WHITEPAPER

Balancing Security and Compliance with an SSL VPN

A best practice guide to securing your data and meeting corporate governance standards

By Cynthia Kawamura

www.safenet-inc.com

Overview

Laws, legislation, guidelines, regulations or standards are starting to significantly impact the way companies conduct their business and make strategic decisions. Companies implement policies, processes, checks and balances to ensure that they meet the business goal of legal, regulatory or contractual compliance. Failure to comply can often carry heavy consequences, ranging from fines, regulatory actions, lawsuits, to even criminal prosecution.

The Gramm-Leach-Bliley Act (GLBA or GLB Privacy ACT) was enacted in 1999 for the financial industry implementing standards for insuring the security, confidentiality, integrity and protection of customer financial records and information. This act prohibits the disclosure of nonpublic personal information regarding a consumer unless previously authorized by that consumer. Financial institutions are now required to provide notices to their customers regarding their information-collection and information-sharing practices, and must give them the option to “opt-out” of sharing their information to non-affiliated third-parties at any time. The ability to manage and update information quickly and timely is critical to the implementation and overall compliance of this policy.

HIPAA was signed in 1996 with the first deadlines for compliance starting in April 2003. This act outlines the security and privacy requirements regarding medical information. Within the healthcare industry, security refers to protecting the confidentiality of patient information and decreasing the means of inappropriate access, tampering or destruction of healthcare information. It identifies privacy as an individual’s right to keep individual identifiable healthcare information private, however, information can be disclosed with an individual’s prior authorization.

The Sarbanes-Oxley Act of 2002 was enacted in response to the ethical and financial problems that exist with public companies in corporate America. This act has rewritten the rules for corporate governance, disclosure and financial reporting. It requires CEOs and CFOs to be personally responsible for reliable financial reporting and it requires auditors to certify the underlying controls and processes companies use to reach their financial results. The intent of the act is to restore investor confidence in publicly held entities. It requires companies practice good corporate governance along with ethical business practices.

SSL VPNs can help organizations comply with these and other standards by enforcing stringent authorization policies on data and ensuring the information is securely managed real-time. Access Control and authorization to applications is locked down to a specific group of users at the application layer giving companies greater control. The capability to ensure data integrity is enforced through industry leading audit policies. Data is always secured via SSL encryption inside and outside the trusted network – even over wireless access.

Corporate Compliance and IT

While these acts are aimed at different types of industries, there is a common thread that binds them together. It is the common bond of information systems. Some of these company's systems house intellectual property and trade secrets while others hold confidential financial or healthcare information. Part of the new, competitive business environment today necessitates businesses move more of their critical applications to the Internet allowing 3rd party vendors, clients and employees remote access to these information systems. As employees become more mobile and travel to remote branches or client companies, the need to access critical data from the road increases. With wireless hot spots appearing in places local coffee shops, employees can not only access info, but also work off their own laptop giving them full application access with files, not just email like a PDA. Physicians are demanding access to their applications over a Web browser; from a home PC, a physician can view a patient's medical history, radiology images, vital signs as they are happening, and lab and test results as they come in to give proper care instructions to an on-site nurse or physician. With anywhere, anytime access to patients' information, doctors can provide them the highest levels of care and improve the overall quality of life.

With these new capabilities, however, come new complexities in the effort to maintain security and privacy. In light of these various regulations, information security is even more critical. Unlike other remote access solutions, SSL VPN technology is critical to these demands and is the only technology to effectively manage the security and access control for multiple groups of users. SSL VPNs provide the freedom to access data anywhere, the security of a VPN, and the ease of use that SSL gives us.

Many institutions today are at a crossroads by having to balance the risks and rewards of innovative technologies. They want new technology with better quality, functionality and ease of use, and decreased delivery time, but they don't want to pay the price. The price can be more than the dollar investment and may include the resources needed to implement and maintain, plus the overall changes in business processes that need to occur to leverage the investment. When it comes to investing in IT for business initiatives, cost is not an issue. The ROI can be calculated and measured. Investment in corporate compliance initiatives, however, is lacking. Many IT administrators are having to struggle with managing complex privacy and data protection issues with tighter budgets and fewer resources. Traditional VPN, leased line and dial-up technology are not appropriate for these new requirements and are harder to justify from a return perspective.

Even with these new rules and regulations, corporate compliance in regards to IT is not getting the support or attention from senior managers. A recent study by Business Software Alliance (BSA) found that 33% of companies think that recent corporate scandals, such as WorldCom and Enron, have impacted the success of their own business and 86% think that IT issues fall under corporate mismanagement. Yet, fewer than 18% of the companies have a system in place for regularly auditing the software on company PCs. There needs to be an increase in technical awareness regarding compliance at the senior level in order for IT administrators to effectively address corporate compliance issues.

While the new federal and state laws are mandating who may access information, how the information can be accessed, where and how information is stored, retained, destroyed, or delivered in the event of an audit, lawmakers maintain a “technology neutral” position. It is up to each organization to find the solution that best fits their needs. Each institution needs to know the details of each regulation and how to comply with it accordingly. For example, one of the most difficult aspects of Sarbanes-Oxley compliance is that it calls for real-time reporting of material events that could affect a company's financial performance. The time-sensitive aspect of this regulation will likely put significant pressure on existing data infrastructures, requiring deeper system integration and more intelligent analytics tools. It will require a significant amount of system integration investment as well as implementation of real-time notification and event-driven alerts. In order to achieve corporate compliance successfully, a secure information system is absolutely crucial.

SSL VPN technology will help meet these needs for real time reporting by allowing data to be accessible from any browser, anytime – yet securely. Also, with the increasing need to enable access to remote employees, partners, and clients, finding a solution that allows for secure remote access is critical. SSL VPN meets these needs and allows you the ability to use one system for all types of users without compromising convenience or security.

Achieving Compliance

Complying with these various laws and regulations can be a challenge, but with the right system in place, it can be accomplished. Effective and efficient internal controls and processes are the keys to making sure a company is compliant within. It is the processes that align policy to ensure the right information is provided to the right people at the right time and to deny access to those not entitled to specific data. Internal controls within a company can provide the means necessary by which senior management and executives can accept responsibility for the internal processes as well.

How are companies going to ensure compliance with these privacy and internal control requirements? How will upper management ensure the company’s compliance to the board of directors and the public investors? Senior management will need to understand the internal controls and processes within their company, and should perform short, high-level internal audits interviewing key players within the organization. This may include legal counsel to senior IT management staff to senior security officer and possibly some user/managers regarding critical business applications.

Part of compliance is the ability to measure or benchmark a company’s position at a specific time. These maturity models range from “do not exist” to “optimum” and depending on the level of maturity exhibited by the company, will likely identify the effort required by executives and senior management to get control over the internal processes. A “does not exist” maturity model is apparent if the organization has no documented policies or procedures, is not aware of the external compliance requirements and no existing processes for compliance with requirements. The goal for meeting compliance is to get internal processes to the point where balance exists between processes that are managed yet measurable.

At the opposite end of the spectrum is the organization displaying optimum maturity. This indicates all policies, practices and procedures are implemented, and internal controls and efficient processes are in place to enforce compliance to external requirements. Data within the IT systems is complete, accurate and valid during all phases of its lifecycle. A good mature model is a reflection that senior management and executives have accepted the responsibility for control of the organization. In this optimum situation, processes for running the organization are routinely monitored, control systems are analyzed, criteria exists by which to evaluate these controls and control deficiencies are identified, reported and repaired in a timely manner.

No matter where in the spectrum the maturity of the organization falls, identifying the benchmark or starting point is an optimum way to exhibit the executives of a corporation having exercised due care. Due diligence is displayed when the executives are involved in the process of developing the roadmap that will move the organization into the more "mature" levels of compliance.

Achieving a "mature" level of compliance entails optimizing your processes, creating a benchmark or baseline for compliance and implementing best practices for reporting approval. These steps document an ongoing effort to document improvement and will lead to a reduction in:

- E&O - Errors & omissions portion of your insurance premium for any information forgotten/omitted within the corporation when reporting
- D&O – Directors and Officers liability insurance. This serves as risk management to protect Directors and Officers in case of lawsuits against them.

In addition to sound policies, SSL VPN technology helps organizations meet this compliance by:

- Providing a central policy manager for all users – employees or outside groups
- Ensuring a high degree of data integrity because of the ability to limit application access and audit data
- Reducing risk management by limiting the ability to access data

Audit Requirements

The following is a checklist from the COBIT® audit guidelines*. These questions and inquiries will assist in bringing the electronic commerce information systems into compliance with external requirements. This list can be used for all systems, not just remote access. Give this list to your information technology management team or your senior IT administrator and have them compare this list to the critical business applications currently being utilized. Completing this checklist will help you determine the level of maturity for IT compliance and identify areas that may need additional evaluation. The focus of this list is how advanced two-factor authentication SSL VPN systems meet this audit need. Areas like firewall and anti-virus protection, along with security policies are not discussed here.

Audit Checklist	Yes
IT staff should check and ensure that security procedures are in place and are correct for: • Password protection • Access control • Authorization procedure • Data encryption technologies	 YES YES YES YES
Does the current authentication mechanism in place provide one or more of the following core features: • Single-use authentication (passwords are not reusable) • Two+ factor authentication (two or more authentication mechanisms are used) • Policy-based authentication (able to specify separate authentication procedures for specific events) • On-demand authentication (able to re-authenticate the user at times after initial authentication)	 NO, but two-factor authentication is stronger than single use methods YES YES
Is user access control based on rule of least privilege?	YES
Do procedures exist to resolve: • Is the user ID suspended after 3 consecutive, unsuccessful logon attempts? • Is authentication time limited to 5 minutes? • Is user informed of logon suspension, but not the reason for it?	 YES YES YES
Does the identified system present a warning screen prior to completing logon, informing the reader that unauthorized access may result in prosecution?	YES (Customized HTML)
Does the password policy include: • Initial logon identifying mandatory password change • Appropriate password length • Enforced frequency of password changes • Password dictionary checking for not allowed password values • Protection of emergency passwords	Two-factor authentication via iKey is better than passwords making this irrelevant
Is access to security data (sensitive transaction data, passwords, public keys) limited to need-to-know basis?	YES
Are security enforcement features implemented such as identification/authentication process repeated after specified period of inactivity?	YES
Are authorization procedures in place for all documents?	YES
Does application provide an audit trail to identify the source of input?	YES
Does the application log programs executed and transactions processed/rejected for the audit trail?	YES
Do audit trails exist to facilitate the tracing of transaction processing and the reconciliation of disrupted data?	YES

*http://www.usmd.edu/Leadership/USMOffice/AdminFinance/IAO/is/cobit-audit-guidelines.pdf

Summary

Corporate compliance is not just about good business etiquette any longer – it is the law. New government laws and regulations are now dictating the way organizations do their business, particularly any type of electronic business. Organizations are now being required to demonstrate better control and accountability to the public. Security and privacy of data, whether medical or financial, is absolutely critical, particularly with the increasing usage of the Internet and Web-based applications. In order to reach optimum maturity, organizations must choose a solution that will not only allow them to be fully compliant in terms of maintaining the privacy of confidential data, but also one that is easy to implement and simple enough for all users to pick up easily. Of all the solutions out in the market today, SSL VPNs are well-suited to meet the anytime, anywhere remote-access needs of all industries in general, while complying with the security demands of government regulations in particular.

www.safenet-inc.com

Corporate: 4690 Millennium Drive, Belcamp, Maryland 21017 USA
Tel: **+1 410.931.7500** or **800.533.3958** eMail: **info@safenet-inc.com**

Australia +61 3 9882 8322
Brazil +55 11 6121 6455
China +86 10 8266 3936
Finland +358 20 500 7800
France +33 1 41 43 29 00
Germany +49 18 03 72 46 26 9
Hong Kong +852 3157 7111
India +91 11 26917538
Japan +81 3 5719 2731
Japan(Tokyo)+81 3 5719 2731
Korea +82 31 705 8212
Mexico +52 55 5575 1441
Netherlands +31 73 658 1900
Singapore (1) +65 6274 2794
Singapore (2) +65 6297 6196
Taiwan +886 2 6630 9388
UK +44 1932 579200
UK (Basingstoke) +44 1256 345900
U.S. (Massachusetts) +1 978.539.4800
U.S. (New Jersey) +1 201.333.3400
U.S. (Virginia) +1 703.279.4500
U.S. (Irvine, California) +1 949.450.7300
U.S. (Santa Clara, California) +1 408.855.6000
U.S. (Torrance, California) +1 310.533.8100

Distributors and resellers located worldwide.