GAO
Accountability * Integrity * Reliability
United States Government Accountability Office
Washington, DC 20548

June 29, 2005

The Honorable Joe Barton, Chairman
The Honorable John D. Dingell, Ranking Minority Member
Committee on Energy and Commerce
House of Representatives

The Honorable Fred Upton, Chairman
The Honorable Edward J. Markey, Ranking Minority Member
Subcommittee on Telecommunications and the Internet
Committee on Energy and Commerce
House of Representatives

The Honorable Cliff Stearns, Chairman
The Honorable Jan Schakowsky, Ranking Minority Member
Subcommittee on Commerce, Trade, and Consumer Protection
Committee on Energy and Commerce
House of Representatives

Subject: *Financial Market Organizations Have Taken Steps to Protect against Electronic Attacks, but Could Take Additional Actions*

The September 11, 2001, terrorist attacks on the World Trade Center exposed the vulnerability of the financial markets to disruption by such events. As part of a series of reviews we have performed at the request of Members of Congress, we have examined and reported on the adequacy of the steps that financial market participants have taken to reduce their vulnerability to attacks and to be better able to recover from such events when they occur.[1] In addition to taking steps to reduce the likelihood that physical attacks will damage their facilities, financial market organizations must also implement protections to reduce the potential for electronic attacks to disrupt their operations. Electronic attacks can be the result of individuals (such as hackers) or groups, such terrorist organizations or foreign governments,

[1]See GAO, *Financial Market Preparedness: Improvements Made, but More Action Needed to Prepare for Wide-Scale Disasters*, GAO-04-984 (Washington, D.C.: Sept. 27, 2004); *Potential Terrorist Attacks: Additional Actions Needed to Better Prepare Critical Financial Market Participants*, GAO-03-251 (Washington, D.C.: Feb. 12, 2003); and *Potential Terrorist Attacks: Additional Actions Needed to Better Prepare Critical Financial Market Participants*, GAO-03-414 (Washington, D.C.: Feb. 12, 2003).

attempting to gain unauthorized access to a specific organization's networks or systems or from malicious computer programs or codes, such as viruses or worms, that seek to damage data or deny access to legitimate users.

Given the importance of this topic, you asked us to review the measures taken by selected critical financial market organizations, including exchanges, clearing organizations, and payment system processors, to protect themselves from attacks and we reported our results to you in September 2004.[2] At the time we prepared that report, we were still completing our reviews of the seven selected organizations' information security protections. For this report, our objective was to assess the information security programs in place at these organizations. To maintain the confidentiality of the sensitive information we examined, this report refrains from naming the organizations we reviewed and presents the results of our work in an high-level, aggregated manner.

To assess these organizations' information security protections, we assessed whether the organizations had in place five key elements of a sound information security program. As discussed in guidance used for reviews of federal organizations, the Federal Information System Controls Audit Manual (FISCAM), five elements key of an information security program can include:

- Information security policies and procedures that cover all major systems and facilities and outline the duties of those responsible for security,
- Access controls to prevent unauthorized access to networks and information systems,
- Intrusion detection systems that monitor for attempts to gain unauthorized access to networks and information systems,
- Incident response procedures to address electronic attacks or breaches, and
- Testing and assessments of an organization's vulnerability to attack and audits of its information security practices and controls.

To determine how these organizations had implemented these five key elements for information security, we interviewed their key operations and information security officials. We also examined the security policies of the organizations we visited and reviewed documentation of their system and network architectures and configurations. We also compared their information security measures with those recommended in FISCAM, other federal guidelines and standards, and various industry electronic security best practice principles. We also reviewed internal security audit reports and their supporting documentation and any third-party network vulnerability assessments that had been conducted within the past year. We conducted our work in various cities in the United States between October 2003 and April 2005 in accordance with generally accepted government auditing standards.

[2]GAO-04-984.

Results in Brief

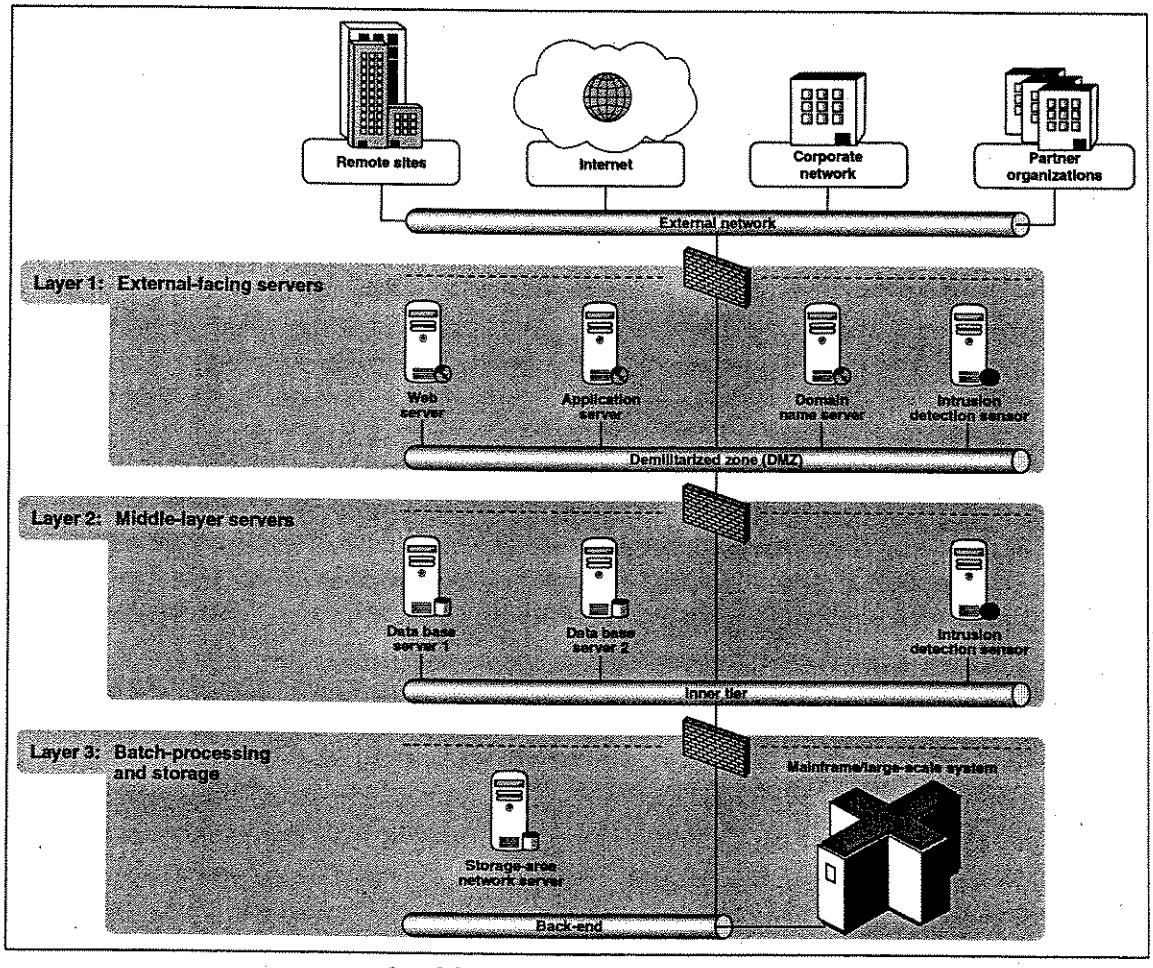
We found that all seven of the selected financial market organizations are taking steps to prevent their operations from being disrupted by electronic attacks. Each of the organizations had implemented the five major elements of a sound information security program. However, we identified actions that each organization could take to further improve their protections against attacks or unauthorized access. At the time of this report, many of the organizations had already implemented some of these improvements and had developed plans to address almost all of the other actions we identified. As regulators of these organizations, staff from the Securities and Exchange Commission (SEC) and the Federal Reserve Board of Governors (Federal Reserve) were briefed on the detailed results of our reviews and both indicated that they plan to monitor the progress of the organizations they oversee in implementing the information security improvements we raised during our reviews.

Financial Market Organizations Had Implemented the Major Elements of a Sound Information Security Program

A sound information security program requires the implementation of security-related policies and all seven organizations that we reviewed had implemented policies and procedures that addressed the information security practices to be followed in designing and implementing their information networks and systems. Implementing controls over access is the second major element of a sound information security program, and all seven organizations had also implemented controls to prevent unauthorized access to their networks and systems. Examples of these controls include firewalls and routers that are configured to only allow authorized messages and data to be passed to and from selected organizations.[3] Other controls these organizations employed on their systems included passwords that were intended to allow only authorized users to access their systems. These organizations had all attempted to protect themselves by implementing multiple controls. For example, all the organizations had implemented layered or tiered information system architectures, which involve placing increasingly sensitive hardware and data behind various layers of access controls. In such an architecture, an organization may place its Web servers that host its public Internet site on its outer layer but position the critical computers that perform its production processing behind several layers that require information to pass through multiple firewalls that restrict access to only authorized users and require various logins and passwords to obtain system access. Figure 1 illustrates a typical layered security architecture.

[3]Routers are intelligent devices that forward data between segments of local area networks. A firewall is a piece of hardware or software that functions in a networked environment to prevent some communications forbidden by the security policy. It has the basic task of controlling traffic between different zones of trust. Typical zones of trust include the Internet (a zone with no trust) and an internal network (a zone with high trust). The ultimate goal is to provide controlled connectivity between zones.

Figure 1: Typical Layered Security Architecture



Source: GAO.

Note: A demilitarized zone is the commonly used term for the portion of the network that sits between an organization's internal network and an external network, usually the Internet.

Another way that several of the organizations had attempted to control unauthorized access to their key systems was by implementing elements of a separate out-of-band network that they used to manage the operations and security of their information systems. Having a separate network for administering systems increases an organization's security because it moves the sensitive management functions, such as the ability to change access authorizations or passwords, to computer workstations that are more isolated from the organization's corporate or production networks.

All seven of the selected financial market organizations had also implemented the two elements of a sound information security program relating to detecting and responding to intrusions. For example, all seven had installed devices or software designed to detect intrusions or attempts to gain unauthorized access to their networks and systems. All the organizations also had developed appropriate procedures for responding to information security intrusion attempts or incidents.

For example, one organization had an internal committee consisting of personnel from its operations and information security areas that met every 2 weeks to discuss the types of intrusion attempts that had occurred during that period. During these meetings, they assess the need to alter their security practices to address emerging issues. Staff from this committee would also share their organization's experiences with the Financial Services Information Sharing and Analysis Center (FS/ISAC), which gathers information from private sector financial markets organizations on information security threats and distributes it to its members.[4]

Finally, each of the seven organizations also had implemented the final element of a sound information security program by having vulnerability assessments of their systems' security performed and conducting audits of their information security practices and controls. For example, many had penetration tests that attempted to obtain access to protected systems performed by external organizations, with some having multiple assessments done each year. Six of the seven organizations also had internal audit staffs that conducted reviews of their information security, and one organization relied primarily on external auditors. For example, two of the organizations had staff within their internal audit departments that, in our technical experts' judgment, were very well versed in highly technical aspects of information security threats and the corresponding controls that the systems at their organizations needed to be secure.

Additional Actions Could Improve the Information Security at These Organizations

Although all seven organizations had the major elements of a sound information security program in place, we also identified additional improvements that each of the organizations could make to further strengthen their protections against electronic attacks. As shown in table 1, we identified anywhere from 11 to 38 suggested improvements at these organizations. In some cases, we identified the same issues at multiple organizations. As the table shows, most of the issues that we identified related to the access controls these organizations had implemented.

Table 1: Numbers of Issues Relating to Financial Market Organizations' Information Security Programs, by Element

	Organization						
Issue by element type	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Policies	2	0	0	0	1	2	0
Access controls	6	25	17	14	20	6	32
Intrusion detection	2	5	2	5	2	2	5
Incident response	0	3	0	0	2	0	0
Vulnerability testing and audit	1	3	1	4	1	1	1
Total by organization	**11**	**36**	**20**	**23**	**26**	**11**	**38**

Source: GAO.

[4]According to an FS/ISAC official, their organization had 1,680 members as of June 2005, and its critical threat alerts were being distributed to almost 9,700 organizations.

The specific issues that we identified as areas in which the financial market organizations could improve varied. For example, one organization had a policy that required minor patches—software updates that address errors or security vulnerabilities—to go through the same quality assurance testing as major updates and revisions to its systems. Having this policy resulted in longer than necessary delays in the removal of vulnerabilities in the organization's systems. In response to our raising this issue, the organization planned to revise the policy by June 15, 2005. At another organization, we noted that the intrusion detection system being used had not been programmed to detect unusual patterns in the specialized message traffic generated by a Web-based system that the organization had recently deployed. In response, this organization told us that its staff would be developing customized "signatures" to allow their intrusion detection system to better identify potentially harmful traffic by mid 2005. In addition, as shown in the table above, we also identified issues at some organizations in their vulnerability testing or audit activities. For example, one organization had not yet fully established a group within its organization with sufficient responsibility and authority to review, analyze, and manage the results of its various vulnerability assessments from a corporatewide perspective.

As shown in table 1, the majority of the issues we identified at the seven financial markets organizations related to the way they were controlling access to their networks and systems. Many of the issues we identified at the organizations involved lack of adequate controls in place at all key points of their networks. The seven organizations also exposed themselves to greater risk by having vulnerabilities on those parts of their networks used to manage network administration or security. For example, to allow its staff to monitor and manage systems from other locations, one organization had been using a remote access software system. However, because this system was used by both key systems administrative staff as well as nonsystems staff in the organization, any attacker gaining access to this system could conceivably also gain access to key security functions, such as firewall management, although these were also protected by other controls. Since our review, this organization told us it has purchased new hardware and software that will be implemented in a manner that removes this vulnerability. At another organization, we noted that staff from an outside vendor had considerable access to the organization's network and, in response, this organization reported revising its contract with the vendor to include subjecting the vendor's relevant staff to fingerprinting and background checks.

According to the discussions we held with staff from these organizations and documents they provided, the financial market organizations were already taking actions in response to almost all of the information security issues we identified. As shown in table 2, the organizations had already completed actions to address about 35 percent of the issues we raised at the time of this report. In response to about two thirds of the issues raised, staff from these organizations indicated that actions to address them were either in progress (28 percent) or were being evaluated or considered for future action (33 percent).

Table 2: Actions Taken by Financial Market Organizations in Response to GAO-Raised Issues

Status of action	Number of actions	Percentage of total
Completed	57	35%
In progress	47	28
Planned or being considered	54	33
No action taken	7	4
Total	**165**	**100%**

Source: GAO.

Financial Market Regulators Plan to Monitor Organizations' Efforts to Improve Information Security

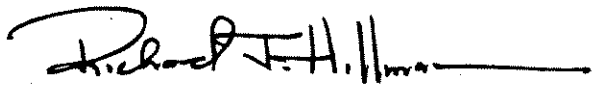
The regulators of the financial market organizations that we reviewed plan to monitor the progress these organizations make in improving information security practices. During the reviews we performed, we briefed SEC staff on the results of our assessments of the information security at the organizations for which SEC has regulatory oversight authority. At several of the briefings we provided to the organizations themselves, SEC staff also participated in the discussions and at one organization SEC staff and GAO staff conducted a joint review. As part of its oversight of these organizations, SEC staff told us they intend to monitor the progress that these organizations make in implementing the improvements we identified during our reviews. Some of the organizations are under the authority of the Federal Reserve Board of Governors. Staff from the Federal Reserve told us that they, in conjunction with other relevant regulators, would also be monitoring progress at these organizations in implementing the improvements we identified.

Agency Comments

We provided a draft of this report to the Chairman, SEC, and the Chairman, Federal Reserve. Staff from these organizations provided technical comments that we made as appropriate.

As agreed with your offices, unless you publicly announce its contents earlier, we plan no further distribution of this report until 30 days after the date of this report. At that time, we will send copies of this report to the Chairman and Ranking Minority Member, Committee on Financial Services, House of Representatives and the Chairman and Ranking Minority Member, Committee on Banking, Housing, and Urban Affairs, United States Senate. We will also send copies to the Chairman, SEC, and Chairman, Federal Reserve Board of Governors. We will make copies available to others upon request. This report will also be available at no charge on GAO's Web site at http://www.gao.gov.

Please contact me at (202) 512-8678 if you or your staff have any questions concerning this report. Contact points for our Ofices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in the enclosure.



Richard J. Hillman
Director, Financial Markets and
Community Investment

Enclosure

Enclosure

GAO Contact and Staff Acknowledgments

GAO Contacts

Richard J. Hillman (202) 512-8678

Staff Acknowledgments

In addition to the individual named above, Cody Goebel, Edward Alexander, Jr., Gerald Barnes, Mark Canter, Jason Carroll, Lon Chin, West Coile, Edward Glagola, Harold Lewis, Eugene Stevens, and Christopher Warweg made key contributions to this report.

(250218)