Security Policy Research

The Insider Threat – Security Policies to Reduce Risk

InformationShield

About Information Shield

Information Shield is a global provider of security policy, data privacy and security awareness solutions that enable organizations to effectively comply with international security and privacy regulations. Information Shield products are used by over 9000 customers in 60 countries worldwide.

Information Shield, Inc.
7549 Highmeadow Dr.
Houston, TX 77063
www.informationshield.com
sales@informationshield.com
P: 888.641.0505
F: 866.304.6704

Table of Contents

Information Shield Whitepaper

The Insider Threat – Security Policies to Reduce Risk

Summary

2011 could be considered the "Year of the Insider." From the RSA hack and Sony Playstation breach, to the Epsilon e-mail breach and the Oak Ridge phishing attack, database breach announcements that started with insider mistakes have become common news. Malicious threats are also on the rise, as Bank of America was hit with over $10 million in losses due to a malicious insider.

In this paper we will break down the various attributes of the insider threat, and suggest some information security policies that can help reduce the likelihood of current and former employees causing harm to the organization.

Limit of Liability/Disclaimer of Warranty: While the copyright holders, publishers, and authors have used their best efforts in preparing this work, they make no representations or warranties with respect to the accuracy or completeness of its contents and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. The advice and strategies contained herein are based on the author's experience and may not be usable for your situation. You should consult with an information security professional where appropriate. Neither the publishers nor authors shall be liable for any loss of profit or any other commercial damages, including, but not limited to, special, incidental, consequential, or other damages.

Defining the Insider Threat

Report after report keeps pointing to the "insider threat" as one of the greatest information security risks within the modern organization. But what exactly IS the insider threat and how to we help reduce this risk in our written security policies?

Since the very notion of an insider threat involves the risk of people's behavior, and security policies are design to impact behavior, it makes sense to look at the problem of the insider threat from the perspective of the "lifecycle" of an employee's access to information.

In this paper we will break down the various attributes of the insider threat, and suggest some information security policies that can help reduce the likelihood of current and former employees causing harm to the organization. We illustrate some of these controls will sample policies from our security policy sample library.

What is the "insider threat"?

In general, the term "insider threat" refers to employees or contractors that, due to their access to sensitive data, are in a position to aid or create a security incident. While some insider threat models only look at employees with malicious intent, to truly address this risk we must look at both accidental and malicious insiders. The Software Engineering Institute and Carnegie Mellon has studied over 200 cases of actual insider incidents, and has developed threat models.

Like all information security threat sources, we can break down the threat into various categories to better understand the nature of the threat and the likelihood of this threat exploiting a vulnerability and causing harm. This is the approach taken during a traditional risk assessment, and the approach can apply in creating security policies aimed at reducing the overall risk of insider threats.

Accidental versus Malicious Activity

When protecting against insiders, one of the first important distinctions to make is between accidental and malicious user activity. Data breach studies often do not make a distinction between these two very different scenarios. But from a control perspective, they may require different protective measures.

Each case presents its own challenges. While the malicious insider is far less common (in other words, the likelihood of having one is much less) their access to information and determination make it much more likely that they will succeed in their attack.

Example: The Malicious Insider Threat

A database administrator for a British company was sentenced to three months in jail, suspended for two years, and fined GBP 3,200 (US $4,858) for breaking into his former employer's computer system to install spyware and delete messages. Julius

Oladiran worked for the company for just three weeks before being asked to leave after it became apparent to management that his resume contained false information.

The Accidental Threat

Far more common than the malicious insider is the employee who makes a mistake that can lead directly or indirectly to an incident or data breach. Some of the many examples include:

1. Employees respond to phishing emails and disclose confidential information.
2. Employees to get malware infections that disclose account credentials.
3. Employees to lose laptops, PDAs or other devices that contain confidential information.

While any employees is generally less likely to have an accident, the sheer number of them and the complexity of the modern IT environment make it likely that some type of accident will eventually occur. The wildcard will be the impact of the accident. In the case of the malicious insider, they are almost always trying to create damage or steal valuable information. In the case of the employee accident, it depends on a variety of factors, including their level of access to sensitive information and the magnitude of the breach as to whether the incident causes real damage.

Example: UCLA Health System was fined $865,000 for HIPAA violations. The fines were based on activities accumulated between 2005 and 2008, when UCLAHS employees accessed patients' private health records without authorization.

In either case, the potential risk to the organization may be similar. Rogue employees have a lower likelihood and higher impact; accidental employees have high likelihood with a lower average impact.

Employee Role and Status

Another important variable to consider is the status of the user accessing the data. Full-time employees who are currently employed present a different risk profile than contractors, or terminated employees. System administrators or other employees with special privileges also pose a greater risk since they have access beyond traditional employees.

In any case, it is important to consider the “lifecycle” of an employee when considering written security policies. This lifecycle approach is reflected in different information security standards and frameworks, such as the ISO 27002 information security standard.

Security Policy Controls - The Employee Lifecycle

In the following sections we will look at some sample information security controls as they apply to each stage of the “lifecycle” of a typical employee. We illustrate some of these with sample policies from our library, Information Security Policies Made Easy. [4]

Pre-Employment and Hiring

Employee Screening

Screening (ISO 27001 Section 8.1) refers to the process of vetting employees before they are given access to sensitive information. The screening process can be an effective control in all cases, but is particularly effective against malicious insiders. Screening can include background checks, employment history verification and checking references. A common mistake made by employers is failing to identify which jobs might require additional screening. To help facilitate this, the organization should consider the information security-related job requirements of every job role. (See examples within Information Security Roles and Responsibilities Made Easy [5].)

Sample Policy: Company X must identify the information security roles and responsibilities of every job role before hiring new candidates. This process must identify the prospective employee’s access to sensitive or confidential information.

Legal Obligations

The primary purpose of screening policies is to prevent risky employees from entering the workforce in the first place. In addition to employee screening, the organization should use the hiring process to make sure that employees are legally bound to protect intellectual property rights by signing Non-disclosure and non-compete agreements.

Another pre-employment control often overlooked is the re-hiring of formers workers who might still have a grudge against the organization. Consider the following sample policy:

Sample Policy: Former employees, consultants, and contractors who were involuntarily terminated must not be re-hired or retained without the written permission of a senior vice president.

During Employment

A different class of controls can be used to help reduce the risk of employee-related incidents during employment. In theory, this includes the entire range of information security policies, since all information security policies apply to people. For the purposes of this discussion, we will limit the focus to some of the highest risk areas. Security policy controls during employee fall into three broad categories: Accountability, Education and Monitoring.

Assigned Security Responsibility

In theory, all persons who handle information are responsible for security. But this is only theory until it is documented in official policy. The first key control is to make sure that information security responsibilities are clearly defined in job descriptions. This policy effectively links the security policies with the people responsible for following and implementing the policies.

Sample Policy: Specific information security responsibilities must be incorporated into all worker job descriptions if such workers have access to sensitive, valuable, or critical information.

The second key control is the signed acknowledgement and agreement to abide by security policies. This control links the assigned responsibilities to individual acceptance. Without it, the organization is essentially giving away its right to pursue legal action against employees.

Sample Policy: Every worker must understand the Company X policies and procedures about information security, and must agree in writing to perform his or her work according to these same policies and procedures.

Education and Awareness

During employment, there are two key pieces of employee education that must take place. First, employees must be educated on basic information security principles. Second, they must be educated on the specific information security policies of the organization.

Sample Policy: All users of information and information systems must attend information security awareness training (on-line or in-person) each year. This material should provide the information security basics and literacy as described in the Company X Training and Awareness Plan.

Sample Policy: All Company X workers must receive prompt notice of changes in the Company X information security policy, including how these changes may affect them and how to obtain additional information.

While both of these policies are designed to reduce risk, they are both required to reduce liability in the event that a security incident does happen that requires disciplinary action. The defense that an employee was not aware of a given security policy has been successful in several cases. Organizations must implement these two fundamental controls to help reduce insider threats and accidents. By failing to establish awareness of policies, the organization is giving up its right to enforcement.

Separation of Duties

Another key control to reduce the risk of malicious insiders is the separation of duties. In many insider cases, a single person had control over an entire transaction of process [3]. This is especially true in the case of system administrators or others that have privilege to actually change system security parameters.

Sample Policy: To achieve proper separation of duties, for all Company X production systems, Systems Administrators must not attend to, or otherwise be responsible for, information systems security administration. Security administration must instead be handled by Information Systems Security Administrators.

Activity Monitoring

To effectively protect information assets, the organization must monitor employee behavior at some level. The most common of these audit controls include internet and web site access, and access to internal systems. The first is designed to help enforce acceptable use policies for external sources, while the internal system monitoring helps deter and detect insider activity.

Sample Policy: Company X routinely logs web sites visited, files downloaded, and related information exchanges over the Internet. Department managers receive reports of such information and use it to determine what types of Internet usage are appropriate for their department's business activities.

When focused on the insider, however, special care must be taken to monitor the activity of system administrators and other privileged users. These controls are most often included as part of a system monitoring policy.

Sample Policy: All privileged system commands issued by computer system operators must be traceable to specific individuals through the use of comprehensive logs.

After Employment

The role of post-employment policy controls is to reduce the risk of malicious activity from former employees. Like pre-screening, this part of the lifecycle is almost entirely focused on preventing malicious activity. These policies include two broad categories – revoking access privileges (both logical and physical) and returning equipment.

Revoking Logical and Physical Access Privileges

It is essential to revoke both the logical and physical access controls of employees as soon as possible. These include disabling user accounts and physical access devices such as employee badges or smart cards. Several studies have revealed some alarming statistics about “stale” accounts. Many organizations fail to enforce these basic policies, enabling former employees to access systems using old accounts.

Sample Policy: Upon termination, the access rights of an individual to Company X assets associated with information systems and services must be removed or reassigned.

Changing Authentication Credentials

In the case where former employees had special privileged access (such as database, network or systems administrators), it is sound practice to change the passwords of any special administrative accounts that they may have used. This will help prevent employees from accessing accounts after they were terminated. Another control would be to provide a security assessment or review of the key systems which the employee had access to. This may uncover any changes to the security configuration made before the employee was terminated. A common source of incidents is where employees have left a "back-door" into existing systems which they later exploited from outside the firewall.

Sample Policy: Upon termination, the passwords of any employee, contractor, or third-party user associated with accounts that remain active must be changed.

Even when it involves a termination, often one policy is not sufficient to reduce the risk associated with different scenarios. For example, employees that are involuntarily terminated (aka "duress" termination) are more likely to cause harm and must be considered a greater risk.

Sample Policy: To prevent back-doors, Trojan horses, logic-bombs, time-bombs, worms, viruses, and other unauthorized software from being used, all workers dismissed in a duress termination must have their computers immediately isolated from both the Internet and the internal Company X network.

Return of Property

Finally, organizations need to make sure that employees do not leave with property or information that can pose a risk to the organization. Typically this includes equipment, such as computers and networking equipment, and other physical devices like access cards and tokens. Portable computers can not only hold a large amount of information, but they can contain stored access credentials. For this to be effective, the organization must maintain an accurate inventory of which equipment has been assigned to which employees, so a proper accounting can be done at the time of termination.

Sample Policy: Employees, temporaries, contractors, and consultants must not receive their final paycheck unless they have returned all hardware, software, working materials, confidential information, and other property belonging to Company X.

Summary

Defending against internal threats is a complex task. One could argue that preventing malicious insiders is close to impossible. However, by looking at real-world cases of insider activity, it is possible to discover common patterns that indicate which controls would be most effective and reducing the threat. By understanding insider risk and adopting sensible information security policies, the risk of both accidental and malicious threats can be greatly reduced.

In all of these policies, it is important to understand and document which employees have access to which systems and information. Without this documentation, it is difficult or impossible to trace the privileges of the user to perform these tasks. Once again, we go back to perhaps the most critical administrative security policy control: The organization must document the information security responsibility and access of key job roles. The policy is the foundation of the others, and enables the protection of information throughout the employment lifecycle.

References and Additional Resources

[1] ISO/IEC 17799:2005 (ISO 27002) – Code of practice for information security management - Published by ISO and available at BSI [www.bsi-global.org/]

[2] Payment Card Industry (PCI) Data Security Standard, Version 1.2 – Published October 2008, PCI Security Standards Council. [www.pcisecuritystandards.org]

[3] Common Sense Guide to Prevention and Detection of Insider Threats 3rd Edition – Version 3.1, January 2009, by Dawn Cappelli, Andrew Moore, Randall Trzeciak, and Timothy J. Shimeall. Published by Carnegie Mellon University, Software Engineering Institute.

[4] Information Security Policies Made Easy, by Charles Cresson Wood - Published by Information Shield, Inc. 2002-20059. [www.informationshield.com]

[5] Information Security Roles and Responsibilities Made Easy, by Charles Cresson Wood - Published by Information Shield, Inc. 2002-2005. [www.informationshield.com]