United States General Accounting Office

GAO

Testimony

For Release
on Delivery
Expected at
1:00 p.m. EST
Wednesday
Feb. 21, 1990

FINANCIAL SYSTEMS: Federal Oversight of Computer Security Needs to be Strengthened

Statement of
Howard G. Rhile, Director
General Government Information Systems,
Information Management and Technology Division

Before the
House Committee on Energy and Commerce
Subcommittee on Telecommunications and Finance
House of Representatives

SUMMARY

Our financial markets report[1] includes a review of the reasonableness of controls used to protect three vital securities trading systems from misuse by authorized users or unauthorized intruders. They are the Common Message Switch system, the Intermarket Trading System, and the National Association of Securities Dealers Automated Quotations system (NASDAQ). These systems provide critical links between our nation's stock exchanges and their customers. They route orders to buy or sell stocks and options, report executed trades, and provide current stock pricing data to our financial marketplaces. Although we found no known instances of hacker or virus attacks on these systems, we did find a number of control weaknesses at the computer centers that pose risks of an insider threatening these systems through security intrusions--such as a computer virus--without being detected. In addition, these computer centers were without an information security program involving formal risk assessments of the threats to the systems, written security plans and procedures, security training, and system and network security audits. We also found that our nation's federal regulator, the Securities and Exchange Commission, needs to be more proactive in ensuring the integrity of these systems.

Our second report[2] being released today includes our assessment of security measures in place to protect three critical banking systems from misuse. These are the FEDWIRE system operated by the Federal Reserve System, the CHIPS system operated by the New York Clearing House Association, and the S.W.I.F.T. system operated by the Society for Worldwide Interbank Financial Telecommunication S.C. While there have not been any reported incidents of fraudulent funds transfers over these systems by employees who operate or oversee them, we have identified a number of control weaknesses and other management weaknesses that, if exploited, increase the risks to these systems of a disruption or degradation of services or the unauthorized use, modification, destruction, or disclosure of data. We also found uncertainties in the regulatory authority over these systems. For example, although the regulatory agencies regularly review CHIPS' operations about every 18 months, CHIPS officials do not agree that the regulators have this authority. Since CHIPS has cooperated with the regulators, there has been no need for formal resolution. The S.W.I.F.T. system, operated by a Belgian cooperative society, has not received oversight in the U.S. or elsewhere in the world. U.S. regulatory agencies are also uncertain as to their authority to do so.

---

[1] Financial Markets: Tighter Computer Security Needed (GAO/IMTEC-90-15, Jan. 5, 1990).

[2] Electronic Funds Transfer: Oversight of Critical Banking Systems Should Be Strengthened (GAO/IMTEC-90-14, Jan. 4, 1990).

Mr. Chairman and Members of the Subcommittee:

We are pleased to be here today to provide you information on the computer security and federal oversight provided to certain critical financial market and banking computer systems. The computer issues we will discuss are the focus of two GAO reports being released today. In these reports, we make recommendations essential to ensuring the health of our nation's financial markets and banking systems. With your permission, I will briefly summarize these reports and place them in the record of this hearing.

Our financial markets report[1] includes a review of the controls used to protect three vital securities trading systems from misuse by authorized users or unauthorized intruders. Information on these systems is shown in the chart before you **[CHART I]**. They are referred to as the Common Message Switch system, the Intermarket Trading System, and the National Association of Securities Dealers Automated Quotations system (NASDAQ). Collectively, these critical systems link our nation's stock exchanges and their customers by doing such things as routing orders to buy or sell stocks and options and providing current stock pricing data to our financial marketplaces. These systems facilitated the trading of about 53 billion shares in 1988.

---

[1]Financial Markets: Tighter Computer Security Needed (GAO/IMTEC-90-15, Jan. 5, 1990).

I am pleased to report that we found no known instances of hacker or virus attacks--attempted or successful--on these systems. In this regard, we believe that the exchanges and the National Association of Securities Dealers (NASD) have implemented a wide range of security controls that protect their systems from the external threat of a hacker or virus attack and, as a result, the risk of such a threat appears relatively low.

We did find, however, control weaknesses at the computer centers that pose risks of an insider threatening these systems by introducing security intrusions--such as a computer virus--without being detected. At the NASDAQ computer center we found 10 control weaknesses. For example, all computer personnel had unrestricted access to the computers that automatically executed small stock orders, new software was not tested to be sure it was virus-free, and there were no data processing auditors to make sure that internal controls were installed and working.

At the computer center that operates the Common Message Switch and the Intermarket Trading System, we found several security weaknesses in the areas of software testing, contingency planning, and internal auditing that increased the security risks to operations. Specifically, new software was not tested to assure that it was virus-free, the contingency plan did not include procedures to be followed in the event of a virus attack, and there

were no data processing auditors to assess the internal controls over computer operations.

Neither computer center nad an information security program involving formal risk assessments of the threats to the systems, written security plans and procedures, security training, and system and network security audits. The organizations we reviewed generally agreed that identified weaknesses pose risks to their operations and have already taken or plan to take steps to improve internal controls over these systems.

We also found that our nation's federal regulator, the Securities and Exchange Commission, needs to be more proactive in ensuring the integrity of these systems. In this regard, the Commission does not examine the exchanges' and NASD's computer centers or networks during its oversight activities to ensure that they are protected from security intrusions. The Commission believes that it does not have sufficient technical expertise to conduct such reviews; rather, it relies on the excnanges and NASD to ensure information security over their own systems.

Accordingly, this report recommends that the Commission follow up on the security weaknesses we identified, oversee the excnanges' and NASD's plans to expand computer security administration programs, conduct or oversee independent assessments of the

exchanges' and NASD's information security programs, and acquire the necessary technical expertise to conduct these activities.

Our second report[2] being released today includes our assessment of security measures in place to protect three critical banking systems from misuse and provides information from bank regulatory agencies on their authority to oversee each system.

These systems--as depicted on the chart before you **[CHART II]**--are the FEDWIRE system operated by the Federal Reserve System, the CHIPS system operated by the New York Clearing House Association, and the S.W.I.F.T. system operated by the Society for Worldwide Interbank Financial Telecommunication S.C. These systems connect thousands of financial institutions located worldwide. In 1988, FEDWIRE electronically transferred about $253 trillion among the Federal Reserve Banks, depository financial institutions, and government agencies. Similarly, CHIPS transferred about $165 trillion among 139 national and international banks located in New York City. S.W.I.F.T. is a major international message processing system used by over 2,500 financial institutions worldwide primarily to initiate electronic funds transfers. It is also used to initiate securities trading.

---

[2]Electronic Funds Transfer: Oversight of Critical Banking Systems Should Be Strengthened (GAO/IMTEC-90-14, Jan. 4, 1990).

The results of our review of the security measures in place to protect these systems have not been satisfying. While there have not been any reported incidents of fraudulent funds transfers over these systems by employees who operate or oversee them, we have identified a number of control weaknesses and other management weaknesses that, if exploited, increase the risks to these systems of a disruption or degradation of services or the unauthorized use, modification, destruction, or disclosure of data.

With FEDWIRE we found 17 control weaknesses at the four Federal Reserve Banks we visited. These included weaknesses in the management of security software that controls access to the system, weaknesses in physical security such as inadequate controls over access to the computer room, and lack of a backup power supply to continue operations in the event of a power failure. CHIPS weaknesses included the performance of incompatible duties by the quality control group--they both tested new software and administered security procedures. Remaining weaknesses involved the lack of an independent internal audit function, and the lack of full-scope independent external reviews over its computer operations. At S.W.I.F.T., weaknesses included a potential computer capacity problem with its existing system that could result in degradation of service to the international banking community, as well as systems development problems with a planned replacement system. These development problems have delayed implementation of the system by about 3 years.

Officials who manage these systems have generally agreed that the weaknesses we identified pose increased risks to their operations and have taken or plan to take steps to improve controls over these systems. In particular, FEDWIRE and CHIPS officials have moved quickly to correct identified weaknesses, which demonstrates a strong commitment to providing secure and reliable operations. We believe the S.W.I.F.T. organization is equally committed to providing secure and reliable services, but their weaknesses are generally more complicated and require continued management attention to resolve.

We also found uncertainties in the regulatory authority over these systems. For example, although regulatory agencies regularly review CHIPS' operations about every 18 months, CHIPS officials do not agree that the regulators have this authority. Since CHIPS has cooperated with the regulators, there has been no need for formal resolution. The S.W.I.F.T. system, operated by a Belgian cooperative society, has not received oversight in the United States or elsewhere in the world. U.S. regulatory agencies are also uncertain as to their authority to do so. In discussing this matter with a senior S.W.I.F.T. official, we were told that, notwithstanding the above uncertainties, S.W.I.F.T. management would cooperate with regulatory authorities to resolve any concerns they may have over the security and reliability of its systems.

Our report includes recommendations to federal regulators to strengthen the oversight of FEDWIRE and CHIPS and to work with the international banking community to assign responsibility for ensuring effective oversight and regulation of the S.W.I.F.T. system. In this connection, representatives from the Federal Reserve Board have recently discussed the operations and level of security of the S.W.I.F.T. system with European central banks and bank supervisory authorities. We are encouraged by this. A consensus seems to be building on the need to provide more effective oversight of the S.W.I.F.T. system and similar systems that serve the international banking community.

- - - - -

This concludes my prepared statement. We will be pleased to respond to any questions.

GAO

SECURITIES TRADING SYSTEMS

COMMON MESSAGE SWITCH

- Links brokers/dealers to NYSE and AMEX
- Routes orders to trading floors
- 20 billion shares processed in 1988

INTERMARKET TRADING SYSTEM

- Links seven exchanges and NASD
- Routes orders to exchanges and NASD
- 1.9 billion shares processed in 1988

NASDAQ SYSTEM

- Links brokers/ dealers to NASD
- Provides price quotations and reports
- Facilitated trading of 31 billion shares in 1988

GAO Critical Banking Systems