CITADEL
INFORMATION GROUP, INC.

An Emerging Information Security Standard of Care

An emerging information security standard of care requires businesses and other organizations possessing sensitive information belonging to others to protect that information with reasonable information security measures.

- Federal laws, such as ***Gramm-Leach-Bliley*** and ***HIPAA***, require the protection of personal financial and health information.
- State laws, including ***breach disclosure*** and other personal privacy laws. California Civil Code 1798.81.5 requires every business to implement reasonable information security measures to protect personal information belonging to California citizens.
- ***Sarbanes-Oxley Paragraph 404*** requires every publicly traded company to protect its own financial information.
- ***MasterCard*** and ***Visa*** require all organizations that accept credit and debit cards to adhere to its ***Data Security Standard*** for protecting card information.
- ***The Federal Trade Commission*** (FTC) is using the full range of their enforcement authority to protect consumers from undue information security risk. [1]

In addition to the information security guidance contained in the above laws and regulations, there are several other sources of guidance in effective information security practices.

- ***FTC consent decrees on information security*** related to deceptive and unfair business practices have begun to establish a legal basis for a required standard.
- Organizations throughout the world are complying with ***ISO standards ISO 27001*** and ***ISO 27002*** for protecting sensitive information.
- The ***U.S. National Institute of Standards and Technology***, along with other Government agencies, has published several documents describing effective information security practices.
- The ***Information Systems Security Association*** and the ***Information System Audit & Control Association*** are both active in identifying effective information security practices.

These information security laws, regulations, and standards point to seven common features that, taken together, have begun to constitute an emerging information security standard of care.[2]

1. Establish ***executive management responsibility*** and authority for the management of sensitive information.
2. Document ***information security policies*** to comply with its responsibilities and duties to protect information, including a classification scheme for confidential information.

---

[1] Deborah Platt Majoras, Chairman, Federal Trade Commission, The IAPP Privacy Summit, March 7, 2007.
[2] See *An Emerging Information Security Minimum Standard of Due Care*, Robert Braun, Esq., Stan Stahl, Ph.D, Handbook of Information Security, Auerbach, 2004. An update was published in the *Privacy and Data Security Law Journal*, March 2006.

3. Provide employees with regular ***information security awareness training and education*** the organization's information security policies and their personal responsibilities for protecting information.
4. ***Securely manage the IT infrastructure*** in a defined and documented manner that adheres to effective industry practices, including secure network design, remote access management, network security maintenance, and network security monitoring
5. Provide appropriate ***physical and personnel protection*** for sensitive information, including screening candidates for employment and incorporating information security responsibilities in job descriptions.
6. ***Conduct information security due diligence with 3rd-parties*** with whom it shares sensitive information to gain assurance that the 3rd-party protects that information with at least the same standard of care as it must.
7. ***Conduct an assessment or review of its information security program***, preferably by an independent 3rd-party, covering both technology and management, at least annually.

Organizations that fail to meet this emerging standard of care expose themselves to significant costs.

- Direct incident recovery costs
- Costs for lost productivity, including employee misuse
- Fraud , embezzlement and other business losses
- Intellectual property losses
- Legal & attorney costs
- Loss of brand value

The direct costs alone can be considerable. The *Ponemon Institute* estimates that ***the average cost to notify a victim of an information security breach is more than $200.*** A company whose databases contain 1,000 financial records can expect to pay over $200,000 to notify their customers if their systems are breached.[3]

Organizations have to be concerned with more than the cost of a security incident. ***Organizations that fail to meet the standard of care may also have trouble asserting their rights to their own intellectual property should it be stolen***.[4]

There is also an upside for organizations that meet this emerging information security standard. By implementing an information security program encompassing these seven information security elements, an organization can not only minimize the frequency and cost of security incidents, it can ***lower its Total Cost of Information Security*** [SM] while more effectively using its information assets. [5]

Meeting the emerging information security standard of care is not only prudent, it is financially sound. That's why ***securely managing information assets makes good business sense.***

[3] http://www.ponemon.org/index.php
[4] Open Secrets: Can You Claim Your Trade Secrets Were Stolen If Your Security Was Sloppy, CSO Online, June 2004.
[5] *Total Cost of Information Security* is a Service Mark of Citadel Information Group.