The advances in information technology during the last part of the 20th century produced an unintended byproduct – the erosion of personal privacy. The American public’s accelerating concern for protecting individual privacy and its fear of such new criminal phenomena as identity theft and cybercrime has been rapidly escalating the past several years. Federal legislation such as the Fair Credit Reporting Act, the Online Children’s Protection Act, effective in April, 2000, and the Health Insurance Portability & Accountability Act of 1996 (HIPAA), was enacted to address these growing concerns. The Gramm-Leach-Bliley Act (GLB Act) became effective on July 1, 2001, and addresses those concerns by imposing upon a wide array of financial services providers the obligation to establish privacy policies and to adopt and implement practices that safeguard customer personal nonpublic information.

Juxtaposed against Americans’ concern for individual privacy rights is the fear for homeland security. The terrorist attacks of September 11, 2001 prompted the Congress to react with record speed by enacting the USA PATRIOT Act of 2001 (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) a mere six weeks after the attacks. This law significantly increased the government’s ability to conduct surveillance under existing authority for government wiretapping in the United States.

American businesses are caught squarely in the middle of these evolving privacy and security issues. Although the pendulum swung significantly towards addressing the nation’s security concerns following the 9/11 attacks, it seems to have swung back to protecting individual privacy interests. Currently, governmental agencies, financial services firms and health care providers and health plans are subject to specific legal and regulatory requirements concerning the confidentiality of the personal information of their customers. But many other private firms, prompted by other legal and regulatory obligations imposed by both federal and state laws, are increasingly adding security enhancements to their agendas.

Businesses are facing a new security issue – the phenomenon of identity theft. Both the Federal Trade Commission and the Treasury Department have recently pinpointed identity theft as the number one consumer
The Impact of the Privacy Laws on Business Cybersecurity

complaint for 2002. Identity theft topped the FTC list for the third straight year, accounting for 43% of complaints in 2002. Published reports of computer hacking incidents, data security breaches and identity theft traced to lax company security systems and practices have grabbed headlines. Firms that found themselves victims of such incidents are both large and small, and are as diverse as universities, restaurants and tax preparers, as well other more traditional financial services firms and medical service providers. Any firm that is doing business and that utilizes a network or other sophisticated information systems, and/or does business on the Internet, needs to place security high on its agenda. Experts say that the cost of responding to security incidents is between 10 and 20 times the cost of planning for it. Failure to give adequate attention to privacy and security could very well cost a company in financial losses and fines.


Businesses should develop a written security policy that has prevention as its goal. It should cover system architecture, including both hardware and software; user rules (i.e., permitting access to customer information on a “need to know” basis only); and organizational and managerial policies. In the process, the policy can promote improvement of authentication, streamline processes, bring employees online faster and restrict access of departing employees faster. As with physical security breaches, businesses should have written procedures for steps to take in the event of a cybersecurity breach.

Increased attention to cybersecurity by American businesses produces both tangible and intangible benefits. Customer goodwill and confidence is enhanced with the knowledge that the business is concerned about the security of customer information. Strong and well-defined cybersecurity policies can have the collateral benefit of combating the increasing incidence of identify theft. As public awareness of privacy rights grows, legal experts anticipate an increase in privacy litigation. Adopting and implementing a cybersecurity plan can provide a victimized company with potential defenses to litigation by its customer-victims. Failure to plan for a security breach or to implement preventive measures can cost a company more than it realizes.