Personnel Security

Himadri Barman

Introduction

It is an established fact that more than 70% of security incidents are attributed to internal threats. The impact of an internal security threat is immense; it provides easy options to jeopardize security of otherwise impregnable system. Human factor probably is the single greatest source of risk. Employees by virtue of their roles, get access to extremely sensitive and confidential information during their tenure of employment. The quantum and complexity of data — that employees are handling — are increasing multifold. The sensitive nature and value of data that organizations are processing demands a greater emphasis on security of human resources. Personnel Security thus plays a crucial role in the overall security preparedness of an organization.

When handling information, the personnel are the most critical element. Personnel are responsible for creating and handling the information assets. They are the end users of the information, as well as custodians of these assets. In brief, they are themselves the most critical asset who handle the information assets of the company. Unlike all the other assets, they can be sentimental, temperamental, emotional or just plain ornery. Those very human characteristics need very careful handling. We need to have two levels of security for handling the personnel assets:

- Identification and classification of personnel as per the asset classification and control scheme.
- Specifications of roles and responsibilities: Personnel are the creators, custodians and destroyers of assets. For these three incarnations, we need to specify roles and responsibilities, do’s and don'ts, training and education, and finally the disciplinary processes.

Elements of Personnel Security

Personnel security has three major elements, which depend on or complement one another:

- personnel screening, for suitability for employment
- granting specific authority to access official and classified material or sensitive sites
- the security clearance system

The human resources department is responsible for personnel screening. This involves obtaining satisfactory character reference(s), at least one business and one personal, also confirmation of 'claimed' academic and professional qualifications and identity checks. While doing these routine checkups, an additional factor is to identify the access level the employee will have to information. If the employee has to handle information of a classified nature, the background check should be more stringent. Since the nature of this responsibility as well as the personal circumstances keep on changing during the job, the background check will have to be repeated periodically and not end with the checkup done once at the entry level alone. If an organization employs contractors and temporary staff, the same level of checking needs to be done for all such staff. If the organization is not in a position to do this checking by itself, it will have to ensure that the external agency providing the staffing service does the check up and takes up responsibility.

The human asset classification involves granting clearance levels to handle information assets. The classification should not be done merely to reflect the organizational chart

but should be decided based on organizational needs and segregation of duties, which could be implemented without compromising efficiency.

The clearance level could indicate the classification level of information that a person is allowed to access. Access to information may be for reading, writing or modifying, storing or retrieving and finally disposing or destroying. For example, a computer operator may have access to information only for taking backup but not for reading or modification. If the current IT technology makes the implementation of such access rights difficult, (the software or the hardware may not support it), they should be implemented defining appropriate procedures as well as segregation of duties.

Aspects of Personnel Security

1. Defining security as part of job responsibilities
Keen awareness of security is possible only when it is defined clearly as part of job responsibility. This should include responsibility of maintaining the security policy of the company, as well as specific responsibilities for the protection of specific assets or security processes or activities. Thus a computer programmer's job description should mention his or her responsibilities about creating a program with security specifications in mind. This will be a new angle as the programmers are usually concerned about functional specifications and not security specifications. This lapse has given rise to most of the security breaches, which exploit bad programming practices like not testing the programs for buffer overflow conditions. A hacker is able to crash a computer by feeding input data, which causes the buffer overflow.

2. Terms and conditions of employment
Terms and conditions of employment should have explicit mention of the employee's responsibility for information security. All the applicable laws related to information security should be considered while drafting the employment contract. The terms of the contract should extend outside the organization's premises and outside the normal working hours, and should cover the period after the end of employment. This means that the information acquired by employees during their employment period should not be used by them at the end of employment, at least for a predefined period.

3. Confidentiality agreements
The strict measures for information security could only be implemented with confidentiality and non-disclosure agreements signed with employees, casual staff and even third-party users. These agreements should be reviewed whenever there is a change of status like an employee leaving the organization or a contract coming to an end.

4. Information security education and training
Ignorance of law is unpardonable, similarly you cannot be pardoned for 'ignorance of information security' to justify inaction. An organization is expected to take all necessary measures to appropriately train its employees as well as third party users about information security policies and procedures adapted by the organization. The training could be customized for the needs and responsibilities of the staff. It should include:

- An information security awareness program for the top management which should educate them about the importance of information security and the measures adapted by the organization to achieve the security objectives.
- Merely issuing the security policy is not enough. A security awareness program customized for the end user should be designed. Every security measure will be viewed as an impediment in the way of efficiency by the end users. Unless the training program explains the cause and effect of every security requirement, the end user may spend their creative intelligence on devising clever tricks to circumvent the security measures.

- Availability of Internet and email facilities at the work place is taken for granted today. Security training to educate everybody about the legal responsibilities and correct use of information processing facilities is necessary before access to information or services is granted.
- Specific training on how to identify *social engineering* attempts and thwart them could be the single most important security measure.

5. Responding to security incidents and malfunctions

Only alert and responsive personnel could take most important preventive and detective security actions by quickly responding to the security incidents and malfunctions. Employees should be especially encouraged to report any security incident immediately. A formal but easy procedure should be established. A feedback process should be implemented so that the actions taken can be reported back to demonstrate the commitment towards security. The incidents could be used as examples during the user training programs.

6. Reporting security weaknesses

Users should be encouraged to report any observed or suspected security weakness to the appropriate authority. At the same time, users should also be educated not to become self-appointed detectives to discover security weaknesses in the system. This may be interpreted as an attempt to breach security. With easy availability of vulnerability assessment tools and also well-publicized security flaws, this may be a temptation, especially to the technical staff. They should be encouraged to join the security teams in official capacity, if they have the time and inclination towards such work.

7. Reporting software malfunctions

Similar to reporting security weaknesses, the software malfunctions should also be immediately reported and immediate actions should be taken to contain the malfunctioning software from affecting other systems.

8. Learning from incidents

There should be a strong process for learning from the incidents. Each incident should be analyzed to identify the root cause and reason for failure of the controls. Based on this analysis, a decision may be necessary to provide additional controls or enhance the existing controls. The cost of each incident should be calculated. This will be required while justifying additional controls as well as review of security policy and procedures.

9. Disciplinary process

A security policy without a well-defined disciplinary process is like having a toothless dog to guard your property. The barking alone is not enough to deter the miscreants, there has to be a threat of being bitten too. Since we are dealing with the most critical asset, i.e. personnel, we have to be careful when framing a disciplinary policy for the organization. The process should be correct, fair and adequate. Legal as well as HR departments should be involved while designing the process. The process should be based on identifying the impact of security lapse. This is similar to the risk assessment while selecting the controls. The disciplinary action should punish the behavior, which exposes the organization to risk. Higher the risk, more severe should be the punishment. Thus, using weak passwords for accessing personal e-mail may not be a very risky behavior, but using the same password for accessing a financial database is definitely a risky behavior. Accessing the Internet for searching business information may not be considered risky behavior, but visiting sites, which are of dubious nature, may be a very risky behavior. It is necessary to clearly identify the behavior, which is punishable by disciplinary action, and convey the same through a security policy, as well as awareness training programs.

Implementation of the disciplinary process is not a very easy task. A step-by-step procedure may be designed. The first step will be to create awareness about the disciplinary process. During this phase, only verbal warnings should be issued to the defaulters. The next phase would be to create 'painful' awareness, by issuing written warnings to defaulters. The last phase could be the punishment phase. The punishment should be commensurate with the offence as well as persistence of the crime and may range from loss of pay to loss of job.

Personnel Security Strategies

The following are important strategic considerations as far as Personnel Security is concerned:

- Preparing a catalogue of all HR processes — pre-employment, during the course of employment, employee exit and post exit elements — where security considerations are critically required
- Identifying all elements of the organization's security initiatives and mechanisms that require involvement of the HR function.
- Creating an inventory of compliance requirements specific to Personnel Security and map these to the HR processes
- Creating an inventory of instances that provide employees access to information resources.
- Analyzing the threat perceptions and scenarios from human resources perspective that may lead to compromise of security or a data breach
- Identifying security requirements for all relevant HR processes — considering the threat perceptions and compliance requirements of an organization
- Creating an inventory of all security trainings and awareness elements that are mapped with resources dedicated and media used to deliver them
- Analyzing how organization's messages on security are communicated to the employees and all stakeholders involved.
- Ensuring that a significant level of resources and efforts are dedicated to Personnel Security functions and activities.
- Developing a strategic roadmap for personnel security using options such as use of collaboration platforms for employee awareness and participation, automation of policy enforcement and breach notification, adoption of techniques for integration with other security mechanisms.

Personnel Security Best Practices

Organizations interested in Personnel Security may adopt the following best practices:

- Ensuring that there exists a significant and visible commitment of the senior management stating importance and demonstrating their involvement for enforcing security across all levels in the organization
- Ensuring that for each scenario — that may lead to leakage of data from employees during employment, in the process of exit and post employment — there exists a control mechanism to avoid data breaches
- Ensuring that pre-employment HR process involves background checks and it is extended to all support functions and external service providers
- Ensuring that terms and conditions of employment explicitly mention adherence to security of data through a confidentiality agreement
- Ensuring that employee induction training incorporates security awareness sessions. This should be followed by routine awareness campaign during the tenure of employment
- Ensuring that employees are aware of their contractual obligations and legal liabilities of their system and online behaviour
- Ensuring that the HR function is involved in access granting and revocation process. This is enabled by a mechanism that integrates HR workflow with

information systems and a collaboration between HR, information security and IT functions

- Establishing a communication plan for conveying enterprise messages on security
- Ensuring that the policies for acceptable use are established for secure usage of organization's resources — email, internet, systems, networks, applications, files, folders and data
- Ensuring that the administrative rules and procedures are established to ensure compliance with information security policies
- Ensuring that a mechanism and supporting disciplinary processes are established to resolve non-compliance issues and other variances in a timely manner
- Ensuring that a mechanism exists for monitoring and reporting employee behaviour as per the policy of acceptable use
- Ensuring that the performance of HR security function is tracked continuously, and the performance reports are made available for compliance and senior management review

Conclusion

New employees get immediate access to sensitive data; during their tenure they may be exposed to critical data as an owner, custodian and user; until the time of their exit they might hold key customer data, attain mastery in the organization's trade secrets, customer personal information, IPRs etc. The human factor, therefore, poses greater risk to the organizations and their customers' data. This concern is increasingly reflected in various compliance regulations, specifying personnel security measures like background screening, confidentiality agreement with employees and monitoring of employee behaviour. The evolution of HR practices that address information security needs of an organization has led to the establishment of Personnel Security as an important domain of organizations' security initiatives. Personnel Security is an important means towards achieving the end goal of data security.

References:

http://www.networkmagazineindia.com
http://www.security.govt.nz
http://www.dsci.in/taxonomypage/94