sageza

Market Review

January 2007

Avoiding Legal Surprises in 2007

Compliance, Privacy, and Electronic Discovery

By Lawrence Dietz

Information Security Practitioners are perhaps more concerned about the legal climate in 2007 than they are about the dangers of the information highway. Many organizations are bewildered about which laws and regulations take precedence and how to prioritize their activities for 2007. This article provides a straightforward approach to reducing compliance and legal agita.

Introduction 1
Compliance: A Result of Good Governance 1
Privacy 1
Electronic Discovery 2
What It All Means 3

The Sageza Group, Inc.
32108 Alvarado Blvd #354
Union City, CA 94587
510·675·0700 fax 650·649·2302
London +44 (0) 20·7900·2819
Milan +39 02·9544·1646

Given all the hype about SOX and watching executives from CA and Enron head off to prison, it's no wonder that many Information Security Practitioners are perhaps more concerned about the legal climate in 2007 than they are about the dangers of the information highway.

It has been fascinating to travel around the world and talk to government agencies and commercial companies about their perceptions of compliance and the dangers of litigation. Many organizations are bewildered about which laws and regulations take precedence and how to prioritize their activities for 2007. The purpose of this article is to provide a straight forward approach to reducing compliance and legal agita.

Compliance: A Result of Good Governance

First of all, bear in mind that compliance is the result of good governance and of documenting what you have done in a logical manner. All organizations are run on principles of good business and service to customers. Customers can be those who buy from the organization, citizens who avail themselves of government services, or fellow employees of other departments within the same organization. Consequently the starting point for any organization is to set down its key business goals.

Business goals should be mapped against legal mandates so that any technical mandates provided in the laws or regulations can be incorporated into the overall IT strategy of the organization. If the CIO deems it appropriate, then the organization can employ frameworks such as ITIL or COSO as well as standards such as ISO 17799 and its successor, ISO 20000.

Once this is accomplished, the organization can set about to establish technology tools that can foster business governance through IT governance. Tools here can enforce vulnerability patching priorities, password characteristics, protection for key personnel data, records retention policies, and so forth.

The organization then ensures that the IT compliance process is continuous and that documentation is accurate, reliable, and timely. Where possible, a third-party validation can be employed to confirm that the organization is following its own guidelines.

Privacy

Research during 2006 from CSI and others has indicated that financial gain has become the dominant motive for computer crime and abuse. There have also been indications that financially motivated attacks are increasingly being undertaken by teams rather than by isolated individuals. The teams consist of talent in spam, malicious code, phishing, and criminal orchestration. Research such as the Symantec Internet Security Threat Report released in September 2006 has shown that attacks are more targeted then ever before. There is also reason to believe that many attacks are designed to extract personal data because it is easy to monetize this data through a number of sources.

Recognizing the significance of the threat and the potential harm to its citizens, California passed the California Security Breach Information Act (SB 1386). This law requires any organization that maintains personal data and experiences a known breach or believes the information was compromised to notify the consumer. "Personal data" is defined as a last name paired with a first name or first initial and one of the following: a social security number, a driver's license or California Identification Card number, or a number from a bank account, credit card, or debit card, along with a password or security code that would give access to the account. Other jurisdictions have passed similar

laws and it is reasonable to assume that U.S. government will get on the data protection bandwagon as well.

In addition to personal financial information, other information is regarded as sensitive and must be protected as well. The UK Data Protection Act of 1998 provides a very clear definition of personal data:

> *In this Act "sensitive personal data" means personal data consisting of information as to-*
>
> *(a) the racial or ethnic origin of the data subject, (b) his political opinions, (c) his religious beliefs or other beliefs of a similar nature, (d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992), (e) his physical or mental health or condition, (f) his sexual life, (g) the commission or alleged commission by him of any offence, or (h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.**

While these descriptions have not necessarily been codified in U.S. law, they have gained general international acceptance and the prudent information security practitioner will take heed.

Know that the information is sensitive; it makes sense to increase the protection in place around this data with increased precautions such as higher levels of authentication and access control, host intrusion prevention, etc. As with compliance, it's necessary to document and test in line with stated policies and procedures.

Electronic Discovery

The electronic discovery field is an excellent example of the proverb "an ounce of prevention is worth a pound of cure." Large organizations are always under some level of threat from litigation and more often than not much of the evidence examined will be in electronic format. Email evidence is becoming the rule rather than the exception. Courts are reluctantly dealing with electronic evidence in most business-related litigation. In fact, the change to rule 26f of the U.S. Federal Rules of Civil Procedure will force attorneys to confront their worst fears: having to make critical decisions and commitments about electronic discovery and production early in the litigation cycle. The new rule mandates that the parties meet twenty-one days before their scheduled conference (required by Rule 16b) to meet and discuss any issues relating to preserving discoverable information; to develop a proposed discovery plan; to discuss any issues related to disclosure or discovery of electronically stored information (ESI) including the form or forms in which it should be produced, and to discuss any privilege issues, including the potential for a "clawback" agreement to be included in a court order.

Public sector organizations are not immune from e-discovery. Their concerns may not center around litigation, but rather around internal investigations and responses to FOIA (Freedom of Information Act) requests and other legitimate inquiries.

This means that organizations must understand the likely scope of the discovery and their ability to either produce or to analyze what the other side produces. In almost all cases there is a reciprocal discovery process so that each party is required to produce something. An organization must understand what information it has, in what format it is stored, and where it is located in

order to be properly prepared for this mandated meeting. The message is clear: archiving software that facilitates the process may be a required part of the organizational IT infrastructure if there is a strong likelihood of litigation.

What It All Means

The legal environment of 2007 may not be certain, but there are forces at work and clear trends that must be taken into account to minimize likely problems. In short there are three main takeaways:

- Compliance is the result of good governance. Any program designed to sequentially comply with multiple laws and regulations is doomed to failure.
- Selected data about individuals is regarded as personal and highly sensitive. This data requires additional information and physical security requirements. Failure to provide these requirements can lead to significant legal exposure.
- Litigation and investigations are going to be as prevalent, if not more prevalent, in 2007 as they were in 2006. Organizations must employ organizational methodologies and tools such as archiving to ensure their ability to respond to requests for production of electronic information in a timely and cost-efficient manner.

*http://www.opsi.gov.uk/ACTS/acts1998/80029--a.htm#2