GAO

United States General Accounting Office

Report to the Chairman, Securities and Exchange Commission

August 1991

FINANCIAL MARKETS

Computer Security Controls at Five Stock Exchanges Need Strengthening

GAO/IMTEC-91-56

GAO

United States
General Accounting Office
Washington, D.C. 20548

Information Management and
Technology Division

B-237674

August 28, 1991

The Honorable Richard C. Breeden
Chairman, Securities and Exchange
Commission

Dear Mr. Chairman:

This report is part of our continuing efforts to improve the systems security and other controls at our nation's stock markets. As we reported in April 1991, the Securities and Exchange Commission lacks the technical capabilities it needs to oversee or perform assessments of such controls.[1] Having found this shortcoming, we conducted this review of six stock markets to determine whether control weaknesses exist.

Our January 1990 report focused on the controls in place to prevent or detect the misuse of several automated systems used by the American Stock Exchange, the National Association of Securities Dealers, and the New York Stock Exchange.[2] Since that report, these three stock markets have made improvements to address the weaknesses we found. This report provides the results of our recent risk assessments of the automated order routing and execution systems and operations at these three stock markets and at the Midwest Stock Exchange, the Pacific Stock Exchange, and the Philadelphia Stock Exchange.[3] In 1990, these six stock markets collectively handled over 98 percent of the stocks traded in the United States, valued at $1.9 trillion.

Because the specific weaknesses we found are, according to the stock markets, business sensitive and could compromise their operations, this report does not associate weaknesses with individual markets. We discussed the results of our review with senior officials at the six stock markets and the Securities and Exchange Commission. Stock market officials were briefed on their specific weaknesses. We also briefed the Securities and Exchange Commission on all the specific weaknesses. Appendix I provides details on our objective, scope, and methodology.

[1] Financial Markets: Active Oversight of Market Automation by SEC and CFTC Needed (GAO/IMTEC-91-21, Apr. 2, 1991).

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

[3] Because the National Association of Securities Dealers does not have centralized trading floor operations to execute trades, our assessment focused on its automated systems used to support trade execution and reporting.

Results in Brief

Our risk assessments of 10 functional areas at six stock markets found that they all have controls in place to mitigate many of the risks associated with automation. However, we found 68 systems security and other control weaknesses at five stock markets: 3 at the New York Stock Exchange, 5 at the American Stock Exchange, 18 at the Pacific Stock Exchange, 18 at the Philadelphia Stock Exchange, and 24 at the Midwest Stock Exchange. No such weaknesses were found at the National Association of Securities Dealers. The lack of adequate controls at the five stock markets could impair their ability to maintain continuous service, protect critical computer equipment and operations, and process correct information.

Background

In 1990, U.S. stock markets processed about 83 billion shares, valued at nearly $2 trillion. To process these trades, stock markets are increasingly relying on automated systems. As we reported in May 1991, the New York, American, Midwest, Pacific, and Philadelphia Stock Exchanges, and the National Association of Securities Dealers, have all made improvements to increase the capacities of their automated systems used to facilitate order routing and trade execution.[4] Because such systems are critical to the markets' ability to provide smooth and continuous service to participants, adequate security and other controls are also needed to mitigate the risks associated with automation. For example, power outages and fires have caused stock markets without backup capabilities to stop trading activities.

Systems Security and Other Weaknesses Found at Stock Markets

Our risk assessments of 10 functional areas at six stock markets found that controls were in place to mitigate many of the risks associated with automation. However, we found 68 systems security and other control weaknesses at five stock markets: 3 at the New York Stock Exchange, 5 at the American Stock Exchange, 18 at the Pacific Stock Exchange, 18 at the Philadelphia Stock Exchange, and 24 at the Midwest Stock Exchange.[5] With such weaknesses, the markets are vulnerable to risks such as the destruction of equipment, unauthorized data modification, and the disruption of services.

[4]Stock Market Automation: Exchanges Have Increased Systems' Capacities Since the 1987 Market Crash (GAO/IMTEC-91-37, May 10, 1991).

[5]The Midwest Stock Exchange limited our access to information in two functional areas—communications management and systems software management—because they said that the areas contain information involving techniques and methodologies that are used to market their trading systems technology. They noted that the information is unique and extremely confidential, and if released, could jeopardize their competitive position.

Table 1 summarizes the occurrence of functional area weaknesses at the five stock markets. Because these markets consider these weaknesses to be business sensitive and capable of compromising their operations, this table does not identify the markets with their weaknesses.

Table 1: Weaknesses Found at Five Stock Markets

	Stock market				
Functional area	**1**	**2**	**3**	**4**	**5**
Communications management			X	X	X
Computer operations			X	X	X
Contingency planning		X	X	X	X
Disaster recovery	X	X	X		X
Physical security			X	X	X
Quality assurance	X		X		X
Risk analysis			X	X	X
Security awareness				X	
Systems security software				X	
Systems software management			X	X	X

Communications Management

Data communications equipment is critical to securities trading. It is essential that timely, accurate, and reliable data be transmitted to and from market participants. Access to the markets' communications networks needs to be monitored and controlled to ensure that they operate as intended. We found five communications management weaknesses at three stock markets. For example, telecommunications equipment was not adequately secured, which could result in unauthorized access and destruction. Additionally, two stock markets used telecommunications testing equipment to monitor data flow, but the equipment does not merely provide a monitoring capability, it also provides the capability to alter data. This weakness could result in unauthorized data modification.

Computer Operations

Computer centers contain the critical equipment needed to receive and process trade information. These operations need to have strong security safeguards to maintain the integrity of the information and assure the continuity of operations. At three stock markets, 13 computer operations security weaknesses were found. For example, at one stock market, personal computers with floppy disk drives were in the data center and were linked to a critical system. This setup increases the risk of introducing a computer virus. At another stock market, combustible

materials were found adjacent to and inside the data center, which increases the risk of a fire damaging the center.

Contingency Planning

A written contingency plan identifies critical operations and the key individuals responsible for carrying out specified procedures during various emergencies. Four of the stock markets did not have documented contingency plans for their critical automated systems or trading floor operations. This lack of plans impairs the markets' abilities to restore operations after disruptions caused by events such as power outages and natural disasters.

Disaster Recovery

Backup facilities provide organizations with the ability to reestablish operations after disruptions caused by events such as earthquakes, fires, and electrical power failures. Six weaknesses were found that impair four stock markets' abilities to maintain critical operations in the event of primary system failures. For example, three of the stock markets did not have backup computer facilities and two markets did not have alternate power sources to maintain trading floor operations during a power outage.

Physical Security

Physical security and access control measures such as locks, guards, and surveillance cameras are critical to safeguarding operations from internal and external threats. At three stock markets, we found 17 physical security weaknesses. The following are examples of these weaknesses:

- Windows allowed unobstructed views to critical areas, affording greater opportunity for sabotage.
- Packages and other personal articles were allowed in critical areas, permitting an individual to bring into the data center unauthorized software that could be used to introduce a virus on to the system.
- The security guard stationed at an open trading floor door was not monitoring the individuals entering, thereby increasing the risk of unauthorized access.
- Electronic card key devices that controlled access to critical areas did not adequately limit access to authorized personnel; others could enter at the same time as the cardholder, which could result in theft and destruction of equipment.

Quality Assurance

Among other things, an effective quality assurance program validates that systems software changes are adequately tested, operate as intended, and will not introduce vulnerabilities into the systems. We found nine quality assurance weaknesses at three stock markets. At these markets, systems programmers access to quality assurance acceptance libraries was not restricted to protect against unauthorized modifications and destruction of critical software. At two stock markets, software was not adequately tested to ensure that it operated as intended. These quality assurance weaknesses could result in systems not functioning properly.

Risk Analysis

Risk analysis is a process used to identify security threats, determine their magnitude, and identify areas needing additional safeguards. We found that three stock markets did not conduct such analyses periodically. Without these analyses, systems' vulnerabilities may not be identified and appropriate controls may not be implemented to address them.

Security Awareness

A formal security awareness program communicates to employees the importance of security measures and emphasizes their responsibility for protecting assets. We found that one stock market did not have a formal security awareness program.

Systems Security Software

Systems security software protects computerized resources such as trading systems and data files by limiting access to authorized individuals. Additionally, it maintains records of all access attempts. A security software weakness was found at one market: responsibilities for receiving, testing, modifying, and installing the systems security software were not assigned to separate individuals. This lack of separation reduces the market's ability to detect unauthorized attempts to access the systems and change information.

Systems Software Management

An effective systems software management program uses procedures to physically protect software, such as that used to process trades, and separates duties for receiving, testing, and installing such software. We found nine systems software management weaknesses at three stock markets. For example, two markets did not properly secure systems software documentation, which could result in unauthorized access to, modification of, or destruction of the software. We also found that systems programmers at two stock markets performed incompatible duties

including testing, compiling, and installing systems software, as well as managing systems security oversight, which increases the risk of unauthorized data modifications and the disruption of services.

Stock Markets Take Steps to Control Weaknesses

Officials of the five stock markets where we found weaknesses said that they have taken and plan to take steps to improve controls over their automated systems and operations. For example, a senior official at one exchange said that the exchange has recently replaced its data center and that all of the weaknesses identified at its old data center no longer exist. In this regard, the markets and the Securities and Exchange Commission need to assess the steps taken to ensure that weaknesses have been adequately controlled.

Some stock market officials were concerned that the costs to eliminate certain weaknesses could be prohibitive. We understand this concern. However, it does not reduce the need for markets to explore alternative solutions to minimize the risks associated with weaknesses and to keep the Securities and Exchange Commission apprised of such risks, which could hamper exchanges' ability to continue providing efficient, fair, and equitable treatment to all market participants.

Conclusions

Stock markets increasingly rely on automated systems to enhance their securities trading activities. Our review of the six stock markets found that they all had controls in place to mitigate many of the risks associated with automation, but we also found that five stock markets were vulnerable to 68 systems security and other control weaknesses in 10 functional areas. Because the Midwest Stock Exchange limited our assessment of its systems and communication security procedures, we may not have found all the weaknesses that exist.

Recommendations

We recommend that you ensure, as part of the Commission's oversight responsibilities that

- the American, Midwest, New York, Pacific, and Philadelphia stock exchanges take corrective action to control the weaknesses found during our review,
- the Midwest Stock Exchange has an independent risk assessment performed to evaluate the areas where we were denied access, and that appropriate corrective action is taken to control any weaknesses found; and

- the stock markets keep the Commission apprised of the market risks associated with any outstanding weaknesses that are not corrected.

Agency Comments

We discussed the contents of this report with senior officials of the Commission's Division of Market Regulation. In a letter from the division's deputy director, we were told that they generally agree that our evaluation of the six stock markets has highlighted areas of concern that call for careful review by the Securities and Exchange Commission and the markets (see app. II). He noted that the Commission's automation review policies should provide the oversight needed to control market risks. However, he also indicated that without further analysis of the risk assessments performed or the cost effectiveness of our recommendations, the Commission was unable to comment officially on GAO's specific findings and recommendations.

As you know, 31 U.S.C. 720 requires the head of a federal agency to submit a written statement on actions taken on our recommendations to the Senate Committee on Governmental Affairs and the House Committee on Government Operations not later than 60 days after the date of this report. A written statement must also be submitted to the House and Senate Committees on Appropriations with the agency's first request for appropriations made more than 60 days after the date of this report.

We are providing copies of this report to the Chairmen of the Senate Committee on Banking, Housing, and Urban Affairs and the House Committee on Energy and Commerce, and to other interested members of the Congress and the public. We will also make copies available to others upon request.

Should you have any questions about this report or require additional information, please contact me at (202) 275-3455. Major contributors to this report are listed in appendix III.

Sincerely yours,

Howard G. Rhile
Director, General Government
Information Systems

Contents

Abbreviations

GAO	General Accounting Office
IMTEC	Information Management and Technology Division

Objective, Scope, and Methodology

Our objective was to assess the adequacy of systems security and other controls in place to prevent the loss or unauthorized use of system resources, errors in information, illegal acts, and lengthy system and operational outages at six stock markets. To assess these controls, we conducted risk assessments at the New York Stock Exchange, National Association of Securities Dealers, American Stock Exchange, Midwest Stock Exchange, Pacific Stock Exchange, and the Philadelphia Stock Exchange. These stock markets were selected because they processed over 98 percent of the stocks traded in the United States, valued at nearly $2 trillion in 1990.

We addressed 10 organizational functions considered to be essential to the secure processing of trade information. The functions reviewed were (1) communications management, (2) computer operations, (3) contingency planning, (4) disaster recovery, (5) physical security, (6) quality assurance, (7) risk analysis, (8) security awareness, (9) systems security software, and (10) systems software management. Our risk assessment document incorporated questions and control tests from GAO's Control and Risk Evaluation audit methodology, and federal standards and guidance from Federal Information Processing Standards Publications of the National Institute of Standards and Technology.

Our work was performed in accordance with generally accepted government auditing standards, between April 1990 and July 1991. However, the scope of our risk assessments was limited by the Midwest Stock Exchange. Although senior exchange officials discussed and provided requested documentation for most of the functional areas included in our risk assessment, they refused to provide us with the information we needed to completely assess two functional areas—systems software management and communications management—because they viewed this information as sensitive and proprietary. We obtained comments from the Securities and Exchange Commission and the six stock markets and incorporated them where appropriate.

Letter From the Securities and Exchange Commission's Division of Market Regulation

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

DIVISION OF
MARKET REGULATION

August 1, 1991

Ralph V. Carlone
Assistant Comptroller General
General Accounting Office
441 G Street, NW
Washington, DC 20548

Re: Draft Report - Computer Security Controls at Five Stock Exchanges Need Strengthening

Dear Mr. Carlone:

Thank you for providing the staff of the Division of Market Regulation with a draft of the General Accounting Office's ("GAO") report, Computer Security Controls at Five Stock Exchanges Need Strengthening ("Report"), and the opportunity to comment on the Report. The Report outlines the risk assessments that GAO performed at six stock markets 1/ and sets forth GAO's findings and recommendations regarding material weaknesses it found. Although GAO noted that all of the reviewed markets have controls in place to mitigate many risks associated with automation, and that concerning NASDAQ, it found no material weaknesses, the other markets had a number of material weaknesses in their controls that could impair the operation of the markets.

In particular, the Report makes three recommendations relating to the Commission's oversight of the automation of the covered markets: (1) Amex, MSE, NYSE, PSE and Phlx should take corrective action regarding the control weaknesses identified in the Report; (2) the MSE should undertake an independent risk assessment to evaluate the areas where GAO was denied access and take appropriate corrective action to control any identified weaknesses; and (3) the stock markets should keep the Commission apprised of the market risks associated with any outstanding weaknesses that are not corrected.

We note, first, that this letter is only a staff response to the Report and may not necessarily reflect the Commission's views. Further, because our review of the Report is preliminary and without the benefit of a full analysis of the standards and

---

1/ The markets reviewed by GAO were: the New York Stock Exchange ("NYSE"), the NASDAQ system operated by the National Association of Securities Dealers, Inc. ("NASD"), the American Stock Exchange ("Amex"), the Midwest Stock Exchange ("MSE"), the Pacific Stock Exchange ("PSE"), and the Philadelphia Stock Exchange ("Phlx").

methodologies used by GAO or a review of the cost-effectiveness of the recommendations, we are unable at this time to provide a specific reaction to GAO's particular findings or recommendations. Based upon our preliminary review, however, the staff generally agrees that the GAO's evaluation of these markets has highlighted areas of concern that call for careful review by the staff and the self-regulatory organizations ("SROs").

In this regard, we would note that your recommendations are covered by the Commission's Automation Review Policy statements and, consequently, those areas identified as risks should be subject to the Commission's oversight. For example, in the course of the Commission's automation review program, especially the Commission's review of SRO-generated independent reviews of automated trading and market information dissemination systems as called for under the voluntary guidelines announced in the second Automation Review Policy statement ("ARP II"), 2/ Commission staff will pay careful attention to those areas identified in the Report as potential sources of concern. Moreover, regarding the recommendation that the SROs take corrective action to control the identified weaknesses, we also note that the report itself indicates that, according to the SROs, some number of the weaknesses identified by GAO already have been addressed by the SROs.

As we have stated in the past, we believe that careful oversight of SRO automated systems is a critical necessity that contributes to investor confidence in our markets. We remain committed to fulfilling our responsibilities in these areas. We appreciate the timely and valuable contributions that GAO has made in this area. We also appreciate the opportunity to comment on the Report and request that a copy of this letter be appended to the Report when it is issued.

Sincerely,

Brandon Becker

Brandon Becker
Deputy Director

2/ Securities Exchange Act Release No. 29185 (May 9, 1991), 56 FR 22490.

Major Contributors to This Report

Information Management and Technology Division, Washington, D.C.	Leonard Baptiste, Jr., Assistant Director William D. Hadesty, Technical Assistant Director Richard J. Hillman, Assistant Director
New York Regional Office	Bernard D. Rashes, Evaluator-in-Charge Richard G. Schlitt, Senior Evaluator Richard D. Burger, Staff Evaluator

Ordering Information

The first five copies of each GAO report are free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

U.S. General Accounting Office
P.O. Box 6015
Gaithersburg, MD 20877

Orders may also be placed by calling (202) 275-6241.

United States
General Accounting Office
Washington, D.C. 20548

Official Business
Penalty for Private Use $300

First-Class Mail
Postage & Fees Paid
GAO
Permit No. G100