Preston|Gates|Ellis &
Rouvelas|Meeds LLP

# Cyber Security Regulation is ~~Coming~~ Here!

Presentation delivered to the 12th Annual RSA Security Conference – April 15, 2003

**by Bruce J. Heiman**

It is often said that Washington, D.C. is 69 square miles surrounded by reality. Unfortunately, for those in the cyber security business, reality is partially defined by what goes on *in* Washington, D.C.

Certainly the private sector should be taking the lead in cyber security protection. After all, it's the private sector that designed, developed and deployed the infrastructure, owns and operates practically all of it, and by far has the greater expertise in knowing how to best protect it. So it is not surprising that much of the government's rhetoric continues to recognize the need for private sector leadership and a "partnership" with the government.

But a closer examination of what the government has actually *done* reveals significant movement toward broader cyber security regulation and a patchwork of current cyber security requirements. As a result, you need to pay particular attention if you: are a health care organization or a financial institution; collect information from kids; do business in California; do business with the federal government; or have a privacy policy.

**Current Political Environment**

It's all about security all the time. Washington, D.C., as well as New York City, disproportionately feels the impact of security alerts. I work a block from the White House and heightened alerts mean we can't park in the building and that we have to practice "sheltering in place" drills to protect against potential chemical or biological attacks.

*A closer examination of what the government has actually done reveals significant movement toward broader cyber security regulation and a patchwork of current cyber security requirements.*

Neither political party wants to appear soft on security. Recent polls show that Americans are 30 percent more inclined to believe the Republicans are doing a good job to protect Americans than Democrats. This has led Democrats towards an even tougher security approach. As Sandy Berger, National Security Adviser under President Clinton, told the RSA Conference: "National security has now become personal security. We no longer feel invulnerable. … Our invincibility came crashing down on September 11."

Cyber security problems are getting worse. CERT reported 82,000 incidents last year, a 56 percent increase. Vulnerabilities increased 70 percent, to 4000. A February 2003 Symantec Internet Threat Security Report reviewed the experience of 400 companies in 30 countries. The report showed that the average company experienced 30 attacks during the last six months of 2002, an increase of 20 percent. Disturbingly, many of the attacks are now targeted at power and energy facilities, not just financial institutions or large businesses. Finally, the problem of proliferating spam also increases the general public's sense of cyber vulnerability.

# Cyber Security Regulation is ~~Coming~~ Here! *(continued)*

**The Government's Response**

The concept of a "security gap" is taking hold, and is defined by the difference between the amount of cyber security provided by the private sector and the amount deemed "necessary" by the government. The Bush Administration's strategy of preemption is finding its way to the cyber security sphere. The President's National Strategy to Secure Cyberspace states that: "We must act to reduce our vulnerabilities to these [cyber] threats before they can be exploited." The strategy says that government action is warranted where alleged "market failures result in under-investment in cyber security."

But of course, this begs the question – *who* decides when there is enough security? The President's National Strategy gives more authority and direction to the Department of Homeland Security. It now has the lead on coordinating partnerships on Internet protocols, router technology and codes of conduct. It also discusses large procurements and product certification as methods of driving the market. Finally, it is important to remember that, *so far*, there has not been a widely reported true terrorist cyber attack. Such an attack could lead to an explosive Congressional reaction.

**2002 Developments in Cyber Security**

The fastest worm ever documented – SQL Slammer or Sapphire, which doubled every 8.5 seconds – affected up to 300,000 servers, cut the speed of major U.S. Web sites in half, disabled an entire Washington State emergency response system and knocked much of Korea off-line.

The most significant governmental reorganization in a generation was created, the new Department of Homeland Security (DHS).

Presidential National Strategy to Secure Cyberspace was developed, and put much less emphasis on a public/private partnership; instead, it gave DHS the lead role in galvanizing certain recommendations and becoming program-driven in search of national solutions.

The largest cyber security R&D bill, authorizing $900 million in spending over five years, was passed.

The Federal government increased appropriations for cyber security to $4.7 billion for the Fiscal Year '04.

The seeds for potential rollback in encryption policy also have been sown. Senator Richard Shelby (R-AL), incoming Chairman of the Senate Banking Committee, which has jurisdiction over export control laws, already has proposed legislation that would give a preeminent role to the security agencies and remove provisions providing for automatic decontrol if there is foreign availability of a comparable encryption security product, or a determination is made that it is a mass-market product. Many, if not most, encryption products on the market today meet these tests. The so-called "PATRIOT II Act" also is reported to include a provision that would make the use of encryption to commit or hide a crime a punishable offense. While on the one hand not objectionable – concealing a crime already is punishable – there are serious concerns that it could lead to a presumption that the use of encryption is for criminal purposes. Even legislation in several states intended to prevent theft of service from cable operators and ISPs would prevent the use and sale of most encryption devices, another example of the law of unintended consequences.

The federal government also has moved to improve its own cyber security. This action is widely applauded and long overdue, but it also could lead to the imposition of similar measures on the private sector. The government could adopt the approach of "what's good for the goose is good for the gander."

The legislation creating the Department of Homeland Security included the Federal Information Security Management Act of 2002 (FISMA). This Act requires the development and implementation of mandatory "policies, principles, standards, and guidelines on information security" for all federal agencies by 2005. The National Institute of Standards and Technology (NIST) is charged with categorizing all federal information systems into "baskets" according to risk level and then developing flexible, performance-based standards for each basket. Importantly, NIST may not specify particular software or hardware security solutions. This prohibition was reinforced by NIST's FY '03 appropriations bill,

# Cyber Security Regulation is ~~Coming~~ Here! *(continued)*

which also precluded NIST from developing technologies that compete with cyber security technologies developed by the industry.

**Sector-Specific Requirements**

Health care, financial services and kids top the list of areas with specific cyber security requirements. The Health Insurance Portability and Accountability Act of 1996 requires health care organizations to maintain reasonable and appropriate administrative, technical and physical safeguards to ensure the integrity and confidentiality of "individually identifiable health information." Organizations must protect against reasonably anticipated threats or hazards to security or integrity, or unauthorized uses or disclosures.

*Health care, financial services and kids top the list of areas with specific cyber security requirements.*

Similarly, the Gramm-Leach-Bliley Act requires a broad array of "financial institutions" to adopt administrative, technical and physical safeguards to ensure the security and confidentiality of non-public personal information and customer records. Organizations must protect against any anticipated threat or hazard to the security and integrity of information and unauthorized access or use.

Finally, the Children's Online Privacy Protection Act requires Web sites to "establish and maintain reasonable procedures to protect the confidentiality, security and integrity of personal information collected from children." Reasonable measures are defined to be "measures that are feasible under available technology."

**Consumer Protection**

At this point, most companies have published policies explaining how they will protect the privacy of personal information. Many of these policies state companies will guard against unauthorized disclosures, but if they say what they are going to do, then they *must* do what they say.

If these companies don't fulfill the privacy policies they published, the Federal Trade Commission has made clear that it will bring enforcement actions. Take the case of Eli Lilly. The company maintained a Web site-based reminder and update service for Prozac users and posted a privacy notice representing they would protect subscriber privacy and that their Web site had "security measures in place." The company decided to shut down the service, and an employee sent an e-mail notice of discontinuation to all subscribers. Unfortunately, he did so collectively rather than individually. Recipients could therefore identify other Prozac users by their e-mail address.

FTC action resulted in a consent order requiring implementation of a detailed, comprehensive security plan. This included personnel policies, the identification of reasonably foreseeable internal and external risks to the security, confidentiality and integrity of information. The company also was required to adopt training policies and response plans, and had an on-going review and adjustment obligation.

Pending privacy legislation introduced by House Commerce Committee Consumer Subcommittee Chairman Cliff Stearns (R-FL) also includes provisions on information security. Many businesses support the privacy bill, which generally provides "opt-out" procedures and establishes federal preemption of conflicting state laws. But these businesses need to examine the infosec provisions, which would force them to take action in response to DHS directives and gives the FTC a strong role in cyber security regulation.

**Conclusion**

If you drop a frog into a pot of boiling water, the frog will instinctively jump out. But if you put a frog into a pot of cold water and gradually turn up the heat, the frog may get lulled into inaction and be boiled to death.

Those working in the cyber security area must realize that governmental regulation is already upon them and must plan accordingly.

---

Bruce Heiman is a partner in the Washington, D.C. law and lobbying firm of Preston Gates Ellis & Rouvelas Meeds LLP and serves as Executive Director of Americans for Computer Privacy (www.computerprivacy.org).