Anastasia Kwit
MIS 798 / Research Paper
March 19, 2012

The Growing Criticalities of Access Management and the Need to Embrace Ongoing Review

Overview: Access management plays a critical role in an organization of any size and requires consistent review and monitoring to ensure IT security within the user realm and prevent security breaches. A stronger partnership between IT and business units needs to be developed to ensure IT and business strategies align, and that IT can properly support business initiatives. As IT architectures migrate to cloud environments and more users connect with personal devices, security of infrastructure, data and applications will face new integration challenges making implementation and constant maintenance of access management even more imperative. IT staff should convert available data into usable metrics to measure the efficiencies of their access management functions and keep a watchful eye out for clues into possible security breaches or malicious behaviors.

****

Since the beginning of computing, access management has been an essential cornerstone of the IT world, but has frequently been inadequately handled – behavior which is becoming more noticeable within and detrimental to the corporate world as it moves from on-premise to public cloud architectures.

In the ITIL landscape, access management is defined as "the process of controlling access to data and information to ensure that authorised users have timely access while preventing access by unauthorised users."[1] Many people might assume access management only applies to applications which require usernames and passwords; however it also applies to file systems, equipment, hardware and physical facilities. The access management function also holds the responsibility of actively monitoring an environment for intrusion attempts and system breaches.

During the not too distant past, access management for data stores, applications and infrastructure could be managed by IT departments through relatively unsophisticated processes. In their earliest days, computer environments were accessible only through onsite visits, and the first line of defense was to prevent physical access to a building or room followed by username and password authentication on the system.

Yet, even in these "simpler" times, password misconduct was not unheard of. In fact, according to an article by Wired.com's Robert McMillan, the early CTSS computer-sharing system at MIT fell victim to the first data breach when researcher Alan Scherr (yes, of former IBM fame) once used a system loophole to print master password files. Not only did Scherr use these passwords to increase his allotted time on the system, but he shared the list with members of his cohort for their not quite white hat use as well.[2]

As network environments evolved and off-site access became available through thin clients and remote connections, access management moved beyond mere user authentication to include secured connection routes through firewalls, VPNs and other security appliances. Today, users often have expectations of corporate data and application access on any number of pieces of equipment whether owned by their company or personally. Similarly, the emergence and quick adoption of the public cloud platform has left gaps between security needs and actual security implementations as IT managers must adapt to working with platforms that are neither owned nor fully controllable by their organization.

Before any discussions about external security can become the focus, a foundation of internal controls and policies must be well-developed and enforced within an organization. So many

[1] (Brewster, Griffiths, Lawes, & Sansbury, 2010)
[2] (McMillan, 2012)

professionals and executive management teams prioritize work around preventing external intrusion that internal access regulation shifts disturbingly to the back burner. While human capital and its productivity are to be appreciated within a business organization, it also needs to be considered as a serious security threat.

In an interview with Forbes' contributor Ben Kerschberg, Nick Nikols, Vice President and GM of Identity, Security and Windows Management at Quest Software, reveals:

> *It is common to find incorrect resource access permission in almost all organizations....Typically there are very few measures to prevent misuse, because employees are already trusted. They have the key and are in the building and can get access to the data center and other assets inside the firewall. Few enterprises have tests to pass. This isn't sufficient anymore. You can't trust everyone on the inside, and that's where the majority of threats come from.*[3]

Recent news is filled with alarming stories of internal users accessing and sometimes stealing sensitive data and systems or performing unauthorized transactions causing severe damage to corporate reputations and even leading to massive financial and customer losses and criminal investigations. Some of the most brazen user abuse has been in the financial investment sector where rogue traders manipulate access in order to steal or misuse inordinate amounts of money. In the case of a UBS incident in 2011, a single rogue trader was able to leverage his system access to pass unauthorized trades over a course of three months causing a loss of $2.3 billion in private UBS investment funds.

> *"If you look at what this trader has allegedly done, working in different roles inside the organizations, moving from what appears to have been a back-office role into a trading role, it seems like the combination of having the knowledge of how those internal systems work as well as having retained the access is what enabled this," says Jason Garbis, vice president of marketing for identity player Aveksa, who wonders if this was a case of Adoboli getting more access to systems than he should have been afforded during the transition. "Often organizations don't have very sophisticated or very rigorous mover processes. When someone changes from role A to role B, they very often don't have a program in place to detect this and then automatically set up what is called an access review to have the new manager look at and validate the access to critical applications.*[4]

This insight shared by Ericka Chickowski in her article about the UBS scandal points out the importance of *ongoing* access management within organizations. Access management should have a middle life between new user setup and termination. At the very least, if access management is not tied to quarterly performance reviews, annual audits should occur to evaluate user access to systems and data and make proper adjustments.[5] Roles for long-term employees change frequently enough and while access to higher levels or different systems are often granted and adjustments made during these shifts, a review of access for systems that are no longer appropriate should be completed at the time of

[3] (Kerschberg, 2011)
[4] (Chickowski, UBS Rogue Trader Incident Stirs Access Management Speculation, 2011)
[5] (Larson, Mani, & Smith, 2012)

transition to prevent unauthorized access either by the promoted user or colleagues remaining behind who may have knowledge of the credentials.[6]

During these access reviews, though, should the onus of knowing what application, data and system access to grant business operations and administrative staff fall on the IS team? In his review of a recent Gartner IAM summit, Warwick Ashford interviewed Kevin Cunningham, president of identity governance software firm SailPoint, who suggests that defining access levels is a responsibility that should be shared by non-technical managers outside of IS.

> *"IT departments began to realise they are not necessarily in the best position to manage identity, and line-of-business managers probably have more insight." Businesses want to be sure employees have the appropriate access only for their current role, which requires mapping information from disparate systems to human resources data, he said. "Many companies recognise that the old way of doing IAM through IT is not cutting it, and that there is a need to include business."*[7]

This suggestion lends to a recommendation being echoed by many IT professionals to shift corporate attitudes towards encouraging IT/IS departments to more closely align with the overall business partners and business strategy. To enable information departments to provide proper access levels, perhaps some business definitions belonging to line managers and department heads need to be modified. Are business tasks and responsibilities properly divided within department roles? If checks and balances are not well-defined by the business unit, it is unrealistic to expect the IT group to implement bulletproof access measures.

David McNeely, director of product management for access management vendor Centrify states, "Many organizations are facing a Catch-22 when it comes to…the cloud. They get the biggest ROI by migrating to the cloud their business-critical apps that need to scale rapidly and on-demand. But these are precisely the applications that need the tightest security and access controls."[8]

And what about the not-so-rare scenarios where business units make decisions that impact IT without consulting or informing the department until post-implementation? Kerschberg paints a vivid picture:

> *Cloud computing highlights the potential for serious disconnects between management and IT. For example, what if the Vice President of a division implements a cloud-based Customer Relationship Management solution without IT's prior knowledge? What if senior management agrees based on cost concerns to shift to a software-as-a-service such as Google Apps for Business without IT's buy-in? These are not idle concerns, and they are "hypotheticals" experienced daily.*[9]

One simple step in the direction of IT and non-IT partnership comes from security consultant Michael Santarcangelo who controversially advocates dropping the term "users" in favor of building relationships with actual people.[10] Santarcangelo believes the term encourages disconnection from the

---

[6] (Chickowski, UBS Rogue Trader Incident Stirs Access Management Speculation, 2011)
[7] (Ashford, 2012)
[8] (Infosecurity, 2011)
[9] (Kerschberg, 2011)
[10] (Santarcangelo, 2011)

individuals being served and takes the burden of good security practices off of people and leaves an unrealistic reliance on technical measures to completely fulfill security needs.

This idea of partnering with non-IT staff to increase security performance success is also reflected in a post by DevCentral blogger Lori MacVittie who believes non-technical steps in security management are just as crucial as firewalls and passwords. Educating the users by holding forums or training to encourage secure business practice is often absent from the workplace. Behaviors some professionals take for granted are alien concepts to many users such as "don't share confidential information on social networks, be aware of corporate data and where it may be at rest and protect it with passwords and encryption if it's a personal device."[11]

How many times have we seen passwords written on neon post-it notes slapped front and center on a user's monitor? How often do viruses enter the system from non-work-related email attachments? What about the presence of inappropriate content copied to corporate servers from personal flash drives or auto-syncing mobile devices? IT departments need to take initiative in combating such behavior by informing people about the serious security implications that can result.

User education is becoming even more critical as more and more employees connect personal mobile devices and tablets to corporate networks or use them to access corporate resources remotely. IT departments are sometimes slow to manage these connections either because they are already bogged down with other priorities, do not have resources who can handle this type of access management, or are unaware of or just ignoring these situations until something blows up. These are tricky situations for sure, since personal devices are not controlled by the business entity. Measures should be taken internally either to prevent access by these types of devices without specific authentication and authorization or to implement controls and policies on precisely what can be accessed and stored on these devices. Further in her post, MacVittie proposes defining strategic points of control within an environment's data architecture and infrastructure. Once these are clear, "a combination of user, location, device and resource must be considered when determining whether access should or should not be allowed, and it is at those points within the architecture where resources and users meet that make the most operationally efficient points at which policies can be enforced."[12]

Similar controls will need to be considered for cloud hosting whether the cloud hosts only data, a selection of applications or entire infrastructures. Much like the challenge to manage corporate security on personal mobile devices that IT departments do not own or control, managing security in cloud environments presents similar roadblocks according to Mark Diodati, Research Vice President at Gartner.

> *When access control was on-premise, it was much easier to integrate the mechanism enterprise-wide so that companies could implement a consistent access rights policy…With cloud services, companies cannot install access control software at the cloud provider's location. "You don't actually control Google Apps but you need a way to harmonize it with what you have. That means having external connectivity to Google, being able to take out the information from Google, being able to make sense of it, and being able to make changes to it. It is a little more challenging because you don't own Google's system. You have to play by Google's rules when configuring the system", he noted.*[13]

[11] (MacVittie, 2011)
[12] (MacVittie, 2011)
[13] (Infosecurity, 2011)

The specific challenge with cloud platforms is the lack of control over resources and the cumbersome tasks of managing policies, roles and users among growing numbers of applications and platforms. Subhash Tantry, CEO of access management vendor FoxT, believes that "enterprises will continue to use multiple solutions for access management until the management burden on IT becomes unbearable. This will force adoption of centralized, automated platforms that can cover granular access control policy management and enforcement across diverse IT infrastructures."[14]

Instead of having the ability to implement existing integrated IAM tools which could be incompatible with cloud access models, IT personnel may need to turn to new access management tools such as Centrify which "enable organizations to control, secure, and audit access to cross-platform systems and applications using Active Directory."[15] Other offerings in the cloud and cross-platform marketplace include Novell's Identity Manager which is touted for its real-time response and ability to "provision and de-provision identities instantly to prevent internal threats;" RSA Access Manager, CA Identity Manager, and Oracle Identity Manager are additional options.[16]

"Small and medium businesses, in particular, are likely to adopt cloud-based identity management services, said IBM's Joe Anthony. 'I think you will see that continually increase, even getting up into the small enterprises in the next year or two,' he said."[17]

Thomas Shinder of Microsoft suggests the adoption of federated, claim-based services through Active Directory Federated Services (ADFS) and Windows Identity Foundation (WIF) to manage environments which "cross security domains, as when two enterprise-level organizations collaborate and enable cross-domain access to users from the partner security domain" or more simply mixed environments with assets hosted on the private cloud "and services accessed on the public cloud." Claims-based (token) security provides wide-reaching, cross-platform data to verify user identity and authentication through demographic information such as email address, full name and birth date.[18]

Perhaps comforted by a marketplace hosting reliable and emerging access management utilities, it is still vital for IS departments to keep eyes on access management after initial implementation, and this is where metrics can lend a hand.

Standard ITIL metrics for access management revolve specifically around security and include:

- The number of security-related Incidents per unit of time.
- The percentage of security-related Incidents that impacted services or users.
- The number of security audit issues and risks identified.
- The percentage of security audit issues and risks resolved.[19]

In her article, "Seven Crucial Identity and Access Management Metrics," Ericka Chickowski gathered best practice metrics from security experts:

1. *Time to provision, authorize or de-provision* – The time it takes to grant, alter or revoke access can indicate potential risks when there is a delay in the revocation of demoted, transferred or terminated employee credentials.

[14] (Ragan, 2011)
[15] (Infosecurity, 2011)
[16] (Information Security Magazine Online, 2011)
[17] (Ashford, 2012)
[18] (Shinder, 2011)
[19] (Brewster, Griffiths, Lawes, & Sansbury, 2010)

2. *Number of "Ghost Accounts"* – Monitoring inactive accounts and scheduling them for deactivation can tighten security and close doors where unattached accounts may provide unauthorized access to privileged systems and data.
3. *Password Hygiene Metrics* – Examining password behavior can highlight poor authentication practices and shine a light on 'policies that are too stringent or being ignored entirely,' says Jim Acquaviva, Vice President of Product Strategy for nCircle.
4. *Failed Log-Ins* – Tracking failed logins can indicate questionable or malicious activities such as external break-in attempts or internal password-guessing or may suggest that users are having a difficult time adhering to password policies which may be too complicated or change too frequently.
5. *Manual Password Resets* – If automated password reset procedures are not already in place, this metric can help justify an investment in such a project.
6. *Anomalous Access Incidents* – Monitoring unusual access behavior can point out and possibly curb malicious behavior.
7. *Service and Cost Metrics* – Metrics can also be defined to capture the cost-effectiveness of account management.[20]

By now, readers should have a strong sense of the critical role access management plays in an organization of any size. Access management requires consistent review and monitoring to ensure IT security within the user realm to prevent security breaches which are often connected to inappropriate access management. Furthermore, a stronger partnership between IT and business units needs to be developed to ensure IT and business strategies align and that IT can properly support business initiatives. Equally, non-IT management should understand and support IT policies and enforce them within their business units whenever possible. As IT architectures migrate to cloud environments and more users connect with personal devices, security of infrastructure, data and applications will face new integration challenges making implementation and constant maintenance of access management even more imperative. IT staff should convert available data into usable metrics to measure the efficiencies of their access management functions and keep a watchful eye out for clues into possible security breaches or malicious behaviors.

****

Now let us briefly peer into a local corporate environment to observe its current access management practices, recognizing strengths and recommending steps for improvement. The company, CJ Inc., has a current workforce of 120 employees. CJI's business model requires users to have 24/7 access to email and custom web applications. Users are provided with on-premise PCs, while management members are issued laptops. Outside of the office, non-management users are expected to use personal equipment to access the web applications and are rarely offered access to corporate file servers remotely. All employees are assigned corporate Blackberries for telephone and email communication outside of the office. Tablets are beginning to infiltrate the environment, and although some are provided by the company, support is extremely limited. Standard productivity applications (MS Office and Exchange) are installed locally or hosted on-premise while two custom web applications are hosted on a private cloud and three other custom web apps are hosted on the public cloud.

[20] (Chickowski, Seven Crucial Identity and Access Management Metrics, 2011)

- **Standard User Accounts** – Every employee at CJI is assigned a master username and password through Active Directory where access to file directories and two of the web apps are defined and controlled through group assignments. There are no rules or policies implemented about password strength or frequency of password changes. These are policies that should be defined and implemented immediately.

- **Active Directory** - The Active Directory needs a good scrub to eliminate user accounts for terminated employees and ghost accounts. IT can partner with the business unit managers to determine former employees whose accounts can be deleted. IT can also encourage quarterly performance reviews (which are not currently in practice) to justify regular review of user access levels and permissions.

- **Web Application User Accounts** – Employees who need access to the non-AD-connected web applications are assigned separate credentials within those systems. However, previous IT staff in charge of issuing these credentials set up passwords that exactly matched the usernames. All of these accounts should be immediately reset with secure passwords. The master account file should also be scrubbed as maintenance for terminated employees only began nine months ago and the applications have been online for 3 years or more.

- **Administrator Credentials** – Administrator passwords for servers, applications, office equipment and other secured network devices are not routinely changed and a current master list is accessible to almost the entire IT staff. All passwords should be changed immediately and at least annually if not semi-annually. Access to the master password list should be restricted and adjusted after IT management more clearly defines which staff members hold roles that require access to the file. If necessary, the password file should be separated into several access-level versions. Staff members who need passwords to some systems do not need passwords to all of the systems. Proper credentials behavior and policies should be enforced and practiced from management down through the ranks.

- **Shared file directory** – All users have access to a main shared file directory, however the Read-Write-Modify-Delete policies are not consistently applied. Some users have inappropriate permissions leading to frequent file deletions and modifications which require backup recovery. A review of the policies and consistent permission application should be a priority project.

- **Restricted shared file directories** – Staff of specific departments (marketing, compliance and accounting) have access to restricted shared file directories. This access is generally well-managed although the AD scrub will likely reveal users who have transferred departments and should have adjusted access.

- **User PCs** – 75% of user PCs have been imaged and have consistent local user permissions. However, some IT staff have altered local access for users either to perform maintenance on their machines (without reverting the access level) or because the users asked them for increased permissions on their machine. IT staff should be disciplined for these unauthorized access changes and an immediate audit of all user PC access levels should be performed. The remaining 25% of user PCs should be upgraded to imaged machines for consistency in OS platforms and application installations and better security monitoring.

- **User Laptops** – Laptops are configured to provide remote access to the corporate systems. However, if a machine is lost, stolen or the owner is terminated, there are no protocols or protections on the machine to prevent data theft. Encryption standards and tracking features should be implemented to help protect the company from such security threats.

- **Personal PCs & Laptops** – Employees can access the web applications and webmail from personal PCs which is acceptable. File and client-based access to email systems need special configuration for access on non-domain machines – information which is not openly available to the staff. However, against policy, users frequently copy corporate files to flash drives and take those drives outside of the office. The policy should be reviewed and redefined with the business managers as it seems to conflict with the business needs. If there is justification for users to take files off-premise, they should be trained on proper protection and handling of those files.

- **Corporate-Issue Blackberry Devices** – Corporate-provided devices are currently managed through the Blackberry Enterprise Server (BES) although existing personnel could benefit from training on features of the application to implement additional security policies on the devices. Devices are easily wiped through BES upon employee termination.

- **Non-Blackberry Mobile Devices** – There are currently no policies or restrictions in place for non-corporate issued non-Blackberry devices. In fact, there is no formal list or way to discern the users who have connected iPhones or Android devices on their own. Remote email access should be restricted or policies defined to control these unknown connections. If the business decides to support a BYOD environment, users should need to interface with the IT staff for proper setup and an MDM program should be implemented.

- **Facilities Access** – The executive team has created a false sense of security with the installation of video cameras inside the on-premise server room, IDF closets and supply rooms. IT management should meet with execs to explain the ineffectiveness of these cameras and the actual security measures that are in place or need to be in place to properly protect the equipment, supplies and hardware inventory. Currently all sensitive rooms are secured by keycard access, although IT staff has given inappropriate access to non-IT personnel. This needs to be addressed and remedied immediately.

****

Bibliography

Amazon Web Services. (2011, August 4). *AWS Identity and Access Management - Now with Identity Federation*. Retrieved from Amazon Web Services Blog: http://aws.typepad.com/aws/2011/08/aws-identity-and-access-management-now-with-identity-federation.html

Ashford, W. (2012, March 15). *Gartner IAM Summit: Identity and access management in flux but progressing*. Retrieved from ComputerWeekly: http://www.computerweekly.com/news/2240146850/Analysis-IAM-In-a-state-of-flux-what-progress

Brewster, E., Griffiths, R., Lawes, A., & Sansbury, J. (2010). *IT Service Management: A Guide for ITIL V3 Foundation Exam Candidates.* BCS.

Chickowski, E. (2011, September 1). *Seven Crucial Identity and Access Management Metrics*. Retrieved from Dark Reading: http://www.darkreading.com/authentication/167901072/security/news/231600619/seven-crucial-identity-and-access-management-metrics.html?pgno=1

Chickowski, E. (2011, September 19). *UBS Rogue Trader Incident Stirs Access Management Speculation*. Retrieved from Dark Reading: http://www.darkreading.com/authentication/167901072/security/news/231601703/ubs-rogue-trader-incident-stirs-access-management-speculation.html

Cloud Security Alliance. (2010, April). *Domain 12: Guidance for Identity & Access Management V2.1.* Retrieved from Cloud Security Alliance: https://cloudsecurityalliance.org/guidance/csaguide-dom12-v2.10.pdf

Information Security Magazine Online. (2011). *Best Identity and Access Management Products 2011*. Retrieved from Search Security: http://searchsecurity.techtarget.com/guide/Best-Identity-and-Access-Management-Products-2011

Infosecurity. (2011, May 23). *Cloud, mobile devices complicate identity and access management, says analyst*. Retrieved from Infosecurity: http://www.infosecurity-magazine.com/view/18109/cloud-mobile-devices-complicate-identity-and-access-management-says-analyst/

Kerschberg, B. (2011, 12 7). *Data Security and Identity Access Management*. Retrieved from Forbes.com: http://www.forbes.com/sites/benkerschberg/2011/12/07/data-security-and-identity-access-management/

Larson, I., Mani, R., & Smith, M. (2012, January-March). IT Service Management class lectures. *MIS 798* .

MacVittie, L. (2011, August 8). *Strategic Trifecta: Access Management*. Retrieved from F5 | DevCentral: https://devcentral.f5.com/weblogs/macvittie/archive/2011/08/08/strategic-trifecta-access-management.aspx

McMillan, R. (2012, February). *The world's first computer password? It was useless, too.* Retrieved from ars technica: http://arstechnica.com/tech-policy/news/2012/01/the-worlds-first-computer-password-it-was-useless-too.ars

Oracle. (2012). *Identity Management*. Retrieved from Oracle.com: http://www.oracle.com/us/products/middleware/identity-management/overview/index.html

Ragan, S. (2011, December 8). *2012 Predictions: Compliance and Access Management*. Retrieved from The Tech Herald: http://www.thetechherald.com/articles/2012-Predictions-Compliance-and-Access-Management

Santarcangelo, M. (2011, July 12). *Why dropping the label of "users" improves how we practice security.* Retrieved from The Security Catalyst: http://www.securitycatalyst.com/2011/07/why-dropping-the-label-of-users-improves-how-we-practice-security/

Shinder, T. W. (2011, July 14). *Identity and Access Management in the Cloud*. Retrieved from Microsoft TechNet: http://social.technet.microsoft.com/wiki/contents/articles/3798.identity-and-access-management-in-the-cloud.aspx