted in regulators putting specific emphasis on the importance of security event monitoring. Other regulations may not be quite as explicit, but it is almost impossible to argue that "information protection" requirements are being effectively met, unless security event monitoring is performed to detect intrusive activity and ensure accountability.

With the above in mind, it is clear that there are many laws and regulations that establish a sound business case for increased information security; organizations subject to laws and regulations that fail to demonstrate due diligence in implementing appropriate information security measures incur elevated risks, including the risk of liability, the risk of being subjected to enforcement actions from regulators, and the risk of experiencing reputational losses with potential loss of customers (and revenue) resulting from negative publicity associated with non-compliance.

As we look toward the future, we must consider the implications of legislation currently before Congress (including many new privacy-related bills) and understand that the legal forces driving the demand for security can be expected to only intensify in the years to come.

Achieving an Effective Level of Security Event Monitoring

Although particular laws and regulations will generally not stipulate what system activities are to be monitored, the implication is that the level of monitoring should be sufficient so unauthorized access to information that should be protected can be recognized and acted upon. A business will need to consider various ways in which information can be compromised in determining the most effective level of monitoring. Opportunities may exist to monitor activity from a number of vantage points including:

- The operating system's perspective (using available system level auditing capabilities).
- The network communication perspective (using network traffic monitoring tools).

BLUE LANCE

410 Pierce Street
Suite 300
Houston, TX 77002

www.BlueLance.com

- From the perspective of the application processing protected information (using available application transaction logging capabilities).

- A database management system's perspective (using available database access logging capabilities).

The importance of a particular level of logging will be situational, where varying circumstances could make the information in one activity log important one day, but less important another day.

In order to design an effective monitoring policy, a business may seek guidance from the widely respected information security management standard, ISO 17799, and in particular, clause 9.7 within the standard entitled "Monitoring System Access and Use." Requirement 9.7.1 within this clause specifically advocates the importance of recording exceptions and other security-relevant events. This includes records of successful/rejected system access attempts (logons, logoffs, and connections) and other successful or rejected resource access attempts (including file access).

The business case for comprehensive monitoring at the operating system level can be further strengthened when considering scenarios that could compromise the confidentiality or integrity of information that needs to be protected. Examples of such scenarios (and potential compensating monitoring practices) include the following:

- Unauthorized review of information in files containing information that needs to be protected, including unauthorized access by employees possessing privileged access to administer access controls at the application, database, or operating system level.

  Compensating Monitoring Practice: Monitor use of privileged accounts and access to sensitive files.

- Ineffective access controls implemented either in error or by a security administrator that is inadequately trained, introducing an opportunity for unauthorized users to access information that needs to be protected.

  Compensating Monitoring Practice: Monitor changes to access controls and compare changes to management approved access authorizations.

BLUE LANCE

410 Pierce Street
Suite 300
Houston, TX 77002

www.BlueLance.com

- Unauthorized changes to application, system software (including operating system components), or other critical control files, with the intent of changing the behavior of the system and introducing opportunities that can lead to unauthorized access to information that needs to be protected.

  Compensating Monitoring Practice: Monitor changes to executable software and critical control files.

- Unauthorized access by someone who logs into a system under the account of someone else that is authorized to access information that needs to be protected.

  Compensating Monitoring Practice: Monitor suspicious patterns of activity following a successful logon.

- Attempts at systematically testing a system for weak controls, looking for unauthorized ways to enter the system and introducing opportunities to access information that needs to be protected without authorization.

  Compensating Monitoring Practice: Monitor rejected attempts at accessing resources.

- System infiltration by a computer virus or worm that is designed to randomly grab files and e-mail the compromised files to randomly selected e-mail addresses. If through a stroke of bad luck a grabbed file contains confidential information that needs to be protected, this type of attack could potentially lead to a violation of privacy related requirements. It may be worthwhile to note that the concept of designing a worm with file grabbing properties was experienced with the highly prevalent Sircam.A computer worm and is likely to be repeated with new viruses/ worms programmed with similar capabilities.[1]

  Compensating Monitoring Practice: Monitor attempts at accessing sensitive files out of a normal context.

- Exploitation of a technical vulnerability in the operating system or some other system software running in a privileged mode, allowing a skilled adversary to obtain "privileged control" over the compromised system and potential unauthorized access

[1]Based on Virus Incident Statistics reported by Trend Micro Incorporated, as of January 28, 2004, 1,765,727 computers were infected with the Sircam.A variant of the Sircam worm.

BLUE LANCE
410 Pierce Street
Suite 300
Houston, TX 77002

www.BlueLance.com

to information that needs to be protected on the penetrated system. Statistics reported by Carnegie Mellon University's Emergency Response Team (CERT) over the last 3 years illustrate a steep increase in reported vulnerabilities, with many vulnerabilities introducing ways to get unauthorized privileged access to vulnerable systems. 7,913 vulnerabilities were reported in 2003 and 2002, compared to 5,033 vulnerabilities reported over the previous 7 years, with many vulnerabilities affecting software that is in widespread use.

Compensating Monitoring Practice: Monitor for suspicious patterns of activity attributed to accounts that vulnerable software runs under.

In reflecting upon the above intrusive scenarios, one may begin to see a networked computer system as an inherently vulnerable environment and it may be easier to understand the challenges businesses will face in ensuring that protected information is effectively protected. Clearly, the statistics reported by CERT demonstrate that most businesses will be faced with continuing pressure to respond to vulnerabilities that affect their computer systems. In general, operating system level monitoring can help a business manage its vulnerabilities in two significant ways:

- By detecting the exploitation of vulnerabilities (many which may not be recognized until they are exploited).

- By monitoring systems that are known to be vulnerable and must remain vulnerable while a business waits for the opportunity to apply corrective measures. Delays in applying corrective measures can be due to delays in receiving fixes from the vulnerable software's manufacturer or delays in applying available fixes due to other reasons (e.g.; the business does not have the time to test and apply an available fix).

Vulnerabilities that are exploited can lead to other important controls and logs becoming compromised, further degrading the integrity of a penetrated environment. Maintaining a detailed record of activity from the operating system's perspective can be advantageous in validating the integrity of other important controls and logs, including logs at the application and database management system levels. Of course, this assumes that the operating system level monitoring capabilities employ reasonably reliable defensive methods to protect its logs. Without a record of activity from the operating system perspective, we would not have an independent "controlled" means to ensure that other logs recording access to protected information have not been tampered with.

BLUE LANCE
410 Pierce Street
Suite 300
Houston, TX 77002

www.BlueLance.com

Leveraging LT Auditor+ Capabilities to Help Achieve Compliance with Laws and Regulations

Organizations that are required to implement an effective security event monitoring practice will be able to take advantage of a number of features in LT Auditor+:

- The ability to use monitoring agents that record system activities from the operating system perspective. A detailed record can be generated of access to any file containing information that needs to be protected.

- The ability to use monitoring agents to implement an effective level of security-event monitoring, achieved through the monitoring of:

    - System access (logons, logoffs, and connections),
    - Administrative activities (e.g.; account management, access control management),
    - Use of privileged accounts,
    - Access to files containing confidential information,
    - Changes to access controls,
    - Changes to executable software and critical control files,
    - Suspicious patterns of activity following a successful logon,
    - Rejected attempts at accessing resources,
    - Attempts at accessing sensitive files out of a normal context,
    - Suspicious patterns of activity following exploitation of vulnerable software.

- The ability to monitor systems in a transparent manner.

- The ability to monitor Windows Servers and Workstations, Netware Servers, and SYSLOG-enabled computers/applications (including Unix Servers, Network Devices, and firewall appliances).

- The ability to install a monitoring agent from a remote location onto a computer that needs to be monitored, provided the installer has privileged access to the desired computer. This remote installation capability eliminates the need to be physically present at the computer and reduces the costs in deploying an LT Auditor+ infrastructure within an organization that has many computers that need to be monitored.

BLUE LANCE

410 Pierce Street
Suite 300
Houston, TX 77002

www.BlueLance.com

- The ability to configure and deploy a monitoring configuration from a central computer functioning as a management console to computers monitored by LT Auditor+ agents. Deployed monitoring configurations can be adjusted, on demand, from the management console, giving Blue Lance Customers the ability to throttle the level of auditing in response to changing monitoring needs.

- The ability of monitoring agents to report events in a real time manner, delivering the reports either through native operating system messaging capabilities, SNMP, or e-mail agents. Real Time Alerting can give a Blue Lance Customer the ability to recognize exceptional events (including attempted security breaches) quickly, so remedial steps can be promptly taken to contain an adversary and reduce the likelihood that information that needs to be protected will be further compromised. Real Time Alerting can be used to notify incident response teams of access to honey pot files (planted files with fake information that needs to be protected), in order to more easily identify an adversary, who has managed to penetrate an organization's infrastructure and who is searching for opportunities to compromise information that needs to be protected.

- The ability to use LT Auditor+ filtering methods in order to ignore extraneous data that is automatically recorded in native Windows logs, increasing the utility of the log files maintained by LT Auditor+ and avoiding unproductive information overload.

- The ability to archive native Windows logs for backup purposes and to enhance a Blue Lance customer's ability to investigate computer crime.

- The ability to protect the recorded activity in LT Auditor+ log files from being tampered with, including an ability to transfer log files to a separate log consolidation computer in order to simplify the management and protection of archived log files. Log file transferring can be configured to occur on a scheduled basis (e.g.; off hours) or can be configured to occur in response to an attempt at shutting down an LT Auditor+ agent (i.e.; a defensive transfer) or in response to certain detected events that may be indicative of an intruder (i.e.; another form of a defensive transfer).

- The ability to protect the integrity and confidentiality of communications between an LT Auditor+ agent and manager, through the use of cryptography and other control mechanisms.

BLUE LANCE

410 Pierce Street
Suite 300
Houston, TX 77002

www.BlueLance.com

- The ability to import LT Auditor+ log files into a relational database management system on the log consolidation computer, giving Blue Lance Customers a high degree of flexibility in querying activity information stored in the database using the LT Auditor+ SQL Report Generator or using other SQL oriented querying tools.

- The ability to use canned database management scripts to simplify the retention and archiving of historical data.

- The ability to audit the actions of an LT Auditor+ Administrator and to monitor the integrity of an LT Auditor+ architecture through status monitoring and transaction logging.

Conclusion

In conclusion, this paper has discussed the role of security event monitoring in helping businesses achieve compliance with applicable laws and regulations. Many laws and regulations are creating pressures on businesses to implement a comprehensive information security practice. Security event monitoring can be viewed as a strategic element of any information security practice and will be useful in validating that controls are working effectively. Through security event monitoring, a business acquires the ability to recognize and respond to intrusive/compromising activities, that if left undetected, could cause a business to fail to comply with applicable "information protection" requirements.

> **Note:** *If you would like more detailed information on how LT Auditor+ meets the requirements of particular laws and regulations cited in this paper, please visit Blue Lance's web site or speak to your Blue Lance sales representative to check on the availability of other relevant white papers.*

Bill Rudolfsky is the Chief Information Security Officer for Blue Lance, and a 23 year veteran in providing Information Technology Services. Within the last 12 years, Mr. Rudolfsky held various information security leadership positions for large organizations in the banking and financial services industry including the Federal Reserve Bank and JP Morgan Chase. His credentials include obtaining Certified Information Security Professional (CISSP) status in 1999.

BLUE LANCE

410 Pierce Street
Suite 300
Houston, TX 77002

www.BlueLance.com