

# SECURITY DEBRIEF

[www.securitydebrief.com](http://www.securitydebrief.com)



Scott Weber

Cyber Security & Waiting for Godot

March 4th, 2009- by Scott Weber

The continued and growing reliance on networked operations, wireless systems and the globalization of information make a cyber attack a growing concern for the private sector and government.

Cyber attacks of computer systems and telecommunication networks are highly developed and increasingly used as a way to gain an advantage in the commercial sector, as well as a viable tool for terrorists seeking to cause economic destruction and ways to fund their operations. As business trade secrets and customer information become more vulnerable, it is clear that the public can wait no longer for cyber security standards.

In late December 2008, the FBI uncovered a worldwide \$9 million ATM scam that defrauded thousands of individuals and misappropriated sensitive personal information. It was one of the most sophisticated cyber attacks that the FBI has seen to date. The attackers targeted the computer systems of RBS WorldPay, an Atlanta based company that is a leading single-source provider of electronic payment processing services including debit and credit cards. By infiltrating a supposedly secure system, the cyber thieves stole information that they then used to duplicate the ATM cards of the unwitting public. Over 130 ATM machines from 49 international cities were hit by the criminal network, including machines in Atlanta, Chicago, New York, Montreal, Moscow and Hong Kong. The attackers used 100 fake ATM cards to access over \$9 million within a span of 30 minutes. Shortly after the theft, RBS WorldPay was sued in a class action for allegedly failing to protect personal information.

A better known case can be found in the massive cyber breach that the TJX Companies suffered. A network of hackers and thieves, over a 14 month period, breached this retail group's cyber system and stole the credit/debit card information, driver license numbers, and government identification numbers of approximately 455,000 consumers who returned merchandise to the stores. Banks claimed that tens of millions of dollars in fraudulent charges occurred as a result of the cyber breach. A subsequent class action lawsuit alleged that the retailer failed to maintain adequate security for consumer information.

The Federal Trade Commission (FTC) investigated the case and found that TJX engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for information contained in its networks. Specifically, the FTC found that TJX: stored personal

information in “clear text;” maintained unsecured wireless access; lacked password security; lacked a firewall to protect credit card information; failed to patch or update anti-virus software; and did not follow up on security warnings and cyber alerts. The FTC settled with TJX in March of 2008 and TJX agreed to, among other things: maintain a comprehensive security program reasonably designed to protect the security, confidentiality, and integrity of personal information that TJX collects from or about consumers; designate an employee or employees to coordinate the information security program; develop reasonable steps to select and oversee service providers that handle the personal information they receive from the companies; and retain independent, third-party security auditors to assess their security programs on a biennial basis for the next 20 years.

Cyber threats are constantly evolving and becoming more sophisticated. In response to this growing threat, a panel of public and private sector cyber security experts published a report entitled, [Securing Cyberspace for the 44th Presidency](#), which was released in December of 2008. The goal of the group was to provide recommendations that the Obama administration could quickly implement and to layout a long-term framework to ensure continued progress for nation’s future cyber security objectives. The commission found that cyber security is now a major national security problem; decisions and actions must respect privacy and civil liberties; and only a comprehensive national security strategy that embraces both the domestic and international aspects of cyber security will make us more secure.

The report issued twenty-five cyber security recommendations. Several of these recommendations are particularly relevant to the private sector:

### **Partner with the Private Sector**

- The U.S. Government should rebuild the public-private partnership on cyber security to focus on key infrastructures and coordinated preventative and responsive activities. We recommend the president direct the creation of three new groups for partnership that provide the basis for both trust and action:
  - A presidential advisory committee organized under the Federal Advisory Committee Act (FACA), with senior representatives from the key cyber infrastructures. This new body would incorporate the National Security and Telecommunications Advisory Committee (NSTAC) and National Infrastructure Advisory Council (NIAC);
  - A town-hall style national stakeholders’ organization that provides a platform for education and discussion; and
  - A new operational organization, the Center for Cybersecurity Operations (CCSO), where public and private sector entities can collaborate and share information on critical cybersecurity in a trusted environment.

### **Regulate for Cybersecurity**

- The president should create and task a new National Office for Cyberspace (NOC) to work with appropriate regulatory agencies to develop and issue standards and guidance for securing critical cyber infrastructure, which those agencies would then apply in their own regulations. Secure Industrial Control Systems and SCADA

- The new NOC should work with the appropriate regulatory agencies and with the National Institute of Standards and Technology (NIST) to develop regulations for industrial control systems (ICS). This could include establishing standard certification metrics and enforceable standards. The government could reinforce regulation by making the development of secure control systems an element of any economic stimulus package that invested in infrastructure improvements.

#### Manage Identities

- The Federal Trade Commission (FTC) should implement regulations that protect consumers by preventing businesses and other services from requiring strong government-issued or commercially issued credentials for all online activities by requiring businesses to adopt a risk-based approach to credentialing.

While the recommendations contained in *Securing Cyberspace for the 44th Presidency* are robust and reasonable — it will take time for the federal government to make meaningful progress on the cyber security front and, while we wait, cyber terrorists and criminals continue to develop more complex schemes that get worse with each attack.

What does this all mean?

It means that the private sector needs to continue to drive cyber security policy and technological advances. Companies that wait for the development of a comprehensive federal cyber security regulatory scheme are playing Russian roulette. Several standards already exist and enable organizations and businesses to practice certain security procedures in order to minimize their exposure to cyber attacks.

Although standards continue to be developed by the National Institute of Standards and Technology and other agencies, the most widely used standard today is ISO/IEC 27002 (ISO Standard). The ISO Standard addresses numerous areas including information security policy, asset management, human resources, environmental security, communications, and most importantly business continuity management and compliance. Although these evolving standards are voluntary, they provide legitimate and reasonable benchmarks to assist a company with prevention and mitigation — indeed, a company’s failure to embrace these standards will provide ample and powerful ammunition for use in lawsuits against that company if it is a victim of a cyber attack that results in loss (e.g., misappropriation of customer information, business disruption, or loss to third parties).

A great example of the private sector taking the lead can be found in the Mandatory Reliability Standards for Critical Infrastructure Protection developed by the North American Electric Reliability Corporation (NERC). These industry-wide reporting standards require certain users, owners, and operators of bulk power systems to establish policies to safeguard physical and electronic access to control systems, to train personnel on security matters, to report security incidents, and to be prepared to recover from a cyber incident. These standards went into effect in 2009 and are the first “mandatory and enforceable” reliability standards addressing cyber security for the United States bulk power system. The Federal Energy Regulatory Commission (FERC) approved these standards and granted NERC the legal authority to enforce the standards.

The implementation of cyber security standards is becoming increasingly more important for the private sector. However, no one can afford to wait. Don't become the next RBS WorldPay or TJX. Every company must be proactive and senior management has to support cyber security efforts to ensure a comprehensive and organic approach. Companies must adopt identity management policies and combine them with appropriate technology as the "threat from within" is just as great, if not greater, than a cyber attack perpetrated by an outsider.

The development of a comprehensive federal cyber security regulatory scheme is an important and lofty goal. However, remember what happened in Beckett's play *Waiting for Godot* — Estragon and Vladimir waited patiently but Godot never showed up.

*Scott Louis Weber is a partner in the law firm Patton Boggs LLP and is the former Senior Counselor to the Secretary of the U.S. Department of Homeland Security.*

<http://securitydebrief.adfero.com/2009/03/04/cyber-security-waiting-for-godot/>  
©2008 Adfero Group. All Rights Reserved.