Financial Institution Letters

Computer Virus Protection

FIL-62-2004
June 7, 2004

TO:	CHIEF EXECUTIVE OFFICER (also of interest to Chief Information Officer)
SUBJECT:	Guidance on Developing an Effective Computer Virus Protection Program
Summary:	*The FDIC is issuing guidance to financial institutions about the importance of maintaining an effective computer virus protection program. The guidance provides information on the risks associated with computer viruses and how these risks can be mitigated.*

The Federal Deposit Insurance Corporation (FDIC) has prepared the attached guidance to assist financial institutions in developing an effective computer virus protection program in order to mitigate the risks associated with computer viruses and other types of malicious software codes. Financial institutions rely on the Internet to conduct business transactions and to communicate with customers, vendors and other business partners. Commonly used electronic mail applications are susceptible to computer viruses that may be embedded in e-mails and e-mail file attachments. Therefore, it is important that management understand the risks of computer viruses and take appropriate action to protect computer systems.

Customer information security guidelines require periodic risk assessments and status reports be provided to the Board of Directors. The effectiveness of the institution's computer virus protection program should be addressed in these periodic assessments and reports. Any control weaknesses should be identified and addressed during the normal course of business.

This guidance is designed to complement the *FFIEC Information Security IT Examination Handbook*, issued December 2002, and to supplement Financial Institution Letter 68-99, "Risk Assessment Tools and Practices for Information System Security."

For more information about computer virus protection programs, please contact your FDIC Division of Supervision and Consumer Protection Regional Office or Kathryn M. Weatherby, Examination Specialist, at (202) 898-6793.

For your reference, FDIC Financial Institution Letters may be accessed from the FDIC's Web site at http://www.fdic.gov/news/news/financial/2004/index.html.

Michael J. Zamorski
Director
Division of Supervision and Consumer Protection

# # #

Attachment: Guidance on Developing an Effective Computer Virus Protection Program

Distribution: FDIC-Supervised Banks (Commercial and Savings)

NOTE: Paper copies of FDIC financial institution letters may be obtained through the FDIC's Public Information Center, 801 17th Street, NW, Room 100, Washington, DC 20434 (1-877-275-3342 or 202-416-6940).

Last Updated 06/07/2004 communications@fdic.gov

Financial Institution Letters

Guidance on Developing an Effective Computer Virus Protection Program

Financial institutions have become increasingly reliant on using the Internet as a vehicle for conducting business transactions and communicating with customers, vendors and other business partners. The most common method to conduct business is through commercially available e-mail applications. Unfortunately, the use of Internet-based e-mail applications can provide computer viruses with an entryway into a financial institution's computer network. Therefore, management needs to understand the risks that computer viruses present to their Information Technology (IT) infrastructure.

Infected systems can harm business processes in many ways. Viruses can force the entire network to be shut down for a period of time and disrupt normal business functions. For organizations that rely on systems to interact in a timely manner, the cost of lost business or opportunities could be significant. Viruses can also be a threat to the confidentiality of data and to an institution's reputation.

A computer virus protection program should be an integral part of an institution's overall information security program. Oversight and accountability should be assigned to an appropriate party; however, the virus protection program should involve management, information security and systems operations personnel. Customer information security guidelines require that periodic risk assessments be provided to the Board of Directors. In these assessments, management details measures taken to mitigate risks. The effectiveness of the institution's virus protection program should be addressed in these periodic risk assessments and status reports. An inadequate virus protection program may adversely affect certain components of an institution's IT examination ratings.

An effective computer virus protection program includes installing and maintaining virus protection software for all hosts and clients. It should be installed on desktops, laptops, servers and gateways, and provide for automatic updates and version tracking.

A qualified individual should be responsible for the institution's computer virus protection program. This individual should have sufficient knowledge and training to manage virus software and patches, and be able to assist users when possible infections occur. In many circumstances, institutions may rely upon an outside entity to provide assistance with anti-virus software and related services.

Policies and procedures should be established to inform employees of how to protect the financial institution's systems from becoming infected by viruses. It is especially important to train employees to be cautious when opening e-mail attachments from unknown sources. Caution should be used even if the attachment comes from a known source.

Management should perform and document an assessment to determine what type of anti-virus software solution to use. Virus detection practices should include protection for servers and workstations.

Since viruses and worms exploit commercial, off-the-shelf (COTS) software and operating system weaknesses, these basic steps can be taken to protect systems:

- Ensure that the most recent patches and releases have been installed on the financial institution's systems, including desktops and laptops.
- Decide what type of attachments will be allowed into the environment. Attachments with file extensions such as .EXE, .PIF, .SCR and .COM are commonly infected by viruses and should be

blocked.

- Scan all programs and files prior to uploading them into the system. On occasion, even purchased software from vendors has been infected.
- At the server level, if possible, perform a daily scan to determine whether any program installed has changed in size.
- Periodically perform an audit to ensure the adequacy of the anti-virus program.
- Provide multiple layers of defense and response in a network to detect, identify, and respond to intrusion attacks.

Individuals responsible for anti-virus programs should check with their anti-virus vendors or their Web sites at least daily to determine if there are any recent viruses that require immediate updating of the virus protection software. Most vendors will provide a system to alert subscribers or users when to perform an update of their software. When an alert is received, financial institutions should update virus protection software immediately.

Alert services are available on viruses and worms to warn users of their existence before anti-virus programs are updated to prevent them. Awareness and education of their characteristics can be critical in protecting a computer before new anti-virus programs are made available.

There are various steps that a financial institution may take when a system becomes infected. The first step is informing employees whom they should contact if they suspect a virus infection has occurred. Employees should also be advised to inform the institution's virus protection support group or security department of the events that occurred prior to the possible infection.

Polices should be established to determine what virus detection software to use and to ensure that the distribution process provides for virus prevention. Management should maintain sufficient controls to prevent the corruption of data or software and to correct problems caused by computer viruses or operating system vulnerabilities.