



The Security Division of EMC

White paper

Securing Insider Access to Enterprise Resources



Accelerate business by leveraging information and providing access to authorized users.

Today, the most valuable asset to a company is its data and information. Furthermore, the ability to leverage company data by making it available to authorized users while also securely protecting the information will accelerate business into the future. However, even the most comprehensive and advanced IT perimeter security technology cannot fully safeguard corporate networks against an often overlooked risk – the insider.

The need for technology to secure enterprise networks from external unauthorized access is well understood and absolutely necessary. Nevertheless, as a standalone solution, it falls short in today's world where many security breaches originate inside the enterprise. Organizations must secure access to critical company resources and assets from the inside in order to fully protect the confidentiality and integrity of sensitive information.

Contents

Defining the “Insider” Threat	page 1
The Source of Security Breaches	page 1
Key Drivers for Securing Critical Company Data	page 2
Secure Insider Access	page 3
Top Use Occasions: Protection Inside the Enterprise	page 4
Two-factor Authentication is Key	page 5
Summary	page 6

Defining the “Insider” Threat

As organizations continue to increase the number of applications on the network and provide more users with access to that information, there is even more reason to address the issue of the insider threat. While “users” historically consisted of internal employees (and perhaps a few employees with remote access), there are many “insiders”, or user segments, accessing the corporate network, which contributes to an increased cause for concern. Therefore, when thinking about security breaches inside the enterprise, it is important to note that we are not only talking about breaches caused by employees. An “insider” is defined as anyone with physical or logical access to corporate resources including contract workers, consultants, visitors, maintenance personnel and interns.

Real-life Insider Abuse Examples

September 14, 2007

Information about 6.3 million online trading customers including their names, addresses and email addresses, plus a variety of account activity information such as the number of trades they had conducted in the last six months, was stolen by what many speculate to be an insider.

September 4, 2007

An employee at a pharmaceutical company removed copies of confidential information from a computer system without the company’s knowledge or approval, publicly exposing the names, Social Security numbers, addresses, dates of birth, phone numbers, bank account numbers, credit card information, signatures and other personal information of nearly 34,000 employees.

July 11, 2007

An employee of a company contractor stole an undisclosed number of credit card details of company customers and attempted to sell them.

The risk of the insider threat is real. According to “The Global State of Information Security 2007” report, released by PricewaterhouseCoopers in conjunction with CIO and CSO, awareness of the insider threat has increased due to the implementation of security monitoring tools and systems over the past five years¹. Despite increased awareness and added security, 40 percent of respondents still could not determine how many incidents they had experienced. So, while IT executives are alert, many are still uncertain about the number of attacks occurring within their organization and the reasons for insider breaches. In order to begin solving the problem, we need to examine the root cause.

The Source of Security Breaches

When we refer to “insider attacks,” the first thing that usually comes to mind is security breaches within the enterprise performed with malicious intent (a disgruntled employee, for example). While malicious attacks do occur, they account for only a small percentage of security breaches by internal persons pursuing financial gain or personal satisfaction. Rather, the most common causes of security breaches inside the enterprise include:

Ignorance

Ignorance is a major contributor to the insider threat. Employees are often unaware of their company’s security policies and how to prevent a breach; therefore, they continue to perform high-risk activities. Such activities could include writing down passwords on a piece of paper or leaving their computer unlocked when they leave their work station for long periods of time.

Carelessness

Employees that are careless in handling sensitive information could unknowingly expose sensitive company data. Sharing personal password information with a colleague is an example of employee carelessness.

¹ “The Global State of Information Security 2007”, CIO, CSO and PricewaterhouseCoopers, 2007

In the survey, only 8% of respondents stated that all of their users were in compliance with company security policies.

“The Global State of Information Security 2007”
CIO, CSO and PricewaterhouseCoopers, 2007

Disregard for Security Policies

Some employees are aware of their company’s security policy; however, they simply disregard the provisions within it. In fact, according to “The Global State of Information Security 2007” survey, only 8% of respondents stated that all of their users were in compliance with company security policies.² An example of a disregard for security policy is failing to follow physical security practices – employees letting an unfamiliar person without an identification badge into the building.

Maliciousness

A small percentage of security breaches occurring from inside the enterprise are driven by network users pursuing financial gain or personal satisfaction. In a recent study conducted by leading business consulting firm Deloitte, survey results showed that only 2 percent of threats to information security were attributed to malicious intent.³

Key Drivers for Securing Critical Company Data

There are several key drivers for companies to secure their critical company data – both inside and outside. Many companies have already taken steps to minimize the risks associated with external access; however, few steps have been taken to lockdown access to the corporate network from users inside the building.

Rising Concern about the Insider Threat

The Deloitte study showed that 91 percent of senior information technology executives at many of the top 100 global financial services organizations expressed concern about the risks to security arising from within their organization.⁴ In another research study, the Ponemon Institute found that 78 percent of IT professionals surveyed claimed that their companies had suffered at least one unreported insider-related security breach.⁵

Increased concern. Unreported incidents. While there is clearly a high level of concern among IT executives, many apparently still fail to report breaches by insiders, perhaps because of the publicity that would likely have a negative effect on their corporate brand. Because many breaches from insiders go unreported, it is nearly impossible to measure the full extent of the ongoing problem; however, it does not diminish the need for security measures to be established to mitigate the insider threat.

High Cost of Security Breaches

Determining the actual cost of a security breach is not an exact science and nearly impossible to determine. Many factors must be accounted for including the type of information stolen, the amount of data breached, and actual financial losses, to name a few. However, there are several things that are incalculable – the negative effect on brand value or the loss of valuable intellectual property, for example.

Consider a recent online trading data breach where over 6 million customer records were put at risk. In the future, there may be dollar amounts assigned to such activities as legal proceedings and remuneration to customers. However, there is no way to measure the long-term damage to the brand – the number of customers and potential new customers lost, for example.

² Ibid.

³ “2007 Global Security Survey”, Deloitte Touche Tohmatsu, 2007

⁴ Ibid.

⁵ “National Survey of Managing Insider Threats”, Ponemon Institute, LLC, 2006

Proliferation of Passwords

Employees are required to memorize and use several different passwords to access the resources needed to perform their job. When the task becomes a burden, users may turn to unsafe password management practices, such as writing them down on a piece of paper or using the same two or three passwords consistently, in order to improve productivity. These unsafe password management practices can unknowingly cause the user to expose sensitive company resources. In addition, when employees have several passwords to memorize, they are likely to forget ones that they do not use frequently thereby requiring password resets and driving up help desk costs.

Growth of Compliance Regulations

There are several industry and government regulations that are driving the adoption of insider threat mitigation solutions such as Sarbanes-Oxley (SOX), HIPAA, GLBA, the European Union Data Protection Directive, Basel II Accord and Japan's Personal Information Protection Act (PIPA). For example, SOX requires companies to "provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the registrant's assets that could have a material effect on the financial statements." (The broad category of assets includes digital assets.) The European Union Data Protection Directive requires that "personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data."

A Continual Trust Model

RSA's Identity Assurance portfolio extends user authentication from a single security measure to a continual trust model that is the basis of how an identity is used and what it can do. Trusted identities managed by RSA bring confidence to everyday transactions and support new business models by providing secure access for employees, customers and partners while striking the right balance between risk, cost and convenience.

Secure Insider Access

Secure insider access is a core component of RSA's Identity Assurance portfolio. The solution utilizes two-factor authentication to validate the identity of users before they are granted access to corporate resources. The use of two-factor authentication assures the identity of users before granting access to high-value digital assets inside the enterprise, greatly reducing the risk of a security breach resulting from unauthorized access. A secure insider access strategy enables companies to:

Strengthen Security

Assuring identities and protecting high-value resources results in increased overall security of the company's most valuable asset – information.

Heighten Compliance

Tracking and reporting user behavior is a key component of complying with most regulations.

Reduce Costs

The use of two-factor authentication can reduce the number of calls to the help desk. At an average of \$58 a call including lost wages and productivity, two-factor authentication can greatly reduce help desk costs. More importantly, a secure insider access solution works to reduce or eliminate the overall costs associated with internal security breaches.

Simplify User Experience

Implementing strong authentication that provides a consistent user experience can eliminate user frustration caused by managing multiple passwords, thereby reducing the risk posed by unsafe password management practices.

Accelerate Business

Providing secure access to enterprise resources accelerates business by allowing users to seamlessly access critical company resources required to perform everyday job functions.

“Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.”

European Union Data Protection Directive

Top Use Occasions: Protection Inside the Enterprise

The key component of a secure insider access strategy is preventing unauthorized access to sensitive company resources. Securing network access with two-factor authentication positively validates the identity of users before granting access, thereby preventing unauthorized access. There are a number of instances where access is requested to critical information and organizations must ensure that the users requesting information are authorized to do so. Some of the most critical access points to secure inside the enterprise include:

Wireless Networks

The proliferation of wireless networks inside the enterprise provides “anywhere” access to the network, resulting in increased productivity in conference rooms and guest offices. However, wireless networks present an opportunity for unauthorized users to access the network. Therefore, securing wireless networks with two-factor authentication is critical to protecting sensitive network resources.

Web-enabled, High-value Business Applications

Certain employee roles require exclusive access to high-value business applications in order to perform their jobs. Such roles include IT, human resources and finance. The use of two-factor authentication to secure high-value business applications enables users to access information necessary to perform job functions, without exposing sensitive information to unauthorized users.

IT Infrastructure

Unauthorized access to the IT infrastructure (servers, routers, etc) has the potential to cause significant damage to the network, or result in downtime. The use of strong authentication for IT administrators ensures that only authorized users gain access to the network infrastructure to manage the network.

Enterprise SSO Deployments

Many organizations implement an enterprise single sign-on (ESSO) solution in order to address the challenge of password management for employees. ESSO provides access to all authorized password-protected applications through the use of a single password. Replacing the single password with two-factor authentication protects the “keys to the kingdom” and provides simple and secure access to applications.

Microsoft® Windows® Logon

A Windows password can be replaced with two-factor authentication to validate the identity of users before providing access to valuable corporate resources accessed through Windows-based desktops and networks.

Hard Disk Encryption

Hard disk encryption provides protection of confidential data stored on computers and networks. Two-factor authentication integrated with hard disk encryption verifies the user before the operating system starts and access to the computer is granted.

Network Access Control

Network access control solutions provide machine authentication and health status checks of machines before they are granted access to the network. Adding two-factor authentication for users enhances the solution by providing the ability to develop access control policies based on the identity of the user in addition to the health status of the machine.

Two-factor Authentication is Key

Two-factor authentication is a key component of a secure insider access strategy. Two-factor authentication is based on something you know (a password or PIN) and something you have (an authenticator)-providing a much more reliable method for authenticating users beyond basic passwords, which can easily be compromised.

The RSA Secure Insider Access solution provides a comprehensive approach to securing access inside the enterprise using two-factor authentication and offers two different types of strong authentication: one time passwords and digital certificates.

Each type of strong authentication provides different features for security, portability, and the ability to leverage the credential for additional security measures.

The RSA Secure Insider Access solution includes:

RSA SecurID® two-factor authentication is based on something you know (a PIN or password) and something you have (an authenticator). The authenticator generates a new one-time password code every 60 seconds, making it difficult for anyone other than the genuine user to input the correct token code at any given time. To access resources protected by the RSA SecurID system, users simply combine their secret personal identification number (PIN) with the token code that appears on their authenticator display at that given time. The result is a unique, one-time-use passcode that is used to positively identify, or authenticate, the user. If the code is validated by the RSA SecurID system, the user is granted access to the protected resource. If it is not recognized, the user will be denied access. RSA SecurID offers a wide array of one-time password authentication form factors – available in both hardware and software formats depending on business and employee needs.

RSA® Digital Certificates can be stored on a range of devices including smart cards, USB devices and desktops and secured with a PIN, providing two-factor authentication for users. In addition, RSA Digital Certificates can be leveraged for e-mail encryption and digital signatures, increasing the return on investment and providing additional layers of security inside the enterprise.

A key component of the RSA Digital Certificate solution is RSA® Certificate Manager, an Internet-based CA solution that provides the core functionality for issuing, managing and validating digital certificates, thereby allowing users to identify themselves and establish trusted relationships. It includes a secure web server and a powerful signing engine for digitally signing end-user certificates and system events; and an integrated data repository for storing certificates, system data, and certificate status information.

The RSA Digital Certificate solution can scale to more than 8 million users and is built on an open standards platform that is interoperable with more than 200 applications.

RSA® Card Manager is a credential management system, bringing centralized credential management to the Enterprise. Central management of multiple credentials including one-time passwords and digital certificates drives improved security and reduced costs inside the enterprise. The ability to centrally control the issuance, replacement and cancellation of multiple credentials reduces the security risks associated with managing access to corporate information in a rapidly changing business environment.

The ability to choose the credential the best meets the security, flexibility and leveragability requirements of the enterprise is an important part of the Secure Insider Access solution. Enterprise companies should evaluate their existing network structure and select the critical access points to secure along with the credential that works best for the needs of the users and the company.

91 percent of senior information technology executives expressed concern about the risks to security arising from within their organization.

“2007 Global Security Survey” Deloitte Touche Tohmatsu, 2007

Summary

There are many issues that companies face when trying to reduce the likelihood of insider security breaches. With the global nature of business today, the explosion of data and increasing numbers of users requiring access to network resources, control over network access is diluted. As organizations continue to expand their corporate networks and the number of people they provide access to inside the enterprise, the insider threat will only continue to grow. In order to address the risk posed by insiders, organizations must consider two-factor authentication to secure access points and protect their most critical asset – information.

About RSA

RSA, the Security Division of EMC, is the premier provider of security solutions for business acceleration, helping the world's leading organizations succeed by solving their most complex and sensitive security challenges. RSA's information-centric approach to security guards the integrity and confidentiality of information throughout its lifecycle – no matter where it moves, who accesses it or how it is used.

RSA offers industry-leading solutions in identity assurance & access control, data loss prevention & encryption, compliance & security information management and fraud protection. These solutions bring trust to millions of user identities, the transactions that they perform, and the data that is generated. For more information, please visit www.RSA.com and www.EMC.com.



RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

The Security Division of EMC

RSA, RSA Security and SecurID are registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. EMC is a registered trademark of EMC Corporation. All other products or services mentioned are trademarks of their respective owners. ©2007-2008 RSA Security Inc. All rights reserved.