



The

Business Report & Journal

Covering Savannah, Hilton Head, the Low Country and Coastal Georgia.



• EDITORIAL & COMMENTARY

Monday, October 08, 2007

'Avoiding Identity Theft: Business Responsibilities'

Business Information Zone

by Robert C. Newman

Biography: Robert C. Newman, CISSP, is a lecturer of information systems in Georgia Southern University's Information Systems Department. He may be reached by e-mail at newmanrc@georgiasouthern.edu or at 912-486-7563.



Robert Newman

The recent explosion of information technology services and the public's embracing of wireless and Internet technology has resulted in a number of undesirable situations. All too often business organizations have not provided the necessary security and control functions to protect the organization's and client's information and database assets. The end result is the number of incidents reported daily regarding theft of customer records from government, public service and commercial computer system resources. Poor planning and decision making by financial and information system managers is a factor in the increase in the number of incidents of identity theft and fraud. This has placed databases containing sensitive data at risk and has increased the potential loss of a substantial amount of personal assets from private savings, checking accounts and credit card accounts. There is also an increasing liability for organizations to reimburse customers because of inadequate protection of the customer database information.

Identity theft financial losses are not isolated incidents! They are even more widespread than what is reported in the news. Many of these information system crimes involving identity theft issues are not reported to the public or to the data record owners. Organizations are hesitant in making these incidents public because of the negative feedback generated or the impact on the credibility of the organizations. Any organization can be a target for identity theft frauds. On-line sales organizations and financial institutions are prime candidates for a cyber attack; however government data assets are also becoming prime targets.

Business organizations should take a proactive stance when addressing the potential for losing or compromising data assets and other consumer records. These activities include the development of written policies that address the data and computing resources' confidentiality, integrity and availability (CIA). Two important policies include a computer-use policy and security standards and procedures.

A computer-use policy defines acceptable and unacceptable computer-use practices, promotes an understanding of responsible usage of organization resources, and serves to protect and conserve those computing resources. Typical sections in a computer use policy include:

- Computer-use policy statement
- Responsibilities
- Description of offenses
- Description of sanctions
- Disciplinary actions and recourse
- Definitions

Security standards and procedures address the user community's responsibilities as they apply to the protection, and prevention of problems, plus incident detection and response of the organization's computer and information system resources. The following sections are typically included:

- General responsibilities
- Security standards
- Prohibited actions
- Guidelines and required actions for:
 - Servers
 - Workstations
 - Physical security
 - Password security
 - Account administration
- Enforcement

Each of these documents contains numerous specifics relating to the organization's and employee's responsibilities and requirements for computer technology and the use thereof. The SANS Institute provides guidance for developing security policies. The Web site, located at www.sans.org/resources/policies/, provides an excellent overview of the acceptable policies and standards that should become part of an organization's security policy. Also included at this site is a template for an InfoSec Acceptable Use Policy.

A number of hardware and software tools available on the market address the various security needs of these organizations. Many alternatives, however, are expensive. The old adage is "pay me now or pay me later." Litigation and loss of intangibles such as integrity could cost much more!