

# Information Technology Security Trends

BY EMILY STAPF, CHRISTOPHER MORRIS, AND DAVID BURG

Companies increasingly come upon external forces that make diligent assessment of the soundness and security of their technology infrastructure and the information stored therein a necessity. Strategic or tactical business decisions resulting in mergers, acquisitions, outsourcing/offshoring, and emerging regulatory requirements, combined with ever-changing technology, escalate the difficulties associated with managing information systems while the dependence on the systems as agents of change and efficiency increase in parallel. From legislative actions such as Sarbanes-Oxley, which mandates tighter security controls, to more stringent requirements for reporting failures, to increased demands for access to data, more than ever companies are faced with the assignment of maintaining a secure environment while meeting dynamic, mobilized, and diversified business needs.

PricewaterhouseCoopers' third annual Global State of Information Security study, conducted in partnership with *CIO Magazine* and *CSO Magazine*, found that companies are addressing the complexities of their information security needs with strategic approaches that are trending proactive rather than reactive. Attorneys who stay connected to and are aware of the change will better serve their clients with a more robust appreciation of the evolving business landscape and potentially gain a competitive advantage in the marketplace. This article provides a high-level overview of key emerging information technology (IT) security trends.

## Trends

Disclosures of IT security breaches have increased public awareness and the perception that IT systems are more vulnerable, if not less secure, than in the past. Whether systems are more or less secure today is debatable, but the increase in the number of disclosures is not. This increase is driven by regulatory changes enacted to encourage the market to remediate weaknesses and ultimately implement more effective security apparatus. Consequences of the disclosure requirements and the subsequent awareness of the importance of IT security have reached the board level. As a result, there is a trend towards substantially increasing the level of responsibility and accountability associated with managing information security. The following sections expound upon these trends.

## Security Events

In a survey, more than 8,200 IT security professionals from 62 countries reported that their respective companies experienced an average of 824 security incidents or events in the prior 12 months. These events can be broken down into two main categories: 1) companies affected by the

event, and 2) the source of attack. Virtually all industries were subject to attack. Some industries such as financial services and government agencies were the focus of significant popular media focus. However, universities, manufacturing firms, health care providers and payers, and other businesses were affected as well.

The source of the attacks and the resulting security breaches ranged from traditional hackers, motivated by economic gain or status among peers, to disgruntled current or former employees, to lost packages and stolen equipment. Hackers are geographically distributed globally, potentially affecting their apprehension and prosecution.

## Proactive Measures

Reaction to the perceived threats includes an increasing trend of adopting proactive measures to protect against such events, and includes:

**Surveillance.** Companies are increasingly monitoring the data that enter and leave an organization. These tools can alert, and even prevent, this type of loss from occurring. Employers are also realizing that one source of data loss can be employees themselves. However, these surveillance approaches have varying degrees of permissibility depending on the privacy rules and regulations that exist globally.

**Encryption.** Recently there have been several media reports regarding laptop and other data or media being stolen where the data were not protected (encrypted) and were therefore easily accessible. Reaction to these events includes deploying methods to enhance the safeguard of information on such devices or the media on which such data are stored. One method of protection being adopted is to encrypt information so that it remains protected from unauthorized use.

**Multifactor Authentication.** Organizations are implementing additional levels of control surrounding authentication mechanisms. In the IT world, authentication means verifying that the person using the system is who he or she claims to be. Since external entry or access points to systems are often widely available (i.e., via the Internet), they are also widely available for attack. Thus, there is an increase in the measures surrounding the authentication processes. Means by which companies are addressing this issue include systems or solutions that require multiple forms of authentication in order to access critical systems and the data contained therein. Multifactor authentication uses a combination of something you know (password), something you have (token), and something you are (biometrics) to validate log-on credentials.

Law firms are increasingly global, with many offices, and are widely connected using technologies, thus suscepti-

ble to such attack like all other businesses. Imagine the impact of a law firm and the information stored on the firm systems being compromised. It is impossible to enforce the attorney-client privilege after a hacker gains improper access to information.

#### *Regulatory Drivers*

Regulatory compliance is one of the most powerful forces driving information security programs forward. Given the maturity of the legal and regulatory apparatus in the United States, there are many requirements that affect virtually all industries in different ways, including information stored in electronic form. Specific examples include the Sarbanes-Oxley Act, the Health Insurance Portability and Accountability Act, the Gramm-Leach-Bliley Act, and International Traffic in Arms Regulations. Surprisingly, given the importance of the regulatory requirements, compliance therewith is less than expected.

**Banking Regulations.** An area where banking institutions are focusing efforts is in connection with the FFIEC Multifactor Authentication in an Internet Banking Environment guidance. This guidance states that high-risk transactions must be protected by more than one factor of authentication. Banks are currently performing risk assessments to determine the number of applications affected and potential solutions to this challenging issue. Strategic actions to address this guidance, for which a December 31, 2006, compliance date has been attached, may include adding additional layers of authentication and notification to Internet banking applications. Banks are currently struggling to determine how to integrate these products while keeping a layer of transparency to the end-user. At this point, since this is the first year of the guidance being part of the annual regulatory audit, it is not clear what the penalties associated with noncompliance will be. In the past, infractions resulted in institutions being fined for each instance of noncompliance, so the same may apply in connection with these new regulations.

**State-Specific Regulations.** Another part of the legal and regulatory apparatus is the California Information Privacy Act (SB 1386), which mandates that personally identifiable data must be “adequately protected.” Additionally, if data are compromised, California residents must be notified. This act directly resulted in many organizations creating plans to cope with information breaches and the integration of privacy and security efforts within the company.

#### *Centralization*

Organizations are elevating governance associated with information security by creating a security intelligence function, centralizing security information management, and investing in new technologies and processes to analyze disparate sets of security-oriented data. The number of companies now employing a chief security officer (CSO) or chief information security officer (CISO) increased from 15 percent last year to 20 percent this year, and a higher per-

cent of senior security executives now report directly to the CEO or to the board.

**Funding.** Many analysts believed IT security budgets would decrease in 2006; instead, IT security is an increasingly larger budget line item. With increasing IT budgets, businesses can expend time, effort, and money to establish preventive programs for security. For lawyers, this translates to increased opportunity for compliance and regulatory policy work.

#### **Implications of IT Security to Lawyers**

IT security is quickly rising to the forefront of most companies’ global initiatives and is drawing increased regulatory compliance scrutiny across industries. The impact to the legal community is threefold:

- Increasing numbers of cyberattacks and breaches of IT environments are leading to a rise in mandatory disclosure associated with such infractions and related litigation.
- Regulatory requirements affect every sector of the global business community; accordingly, new policies, corporate governance, and internal compliance programs are being developed and implemented.
- Executives in CSO or CISO positions have direct reporting responsibility to the senior management or are considered senior management. CSO or CISO management positions will increasingly interact with in-house or outside counsel as a means to manage the evolution of the business and to manage and address shareholder risk.

**Regulatory compliance is one of the most powerful forces driving information security programs forward.**

Legal counsel must be aware of the developments unfolding in this space given the abundance of technology used to connect businesses, the rapidly changing legal rules and regulations, and the increasing importance of information systems on the business community. Furthermore, law firms themselves are not immune to IT security risks, and as firms increase their global reach and their technology dependence, the risks increase in congruence. ■

*Emily Stafj is a manager, and David Burg a director, in PriceWaterhouse-Coopers LLP’s Washington, D.C., advisory practice in the area of dispute analysis and investigations with a focus on forensic technology solutions. Chris Morris is a manager in PriceWaterhouse-Coopers LLP’s Boston advisory practice in the area of performance improvement with a focus on technology security.*