Evaluating Privacy Controls

By Sean M. Price, CISA, CISSP

Privacy breaches are a regular occurrence, as is evident in popular media.1 A more disturbing thought arises when considering the number of privacy breaches that are unknown or are not reported.2 Reported breaches typically involve lost media, unauthorized access by outsiders or inappropriate access by insiders. These types of exposures subject an organization to disincentives such as loss of customer confidence, governmental fines and perhaps cost associated with credit monitoring services for affected individuals. A system that is regularly audited by a nonbiased party may reveal weaknesses prior to an actual breach. System auditors have within their power and ability opportunities to discover security control weaknesses that affect privacy information. This article proposes a methodology by which an auditor can evaluate privacy controls to determine any relevant shortcomings that might impact the confidentiality of privacy information.

Organizations have sufficient incentive to implement the necessary controls to reduce the likelihood of abusive access to privacy information. Governments from around the world are instituting laws and regulations that require organizations to protect privacy information from exposure.1 Those organizations that fail to protect privacy information are reported frequently in the media and may face a loss of public image due to the exposure. Similarly, the result of an acknowledged breach may allow affected parties the right to conduct litigation against the organization. The costs of implementing security controls that can mitigate attempts to breach privacy are more than likely less than government, image or litigation penalties realized from a breach. A system auditor can leverage these disincentives when reporting weaknesses in controls used to protect privacy information.

An important aspect in evaluating privacy controls is to determine what requirements are specified. These can be gathered from applicable laws, regulations and organizational policies supported by documented procedures. These types of requirements form the basis of the security controls that must be implemented. Unfortunately, these sources of requirement may be ambiguous or outdated, given current threats. In such cases, the auditor should consider the ramifications of weak requirements—those insufficient in specifying the necessary privacy controls. Although this may be against the grain of routine checklist auditing, the willingness to step up and identify policy weaknesses supports privacy and security issues in the long run.4

Methodology

It is recommended that a system auditor follow a regimented methodology when reviewing privacy controls. Following a methodology that documents the test conducted, expected result and actual result provides repeatability for those that rely upon the results. This significantly adds to confidence and reliability of the testing conducted and the evaluation of the results. Auditors are advised to consider the management, operational and technical controls of a system when evaluating privacy controls. This article recommends following an evaluation methodology that uses interviews, document reviews, process examination and technical testing of privacy controls. The chosen methodology should focus on the evaluation of the directive, preventive and detective controls used to protect privacy information. A comprehensive presentation of these control types is available in the Official (ISC)2 Guide to the CISSP CBK.5

Directive Controls

The promulgation of policies and procedures that specify handling caveats for privacy information is the first line of defense against a privacy breach. Researchers have identified the importance of policy development, comprehension and automation.4 In this regard, directive controls are used to guide insiders on the appropriate handling methods required to protect the information from unauthorized exposure. Through the use of policy, training and performance evaluations, insiders have sufficient awareness that casual, yet inappropriate, access is not permitted.

• Policy—This establishes the baseline for appropriate handling and protection measures for privacy information. Organizational policy should explicitly identify information types that need to be protected from unauthorized disclosure. It should further specify appropriate and inappropriate types of access to privacy information. The following steps should be taken:
  • What constitutes privacy information is defined explicitly.
  • Authorized methods of handling privacy information are addressed.
  • The various roles of those with authorized access to the information are identified.
  • Actions required in the event of a privacy breach are identified.

• Procedures—Insiders should have explicit written guidance detailing the processes and procedures used to appropriately handle privacy information and reporting of suspected
compromises. The guidance should have qualities which can be implemented and easily understood. Procedures should specify these aspects:
- Applications authorized to process privacy information
- Acceptable storage locations and media
- Proper transmission methods
- Additional protection measures, as applicable
- A protocol for validating requestor access to privacy information
- Detailed processes used to investigate and report a suspected or actual privacy breach
- Procedures that address all areas specified in the policy

• **Configuration guides**—Operating systems and applications used to process privacy information provide an opportunity to enforce organizational policy electronically. Security configurations supporting the policy should be explicitly documented, including:
  - Operating system configurations
  - Application configuration guidance

• **Training**—Individuals with authorized access to privacy information should be trained regularly regarding the applicable policies and procedures. The training should supply the necessary skill set an individual needs to make appropriate judgments regarding the processing, storage and transmission of privacy information. The documented training material:
  - Covers policies and procedures
  - Focuses on the roles appropriate for the trainee
  - Is conducted periodically
  - Provides trainer and trainee with acknowledgment that the training has been provided and retained as a matter of organizational record
  - Assesses trainee understanding through a test or quiz of the material

• **Performance evaluation**—Subordinate evaluations provide an opportunity to document compliance or noncompliance with privacy handling policies and procedures. This is an important tool that can be used to discipline or reward subordinate actions. The following steps should be taken:
  - Subordinate evaluations should consider compliance with policies and procedures.
  - Management should take administrative actions based on evaluations and any relevant investigations.

**Preventive Controls**

Ideally, a system prevents unauthorized access to privacy information at all times. This is difficult to accomplish in practice. A significant impediment occurs due to reliance on discretionary access control (DAC). There are known weaknesses with DAC systems, e.g., the issue of the Trojan horse.¹ Researchers proclaim that end-to-end solutions are needed to prevent unintended releases of sensitive information.² Consider the following techniques when evaluating preventive controls supported by a system:

• **Separation of duties**—System users with access to privacy information should be separated through groups or roles. The extent of access to privacy information should be limited where possible. For instance, if a particular user needs access to only a subset of the privacy information, the system should be configured to support the constraint. The following steps should be taken:
  - Roles or groups are established and supported by the system.
  - Individuals assigned to roles or groups are documented. This provides a means to identify inappropriate or unauthorized accounts given access to the privacy information.
  - Access to privacy information is restricted by the system to only those roles or groups authorized.

• **Least privilege**—Implementing the concept of least privilege potentially aids in the unauthorized propagation of privacy data through information flows. Preventing unauthorized flows of privacy information is the principal goal in mitigating breaches. The following steps should be taken:
  - Resource access is restricted to only what is needed to support user duties.
  - Workstation controls prohibit the execution or installation of unauthorized software.
  - Least-privilege implementations support policy.
  - Moving privacy information to removable media or through network connections is considered.

• **Ad hoc access prevention**—Excessive access is the bane of security. Allowing *ad hoc* enumeration of files or records containing privacy information magnifies the damage of a privacy breach. The following steps should be taken:
  - Where possible, *ad hoc* enumeration of files or records containing privacy information is prohibited.
  - Roles and groups allowed *ad hoc* enumeration are documented and justified.

• **Restricted applications**—Only designated applications should be allowed to retrieve, store, process and transmit privacy information. Where possible, the system should enforce this restriction and prevent unauthorized applications from executing on the system. Technical methods of restricting application access to privacy information or credentials, such as keystroke logging countermeasures, are advisable.³ The following steps should be taken:
  - Applications used to access privacy information are documented.
  - Operating system access control and application configurations are used to protect the integrity of the application, the data and the confidentiality of the information processed.
  - Where possible, the system restricts access to the privacy information to only those applications authorized.

• **Network controls**—The ports and protocols used to access privacy information should be controlled. Restricting ports and protocols through firewalls or related techniques will make attempts to compromise the information more difficult. The following steps should be taken:
  - Ports and protocols authorized to access privacy information are documented.
  - Unauthorized ports and protocols are blocked.
  - Network access to privacy information occurs only after the requestor is authenticated by the system.
• **Encryption**—Privacy information in transit and storage should be protected from compromise through the use of encryption. End-to-end techniques that employ encryption are a reasonable approach.\(^{10}\) The following steps should be taken:
  - Network access to privacy information is encrypted using an approved protocol such as Secure Sockets Layer or IP Security.
  - Authorized removable or mobile media are encrypted.
  - Privacy-related files or records on the system are encrypted, where possible.
  - Strong algorithms, such as the Advanced Encryption Standard, are implemented.
  - Encryption keys are managed.

• **Strong authentication**—Strong authentication techniques such as tokens or smart cards that provide an extra layer of protection for individuals accessing privacy information should be implemented. The following steps should be taken:
  - Use of tokens or smart cards is implemented according to policy.
  - Distribution of strong authentication devices is controlled strictly.
  - Authentication devices are integrated with applications to strengthen access controls to inhibit attacks by malicious software.

**Detective Controls**

The last lines of defense against inappropriate access to privacy information are detection controls. These types of controls reveal access actions to privacy information and can be used to evaluate the appropriateness of the activity.

• **Auditing**—This is an important control used to detect inappropriate access to privacy information. The proper implementation of auditing involves implementations that consider people, processes and the system. Each implementation aspect should be scrutinized to identify any weaknesses. The following steps should be in place:
  - The aggregation of audit records provides sufficient information to recreate events leading to a breach.
  - Files and records containing privacy information have auditing enabled for successful and failed access attempts.
  - Audit records are protected from tampering or disclosure.
  - Individuals are assigned to periodically review audit logs. Records exist of their reviews and any subsequent investigations.

• **Conspicuous privacy information**—Managers should take note of privacy information on individuals of special interest. An insider might be tempted to learn juicy information on corporate executives, politicians or others with celebrity status. Managers should regularly correlate access to records of these individuals with successful audits to identify any inappropriate access. The following steps should be taken:
  - High-profile individuals are identified and documented.
  - Reviews of audit logs are conducted to identify inappropriate access to the privacy information of high-profile individuals.

• **Information flow monitoring**—Inappropriate flows of privacy information are bound to occur. Monitoring of information flows provides a means to determine if privacy information is being diverted to improper destinations. Specialized tools should be implemented on the system to detect inappropriate information flows or privacy policy violations.\(^{11}\) The following steps should be taken:
  - Host-based monitoring is conducted to determine if removable media are being used to store privacy information inappropriately.
  - Network analysis equipment is deployed to determine if privacy information is traversing the network through unauthorized ports or protocols.
  - Shared directories are reviewed periodically to determine the existence of unauthorized privacy information.
  - Commands such as “grep” on UNIX or “Search” on Windows are automated to identify keywords indicative of privacy records within shared files.
  - Dirty-word filters are used to detect information passing through e-mail servers.

• **Supervisor involvement**—Managers need to be cognizant of subordinate activities. Indeed, managers play a key role in information security.\(^{12}\) They should take an interest in training and monitoring to help protect privacy information. The actions of managers provide a cue to subordinates of what they might be able to get away with doing. Managers who regularly emphasize the need to protect privacy data represent an excellent deterrence. Managers who are involved with the process of reviewing questionable subordinate access to privacy information can expedite internal and external investigations when armed with the knowledge of the types of access for which a subordinate is authorized. The following steps should be taken:
  - Management regularly emphasizes the need to protect privacy information through words and actions.
  - Supervisors support investigations of possible subordinate abuse of access to privacy information.
  - Managers take immediate corrective action when weaknesses in privacy controls are discovered.

**Conclusion**

Evaluating privacy controls is best accomplished when it is pursued with an appropriate methodology. When deterrence, prevention and detection controls are implemented properly, the result is a reduction in the likelihood of inappropriate access to privacy information. A systematic evaluation of these controls supports a comprehensive review that enables the identification of opportunities to enhance the organization’s security posture. An independent auditor can make substantial contributions to the evaluated entity through a rigorous evaluation of the privacy controls implemented.

**Endnotes**


Tipton, H., K. Henry (Eds.); Official (ISC)² Guide to the CISSP CBK, Auerbach, USA, 2006


Myers, A. C.; B. Liskov; “Protecting Privacy Using the Decentralized Label Model,” ACM Transactions on Software Engineering and Methodology, 2000, p. 410-412


Op cit, Brodie

Op cit, Polstra

Sean M. Price, CISA, CISSP

is an independent information security consultant located in Virginia, USA. He provides security consulting and architecture services to commercial and government entities. Price has more than 12 years of information security experience, including system security administration, user information assurance training, policy and procedure development, security plan development, security test and evaluation, and security architect activities. Security research areas of interest to Price include access control, information flow, insider threat and machine learning. He can be reached at sean.price@sentinel-consulting.com.