

Defending Against Insider Threats To Reduce Your IT Risk

Excerpts from a White Paper published by CA Technologies (ca.com) in January 2011

Executive Summary

Challenge

The threat of insider theft or malicious acts is significant and something all organizations must continually contend with. Organizations have users who have access to sensitive or confidential information that should not, and must not, be communicated outside the organization. They also have privileged users (administrators) who often possess complete privileges to perform essentially any operation on critical systems. Finally, there are regular users who often have accumulated more entitlements than they need for their current job role. All of these factors dramatically increase the risks of insider security and privacy breaches.

Opportunity

Organizations must confront the reality that insider attacks are a significant threat and increasing in complexity. Given that so much of an organization's assets and information are online and accessible, organizations must take a proactive approach to defending against the insider attack. This proactive approach should involve a range of solutions that address identity and access management and information protection. Nothing can completely prevent all insider attacks, but those who adopt an aggressive proactive approach can help reduce risk, improve compliance, and enable the IT organization to better support business initiatives.

Benefits

The benefits of a robust program to defend against the insider threat are clear. First, it allows organizations to better manage the significant risks resulting from insider attacks. Deploying a program to mitigate the insider threat can also help the auditors, reduce compliance costs and improve business efficiencies. Lastly, deploying a multi-faceted solution for insider threat can actually help the organization grow and expand because managing the insider threat better enables the organization to collaborate and partner with other external organizations without significantly increasing risk.

Defending Against Insider Threats To Reduce Your IT Risk

Insider Threats Are Increasing

Increasing sophistication of attacks

The Computer Emergency Response Team (CERT) at Carnegie-Mellon University has defined a malicious insider as “a current or former employee, contractor, or business partner who has or had authorized access to an organization’s network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization’s information or information systems.” Historically, the insider was an employee, but as CERT has noted, the scope of insider threats has expanded beyond the employee population to include collusion with outsiders, “trusted” business partners and others. This development, combined with the highly distributed and mobile nature of today’s workforce, means that the insider threat is more severe than ever before.

Industry statistics confirm the severity of the insider threat. The 2009 e-Crime Watch surveyed 523 organizations and found that 51% of these organizations had experienced an insider attack, up from only 39% of organizations three years earlier. Given that surveys tend to rely on organizations to self-report on insider attacks (and thus may be conservative in their survey responses) and that many insider attacks may actually go undetected, the insider threat problem is likely even more widespread than reported in general surveys. The WikiLeaks story that dominated global headlines in late 2010 was yet another example of the consequences that can result from an insider attack.

Organizations who write off insider threat as a low risk activity and natural consequence of operating in a competitive marketplace (such as a salesperson defecting to a competitor and bringing a price list with him) need to understand the reality and severity of the problem. The insider threat today can range from the disgruntled employee (passed over for a raise or promotion) who has the technical expertise to embed a “logic bomb” in the production code of a critical system to a foreign national actually cooperating with a foreign intelligence agency to steal intellectual property. These examples are real insider thefts ripped from the headlines in the last five years and involve well-known companies. In addition to these malicious examples, careless or inadvertent actions by employees also represent another significant insider threat vector. These inadvertent actions can occur because individuals have accumulated more privileges than they need for their current job functions or because individuals may just be careless about usage and distribution of sensitive data. The end result is that organizations need to defend against the malicious insider as well as the careless user.

Defending Against Insider Threats

Several macro trends are also behind the increase in insider threats.

- **low data storage costs.** The continuing drop in data storage costs means that it is often cheaper for organizations to store and archive all data rather than spending time examining it to determine what should be saved or deleted. The low storage costs means that data is always accessible, so if malicious insiders are looking for data, they can find it.
- **Increased sophistication of attacks.** Not surprisingly, individuals with technical acumen are often the ones committing insider attacks. If they have the skill to conduct the attack, it also means that they also likely possess the skills to cover up the theft, either by modifying/deleting log files or other actions.
- **Highly distributed work force.** Today, employees are much more distributed and access data and applications over multiple channels (Wi-Fi, Ethernet, 3G) from multiple platforms (PC, smart phone, tablet, kiosk). Organizations need to support these multiple access methods to keep workers productive, but each new channel and platform introduces a new set of potential risks that must be managed. When other factors like cloud computing and outsourcing are factored in, the unfortunate reality is that data is essentially everywhere.
- **Inadequate end-user awareness.** Many employees simply lack knowledge of the organization's policies on information use as well as how data is to be used, shared and distributed. This can lead to actions such as users emailing confidential documents to a wide distribution. These instances are not driven by malicious insiders but can be just as damaging to an organization as a malicious insider.

Organizations have attempted to combat the insider threat, but these approaches have generally focused only on detecting outright fraud - for example, controls are implemented to ensure proper segregation of duties within a financial application. The challenge is that we know from recent stories like WikiLeaks that the insider threat is more than just fraud and can also comprise theft of data and intellectual property.

Organizations seeking to mitigate insider threats face three other challenges:

- Sheer volume of audit and log data impedes forensics investigation and detection. Logging all IT activity is an important first step in combating insider attacks and today's highly distributed and complex IT environments generate massive volumes of logging data, but the sheer volume of data is very difficult to manage.
- Most current approaches to addressing insider threats are reactive, not predictive. This helps immensely in forensic investigations, but the problem is that the attack or theft has already occurred. Therefore, organizations should be looking for solutions that can provide more analytic and predictive capabilities that if not able to prevent insider attacks, may still identify "at-risk insiders" and then implement more detailed logging on those individuals in response.
- Delicate balance of risk versus productivity. IT managers need to balance the risk of employees' need for additional access versus the lost productivity that would result if access was not granted to certain users. Many organizations also lack the necessary reporting tools to examine an individual's

Defending Against Insider Threats

expanding entitlements over time, which further compounds the problem. The result is that IT often struggles to answer the critical question, “Who has access to what?” confidently and accurately.

Factors that increase risk of insider threats

There are numerous security vulnerabilities that if not properly managed and controlled, can increase the risk of insider threats.

- **No comprehensive written acceptable use policies.** All organizations should have detailed acceptable use policies for all employees and should make employees review and sign the policy annually. This is a basic step but one that organizations often overlook. Having a written security policy will not necessarily prevent insider attacks, but it can still be useful for providing the entire organization with a baseline of what is acceptable usage and the proper methods for handling sensitive data.
- **Ineffective management of privileged users.** All IT environments have privileged users (admin, root) that have total access to key systems, applications, and information. This is not only a security risk, but it can also make compliance much more difficult. Sharing administrator passwords is another common problem which could lead to inappropriate access to your systems and information and an inability to identify specifically who performed which action on each system.
- **Inappropriate role and entitlement assignment.** The management of user roles and entitlements is one of the biggest challenges that many IT organizations face. Overlapping roles and duplicated or inconsistent entitlements are all common problems that can lead to improper access to, and use of, sensitive information. In addition, the lack of automated de-provisioning can lead to excessive entitlements or orphan accounts, both of which provide openings through which disgruntled insiders can launch an attack.
- **Poor information classification and policy enforcement.** Many organizations do not even know where all their sensitive information is, and often have poorly defined and communicated policies for how that sensitive information should be handled. But, most importantly, many organizations have no controls in place to detect and prevent inappropriate transmittal or disclosure of sensitive information.
- **Weak user authentication.** Access to highly sensitive information often only requires simple password authentication, and does not take into account other contextual information (e.g., the user’s location) that might raise the risk of breach.
- **Poor overall identity governance.** Effective protection against improper access or use of information requires strong control over user identities, access, and information use. Most organizations have some controls in these areas, but do not have a unified and robust approach to truly protect their information assets.
- **Inadequate auditing and analytics.** Many companies have no way to continuously audit

Defending Against Insider Threats

access to help ensure that only properly authorized individuals are gaining access, and that their use of information complies with established policy. Even if they have auditing tools in place, the sheer volume of log data generated makes it very difficult for organizations to sift through the data and identify breaches or threats.

Cloud computing and virtualization and insider threats

In addition to the previously mentioned challenges, today's IT organization must also contend with new computing models and platforms like cloud computing and virtualization. Cloud computing and virtualization offer significant benefits to all organizations, but also introduce further security challenges.

With cloud computing, the notion of what constitutes an insider changes considerably. The insider is no longer just an employee inside the firewall, but also includes individuals at the service provider delivering cloud services to the organization. In addition, the cloud can be very opaque, giving you little or no real visibility into how and where that service is deployed or how it is controlled. The cloud service may very well consist of a "mashup" of many services from multiple vendors, physically hosted in separate data centers in different geographies. This decoupled model significantly impacts the customers' ability to implement their own controls.

Virtualization is an equally important computing trend that has broad implications for insider threats. Many organizations have made considerable investments in virtualization to take advantage of virtualization's numerous benefits. The challenge is that as critical servers are virtualized, tight controls are necessary to limit the entitlements of the privileged users accessing those virtual servers.

The good news is that while cloud computing and virtualization increase the complexity of the insider threat, the same solutions that exist to combat insider threats can be extended into the cloud or virtual environment to deliver the same layer of protection. And these same capabilities can be deployed by service providers and cloud providers to help secure their environments and mitigate the insider threat. However, organizations must remain vigilant in assessing the insider risk in virtual and cloud environments and also seek to partner with service providers that can deliver robust and secure cloud-based services.

Conclusions

The threat from insiders is real and growing. Organizations must sober up to the reality that the insider threat is no longer an abstract concept, but something that could happen at any time. But instead of adopting a bunker mentality and accepting the inevitability of such an insider attack, organizations should adopt a more aggressive stance towards combating the insider threat. A central part of this aggressive stance should be identity and access management (IAM). By deploying solutions like IAM and DIP, organizations can make progress defending against insiders.

Defending Against Insider Threats

Organizations that choose to adopt an aggressive posture based on IAM and DIP can realize real benefits. The most obvious benefit is the risk reduction that comes from being able to defend against insider attacks. By controlling user identities and access and information usage, CA Content-Aware IAM helps reduce the risk of an insider attack. The CA Content-Aware IAM solution also provides other advantages that help in the battle against insiders, including support for a wide range of computing platforms, proven scalability, and centralized management and reporting all of which are essential for not only providing a solution that can prevent insider attacks, but can also make the management of this risk efficient and simple to manage.

The insider threat can never be completely removed, but the capabilities described in this paper describe the building blocks upon which to base a successful insider threat prevention program. Organizations serious about combating the insider threat should deploy some or all of these capabilities, because doing so is an efficient and proven mechanism to keep insider attacks in check.