

Control Essentials

Volume III, Issue VIII

August 2008

The Inside Job

The inside job is not the title of Martin Scorsese's latest movie or the remake of the popular *The Italian Job*. It refers to an intentional, pre-meditated criminal activity such as theft, or disruption of assets or services performed by an insider, that is, a company's current or former employee, contractor, temporary worker or consultant. An insider has the main advantage of being trust worthy to the company and has the knowledge of the location of the company's assets and types of controls in place. Let's take some examples to illustrate exactly how inside jobs have caused serious headaches to organizations:

The Inside Job	The Price to Pay
1/10/2008, <i>Cox Communications</i> : A former employee shut down portions of the company's system, causing a loss of computer and telecommunications services, including access to 911 emergency services, for Cox customers in Texas, Las Vegas, New Orleans and Baton Rouge.	The former employee was sentenced to five months in prison and five months of home confinement. He was also ordered to serve two years of supervised release, perform 200 hours of community service, and pay more than US \$15,000 in restitution.
12/28/2007, <i>3DPLM Software Solutions</i> : A former engineer transferred confidential information before quitting the job.	The theft was worth \$12 million.
10/11/2007, <i>Pentastar Aviation LLC</i> : Former employee destroyed critical payroll and personnel data.	The man faced up to 10 years in prison and a \$250,000 fine. The company spent about \$30,000 to repair the damage.
10/9/2007, <i>San Jose (California) Medical Group</i> : The branch manager at San Jose (California) Medical Group stole medical record data such as names, social security numbers (SSNs) and medical diagnoses.	Approximately 187,000 patients were affected by the breach. The manager faced 21 months in prison and three years of supervised release. He was also ordered by the judge to pay \$145,154 in restitution.
9/29/2007, <i>A hospital in Greece</i> : Greek authorities arrested a woman for allegedly sending files from her job at a hospital to her home computer. Police also found two hard disks full of similar files at her home.	Information not available

IT Security:

Information security design and Implementation
 Vulnerability Assessments
 Penetration Testing
 Security Breach Investigation and Remediation
 Business Continuity Planning
 Logwatch
 Training

Risk Management:

Risk Assessment
 IT Risk Advisory
 Fraud Detection

Forensic Services:

Computer Forensics
 E-Discovery

IT Audit Services:

Application and System Implementation Reviews
 Internal Information Systems Audits

Regulatory Compliance:

Bank Secrecy Act
 Gramm-Leach-Bliley Act
 Fair and Accurate Credit Transactions Act
 Sarbanes-Oxley Act
 Health Insurance Portability and Accountability Act
 Family Educational Rights and Privacy Act
 Payment Card Industry

Attestation Services:

SAS 70 Reviews
 Other Attestation Services

The majority of these publicly-known stories ended with the betrayer captured and facing the consequences of his/her actions and the victim organization getting, hopefully, commensurate compensation. In all those cases, there was enough evidence to incriminate the person as in the case of the Greek theft, where the authorities found at the employee's home two hard disks containing data similar to the stolen data that brought to the arrest of the woman.

But what if substantial evidence is not enough to convict the criminal? What if the possibility to prosecute the criminal failed due to deficiencies in the monitoring and auditing controls in place at the organization? Or what if the inside job could have been prevented or at least mitigated before the pre-meditation of the act?

Minimize the Risk of Inside Jobs

The whole deal of minimizing the risk of an inside job is a well-known concept in information security: preventing an authorized person from committing unauthorized actions. Preventive controls alone may not be sufficient, thus they must be compensated by detective mechanisms and a sound incident response plan.

Preventive Controls

Policies & Procedures: Policies and procedures are the foundations of the security of any organization. To prevent inside jobs, organizations should begin from here, that is, from developing, maintaining and enforcing their policies and procedures. Below is a checklist of topics aimed at preventing inside jobs that should be addressed in a company policies and procedures manual:

- Acceptable Use of Company Resources
 - This policy should be signed by all employees upon hire
- Information Classification
- Access Control based on "least privilege" and "need to know" principles
- IDs and password management
- Employee Role and Responsibilities
- Remote Access (e.g. Dial-up connections, VPN, etc.)
- Physical Security Access Controls (e.g. Use of badges, cameras and alarms)
- Disposal of digital and physical data
- Clean Desk
- Use of encryption to protect the confidentiality and integrity of non-public
- Review of system logs to monitor employees and system administrators activities
- Prohibition of USB, CDRW, and DVD-RW drives on workstations
- Regular media inventories
- Employee hire, transfer, and termination processes
- Enforcement of the policies and penalties for non-compliance

Hardening network and systems: Along with developing and enforcing policies and procedures, organizations need to harden the network and systems within it. To heighten the security of those components, configuration standards for all critical network devices such as firewalls, switches, load balancers and servers should be developed and regularly updated. Configuration standards should state the services/ports necessary for the system to run, process hardening, audit settings and optimization tunings. Access controls on applications and operating system audit logs should also be included in the standard. Additionally, internal penetration testing (yearly) and vulnerability assess-

assessments (quarterly) should be performed to further assess the overall network security from an internal perspective and identify vulnerabilities that may be exploited by an insider.

Encryption: All channels transmitting sensitive data such as credit card numbers, SSNs, etc. should be encrypted to prevent malicious insiders from sniffing or tampering the communications. Encryption should also be applied to sensitive data while on storage.

Remote Access Controls: A formal process should be in place to assign remote access via dial-up or VPN connections. The process needs to address:

- Remote access request
- Extension and termination of remote access
- Daily monitoring of remote access activities
- Use an extra-layer of security such as a token or key in addition to username and password

Use unique and unconventional IDs: IDs assigned to employees for accessing the network resources should be unique to ensure accountability. The use of a naming convention for creating IDs (e.g. first letter of the first name followed by last name) is not optimal since it would make IDs very predictable. Instead, IDs should be treated more secretly just like passwords. For example, an internal random, unique number (e.g. employee identification number) combined with the employee's first name and/or last name would further deter an insider from impersonating a loyal employee.

Dual control: Dual control refers to two people having control over each other. Dual control is typically implemented for critical, high sensitivity tasks. An example of dual controls would be two administrators knowing, respectively, half of the QSECOFR password of the AS/400 mainframe. Dual control can be also used as a compensating control over system administrators when no audit trails to monitor a system administrator's activities are available. Dual control reduces the likelihood of fraudulent actions since it requires the collaboration of two individuals.

Segregation of duty: Segregation of duties is a control aimed at preventing one single person from being able to bypass all the security controls of a process. Segregation of duties is typically implemented by having employees occupying different roles (e.g. supervisor and operator) controlling one another. For example, a programmer should not be able to develop, test and deploy the software. Rather, a second person should test the software and a third one should be in charge of the deployment. This way, all three individuals involved control and limit one another.

Physical Security: Tight physical security controls such as the use of badges and electronic card readers should be particularly enforced where the systems containing confidential information reside.

Awareness & Training: Employees need to be aware and trained to differentiate authorized from unauthorized access. Training should be provided as part of the hiring process. Additionally, training sessions covering topics such as social engineering should also be provided at least annually for all employees.

Background and Criminal Checks: The Human Resources Department should perform background and criminal checks on every individual being hired.
on mission critical segments will observe unauthorized or suspicious traffic leaving the network.

Detective Control

Intrusion Detection System (IDS): IDSs are not only used to detect intrusion attempts from the outside to the inside of the network, but also vice versa. Placing a sensor inside the innermost firewall on mission critical segments will observe unauthorized or suspicious traffic leaving the network. However, if organizations have several DMZs in place within the network, it will be necessary to install one IPS sensor per DMZ to monitor the traffic directed to each of the DMZs.

Log Monitoring: Logs can be configured at operating system and application level. Logging should be configured so that audit trails can provide enough details to uniquely establish the user identity and the action performed. Audit trails review should be performed on a daily basis for critical systems, and weekly for other non-critical systems including printers. However, the review of alerts and events detected by IDSs should be made available 24/7.

Physical Security: Closed Circuit Television (CCTV) video cameras are probably the most common detective control utilized. Security guardians should monitor the cameras 24/7 and the tapes should be securely retained for at least 3 months. Many modern CCTVs are provided with an administrative console accessible via web. Administrators of the console should use strong passwords, and encryption should be employed to ensure the confidentiality of the communication.

Incident Response

Organizations should be prepared to respond to inside jobs. The Incident Response Team (IRT) designated to the handling of inside jobs should involve at least the following individuals:

- Manager of IT Security Department
- Manager of Security Department
- Manager of Human Resources Department
- Manager of Legal Department
- Manager of Public Affairs and Media Relationships Department

The Incident Response strategy should include detailed procedures to report the incident to law enforcement agencies, media, and any external party directly affected by the incident. As described in the NIST Special Publication 800-61, the incident response process has several phases, from initial preparation through post-incident analysis.

Preparation: During the preparation phase, the IRT should identify all the tools (e.g. monitoring, and forensic tools) and data (audit trails) that may be required during the incident response. Detailed procedures should be developed and tested to handle the response.

Detection and Analysis: Due to the high number of ways an inside job can occur, it is not feasible to develop a single strategy to detect the incident. Nevertheless, at a minimum, organizations can increase the monitoring by observing certain activities and systems more frequently. Once the incident has been detected, the IRT needs to analyze it, that is, assess the scope and classify the incident. Depending on the assessment results, specific steps are to be taken, thus specific procedures need to have been developed. Further, it is essential that all the steps followed by the IRT are properly documented so that they can be used as evidence in a court of law if legal prosecution is pursued.

Containment, Eradication and Recovery: During the containment of the incident, evidence should be collected according to procedures that meet all applicable laws and regulations, developed from previous discussions with legal staff and appropriate law enforcement agencies, so that it should be

Post-Incident Activity: During the post-incident activity, the IRT learns from the received “lesson”. The IRT will need to fully understand how the incident took place and whether new preventive or detective controls need to be established, or whether the existing ones require improvement. The IRT should also evaluate the incident response plan and improve it if necessary.

Conclusions

The controls described in this article are not aimed at providing an utopist “perfect security” against inside jobs. Nevertheless, their implementation can help management sleep better at night. A key element to succeed in business is predicting behaviors and situations and taking action proactively. This is true also in information security. Identifying the security deficiencies, the potential exploitations and filling the gaps is the approach to be followed when dealing with the threat of inside jobs. As in the myth of Troy, the city with undefeatable walls was sacked by Greeks hidden inside a horse that was believed to be harmless. Safeguard your perimeter, but what are you doing to protect yourself from inside jobs?

Best Boutique Risk Management Firm in South Florida.

SOUTH FLORIDA CEO MAGAZINE, 2006

They have the ability to understand the needs of our organization and work well with our employees.

THE INTERNATIONAL BANK OF MIAMI

We selected ERM because of their professional references, experience and reasonable professional fees.

R G PREMIER BANK OF PUERTO RICO

ERM accomplished and exceeded objectives planned

BACARDI - MARTINI, INC.

KEEPING WATCH OVER YOUR BEST BUSINESS INTERESTS

ERM professionals bring a unique mix of strong academic backgrounds complemented by professional experience ranging from "Big Four" consulting firms to major corporations and prestigious professional certifications. A snapshot of ERM's profile can be seen below:

Education

Qualifications

M. S. in Computer Information Systems
M. S. in Information Networking
M. S. in Management Information Systems
Master of Accounting Information Systems
Master of Business Administration

Universities

Carnegie Mellon University
Syracuse University
Xavier University
University of Miami
Florida International University

Certifications

Certified Public Accountant (CPA)
Certified Information Systems Security Professional (CISSP)
Certified Information Systems Auditor (CISA)
Certified Information Systems Manager (CISM)
Certified Information Technology Professional (CITP)
GIAC Security Essentials Certification
GIAC Systems and Network Auditor
Microsoft Certified Professional

Prior Work Experience

PriceWaterhouse Coopers
Deloitte
CERT® Coordination Center
SONY Electronics Latin America, Inc.
RJR Nabisco
Diageo plc
Arthur Young
Carnegie Mellon CyLab
Evertec Inc.
American Bankers Insurance Group
Chesbrough Pond's
Starboard Cruise Services, Inc.

Some of our Clients...

ABN AMRO Private Banking
Bacardi-Martini, Inc.
Carnival Cruise Lines
CitiBank
Commerce Bank
Florida Power & Light Company
Knight Ridder
North Broward Hospital District
Ocean Bank
Rinker Materials
Sylvania Lighting International
The International Bank of Miami

enterprise risk management

The Control Professionals

800 S. Douglas Road, North Tower # 835,
Coral Gables, FL 33134.
P: (305) 447 6750 F: (305) 447 6752
Email: info@emrisk.com
Web: www.emrisk.com