NEWS RELEASE

Information Security Paramount Concern for CEOs – Especially Now

For Immediate Release
By Pam Parry

If corporations want employees and shareholders to be their top priority, then information security must become their paramount concern, according to industry experts.

Since February 2005, the media has reported 300 high-profile security breaches, such as the recent incident at Coca-Cola in which an administrative assistant allegedly tried to sell trade secrets to Pepsi.

“Increasingly information security is becoming a legal obligation,” said Thomas J. Smedinghoff, a partner in the Chicago law firm of Wildman Harrold. “It was historically a technical job for the IT department, but it is now a far bigger legal issue. An increasing number of laws, regulations, lawsuits and court decisions indicate senior managers have a legal obligation to protect their company’s information. Merely using passwords and a firewall is not enough today,” he added.

John DiMaria of BSI Management Systems agreed with Smedinghoff, adding that information security has never been more important because of its global consequences.

“Cyber Terrorism is a real threat as it presents the greatest opportunity to destroy the economic environment in the United States,” he offered as an example. “We have an obligation to protect our country and therefore our information. What is lacking in security is that we do not have a true security system in place globally. One solution may be ISO 27001, the internationally accepted standard for Information Security Management Systems (ISMS).”

More than 100 countries are members of ISO, who has now endorsed and supported ISO 27001, which was adopted in 2005. The standard outlines a framework for an ISMS – a process approach to managing vital corporate information. Once a company has implemented ISO 27001, it can then have the system certified or registered by an outside third-party that audits and verifies its conformance to the standard.

Although the standard is a voluntary approach, and does not guarantee regulatory compliance, it provides a critical tool for CEOs and other senior managers who are grappling with legal requirements that they provide “reasonable security,” Smedinghoff said.

“The international mutual recognition certification scheme for ISO 27001 makes it the touchstone for comprehensive and verifiable information security management practices,” said Barry L. Kouns, security consultant and principal with SQM-Advisors, a security, quality and management consulting firm.

“When organizations implement ISO 27001, not only do they safeguard assets through best practice controls, they empower their organization with a risk assessment methodology that assures the proper treatment of all risks to the business,” Kouns continued. “The risk assessment

methodology allows an organization to be ever responsive to new risks and to address each risk in a manner most suitable to their organization at the time."

"Information security is not about a specific technology," Kouns said. "While a technical security control may provide protection for a time, a well-established risk assessment methodology will provide the means for an organization to protect their business at all times."

In the United States, only 39 companies have sought certification, which indicates America has not yet grasped the urgency of the problem, according to DiMaria. Pointing to the Coca-Cola incident, DiMaria said companies need a systematic approach to training, policies and awareness of potential security breaches.

"If you have no process, you lose every time."

One organization that has embraced ISO 27001 as a tool for information security is the United Nations. Dino Cataldo Dell'Accio, information security officer at the United Nations, said the U.N. discussed a variety of options for managing its information and decided the international standard was "the best option for us" because it was comprehensive enough to meet organizational needs. "The ISO programs we felt were the best because they include all types of securities," Dell'Accio said.

This comprehensive approach to security concerns may well be the solution for many companies and their CEOs who want the best possible protection.

"Certification to ISO 27001 makes a statement globally to your employees and stakeholders about the commitment levels you take to secure your company," DiMaria said.

For senior managers considering ISO 27001 certification, one security specialist makes three primary arguments for why they should invest in the standard.

Taiye Lambo, founder and chief technology officer of eFortresses Inc. in Atlanta, argued that ISO 27001 is the only internationally accepted Information Security Management Systems standard that provides a "comprehensive, holistic security framework." This approach allows companies to address regulatory compliance and to mitigate legal, contractual and regulatory problems, if a breach does occur.

"The standard also provides for third-party verification – this can provide a publicly traded company tremendous protection in investor and customer confidence," Lambo said.

Lastly, he contended that companies should implement ISO 27001 because they want to do the right thing in terms of information security. Taking all necessary precautions in the form of international best practices simply represents doing the right thing.

"Implementation and certification can take six months to two years, depending upon the complexity of the organization and existing safeguards," he said.

"Certification to ISO 27001 is a powerful step for an organization toward effecting and demonstrating compliance with internationally recognized best practices in information security," Kouns said. "The standard provides an organization with a continuous protection methodology

NEWS RELEASE

allowing a flexible, effective and defensible approach to security and privacy compliance. The most powerful aspect of certification is the demonstration to customers, employees, suppliers and business partners the validated existence of a fully operational risk assessment methodology and information security management system," Kouns added.

Pam Parry is a freelance writer based in Nashville, Tenn., who has written extensively about ISO standards.

- ENDS -

About BSI Management Systems

BSI Management Systems provides organizations with independent third party certification of their management systems, including ISO 9001:2000 (Quality), ISO 14001:2004 (Environmental Management), OHSAS 18001 (Occupational Health & Safety), ISO/IEC 27001 (Information Security), ISO 22000 (Food Safety) and ISO 20000 (IT Service Management).

As one of the world's leading management systems registrars, BSI Management Systems has more than 40,000 clients worldwide thereby helping all kinds of organizations improve their business efficiency and reduce their risk. BSI Management Systems operates from four regional hubs based in the UK, Europe, Asia and America, with the capability to deliver assessments worldwide, reinforcing BSI's commitment to deliver assessments with an unrivalled level of consistency across the world. This assessment capability is further augmented by training and advisory activities deemed essential to guiding clients towards the successful adoption and implementation of best practice.

For further information about BSI Management Systems information security services, please visit: www.bsiamericas.com/infosecurity

Contacts:

BSI Management Systems, 12110 Sunset Hills Rd, Suite 200 Reston, VA 20166
800.862.4977 www.bsiamericas.com

eFortresses Inc., 3340 Peachtree Road NE, Suite 1800 Atlanta, GA 30326
404.238.0588 www.efortresses.com

Wildman Harrold, 225 W. Wacker Drive, Suite 3000 Chicago, Illinois 60606
312.201.2000 www.wildmanharrold.com

Security-Quality-Management Consultants, 350 Osprey Circle St. Mary's, GA 31558
912.227.1323 www.sqm-advisors.com