

## **Securing the Financial Infrastructure**

Professor Kevin F. McCrohan<sup>1</sup>

Financial Services are unique among all of the critical infrastructures that support the global economy. It faces both physical and cyber threats, is considered a strategic target by all potential adversaries, and is threatened by a wide variety of groups and individuals. These groups include terrorists, criminals, hacktivists, social and economic anarchists, and cyber-vandals. At this time it appears that cyber attacks are most useful for targeting, espionage, and fraud. Physical attacks on major financial data centers or telecom nodes would have the most impact, with the loss of personnel in some areas also having a significant impact.

This paper will present an overview of the physical and cyber threats to financial services as well as suggesting strategies to limit the risks associated with these threats.

### **Terrorist Threats**

According to Symantec Internet Security Threat Report, banking and utilities are two of the most at risk sectors when it comes to threats from hackers and viruses writers, with the threat increasing as the size of the institution increases. These attacks certainly represent a mix of criminal activities and to a lesser extent terrorist and other malcontents. However there are indications of a strong interest on the part of "Jihad" related groups to attack US and allied banking and finance infrastructures.

In September 2002 a Jihadist hacker site announced a planned attack on Israeli financial sites. This was followed by a release from the "Center for Islamic Studies," which is believed to be close to Al Qa'ida. This organization called for Islamic fundamentalist programmers to "strike blows" against American organizations' sites and "teach them a lesson." There are some indications that this threat will grow as these groups become more sophisticated or develop links to organized criminal groups.

Of greater concern at this time is the threat posed by physical attacks. Interrogations of captured Al Qa'ida personnel indicate that the destruction of the financial infrastructure of the United States is a major goal of the organization. Were they successful the ramifications would be felt far beyond the US. For example, in April 2002 threats of suicide bombers were reported against US banks in the North East. This was followed by a steady flow of information, including statements by Bin Laden in October 2002. Given the goals of Al-Qa'ida, these statements were indicative of a potential terrorist threat against the US banking infrastructure. Following this, the then Office of Homeland Security to engage in a series of teleconferences with US industrial leaders. In these teleconferences a heavy emphasis was placed on increasing physical security, to include the deployment of counter surveillance teams. During this period the world witnessed attacks against soft targets in Bali and Manila.

Also at this time reports of the seriousness of the threat to the banking infrastructure was received from Manila. These reports noted that Abu Sayyaf had planned to use cell phones to electronically detonate

---

<sup>1</sup> Kevin F. McCrohan is a Professor of Marketing at George Mason University in Virginia, USA. He is presently serving as a US Army Colonel assigned to the National Infrastructure Protection Center (NIPC). The NIPC is located in the FBI and will move to the Office of Homeland Security on March 1, 2003.

ammonium nitrate bombs in trucks in a series of attacks on targets including the Manila Stock Exchange. Abu Sayyaf reportedly had engaged in target surveillance, prepared target folders, sought technical and financial support from Al-Qa'ida, and had met with Al-Qa'ida in Kuala Lumpur in July 2001. Additionally, a member of an outlawed Pakistani Islamic movement arrested in connection with parcel bomb attacks on Pakistani government agencies told authorities that one faction of his extremist group had actually wanted to use the parcel bombs to attack U.S. banks.

Current reports from the US indicate that the threat to critical infrastructures, including the banking and finance sector continues as the US Department of Homeland Security increased the threat level on February 7, 2003.

### **Criminal Threats**

In addition to terrorists the financial services industry is threatened by attacks from organized crime groups, with the most significant threat coming from the Russian and Eastern European groups. These groups exploit known vulnerabilities in Windows NT and 2000 operating systems. Their modus operandi includes scan, attack, and extort methodology. In these attacks, propriety information on customers, financial records, and credit card information is stolen. The victim bank is then contacted and uncooperative victims are threatened with the public release of information, the notification of victims, and direct attacks on victims.

### **Hactivists, Vandals and Anarchists**

In addition to the threats poised by criminals and terrorists, financial services are also threatened by hactivists, vandals and anarchists. Hactivists may be organized or unorganized groups that are engaged in cyber actions due to a particular incident, such as the May 2001 US-China cyber war, or long term issues, for example, the Pakistan Hackerz Club's anti-Indian actions. Cyber-vandals keep us busy by producing viruses and attacking networks. And, the social and economic anarchists threaten the banking community both physically, for example the animal rights groups, as well as through cyber attacks, for example the Electronic Disturbance Theater.

### **Mitigation Strategies**

As the preceding comments indicate, the threats against the banking and finance infrastructure are extensive. This implies that the involvement of senior managers is necessary if the firm will be able to harness the necessary physical and cyber security solutions. In a recent article, Dutta and McCrohan (California Management Review, Fall 2002) note that information security rests on three cornerstones. These are the structure of the organization; the technology deployed for operations and security, and the firm's involvement with public sector critical infrastructure protection programs.

One of the most critical aspects of this involvement with the public sector is the need to engage in information sharing between the public and private sectors. Certainly, only senior managers will have the authority to engage in such actions.

### **Conclusions**

The information presented in this paper indicates that the threat is real and growing. It also indicates that technology alone will not solve the problem. What will assist both the private and public sector is for managers in both sectors to take responsibility for the information security of their organizations and to strongly encourage information sharing initiatives.