Secure Coding.
Practical steps to defend your web apps.

Employee Management Security Controls

James E. Purcell

Employee Management Security Controls

Introduction

The purpose of this paper is to help the CISSP student understand employee management security controls and the need for such controls.

Security controls are measures taken to safeguard an information system from attacks against the confidentiality, integrity, and availability (C.I.A.) of the information system. Note that the terms *safeguard* and *countermeasure* are sometimes used as synonyms for security control.

Security controls are selected and applied based on a risk assessment of the information system. The risk assessment process identifies system threats and vulnerabilities. Then, security controls are selected to reduce (mitigate) the risk.

"We have met the enemy... and he is us" – Pogo (Walt Kelly)
http://www.igopogo.com/we_have_met.htm

Information security practitioners tend to focus on threats from sources outside the organization. Crackers, competitors, foreign governments, and organized crime account for a large number of attacks. But in terms of damage, the insider employee is a much more dangerous threat. The employee has detailed knowledge of organizational policies and procedures used to protect sensitive information. Therefore, the employee also knows ways and has the means to circumvent those protections. Employees have many motivations to do damage to the organization. These include revenge, entitlement, and greed. But in many cases, the damage is done from unintentional actions such as errors or even good intentions gone badly.

“Trust, but verify.” – Ronald Reagan

Employee management security controls provide the “verify” for trusted employees. Employee management security controls mostly fall into the administrative control category. Administrative security controls are primarily policies and procedures put into place to define and guide employee actions in dealing with the organization’s sensitive information. The following sections detail the most common employee management security controls.

Employment Agreements

An employment agreement (or contract) sets out the conditions for employment with the organization. The employment contract is agreed to and signed by the employee before employment begins. The employment agreement specifies the employee’s job title, pay rate, vacation and holidays, benefits, and so on. The employment agreement might require that the employee pass a drug test and other types of pre-employment assessments. The employee agrees to abide by

organizational policies and procedures. The employment agreement usually specifies grounds and processes for termination of the employee.

From an information security standpoint, an important component of the employee agreement is how intellectual property (IP) is handled. The employment agreement should specify who owns IP developed by the employee and place restrictions on what can be done with IP when the employee leaves the company. This portion of the employment agreement is also called a Nondisclosure Agreement (NDA), which can also be used to control ownership and distribution of sensitive information and IP among nonemployees (that is, contractors, vendors) doing business with the organization. Many employment agreements contain noncompete clauses that restrict who an employee leaving the company can go to work for.

The employee agreement is an important employee management security control that protects the organization and the employee by defining the employment relationship in legal terms.

Job requirements

A job requirement (or job description) document details the responsibilities and duties of the employee. This employee security control sets boundaries for what the employee can do. For example, a payroll data entry clerk's job description would specify an "enter payroll data" duty. If the payroll data entry clerk attempted to print payroll checks (not a job duty), that employee would be performing an unauthorized activity.

The job requirements' security control expands on the employment agreement by providing specific job duties for the employee's job title. Organizations need a system of classifying jobs and keeping job descriptions up-to-date. Having well-defined job classifications and job descriptions makes it easier to implement the separation of duties and least privilege security controls discussed later in the paper.

Background Checking

The background check employee security control provides the organization with assurance that the employee has not lied on the job application, and that the employee does not have something in his past that could be used to blackmail or otherwise compromise him in his position. For example, an employee with a substance abuse or gambling problem would be more likely to defraud the organization.

Background checks are especially important for employees in trusted positions (such as system administrators, payroll system managers). Background checks can be as simple as verifying employment application information and doing a credit check. They can also be extensive by interviewing the employee's friends and neighbors. Background checks should be carried out on new employees but

also should be done on existing employees when job responsibilities increase. The background check should be renewed on a regular basis to look for new information that might compromise the employee.

Example formal background checks carried out in U.S. government organizations are Top Secret, Secret, and Q.

Awareness and Training

Awareness and training are ongoing activities to be sure that employees know their security roles and responsibilities. When new employees are hired, they should be formally trained in organizational security policies and processes. If the employee has specific information security-related duties, the employee should be formally trained to carry out those duties. To reinforce security awareness and training, the training should be carried out on a regular basis (at least annually).

Following are three types of security awareness and training:

Security awareness – The goal of security awareness is informing employees of their security roles and responsibilities and keeping those roles and responsibilities in their minds as they go about daily tasks. Security awareness training takes place when an employee is first hired and then at regular intervals (at least annually) afterward. Security awareness can be provided through formal classroom training, but more often, it is in the form of special security newsletters, emails, or events. Examples of security awareness training would be going over the organization acceptable use policy in new employee orientation, and then reminding the employees of the acceptable use policy with occasional emails that give examples of correct and incorrect system use.

Security training – For employees with specific security roles and responsibilities that require special knowledge and abilities, security training provides the needed skills. Security training is specific to a technology or job function. For example, a firewall administrator would take training for the brand of firewall used by the organization, as well as receiving training on general firewall concepts.

Security education – Security education is broad-based and applies to employees with overall organizational security responsibilities. Security education supplies the theory behind specific security techniques and technologies. Obtaining the CISSP certification is an example of security education.

Separation of Duties

Separation of duties is an important concept for protecting sensitive information systems. Used extensively in financial institutions, separation of duties requires at least two people to accomplish a sensitive task. For example, a bank teller can initiate the withdrawal of a large amount of money, but a bank manager must approve the transaction. In an information system, an example is that a system

administrator can examine security logs, but only a security administrator can clear the logs. Another classic example is separation of duties between programmers and production systems. A programmer can make changes to application code, but only a system administrator can apply the change to the production system after Quality Assurance has tested the change.

The separation of duties security control can be defeated through collusion. If the bank teller and the bank manager work together to defraud the bank, they have used collusion to overcome the separation of duties control. But the more people involved in a crime, the more likely the crime will be discovered.

The CISSP student should be aware of two types of separation of duties. The most common type for information systems is Split Knowledge. With split knowledge separation of duties, each person involved in the transaction knows only her own job function. For example, the bank teller would not have the information to know how to approve the withdrawal, and the bank manager would not have the information needed to initiate the withdrawal. The second type of separation of duties is Dual Control. In the dual control type, both persons know how to carry out the task, but they must both synchronize their actions to accomplish the task. For example, in a bank, two people must turn a key or enter a code simultaneously to open the bank vault. Nuclear weapons under military control are another example of a dual control system. Two keys must be inserted and turned to arm the weapon.

Least Privilege

The least privilege principle is implemented through various employment management security controls. Least privilege means that the employee is given access only to the resources and information needed to accomplish his specific job. The employee's official job description should be the basis for the assigning privileges. Least privilege can be used to set up separation of duties as in the example of the bank teller and bank manager previously described. If the bank teller does not have access privileges to the application to approve high-amount withdrawals, the access control system implements separation of duties and least privilege.

"Need to Know" is similar to least privilege. The "Need to Know" right restricts sensitive information to only those that need that information to accomplish a task or make a decision. "Need to Know" is generally more granular than least privilege and can have content and time limits assigned. For example, a general may have a Top Secret clearance (can see anything), but only a Need to Know for the details of the troops under his command. The general might see this year's strategic plan because he is implementing it for his command, but he cannot see next year's plan because he does not yet have a need to know it.

Job Rotation

Rotation of job duties and responsibilities is an employee security control that breaks up opportunities for collusion and fraudulent activities. An employee working alone or in concert with others to defraud the organization is more likely to be caught when a new person examines the system's work processes and notices irregularities. Job rotation is difficult in small organizations with limited staff. A possible downside to job rotation is that an employee, over time, gains knowledge of enough business processes to make it easier to the employee to commit an attack. As employees rotate through positions, careful attention must be paid to control logical and physical access to information resources.

Vacation and Leave

Mandatory vacation is a less extreme (compared to job rotation) employee security control used to detect fraud. In many fraud schemes, the attacker must be present each day to carry out some action to commit the fraud or cover his tracks so he will not be caught. But while on vacation, it is more likely the illegal activity will be detected. For sensitive positions (such as system administrator), many organizations schedule audits of the employees' system activities while they are on vacation.

Terminations

Voluntary and involuntary terminations of employees from the organization are danger points for sensitive information systems. Security controls put into place around terminations attempt to reduce the risk the terminated employee will do damage to the organization. Employees terminated involuntarily may sabotage systems or attempt to disrupt operations. Even employees who terminate employment voluntarily may attempt to take organizational intellectual property or other assets. An example of a termination control is to revoke system access and privileges immediately after termination. Many organizations require terminated employees be escorted from the property to reduce the risk that they would leave with organizational property.

Care must be taken when invoking termination control processes not to overdo things and turn what may be an amenable employee into a resentful employee.

Related to termination employee security controls are job action controls. Job actions are punishments or consequences of an employee violating organizational policy (that is, acceptable use policy). One such action is unpaid time off. Another job action is demotion or reassignment of responsibilities. When job actions take place, the employees' system permissions should be reviewed and adjusted as needed.

Monitoring and Audit

Monitoring and Audit security controls are used to verify that the employee is complying with security policy and procedures. The goal of monitoring and audit

security controls is to make the employees accountable for their activities. Note that in most cases, the employees must be informed that their business activities are subject to monitoring. Otherwise, in most societies, there is an expectation of privacy. The knowledge that monitoring is taking place is a deterrent to unauthorized activity in itself.

Monitoring is generally the activity of looking for violations of security controls. For example, a security administrator checks systems access logs to look for entries where employees have attempted to access files they are not authorized to see (violations of least privilege). Or outgoing emails are scanned for phrases such as “secret formula” or “strategic plan.”

The term audit is sometimes used in the same context as monitoring, but audit is different. *Audit* is the activity to ensure that security controls are properly implemented and applied. For example, an audit would examine all the resource permissions assigned to an employee and be sure only the appropriate permissions were applied. An audit would determine that all employees have received security awareness training and have signed appropriate NDA and employment agreements.

Summary

In the short history of computer information security, the most damaging attacks have been carried out by trusted inside employees. The CISSP must understand this threat and apply appropriate employee management security controls.

Extreme care must be taken when implementing these controls. Employees want to feel the company trusts them. If these controls are implemented in a heavy-handed manner, employees will be resentful, and the overall effect could be more damaging to the organization than if the controls had not been implemented. Senior management must be 100% behind these controls, and senior management must be subject to the controls as an example to the employees. These controls are best implemented slowly with plenty of security awareness training so that employees understand why the controls are needed. A good tactic is to demonstrate to the employees how the security control protects them and the company from bad consequences.

Last Updated: May 27th, 2017

Upcoming SANS App Sec Training

SANS Stockholm 2017	**Stockholm, Sweden**	**May 29, 2017 - Jun 03, 2017**	**Live Event**
SANS Minneapolis 2017	**Minneapolis, MN**	**Jun 19, 2017 - Jun 24, 2017**	**Live Event**
SANS London July 2017	**London, United Kingdom**	**Jul 03, 2017 - Jul 08, 2017**	**Live Event**
SANSFIRE 2017	**Washington, DC**	**Jul 22, 2017 - Jul 29, 2017**	**Live Event**
Community SANS San Francisco DEV541	**San Francisco, CA**	**Aug 28, 2017 - Aug 31, 2017**	**Community SANS**
SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
Secure DevOps Summit & Training	**Denver, CO**	**Oct 10, 2017 - Oct 17, 2017**	**Live Event**
SANS Seattle 2017	**Seattle, WA**	**Oct 30, 2017 - Nov 04, 2017**	**Live Event**
SANS Cyber Defense Initiative 2017	**Washington, DC**	**Dec 12, 2017 - Dec 19, 2017**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**