



Is Your Computer System Vulnerable to Cybercrime? Find Out With an IT Audit

By Jonathan Holleb, President, Holleb Consulting, Inc.

If you think information technology (IT) fraud happens only to large companies, think again. A significant problem with small and mid-size businesses is that they depend on limited resources and in some cases, lesser-skilled IT professionals. Often, small staffs with narrow experience are responsible for IT functions outside their skill set. The consequences can be devastating.

What is at risk?

Your company's finances are certainly vulnerable to cybercrime if your computer network is not secure. But money is not the only valuable commodity at risk; the same techniques used to steal money can be used for identity theft, data breach and accessing intellectual property such as trade secrets.

Extortion is yet another risk: Hackers may break into your system and threaten to disrupt your business unless you pay them enormous sums of money.

Case in point: Senior care facility operator

Recently, the main office of a Midwestern operator of senior care facilities was hit by \$250,000 in IT fraud.

Situation—The company's independent IT contractor spent two to three days a month handling network administration, e-mail maintenance, workstation support, anti-virus protection and back-ups. Management had reservations about

the contractor, but assumed he knew what he was doing because he had other notable clients.

Banking practices—The company regularly processed ACH (Automated Clearing House) transactions in batches to a handful of standardized banks and accounts. Only one authorization was required on wire transfers; account activity and balances

were checked every morning. This process continued for six months with no problems.

Fraud detection—During a normal review of account activity, the company noticed that a large number of transactions had been processed, including wire transfers to unfamiliar banks and accounts. The company contacted its bank immediately to

'Often, small staffs with narrow experience are responsible for IT functions outside their skill set. The consequences can be devastating.'

Is Your Computer System Vulnerable to Cybercrime? Find Out With an IT Audit (continued)

stop the transactions, but it took some time to convince the bank that the company was sure the transactions were fraudulent.

Extent of damages—In all, five batches with 20 transactions had been processed, wiring \$250,000 to unauthorized accounts across the U.S. The money was then withdrawn and wired to accounts in Ukraine.

Fraud mechanism—The workstation of the staff accountant who performed ACH transactions had been compromised by a trojan horse program he inadvertently downloaded from an e-mail attachment or web site. (A trojan horse is a program that installs malicious software under the guise of doing something else.) In this case, the Trojan horse provided a back door allowing the perpetrators to access and install a key logger program.

The perpetrators used the key logger program to capture all keystrokes typed by the accountant, thus exposing the login information for performing electronic wire transfers and ACH transactions. Then the perpetrators accessed the ACH application, modified the standard batches, changed the routing information to different accounts, submitted the transactions—and the money was in their hands.

Fraud source—The FBI traced the fraud to the Russian Mafia. The source that

gained access to the company's computer was traced to Nigeria.

How could this fraud have happened?

The company thought its IT contractor had implemented controls to protect it from hackers. Management assumed they had firewall protection and that their network was monitored and protected from malicious software. But the IT contractor had dropped the ball. What went wrong?

- IT controls were performed inadequately. The company's installed anti-virus software was not kept up-to-date with signatures and was ineffective. No scanning for spyware was performed and employees were allowed unrestricted access to the Internet. The company had no use policies or training about "social engineering"—the practice of obtaining confidential information by manipulating users.
- Accounting controls were ineffective. The company required no second authorization for ACH transactions and had no restrictions on which accounts were authorized to receive wire transfers.
- The bank's transaction monitoring was lacking. Effective monitoring by the bank could have flagged the unusual transactions and required verification before processing.

How do hackers get into your system?

1. **E-mail attachments.** In 80% of cases, hackers gain access to personal computers through e-mail. When you click on an e-mail attachment, the malicious software is installed on your computer.
2. **Web sites.** Many web sites laden with viruses and trojan horses are "honeypots" that lure visitors with intriguing, often pornographic, content.
3. **Phishing.** In this form of social engineering, hackers send e-mail messages that falsely claim they're from companies that the recipient does business with, such as a bank. Often the messages ask the recipient to send sensitive information such as bank account numbers for "verification".

Protecting your data beyond the office

Sometimes computer viruses and trojan horses come into corporate computer networks from home PCs. Employees who work from computers outside the office setting pose several security risks:

- **Virus risk.** If an employee does any work on a home PC, that machine may be infected with a virus or trojan horse—one that could infect your office system if you don't have proper safeguards in place.
- **Information security risk.** When employees take confidential information from your system and use it

"In 80% of cases, hackers gain access to personal computers through e-mail. When you click on an e-mail attachment, the malicious software is installed on your computer."

Is Your Computer System Vulnerable to Cybercrime? Find Out With an IT Audit (continued)

on a home computer, you have no control over information security.

How can an IT audit help?

An independent IT audit can help protect your company by examining your computer systems, applications and databases, and alerting you to any deficiencies that could put you at risk. The audit covers IT controls, accounting controls, user training and awareness, as well as key issues such as maintaining physical security over your network servers and back-up data.

Questions about independent IT audits?

Contact Jon Holleb, Holleb Consulting, Inc., at 847/849-2100, ext. 330.

12 Ways to Protect Your Company from Computer Crime

Be sure that:

1. Your computer network has proper controls in place, including a well-configured firewall to keep intruders out and good anti-virus software that monitors and scans all incoming and outgoing data.
2. Your anti-virus and anti-spam software is working properly. It should be centrally managed, properly configured and installed, and kept up-to-date.
3. The people responsible for security are doing their jobs. Verify this through periodic independent audits.
4. Your system is constantly monitored for spyware and other types of malicious software. This might require more than one type of tool, such as Spybot or Adware.
5. You educate your employees in safe practices by implementing a corporate Internet use policy and including it in your new-employee orientation. The policy should spell out what employees should—and should not—do on their computers and the Internet.
6. Your system has content filtering that does not allow employees to access questionable Internet sites, such as those with adult content or gambling.
7. Your system is configured so that users do not have the right to install software applications.
8. Your system requires complex passwords and mandates users to change their password regularly.
9. Employees are granted access only to what they need to perform their work. This applies to both network and application access.
10. You monitor people's system access and activity to ensure that they are logging on only when they should be and doing what they should be doing. Most computer crime happens after work hours.
11. You store all data on servers, not on workstations; this is also important for data back-up, which should be encrypted.
12. You maintain physical security over your network servers. Keep your servers and back-up data locked in a controlled room where only a limited number of people have access.

"Monitoring is the key to effective controls"