Information is widely exchanged in business transactions among employees, partners, customers, and other stakeholders. Organizations have a responsibility to protect consumer privacy and organizational proprietary information while ensuring compliance with laws and regulations. However, the explosive growth of internet use has brought about an escalation of concerns, including consumer confidence in online business activities, threats to data integrity, legal liability, and risk of financial loss from sources categorized as both external and internal to the organization. These and other types of risks result in ever-increasing threats to organizations.

The current regulatory environment within the United States has made the consideration of ethical and social responsibility issues of information technology use a strategic necessity. Several federal laws are directed toward specific industry sectors to increase corporate responsibility in protecting consumer privacy and accountability for the substance of their financial reports. For example, the Financial Services Modernization Act of 1999, also known as the Gramm-Leach Bliley Act (GLBA), requires financial institutions to maintain the privacy of electronically stored customer information through security controls for data integrity and for identifying with whom this information is shared (Federal Trade Commission, n.d.). The Health Insurance Portability and Accountability Act (HIPAA) of 1995 is intended to protect electronic health information (Hewitt, 2004). Standards for policies and procedures to limit unauthorized access to medical information were set in the Security Rule, published February 2003 (Gue, 2003). Section 404 of the Public Company Accounting Reform and Investor Protection Act of 2002, or Sarbanes-Oxley, requires publicly held companies to annually evaluate their financial reporting controls and procedures (AICPA, 2004). Although information security is not explicitly addressed, compliance may be incomplete without adequate security controls. Another example of federal legislation is the Family Educational Rights and Privacy Act (FERPA), which protects the privacy of student education records (ED.gov, n.d.). Controls are required to prohibit unauthorized access and to control the sharing of the information.

A STRATEGIC RESPONSE
Organizations must formulate a strategic response to oversee privacy concerns and remain compliant with applicable laws. This entails (1) an understanding of the sources of threats to privacy; (2) determining the lines of defense and identifying the specific tools, controls, and procedures to implement the defense; and (3) monitoring this initiative for effectiveness.
Understanding Sources of Threats to Privacy

Sources of threats may be categorized as internal, external, and both internal and external to the organization. Each of these sources may have differing motives, ranging from seemingly innocent to self-interest to malicious intentions, but may nonetheless cause financial loss or reduced confidence in internet-related business activities of the targeted organization.

External Sources

The diversity of challengers from the external environment include competitors, consumers, criminals, cyberterrorists, the government, and intruders. Competitors and industry spies may undertake intelligence gathering to gain access to copyrights, intellectual property, trade secrets, and other proprietary information. Consumer concerns regarding privacy may result in outrage or filing lawsuits against companies who fail to disclose data collection practices or comply with their own published privacy policy. Criminals may engage in various activities ranging from simple criminal trespass to sophisticated Web site defacing; distributed denial of service (DDoS) attacks; hacking and cracking; malicious code; identity theft; and stealing proprietary information. Cyberterrorists, whose activities are increasing in volume, sophistication, and coordination (Institute for Security Technology Studies at Dartmouth, 2001), undertake criminal activities to promote their political messages.

Government agencies investigating illegal activities may present a search warrant, or issue a subpoena as part of a discovery process, to digitally gather evidence from files and e-mail messages, subjecting internal information to external scrutiny. Other intruders, such as marketers, are able to impose upon the privacy of employees through cookies, pop-ups, and spam.

Internal Sources

Those within an organization, including consultants and employees, may inadvertently or intentionally cause their employer shared liability for their actions. If an employee engages in wrongful acts in the course of employment, then the employer bears legal responsibility for the consequences of these acts, even if the act was unauthorized.

Sources Both Internal and External

Threats may overlap the external and internal environments through sources such as business partners and technological failings. Business partnering may include formal and informal alliances established for a joint project, adding complexity to the already multifarious global nature of the internet. Technological glitches can expose organizational content to perusal by unintended sources.

Lines of Defense

Based on an understanding of threats, the defense against them must be formulated and reformulated as a continual process. Organizational defenses include an acceptable internet use policy, undertaking on-going employee training, monitoring and auditing of employee activities and documents, implementing automated defenses and procedures to update them, and securing adequate liability insurance. The effectiveness of this strategic response would be determined by assessing current operations, implementing proactive measures to reduce potential misuse, and continuously keeping abreast of technological advances, legislative and regulatory initiatives, and new areas of vulnerability.

CONCLUSION

Threats and vulnerabilities continue to evolve, resulting in a continued challenge to reduce risk. Organizations must be vigilant in keeping up to date on the latest threats and defenses. The response to threats must be proactive not reactive. A centralized approach, will promote enforcement of consistent policies and procedures throughout the organization. While the strategic response is important, it is critical that it becomes an integral part of the strategic planning cycle.

REFERENCES


Janice C. Sipior is associate professor of management information systems at Villanova University, Pennsylvania, USA. Her academic experience also includes faculty positions at Canisius College, USA; University of North Carolina at Greensboro, USA; Moscow State Linguistic University, Russia; and University of Warsaw, Poland. Her research interests include ethical and legal aspects of information technology, system development strategies, and knowledge management. She is chair of the Association for Computing Machinery - Special Interest Group on Management Information Systems (ACM-SIGMIS) and serves as a senior editor of Data Base, an associate editor of Information Resources Management Journal, and an editor-in-chief of Information Systems Management.