Policy Considerations for Securing Electronic Data

CYBER SECURITY INDUSTRY ALLIANCE

APRIL 2005

A firestorm of reaction to recent breaches of security at data brokers, universities, and other entities that have large databases filled with personal information has resulted in calls for regulating the storage and processing of personally identifying information. Toward that end, new legislation is expected to be debated before Congress in coming weeks. Additionally, hearings in both the House of Representatives and U.S. Senate are underway to identify policies for protecting consumer privacy, reducing identity theft, and ensuring the safekeeping of individually identifiable information.

Accomplishing those objectives requires not only implementing many technical security safeguards and best practices, but also requires application of security policies governing the processing and storage of personal data. Members of the Cyber Security Industry Alliance have extensive experience creating solutions for the technical safeguards and recognize that while these safeguards are not a "silver bullet," preventing further disclosures, they can significantly reduce the risks of such breaches.

The CSIA offers this briefing to explain the role of security technology as it applies to proposed legislation for securing personally identifiable information. CSIA also suggests policy considerations for the proposed legislation.

PROBLEM SUMMARY

Many large organizations, from corporations to universities and health care systems, are conducting more of their business using network technology such as the internet. Therefore, customers, employees, students and patients are having their personally identifiable information gathered into vast electronic data storage repositories. Some industries already have requirements to protect personally identifiable information, such as the banking and health communities. Laws and regulations are being created at various levels to address security and privacy because the criminal activity related to stealing these electronic data is increasing exponentially. Multiple laws requiring potentially different requirements will quickly make compliance an overly complex task. A properly crafted statute from Congress may alleviate much concern and consternation within the industry and the public as a whole.

The problem of ensuring security and privacy of electronic data is complex. There are two fundamental issues requiring protection. First is ***protecting the storage*** of personal information in data warehouses such as names, addresses and Social Security numbers. The second issue is ***protecting the movement*** of these data to and from the data warehouse.

Technical security safeguards are used to address both the storage and movement issues. Policy is also crucial for it governs implementation of the technical safeguards and access to the data. Movement of the data amplifies the challenge of security because it creates weak points in the system. Those points are often outside the direct control of security administrators overseeing data warehouses. Policy plays a pivotal role in shoring up those weak points.

SECURITY TECHNOLOGY SAFEGUARDS

The core information technology application of large data holders is a data warehouse. It accumulates disparate records then analyzes, stores and distributes a vast amalgamation of information – billions of records about hundreds of millions of Americans. Many elements of the technology require special provisioning for security, including applications, systems and networks. A secure solution requires security provisions at the original source of data, at the data holder, at service providers, and at each customer location accessing the warehouse. The holder's control of security diminishes as information passes over external networks. Control vanishes once information is injected into the customer's internal applications.

Data Warehouse Security
The data warehouse's database management system handles security and access control. Securing the warehouse is mostly a function of establishing, granting and updating access control permissions and rights – a configuration process based on policy. Security requirements extend to appropriate configuration of access controls and permissions for software applications feeding information into the data warehouse.

Systems Security
Data warehouse technology operates on a networked system of servers. The servers may physically exist on premise at the data holder or at an external hosting service provider. Other systems for the data warehouse include access devices such as PCs, laptops, handheld computing devices, and telephones. Primary security for all systems is mostly a function of their operating systems. Proper installation, configuration and patching of bugs in the operating system software are crucial for secure systems.

Network Security
Network security requires three areas of focus: the internal network of the data holder, connections to and over the public Internet, and the internal network of the customer. Security provisions for these networks include a "multi-layer" strategy using a variety of solutions described in the box below.

Strategy: Definition	Importance
Policy Management: Enforces security rules and regulations.	Provides guidance to management on who should access what, when and where
Vulnerability Management: Remediate vulnerabilities through scanning devices that identify and patch vulnerabilities, as well mitigate misconfigurations, unnecessary services, unsecured accounts, and malware.	Addressing major classes of network and desktop vulnerability improves IT enterprise and operational stability.
Intrusion Detection/Prevention: Technologies that monitor content of network traffic for infections and block traffic carrying infected files or programs.	Reducing incoming sick traffic closes another window for criminals to access these data
Authentication: A critical step to ensuring appropriate users access the data using digital certificates and two factor authentication.	A way to confirm legitimate customers and control internal end user access. Strong authentication also prevents weak passwords from being hacked.
Encryption: Transforms data into password (key)-protected packets that prevent reading by unauthorized users.	Secure communication enables data warehouse vendors to safely and efficiently serve their customers.
Anti-Virus: Software automatically checks new files for infection.	Inoculates PCs and applications from diseased software code attempting to cause harm.
Firewall: Blocks unauthorized traffic from entering PCs and servers from the Internet.	Protects end users from unwanted activity on their PCs.

SECURITY POLICY CONSIDERATIONS

The security of data warehouses will require a blend of appropriate policies, technical expertise, and security technologies.

Technical provisions for security are aimed to thwart unauthorized access to personally identifiable information – whether by electronic hackers who break in by securing a legitimate password (e.g. NexisLexis), or by in-person fraud (e.g. ChoicePoint). Technical provisions are only as strong as the security policy which implements them.

Security breaches of data warehouses can adversely affect the life of any American so it is appropriate for Congress to establish national policies in conjunction with the private sector for the protection and privacy of personal information. As they develop these policies, CSIA urges Members of Congress to incorporate a framework for protection by denoting key areas of risk, security solution requirements and best practices.

In this context, CSIA recommends Congress to consider the following:

- Take a comprehensive approach to addressing cyber security issues. Currently, Congress is considering cyber security problems such as spyware, phishing, and data warehouse security on an individual basis. Understanding information security issues with a broad perspective, such as the Congressional Research Service report, "Creating a National Framework for Cybersecurity" can help lay the foundation for successful policymaking.

- CSIA supports federal preemption of the multitude of breach notification laws being passed in State legislatures.

- CSIA encourages the investigation of incentives, such as tax benefits, to encourage businesses to implement stronger cyber security.

- Harmonize any new legislation with existing legislation at the federal level, filling gaps rather than duplicating requirements already contained in existing law, such as Gramm Leach Bliley Act (GLBA), the Health Insurance Portability and Accounting Act (HIPAA) and the Fair Credit Reporting Act (FCRA). Use existing security standards wherever possible, rather than creating new ones.

- Encourage broader use of security technologies without mandating specific technology solutions. Urge adoption of the approach utilized in CA 1386 which calls for disclosure of a breach involving unencrypted data.

- Advocate for the Senate ratification of the Council of Europe's Treaty on Cyber-Crimes, which assures the public that appropriate resources will be available to prosecute cyber-criminals on a global basis.

ABOUT THE CYBER SECURITY INDUSTRY ALLIANCE

Launched in February 2004 by a group of cyber security software, hardware and services companies, the CSIA is an advocacy group whose mission is to enhance cyber security through public policy initiatives, public sector partnerships, corporate outreach, academic programs, alignment behind emerging industry technology standards and public education. The CSIA is the only CEO public policy and advocacy group comprised exclusively of security software, hardware and service vendors that is addressing key cyber security issues.

Members of the CSIA include BindView Corp. (NASDAQ: BVEW); Check Point Software Technologies Ltd. (NASDAQ: CHKP); Citadel Security Software Inc. (NASDAQ: CDSS); Citrix Systems, Inc. (NASDAQ: CTXS); Computer Associates International, Inc. (NYSE: CA); Entrust, Inc. (NASDAQ: ENTU); Internet Security Systems Inc. (NASDAQ: ISSX); iPass Inc. (NASDAQ: IPAS); Juniper Networks, Inc. (NASDAQ: JNPR); McAfee, Inc. (NYSE: MFE); PGP Corporation; Qualys, Inc.; RSA Security Inc. (NASDAQ: RSAS); Secure Computing Corporation (NASDAQ: SCUR), Symantec Corporation (NASDAQ: SYMC) and TechGuard Security, LLC.

Cyber Security Industry Alliance
2020 North 14th Street
Suite 750
Arlington, VA 22201
703-894-2742
www.csialliance.org