Global Information Assurance Certification Paper

GSEC (v.1.3)
Internal Threats Should Not Be Forgotten
Linda Robinson
March 26, 2002

Internal and external threats from computer crime continue unabated. Several studies have been done to gather statistics on the origination of the threats, and one common thread is that a majority of them are internal threats. Therefore, companies need to find ways to better protect themselves and focus more on potential internal threats from employees, consultants, contractors, vendors, and others intent on bringing harm to their organizations.

Obviously, good employees can reduce security breaches, and companies need to continue efforts to hire, train, and keep them. However, since disgruntled employees can pose significant security risks to companies, they need to be prepared for such risks. While a lot of companies develop a number of procedures when hiring new staff, fewer companies develop adequate procedures when they leave. This paper will address these issues. It also will address ways to help curb retaliation, combat internal threats, and emphasize the importance of reporting cyber threats to legal authorities.

Cyber Threats:

The Computer Security Institute (CSI) recently announced the results of its sixth annual "Computer Crime and Security Survey," which is conducted by CSI with the participation of the San Francisco Federal Bureau of Investigation's (FBI) Computer Intrusion Squad. The aim of this effort is to raise the level of security awareness, as well as help determine the scope of computer crime in the United States.

Based on responses from 538 computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions and universities, the findings of the "CSI/FBI 2001 Computer Crime and Security Survey" confirm the trends that have emerged over the previous years:

- Organizations are under cyber attack from both inside and outside of their electronic perimeters.
- A wide range of cyber attacks has been detected.
- Cyber attacks can result in serious financial losses.
- Defending successfully against such attacks requires more than just the use of information security technologies.

The survey also revealed that 85 percent of respondents had suffered computer security breaches in the past 12 months. Sixty-four percent of American

businesses surveyed also acknowledged financial losses due to such breakdowns in security.

It is encouraging to note that the survey revealed that more respondents are reporting intrusions to law enforcement: 36 percent of respondents reported the intrusions to law enforcement in 2001. This is a significant increase from 2000, when only 25 percent reported them. Hopefully, this number will increase even more in 2002.

Before Hiring Employees:

The following steps should be taken before employees are hired:

- Do a background check
- Hire a firm to investigate the potential hire
- Give some basic skill tests before hiring
- Do a management interview
- Contact references: both the references provided AND previous employers not listed as references
- Require a rigorous technical interview
- Make sure that the potential hire will really fit in with others
- Don't get greedy and let a potential hire convince you he or she has another job just waiting, call their bluff
- If someone's resume is too good to be true, then it's probably not true
- If your developers paint you in a corner so that you have to have them to complete a job, remember who they are and don't allow it to happen again. Make sure they find a new place to work as soon as you can.

A new online program is being tested by the Social Security Administration (SSA), which is designed to authenticate Social Security Numbers (SSN) for organizations' new hires. This program will pilot test a web site where the SSA can find if the SSN is fraudulent and if it belongs to the person. If this moves forward, it will be a help to companies in their background checks, etc.

Employment Documents:

New statutes and court decisions constantly change our labor laws. Out-of-date and improperly implemented policy manuals and employment documents can lead to trouble for management, especially if employees sue the company for taking action against them for retaliation. To potentially avoid claims of unfair firings, companies could improve wording in employment documents by adding "employment-at-will" wording. Employment documents could include job applications, employee handbooks, employment contracts, etc.

Security Policies/Awareness Programs/Education:

At the very least, companies should have security policies and procedures in place, as well as security awareness programs. Employees should be educated on the basics of a secure environment, and know how to report security incidents. Several System Administration, Networking and Security (SANS) papers have been written on these topics and can be found in the SANS Information Security Reading Room at http://rr.sans.org/index.php.

The National Institute of Standards and Technology (NIST) Computer Security Division also contains useful resources on information system security awareness, training, and education, which can be found on the Computer Security Resource Center web site at http://csrc.nist.gov/ATE/index.html

Exit Employee Policy and Procedures:

Terminating employees is never easy. When an employee leaves the company, procedures should be in place to ensure that all access has been revoked and all company property returned. The following policy statements could be used in the employee separation process:

- On or before the employee's last day of work, the employee's supervisor will implement procedures to assure security of company property. For state property, a statement should be included that removal of state property may be construed as theft and appropriate legal action taken if the property cannot be recovered.

- Company property that has been issued to the employee, if any, shall be returned to the supervisor and checked in by the employee.

Procedures need to be taken to ensure that all company property has been returned and all access has been revoked. Areas include building access, system access, credit cards and/or other possessions that the employee may have. These procedures could take place with a Departing Employee Checklist. This checklist could be set up as a web-based program (shown below). Security designs should be in place, i.e., logging enforced, protected on an intranet server that has been hardened, encryption applied, and appropriate access and permissions set. The web-enabled form should be thoroughly tested to be sure appropriate access has been given, and private information is encrypted.

Departing Employee Checklist

Official Separation Date:_____ Date to Revoke: _____

Employee Name:
Social Security Number:
Division/Phone:
Resignation Date:
Transfer Out Date:
Retirement Date:
Mainframe UserID:
Returning as Contractor:
Was Exiting Individual a Manager?

Other Management Actions Required for Departing Employees:

Supervisor's Name: _____

	Item Revoked/Received	Completed	N/A
Employee Evaluation		___	___
Notify Upper Levels of Management		___	___
Gasoline Card – Cancellation		___	___
Telephone Card – Cancellation	___	___	___
Procurement Card – Cancellation			
Cell Phone/Pager	___	___	___
Laptop/Computer/Home Workstation	___	___	___
Voice Mail Deactivation	___	___	___
Building Keys/Cabinet File Keys			
Software to be Removed from Workstation		___	___
Wireless Device Turned in	___	___	___
Complete Personnel Action Form and Forward		___	___

Personnel (this section is not required for vendors and contractors):

Schedule Exit Interview	___	___
Letter of Resignation	___	___
Leaving Company Brochure	___	___
Revoke Access to Payroll/Personnel System	___	___

Security:

Notify Building Systems Administrator	___	___
Network User ID Disabled and/or Deleted	___	___
Electronic Files and Directories Deleted	___	___
Electronic Mail Account Disabled	___	___
Server Account Disabled	___	___
Remote Access Service Removed	___	___
Security Badge Disabled and/or Deleted	___	___
Parking Tag Turned In	___	___
Other User Ids and Access	___	___

Comments:
Date Personnel Received Completed Departing Employee Checklist:

Departing Employee Checklist Instructions:

The supervisor initiates the first section, with the following departing employee information:

- Date of resignation or transfer
- Social security number

The supervisor will then select the appropriate button for company employee, contractor, or vendor (the required information will differ depending on the choice that is made) and proceed to complete the information on the screen as requested and select the “continue” button that should be displayed at the bottom of the screen. (This must be completed even if employee/contractor is returning.)

At this point, the program should be set up to automatically notify the appropriate departments of an impending departure, such as Personnel and Security, via an e-mail message to appropriate parties. The appropriate parties would then complete the items for which they’re responsible, and submit the form via a “submit” button.

The form should be set up so that an e-mail message is generated for those areas that have not been checked. Once the appropriate parties check the items, a final electronic e-mail message should be generated to inform all the parties that the checklist has been completed, at which time the personnel department can print out a hard copy and file it with that employee’s personnel file.

It is important for companies to keep in mind that employment records are subject to federal, state, or organizational retention requirements. Therefore, back-up tapes should comply with these requirements. Another good suggestion for employment records is that I-9 forms should not be included in the personnel files. I-9 forms are mandated for every employee hired after November 6, 1986. Employers are required to log document numbers that prove the employee's identity and right to work in the United States. If government officials are in a company’s work location, they can request to inspect I-9 forms.

Companies need to ensure that supervisors are aware of their responsibilities in completing the Departing Employee Checklist. Notices should be sent to those individuals that when an individual transfers, resigns or has their employment terminated, the supervisor is responsible for completing the checklist and submitting it to Security prior to the individual’s last day. For situations involving termination, Security must be contacted immediately.

Exit Interview:

If exit procedures cannot be developed, at a minimum, companies should conduct exit interviews to help determine an ex-employee's attitude about leaving.

A sample exit interview follows:

Employee Exit Interview

Employee:_____ Position: _____
Department: _____ Supervisor: _____
Employed From: _____ To: _____
Reason For Termination:_____

Employee Returned:

___ Keys	___ Gasoline/Phone Cards	___ Phones
___ ID Badge	___ Company Documents	___ Credit Cards
___ Laptop/Pager	___ Other	___ Other

Employee was Informed About Restrictions on:

___ Trade Secrets	___ Removing Company Documents
___ Patents	___ Employment with Competitor (if applicable)
___ Other	

_____

Employee Exit Questions/Answers

a. Did management adequately recognize your contributions?
b. Did you feel that you had the support of management?
c. Were you properly trained for your job?
d. Was your work rewarding?
e. Were you fairly treated by the company?
f. Was your salary adequate?
g. How were your working conditions?
h. Did you understand all company policies?
i. Have you seen theft of company property?
j. How can the company improve security?
k. How can the company improve working conditions?
l. What do you feel are the company's strengths?
m. What do you feel are the company's weaknesses?
n. Other employee comments or suggestions?

Other Ways to Combat Internal Threats:

There are several other actions that companies can take to combat internal threats, such as training, system-use policies, in-house hackers, removing unneeded services, and security alert services as follows:

- Training - companies should be sure that systems administrators are trained appropriately. Training is offered by many organizations to help employees deal with insider threats. At the SANS security essentials training, the issues in this paper are identified, including threat vectors to find ways to identify the avenues from which the attacks may come (including two that deal with insider attacks). Identifying the avenues from which attacks originate helps to defend against them and provides valuable ways to target effective countermeasures. More information on SANS security training can be found at the SANS website at http://www.sans.org/newlook/home.php.

  The National Security Agency (NSA) also has security training, and more information can be found at http://www.nist.gov/cgi-bin/exit_nist.cgi?url=http://www.nsa.gov/isso/programs/nietp/newspg1.htm

- System-Use Policies - Wayde York, in his SANS Paper, "Weakening the Infrastructure from within," states that every good security effort depends upon relevant and current policy. To assess the effectiveness and efficiency of the policies, an audit should be conducted to ensure compliance of policies and that they are being followed at all levels of the company. This also provides a means for corrective action before operational efficiency of companies is affected. Combating the insider threat is no exception. System-use policies should be designed to clearly articulate restrictions and enforcement measures. In order to mitigate the insider threat, system-use policies may include the following prohibitions:

  - Port scanning on the network
  - Assigning share drives without passwords
  - Enabling ftp servers on their systems
  - Operating modems in any mode other than a "no auto answer" mode
  - Excessive use of the ICMP Ping application
  - Possession or use of password cracking tools
  - Usage of unauthorized remote control tools
  - Additionally, the policy should address privacy rights while using organizational systems. The more specific the policy is the more latitude network security professionals will have in enforcing these policies.

- In-House Hackers - Ben Hermann, in his SANS paper, “Routine External and Internal Hacking,” states that the idea of having in-house hackers is not a new concept and the need for this helping hand has never been greater. He references Dan Farmer and Wietse Venema’s paper, "Improving the Security of Your Site by Breaking Into it” and states that every day all over the world, computer networks and hosts are being broken into and that systems administrators are often unaware of the dangers presented by anything beyond the most trivial attacks. As the title suggests, companies need to conduct the attacks to learn what evidence is left behind, and harden the network/systems accordingly to help prevent further attacks.

  As companies do this, they shouldn’t forget to take laptops into account. While laptop users used to represent a small percentage of an enterprise’s overall user community, they now represent 20 to 25 percent. Personal devices (wireless devices) make up another device platform that is quickly making inroads in users’ computing environment and also should not be overlooked. If someone leaves on bad terms and keeps their wireless network card, they could drive up to the outside of the company building and capture all the network traffic they would like.

- Remove Unneeded Services – A lot of Internet attacks are against services that are running on companies’ systems without the companies’ knowledge. Companies need to be sure that any unneeded services are removed. To help administrators eliminate the most critical Internet security threats, SANS has published a continually updated document, which can be found at http://www.sans.org/top20.htm.

- Security Alert Notices – Companies should consider subscribing to a security alert notification system in order to be notified of their systems’ vulnerabilities. They should also check their vendors’ and other security-related websites for appropriate measures to minimize risks.

Taking Action:

In industry, few companies take action against retaliation by employees even though under the Computer Fraud and Abuse Act, it is a crime to break into or damage someone else’s computer. This act was amended in 1994 to include provisions outlawing destructive devices such as viruses, worms, and denial-of-service attacks. Perhaps one of the reasons companies haven’t been taking action is because until recently, industry was suffering from a lack of case law in this area. However, a network administrator was recently sent to prison for nearly three and a half years and ordered to pay $2 million in restitution for

planting a time bomb that destroyed the manufacturing software developed by his employer. Industry analysts say his sentencing is important in sending a message to disgruntled information systems workers and in setting case law for the increasing stream of computer crime cases. Since the jury handed down the guilty verdict, there have been several other insider sabotage cases that have gone to court. According to numbers from the U.S. Secret Service, which investigated this case, insiders are responsible for about 80 percent of the cases they're now investigating.

Role of NIPC:

The ability of attackers to remain anonymous on the Internet has been a huge problem for law enforcement. U.S. Attorney General John Ashcroft acknowledges, "for the government to be successful in its prosecution of cybercriminals, businesses must overcome the perceived stigma of being a victim of cybercrime." The National Infrastructure Protection Center (NIPC) was created in 1998 to protect the nation's most critical computer systems. NIPC brings together representatives from U.S. government agencies, state and local governments, and the private sector in a partnership to reduce vulnerability to attack and increase capabilities to respond to new threats. However, its fate presently remains unclear, since it has recently been suggested that it be decentralized. More information can be found in the March 25, 2002, Security Wire Digest.

The First Cybercourt:

In the future, some cases (including those related to information technology) could take place online. In early January of 2002, the first "cybercourt" was established in the United States and perhaps the world. In Michigan's cybercourt, a judge (no jury will be involved) will hear business and commercial cases in which the amount in dispute exceeds $25,000. Decisions can be appealed to the (noncyber) Court of Appeals. The court's jurisdiction will be concurrent with that of other courts - meaning that it is the plaintiff's choice whether to sue in the virtual court.

Only certain types of business disputes can be heard, and the category is wide - including disputes related to information technology, the internal organization of business entities (including partnerships), business agreements and commercial transactions. Tort and employment cases are specifically excluded.

Conclusion:

In today's working environment, companies may face disgruntled employees and potential violent acts and should attempt to minimize them by building a culture

or cultures that promote a healthy work atmosphere for everyone. Security policies and procedures should be implemented, including adequate entrance and exit employment procedures. Once disgruntled employees and/or other security incidents are identified, companies need to deal with them appropriately and report the crime to legal authorities.

References:

Balian, Cheryl. "FBI Director Says Future of NIPC Cybercrime Unit Uncertain." Security Wire Digest, Vol. 4, No. 23, March 25, 2002.

Company Document. "Departing Employee Checklist."

Computer Security Institute, "2001 Computer Crime and Security Survey" March, 2001.

Danda, Matthew, "protecting yourself online." Microsoft Press, Redmond Washington, 2001.

E-Z Legal Forms, Inc. "Managing Employees Made E-Z." Florida, 1999

Edwards, Mark Joseph. "When Employees Leave the Firm." Windows 2000 Magazine Security UPDATE Email Newsletter, June 6, 2001.
URL: http://www.winnetmag.com/email.

Gaudin, Sharon. "Net saboteur faces 41 months." Network World, March 4, 2002.
URL: http://www.nwfusion.com/news/2002/0304lloyd.html.

Harris, Jack. "Malcontent and Disgruntled Employees…What's a Supervisor to Do?" The Police Chief Magazine, February 2001.

Herman, Ben. "Routine External and Internal 'Hacking', An Important Part of Information Assurance." (paper for SANS certification), Ben Herman, April19, 2001.

Consulting Times. "Business Insights: Dealing with Disgruntled Ex-Employees. *Taking an Assertive Approach with the Technically Inclined."* April 25, 2001.
URL: http://www.consultingtimes.com/business_insights.html

National Institute of Standards and Technology's Computer Security Resource Center. "Awareness, Training, and Education."
URL: http://csrc.nist.gov/ATE/index.html.

National Security Agency. "National INFOSEC Education & Training Program."
URL: http://www.nsa.gov/isso/programs/nietp/newspg1.htm.

Ramasastry, Anita. "MICHIGAN'S CYBERCOURT: Worthy Experiment Or Virtual Daydream?" February 6, 2002.
URL: http://writ.news.findlaw.com/commentary/20020206_ramasastry.html.

System Administration, Networking and Security (SANS) Institute. "SANS Information Security Reading Room."
URL: http://rr.sans.org/index.php

System Administration, Networking and Security (SANS) Institute. "SANS Security Training Programs."
URL: http://www.sans.org/newlook/home.php.

System Administration, Networking and Security (SANS) Institute. "The Twenty Most Critical Internet Security Vulnerabilities (Updated) - The Experts' Consensus." January 30, 2002.
URL: http://www.sans.org/top20.htm.

Truesdell, William H. "What's in a Personnel File? (And What Should Not Be)." The Management Advantage, Inc.
URL: http://www.management-advantage.com/products/free-personnel.htm

Vasishtha, Preeti, "SSA set to test online authentication app for businesses." Government Computer News, March 5, 2002.
URL: http://www.gcn.com/vol1_no1/daily-updates/18116-1.html.

York, Wayde. "Weakening the Infrastructure from Within." (paper for SANS certification) April 20, 2001.