WHITE PAPER | January 2015

I Have to Trust *Someone.* ...Don't I?

Dealing with insider threats to cyber-security

Russell Miller

Merritt Maxim

CA Technologies, Security Management

ca technologies

Table of Contents

Executive Summary

"When you're in positions of privileged access, like a systems administrator for these sort of intelligence community agencies, you're exposed to a lot more information on a broader scale than the average employee."

– Edward Snowden

Challenge

While many organizations focus their security efforts on their network border, it is the insider that perhaps poses the most risk to cyber-security. From executives to IT administrators to partners, many people have access to sensitive data that if publicly exposed, could have significant ramifications to an organization's business—or even its existence.

Cyber-security is usually thought of as a technical field, with highly-skilled defenders seeking to outwit attackers in a contest of intellect and will. While there is some truth to this characterization, it misses what is perhaps the most important aspect of security: the human element. People have a tendency to trust people they know, leading them to share passwords or other information that they shouldn't.

Trust is an essential element to operating any type of organization. People need access to sensitive information and critical systems for many reasons and a level of trust has to be associated with that access. Understanding and managing that trust is the most critical—and difficult—challenge of dealing with insider threats.

Opportunity

"Trust" does not mean giving employees unrestricted and unnecessary access to information. With the right security controls, organizations can significantly reduce their exposure to the risk of insider threats. The key is to find the right balance between employee enablement and control, while holding employees accountable for their actions. This requires a broad approach to allow an organization to carefully manage its identities, access and data, from identity management, to governance, privileged identity management and data protection.

Insider fraud is a common occurrence.

On average, organizations have had approximately 55 employee-related incidents of fraud in the past 12 months.[1]

– The Ponemon Institute

Benefits

Strong security controls not only reduce risk, but can enable information sharing in an organization. Access to highly-sensitive information is often highly-restricted due to the risk of that data being exposed. With the proper security controls, data can be shared with a larger group of people, who can then be more efficient and innovative.

"In today's world, the most valuable thing that anyone has is technology. The most important thing this country can do is protect its trade secrets."[3]

– U.S. District Judge Ruben Castillo

Section 1:

Challenge

Insiders can maliciously or unwittingly steal, erase, or expose sensitive data for a variety of reasons. At the same time, insiders must be given a certain level of access in order for a business to function or an organization to operate. It is critical to understand insider threats at multiple levels, from motivations to damaging examples to how the threat has evolved, in order to intelligently approach risk mitigation strategies.

Types of insider threats

Insider threats are not all the same. There are three types of insider threats, malicious insiders who deliberately steal information or cause damage, insiders who are unwittingly exploited by external parties, and insiders who are careless and make unintended mistakes:

- **Malicious insiders** are the least frequent, but have the potential to cause significant damage due to their insider access. Administrators with privileged identities are especially risky. According to the Ponemon Institute, "data breaches that result from malicious attacks are most costly."[2]
- **Exploited insiders** may be "tricked" by external parties into providing data or passwords they shouldn't.
- **Careless insiders** may simply press the wrong key and accidentally delete or modify critical information.

Insider threats may also come from privileged users (administrators) or regular users with access to sensitive data. Administrators often possess complete privileges to perform essentially any operation on many critical systems. People of all types often have accumulated more entitlements than they need for their current job role, leading to increased risk that is entirely preventable.

What's changed?

The stakes. As we become an increasingly information-based economy, intellectual property and trade secrets are more critical than ever to an organization's survival. The rise of "Big Data" analytics has compounded the problem. Businesses are now storing vast quantities of data in order to uncover patterns and insights that would have been impossible just a few years ago. While potentially a critical business differentiator, that data is in some cases highly-sensitive, containing information such as customers' personal information, credit card numbers, transactions, communications, and even locations. A security breach of a customer data store can result in broken privacy laws, class-action lawsuits, and reputational damage that can lead to loss of business.

The Computer Emergency Response Team (CERT) at Carnegie-Mellon University has defined a malicious insider as "a malicious insider threat to an organization is a current or former employee, contractor, or other 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."[4] 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.

Insider risk factors

All organizations face common challenges when attempting to reduce their risk of insider security breaches:

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 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.

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.

Inadequate auditing and analytics. Many companies have no way to continuously audit 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.

Audit log complexity. The 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.

Reactive response. Most current approaches to addressing insider threats are reactive, not predictive. While this may help immensely in forensic investigations, 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 even if not able to prevent insider attacks, may still identify "at-risk insiders" and then implement more detailed logging on those individuals in response.

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.

About 65 percent of employees who commit insider IP theft had already accepted positions with a competing company or started their own company at the time of the theft. About 20 percent were recruited by an outsider who targeted the data. More than half steal data within a month of leaving.

Behavioral Risk Indicators of Malicious Insider IP Theft: Misreading the Writing on the Wall,

– Eric D. Shaw, Ph.D., Harley V. Stock, Ph.D.

Why it's difficult: Risk reduction vs. business enablement

Trust is critical to the operation of any organization. In order for an organization to benefit from sensitive information, the right people and systems need to be able to access it, and overly-restrictive policies damage an organization's ability to be responsive, innovative, and even functional. At the same time, unnecessary trust leads to unnecessary risks. For example, the people who are often trusted the most have the ability to cause the most damage: those are an organization's privileged users. These administrators often possess the privileges to perform essentially any operation on critical systems and users often have accumulated more entitlements than they need for their current job role. Another unnecessary risk associated with privileged identities is the use of shared accounts. Multiple people with access to the same account leads to a lack of accountability.

Managing the human element is the most challenging aspect of managing insider threats. Many people feel the need to believe that their company trusts them and feel personally slighted at new controls that remove access to information they previously had access to. Furthermore, access is often thought of as a form of status—particularly with IT administrators—and attempts to reign-in access are often met with resistance.

Examples of insider security breaches

Many security breaches committed by insiders are never made public. Organizations would rather keep these breaches private to avoid the reputational hit and customer concerns about their security that may result. However, many highly-damaging insider breaches have been disclosed. Here are a few of the best-known:

Well-known insider security breaches

National Security Agency	San Francisco	Motorola
Edward Snowden, working for Booz Allen Hamilton as a contractor for the NSA, provided highly-classified documents to journalists on programs called "Prism" and "Boundless Informant." Snowden's information exposed details of the NSA's storage and processing of communications, including phone calls and emails.[5]	A disgruntled San Francisco employee locked the city out of its own FiberWAN network, which contained confidential documents including police records. Even worse, emails were inaccessible and payroll checks could not be issued. The city spent over one million dollars in an unsuccessful attempt to gain access to the network.[6]	Hanjuan Jin, a software engineer at Motorola for nine years, was caught by U.S. Customs officials boarding a plane to Beijing with $30,000 in cash, along with over 1,000 documents marked "confidential and proprietary information," representing $10-$15 million dollars in trade secrets. Jin was found guilty of stealing trade secrets in a U.S. Federal Court and sentenced to four years in prison.[7]

Section 2:

Opportunity

Organizations must confront the reality that insider attacks are both 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 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.

Finding the balance

Tools to manage identities, access and data can enable an organization to find the right balance between enablement—and the sharing of sensitive data—with the controls needed to reduce the risks of insider security breaches. Organizations can reduce the risk of all three types of insider threats (malicious, exploited, and careless) by enabling accountability, implementing least privilege access, and controlling sensitive data. Accountability will make malicious insiders think twice before acting, help to identify exploited insiders and make users more careful with their actions. Least privilege access will deny actions and limit the damage done by all types of insider attacks, including inadvertent but damaging actions. By controlling sensitive data directly, businesses can prevent it from being exported out of their network using tools such as USB drives or even email.

"Trust" does not mean giving employees unrestricted access to information that is not relevant to their jobs. Organizations do place a level of trust in any employee that accesses sensitive data or systems. Granting access beyond what is needed is an unnecessary risk that does not mean that an organization doesn't trust their employees. It is simply smart business.

To support new security controls, it is critical to establish a cultural norm around least-privilege access by applying controls in a standard manner across the organization. By doing so, individuals perceive data security as an organizational priority and not a lack of trust in a specific person. This reduces the negative feelings associated with a carefully controlled approach to data access.

An in-depth approach to mitigating insider threats

Today's security capabilities can reduce the damage of an insider security breach, identify a breach after-the-fact to enable an effective response, or even prevent a breach in the first place. The most critical capabilities include:

Privileged Identity Management

Privileged Identity Management lies at the heart of any insider threat cyber-defense. Privileged accounts have the access needed for a person to view and steal an organization's most sensitive information, or cause the most damage to critical IT systems. They are also typically shared, with multiple people having access to the same accounts and passwords, resulting in a lack of accountability.

Managing privileged identities requires a multi-pronged approach. In addition to managing shared accounts, additional controls enable accountability for insiders and can limit the damage done by an external attacker that gets access to an administrative account.

56%. "Percentage of execs who say their most serious fraud was due to a privileged user."[8]

– Pricewaterhouse Coopers

Key Capability	Need	Description	Benefit
Shared Account Password Management	Privileged accounts, such as 'root' on UNIX and 'Administrator' on Windows, are often shared, reducing accountability.	Control access to privileged, administrative accounts with password storage and automatic login capabilities. This is the starting point for most privileged identity management solutions.	Reduces the risk of unauthorized users gaining access to privileged accounts. Prevents password sharing.
Fine-Grained Access Controls	Access to privileged accounts is often "all or nothing"—an unnecessary security risk that leads to users with more privileges than they need.	Manage privileged user access after login. Control what access users have based on their individual identity, even when using a shared administrative account.	Reduces risk by providing administrators with only the minimum privileges they need to do their jobs.
User Activity Reporting/Video Session Recording	Track all user actions to determine what occurred and "who did what" in an investigation. Not all user activities are recorded and many applications do not produce logs, reducing accountability and making forensic investigations difficult.	Records all user actions, tracking all records by individual, even when a shared account is used. Ideally, track an IT system in a video-like format.	Makes it simple to find out "who did what" in a forensic investigation, using an understandable video instead of searching through incomprehensible log files. Enables accountability for users of IT systems. Creates logs for applications that do not natively produce logs.
Virtualization Security	Virtualization adds a new infrastructure layer that must be secured—the hypervisor.	Manage privileged users on VMware, while providing virtualization-aware automation of security controls on virtual machines.	Reduces the risks of virtualization, from VMware administrators to virtual machines.
UNIX Authentication Bridging	Managing user accounts and access on individual UNIX and Linux servers are an administrative burden that can lead to errors and oversights.	Authenticate users on UNIX and Linux systems to Microsoft Active Directory.	Consolidates authentication and account information in Active Directory, as opposed to managing UNIX credentials locally on each system. Reduces administrative overhead.

"If you don't implement proper controls for privileged users, you run the risk of service-level degradation, audit remediation costs, developers accessing (sensitive) production data, and disgruntled employees taking down your infrastructure or holding you hostage."[9]

– Forrester Research, Inc.

Identity management and governance

A significant cause of security breaches is inappropriate entitlements. This can be caused by incorrect initial access rights settings, accumulation of entitlements over time, or even improper access rights for a user that were intentionally set by a rogue collaborating administrator. Entitlement accumulation can result from a lack of maintenance when an employee changes positions and maintains all of his or her old access rights. While incorrect user entitlements primarily increase the risk of insider threats, outsiders can also gain access to those accounts or find unused accounts that make it easier to hide their activities. One frequent mistake many organizations make is not immediately de-provisioning their accounts and removing all access rights when terminating administrators.

A best practice solution is a comprehensive and continuous process to understand which users should have access to which resources, then validating that each user has the appropriate access entitlements on a regular basis. Identity Governance—segmented at a high level as Role Management and Identity Compliance—involves various identity-related processes including verifying and cleaning up existing user entitlements, building accurate role models and enacting policies and processes which help ensure appropriate assignment of privileges to users. Identity Governance solutions can deliver a variety of benefits including:

- Increased security by automating processes needed to help meet compliance audits and establishing cross-system identity security policies
- Reduced identity management costs by streamlining the steps involved in projects such as role discovery, privilege clean-up and certification
- Improved IAM time-to-value and adherence to policy by more quickly delivering a consistent, accurate role and security foundation

Data controls

The end goal of every cyber-attack is to steal sensitive information or cause damage, so having control over data is an essential component to a successful defense. Likewise, many insider security breaches are the result of an employee downloading valuable data intellectual property (such as source code). To protect sensitive data, an organization should protect and control data in four states:

1. **Data at-access.** Sensitive information attempting to be accessed by an individual in an inappropriate role.
2. **Data in-use.** Sensitive information handled on the local workstation or laptop.
3. **Data in-motion.** Sensitive information communicated over the network.
4. **Data at-rest.** Sensitive information stored in repositories such as databases, fileservers or collaboration systems.

To achieve this, organizations must define policies to enforce control if inappropriate access or usage of the data is detected. Once a policy violation occurs (such as attempting to access intellectual property, copying the information to a USB drive or attempting to email it) the solution should mitigate the compromise while generating an alert.

Information classification is at the heart of any data security initiative. Without understanding information in context, including what the information is and where it is located, it is impossible to implement a comprehensive data protection program. An organization must accurately discover and classify sensitive information based on its level of sensitivity to the organization. This includes intellectual property, but also personally identifiable information, private health information, and other non-public information.

Once information has been properly classified, policies have been defined, and controls have been deployed, an organization can then monitor and control the access and handling of all sensitive information. This includes user actions from simply attempting to access and read sensitive data, to copying to a removable device or printing, to emailing outside the network, to discovering data stored in a repository such as SharePoint.

"Only amateurs attack machines; professionals target people."[10]

– Bruce Schneier

Advanced authentication

While authentication methods usually aren't considered when discussing insider threats, they are very relevant in the event that an outsider exploits an insider into providing his or her credentials. Passwords don't provide adequate security for today's critical applications and information. When attackers authenticate to a system, there are often contextual factors that could, if recognized, raise a warning about the validity of the authentication. For example, if someone from Finance working in New York suddenly logs in from Russia, or if someone logs in from Rome, two hours after logging out in New York, it is clear that a fraudulent authentication is in progress.

Risk-based authentication solutions provide a risk score of each attempted authentication that can help determine whether an attempted breach might be in progress. In these cases, additional, "step-up authentication" methods could be required, the attempt could simply be rejected, or an alarm could be raised.

Virtualization security

The potential for damage from insider threats has recently increased with the quantity of sensitive data exploding and more powerful administration tools. The rise of virtualization, in particular, has given rise to new risks. First, there is a new class of administrators on the hypervisor that must be managed, monitored and controlled. Second, those hypervisor administrators can change, copy, or delete dozens of virtual machines with only a few clicks of the mouse, making theft and damage simpler, faster, and more damaging and difficult to detect than ever.

To overcome security challenges in a virtualized environment, organizations need to take a proactive, rather than reactive, approach to impending threats and oversights. A start is to apply the security fundamentals that are already embedded in a traditional infrastructure into the hypervisor layer.

These actions allow a solid security foundation to be established, but alone are unable to address all the dynamic changes that make virtual servers less secure than physical servers. The virtual infrastructure must be further secured by also implementing capabilities that are virtualization-specific. Virtualization-aware automation offers breakthrough capabilities to manage the risks associated with hypervisor security. Applied in conjunction with security fundamentals, it safeguards your virtual environment while supporting the fast-paced demands of your business.

Section 3: Benefits

Control to Enable

By using identity and data-based security controls, organizations both reduce their risk of insider breaches and improve their compliance programs. Automated and centrally managed capabilities help reduce costs while strengthening IT security controls. With robust auditing, compliance challenges become less daunting by enabling organizations to provide proof of controls and demonstrate to auditors the effective operation of established security controls.

Defending against insiders of any type is a fundamentally challenging problem. Information flow is critical to the functioning of a business. Restrictions can lead to operational issues or keep employees from having access to the information they need to be efficient or innovative.

Having the ***right*** controls, however, can enable an organization to share information with a wide variety of people. These controls allow an organization to operate with ***limited trust.*** No longer restricted to granting only "all or nothing" privileges, organizations can share specific information with people who would previously have been denied such access! Organizations that use controls in this way are making security a tool to enable the business.

Organizations should also keep in mind that by protecting themselves from insider threats, they are also protecting themselves from external attackers. Identities, including privileged identities, are often used by outside parties after the attacker has breached the network perimeter. By employing a solid core of internal security controls, an organization has built a solid foundation for preventing or reducing the damage of external attacks.

Section 4:

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, along with Data Loss Prevention.

The insider threat can never be completely removed, but identity-based controls are 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.

Section 5:

References

1 The Ponemon Institute, “The Risk of Insider Fraud: Second Annual Study.” February 2013

2 The Ponemon Institute, “The Risk of Insider Fraud: Second Annual Study.” February 2013

3 bigstory.ap.org/article/sentencing-set-corporate-espionage-suspect

4 cert.org/insider_threat

5 newyorker.com/online/blogs/closeread/2013/06/edward-snowden-the-nsa-leaker-comes-forward

6 slate.com/articles/technology/future_tense/2013/02/fiberwan_terry_childs_gavin_newsom_on_why_governments_should_outsource_technology.single

7 articles.chicagotribune.com/2012-08-31/business/ct-biz-0830-moto-theft--20120831_1_trade-secret-case-hanjuan-jin-trade-secrets

8 online.wsj.com/article/SB10001424052970203753704577255723326557672

9 Forrester Research Inc., “Assess Your Identity And Access Management Maturity.” September 26, 2012

10 schneier.com/crypto-gram-0010

Section 6:

About the Authors

Russell Miller has spent over six years in network security in various roles from ethical hacking to product marketing. He is currently a Director of Solutions Marketing at CA Technologies, focused on privileged identity management and virtualization security. Russell has a B.A. in Computer Science from Middlebury College and a M.B.A. from the MIT Sloan School of Management.

Merritt Maxim has 15 years of product management and product marketing experience in the information security industry, including stints at RSA Security, Netegrity and CA Technologies. In his current role at CA Technologies, Merritt handles product marketing for CA's identity management and cloud security initiatives. The co-author of "Wireless Security" Merritt blogs on a variety of IT security topics, and can be followed at www.twitter.com/merrittmaxim. Merritt received his BA cum laude from Colgate University and his MBA from the MIT Sloan School of Management and is the author of "Wireless Security."

Connect with CA Technologies at ca.com

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate – across mobile, private and public cloud, distributed and mainframe environments. Learn more at **ca.com**.

CS200_87340_0814