
# Risky Business

*Insights into Information Risk*

## Dear Friends,

Welcome to the first edition of Aujas' **"Risky Business"** eBook. Over the last three years we have published many key articles covering best practices, happenings in the industry, critical items to watch for in the Information Risk management domain.

Our objective always has been to inform and create awareness on the critical aspects of information security and risk management.

Over the last 35 editions we have covered a lot of ground. We have created this eBook which is a compilation of some of our best articles we have published. We hope this is an exciting addition collection to your digital library.

And we promise to publish a "Risky Business" eBook every year which will cover all the important articles. We hope you like this.

If you have any thoughts or suggestions, we would be keen to hear you. Please write to me on karl.kispert@aujas.com

Thank you,


## Karl Kispert

Vice President
Sales & Business Development
North America

## Table of Contents

# *Data Protection*

Data protection is gaining importance and becoming one of the most serious concerns amongst the CIO and CISO community nowadays. Many aspects of data protection are discussed, insider threat v/s other threats, should we buy DLP or DRM, how can we protect against new technologies like mobile, social networks and cloud.

But there is a lot of noise, opinions on what needs to be done and views on how to get it done. This section on "**Data Protection**" includes a few articles which look at what you need to consider when you are embarking on an **Enterprise Data Protection** program. We hope these articles help address a few queries and assist you in defining a roadmap for Data protection for your organization.

# *Data-Breach Risk is not just from Insider Threats*

Over the last few years, many organizations have focused their data protection efforts mainly on the "Insider Threat" – the employee or temp with access, who decides to misuse or abuse those privileges. While this should be addressed; it is possible that some of us may have lost sight of what may be happening on the outside.

The question to consider is: "What about the critical data assets that businesses willingly send out to external organizations?" Delivering data to external parties is, after all, a necessary part of doing business. A bank, for instance, must share information with auditors, regulators, suppliers, vendors, and partners.

Sharing data is quite a risky activity, with an elevated probability of data loss, and can potentially have a huge negative impact on a firm's reputation when not monitored properly. Here's what you should consider when you share data outside your company:

## *Threats*

What or who is placing the data at risk? As your data flows externally from your firm's environment, it is subject to many threats ranging from man-in-the-middle attacks while in transit to social engineering hacks while stored at the 3rd party's network.

## *Risks*

The threats mentioned above may lead to serious risks to a firm's critical data assets. One is the obvious loss or breach of confidentiality or data. If your firm does not have proper data transmission controls, such as TLS, SSL or sFTP, the man-in-the- middle threat can materialize in data loss.

Such loss may then impact the organization through revenue loss, negative reputation, remediation cost, customer notification expenses, and loss of client trust.

## *Security Controls*

The set of controls for countering threats and mitigating risks are not only those pertaining to electronic data protection, such as software/hardware encryption, but beyond the electronic realm as well.

Think beyond technology – to Social, Governance, Operational and Process controls that protect against the Social Engineering hacks and also ensure that other controls are in place, such as a strong Password Policy, User-Access/Entitlements processes and Data- Security Awareness activities.

The bottom line is that once your firm's data leaves its own environment, most of your internal controls no longer apply. Your firm's data is now sitting on a third party's infrastructure, and is therefore dependent on their data security controls and processes. This is not just about whether the data is being encrypted in transit to the third party, but very much about how that data is safeguarded all through its lifecycle. Here are some relevant questions to ask:

a) Do you have the proper Confidentiality or Non-Disclosure agreements being executed with the third party receiving the data from your firm?
b) Who and how many people will have access to your data while it is at a third party?
c) Do you know the third party's protocols to give only the limited and necessary group of people in their environment access to your data? What about the access rights to people outside their organization (such as their partners or vendors)?
d) How are the servers and firewalls at the third party configured to adequately protect your data while in their environment?
e) Does the party receiving the data have the technology and processes in place to respond to and sufficiently investigate a data-loss incident?

These are only few of the many questions to ask before sharing sensitive information. You also must take into account various perspectives including technological, operational and process controls. As an example, take the real-life case of a bank business manager who decided one day to send the bank's tax data to its audit firm via plaintext email, instead of the approved sFTP or PGP encrypted email transmissions.

The email was intercepted at the auditor's ISP mail server. A rogue administrator at the ISP saw the email with critical valuable data and used it to tap into the bank's equity funds to steal $1.2 million.

As per the Open Security Foundation's DataLossDB (http://datalossdb. org/statistics) data loss statistics for YTD 2011:

*"…a trend that indicates data loss incidents involving third parties, on an average, result in a greater number of records lost than incidents that do not involve third parties. This may be as a result of the type of data handled by third parties, the process of transferring the data between organizations, or other hypothesis, mostly all speculative as little data exists to establish one cause as dominant. The trend is, however, concerning."*

In the end it is almost certain that the riskiest environment for data is one that is not controlled by the enterprise owning that data. Though an insider with access and intent can cause havoc with data on the inside, the enterprise should be able to implement the proper technical, process and operational/people controls to safeguard its own data.

It is when the data leaves that environment that we are truly no longer in complete control, which is when the proper audits, interrogations and testing will come in use OR will become useful.

# *Data Protection and Controls – Does Format Really Matter?*


No one will argue that the most valuable asset of any enterprise, regardless of industry (military, finance, healthcare etc) is it's Data. Whether data includes an investment strategy/portfolio, personal identity, or national security, it must be safeguarded and controlled.

We are all familiar with the data lifecycle and related security controls, including storage transfer encryption and effective destruction. But do we also consider the format of the data? Data lives in many forms outside the regular electronic email, Internet, PC, server or mainframe types that we normally work with. Unfortunately, some of our biggest vulnerabilities also live in many other forms.

Printed paper is not the least of those forms. Scribbled notes, copied material, casual conversations on an elevator, voicemails or even a fellow passenger's laptop (with a curious snooper peering over) are other forms of sensitive data. The main issue here is that most of us may not view these as "data types." The truth is that they can cause the same amount of harm as a DVD, USB or PC packed with information, and can just as easily land you on the front page. Let us take a look at an unfortunate use-case to bring this into context.

Henry S., a database administrator, was working over the weekend to complete a presentation to his board of directors. His area of focus was his firm's strategy on the proprietary development of database-software that would revolutionize the storage and sharing of information with clients. Henry's developments were ahead of all others in the enterprise and possibly in the industry. What got overlooked was how valuable the referred information was to the firm's competitors.

It was late Sunday night and Henry had finished and saved his presentation. Now he just had to print it. At about 11:30 that evening he found himself printing 20 color copies of his "master presentation" at the neighborhood copier. He felt the data he was bringing with him was safe since he had it on an encrypted USB drive. However, at one point Henry's copying spree went awry – after about 10 copies the machine began spitting out green paint. Henry did not panic – he knew there was plenty of time and his current set of copies were safe.

After getting assistance and finishing the job on another machine, he found himself in the middle of a chaotic frenzy of paper thrown crazily all around. He was able to get things cleared up, but he had forgotten about the 5 copies he had left behind in the malfunctioning printer. Though a good multitasking person, Henry was exhausted, although buoyed up with the thought of the next day's presentation and the effects it would have on his career and department. All he could think about was getting the deck right and being well prepared for the audience.

He got home with all the paperwork in his backpack and went to bed. The next day at the presentation all went well, the board loved it and Henry was on top of the world. There had been a moment of disquiet, though, when he found that there weren't enough hard copies to go round. That was surprising – he was sure he had made enough. Everything had gone well, except for those 5 mysteriously missing copies of the presentation.

What then seemed to be a small loss, landed Henry and his firm on the front page of the paper within next few days. The headline read "Leading Financial Firm's Innovative Software Idea up for Grabs at Local Print Shop" – not quite the fabulous outcome he had hoped for. It turned out that whoever had gotten hold of the lost copies managed to re-engineer the software and get it to market.

To make things worse, the data-loss incident was widely publicized; the fall- out including Henry's suspension and investigation, a full 10 point drop in his firm's stock price and a long-term negative reputational impact for his firm.

Data in any format is an extremely critical asset and a liability when not controlled or secured properly. The effect of negligence over that asset can be detrimental to a career, to an innovative idea and possibly an entire franchise. Proper due diligence and controls for the entire lifecycle of the data; is necessary, be it encryption while in storage or transit for electronic material, or locks/safes for storage and shredding for destruction of hardcopy material.

Had Henry only given a little more thought to data security, then reputations and careers may have been saved (and more likely grown astoundingly). Instead everyone had to run for cover, hope to avoid getting hit by the shattering fallout, and struggle to keep their shirts on their backs.

# Data Governance – What We Need To Think About


These are some outcomes that you may want to consider while discussing Data Governance with your team:

1. Disparate sources of data across the organization's applications, produce incomplete and incorrect production data used in key decision making processes for capital investment. (Accuracy)
2. Trading ledger for risk management review is typically delayed because of multiple data feeds, the availability of which is impeded by network speed due to file size in two custom applications. (Availability)
3. Inability to solve data quality issues in the sales division because data is spread across multiple systems and owners, resulting in a blame game. (Agility)
4. Customer service representatives are not presented with a single view of a customer account, and have to use multiple programs to achieve unified profile presentation, requiring more time to solve issues, and increased call center costs. (Access)

## Analyze

- Perform data governance readiness assessment
- Define guiding principles
- Identify decision making bodies

## Design

- Determine focus of data governance program (security/privacy, data quality, architecture, etc.)
- Design data governance program (standards, policies, strategy)
- Determine cross - functional teams and data stewards
- Define decision areas and decision rights

## Transform

- Conduct employee training and awareness
- Enact data governance program
- Deploy data governance mechanisms and tools

## Sustain

- Monitor and adjust key performance metrics
- Ensure accountability and ownership through periodic review.

# *Wikileaks Fallout: DLP Helps but does not Solve, Analysts say*

*by George V. Hulme*


In the aftermath of the Wikileaks fiasco, enterprises are wondering what the breach of so many sensitive documents means, and if such an event could ever happen to them. One of the technologies the vendors and solution providers are feverishly pushing as the answer is Data Leak Prevention (DLP) technology.

According to IDC, while sensitive information leaks were seen as the second greatest threat to enterprise security, only 31.4 percent of the organizations had adopted DLP. At December 2009 a study showed that only 14.5 percent organizations had plans to purchase DLP. Since the Operation Aurora attacks and the more recent Wikileaks phenomenon, it is evident that many enterprises are today looking far more closely at DLP than ever before.

DLP is widely marketed as a way to stop confidential information from escaping out the door using notebooks, smart phones, iPods, portable storage and other devices. Or, as US Army intelligence analyst Private First Class Bradley Manning is alleged to have done: copy and walk away with reportedly 250,000 files designated (at the least) as classified — on a writable CD labeled as Lady Gaga music — from the Secret Internet Protocol Router Network (SIPRNet). SIPRNet is run by the US Department of Defense and the U.S. Department of State.

Would strong DLP protection have prevented that leak? Analysts are doubtful. DLP technology is very good at protecting specific types of information, but not protecting all of the information generated and managed by an organization. “In this case, the content taken appears to have been a mass amount of information that Manning had legitimate access to,” says Rich Mogull, founder and analyst at the research firm Securosis. “DLP is not good at stopping this sort of incident, where a broad amount of data is taken.”

Experts also agreed that while DLP has its place in the enterprise, it cannot provide definitive protection against similar attacks from trusted insiders. “There is no 100 percent solution to stop a motivated insider from stealing information,” says Mike Rothman, president and analyst at Securosis.

It is useful to pause and define what we mean by DLP. According to Mogull, DLP, at a minimum, identifies, monitors and protects data in motion, at rest and in use through deep content analysis. The tools identify the content, monitor its usage and builds defenses around it. There is also an emerging class of DLP that I call DLP Lite. These are single channel solutions that only look at either the end point, or the network,” he says.

For the most part, experts agree, whether considering full-blown DLP or DLP Lite, the technology excels at stopping specific kinds of data from leaking from where it should not – credit card data, engineering plans and details, health care forms. “For enterprises, compared to a government situation like Manning’s case, you can certainly do more to protect the data,” says Mogull.

But, experts caution, DLP cannot prevent many types of attacks on data “There is a rumor that WikiLeaks has a trove of information on one of the major US banks. While we are not sure what type of information it is, or how it is stored, if that information is reams of e-mails with free flowing conversations, DLP is not necessarily going to pick up on and stop that kind of breach,” Mogull explains.

That is why it remains important that enterprises, in their own efforts to protect data leaks, not place too large an emphasis on DLP technology, and that DLP be used as an additional layer of defense to supplement other important defenses such as access control, encryption, segmentation, and security event monitoring, among others. Most importantly, enterprises must understand what information it is that they want to most protect, and how that information normally flows throughout their organization.

“They need to understand the context of the data they use and want to protect – why and how it traverses their network – as part of the normal course of using that data,” says Nick Selby, managing director at security consultancy Trident Risk Management. “For DLP to work in the limited way it is intended, organizations must know what normal looks like before they have any hope at stopping abnormal activity.”

# *Effective Data Protection requires more than Technology*

Many companies are finding that despite their technology investments, effective data protection remains elusive. Data protection technology has become as commonplace as anti-malware technologies and most organizations implement it as a standard desktop endpoint and gateway security. The technology works by using a combination of document 'fingerprinting, key words, and policies defined around what is allowed and what is not.

The technology has matured to support endpoints and email data leakage risks as well as social networking risks. However, even with a mature technology and rigorous implementation, organizations often find their data protection ineffective. IT departments are able to quickly implement a data protection technology, but struggle with effectiveness.

They are unable to bridge the gap between implementation and effectiveness, and the result is a large numbers of data leakage 'incidents,' which usually turn out to be false positives. In many cases, organizations end up operating DLP tools in 'audit only' mode which completely defeats the tools' purpose. This gap is usually due to the approach taken to data protection and not to the organization itself.

Most organizations identify data protection as a risk and the IT/IS department then chooses a vendor for implementation. The vendor usually 'scans' the file stores for 'important' files and policies are created to safeguard those files deemed important. While this approach seems simple enough, it is the root of the problem. IT organizations are basing policies on their own interpretation, rather than on what is important or appropriate for the business.

Data, even if critical, may need to be exchanged with outsiders for valid business reasons. The challenge is to establish policies that allow the business to operate seamlessly while stemming the data leakage. Another challenge is to build an ecosystem that supports this on an ongoing basis. The solution ideally integrates technology, process and a governance framework.

The first step is data classification policy that clearly establishes how to classify data within the organization; the users should be made aware of how the classification policy is applied. Next, the data flow within the business processes should be understood to identify the type and nature of data, its classification and authorized data movement of 'important' data across organizational boundaries.

Also, the important files, templates and data base structures that were identified during this exercise should be 'fingerprinted.' The policies should then be configured and applied, based on the authorized movement of data.

Taking these steps will help improve the data protection technology effectiveness because it incorporates business rules for data. However, it still is a point-in-time exercise that does not address the fluid business data environment. For sustained data protection, a governance process is required. One approach is to integrate with the data governance framework if one exists within the organization. If a data governance framework does not exist, a similar structure should be created. An additional benefit of this approach is the close integration with data governance when such a framework is actually created.

At a high level, the governance function should be responsible for both the strategic and operational management of data protection. At a strategic level, the function should study how data flows and is managed and its impact on the data protection technology employed. At an operational level, the function should examine how data protection incidents are managed, how false positives may be reduced, and how the user awareness on classification and protection can be improved.

Many organizations also employ active data protection through the use of data/digital/information rights management tools which require users to 'protect' based on allowed rights, time limits and expiry dates. Though the above approach remains the same for these technologies too, organizations should spend more efforts on user awareness as their cooperation defines the success or failure of the technology.

Though data protection technologies have changed the data confidentiality playing field completely, effective data protection cannot be achieved by technology alone. It requires a focused lifecycle management approach for it to be most effective and sustainable.

# *Software, Application and Cloud Security*

Web based applications are making life very convenient for users, be it Internet banking, mobile banking, electronic bill payment or any of the varied applications you use daily on the internet. But is Security a prime concern for the application? Software applications are a high-value target for cyber crime and today most of the vulnerabilities are seen at the application layer.

Cloud, though it provides significant business benefits, it has its own risks. Authentication, access rights, Data integrity, Governance control, communication, service integration etc. are many aspects that need to be taken into consideration.

This section on "**Software and Cloud Security"** throws light on some of the trends in this space and some tips on what needs to done.

# The Business Case for Secure Development Lifecycle


Software is integral to the business operations of most organizations. Unfortunately, the increasingly indispensable nature of software-based systems has also made them high-value targets for cyber crime. Today, most of vulnerabilities targeted by cyber criminals are at the applications level rather than at the operating system or network levels. The cost involved in fixing these vulnerabilities is very high due to the related high costs of:

- Incident response
- Customer compensation
- Penalties for compliance violations
- Short-term fixes

## Remedying the problem

When a cyber attack is successful, fixing vulnerabilities can grow even more costly. Although recognition of the importance of secure systems is growing, software security must still compete for a place in an increasingly tight enterprise budget. However, a well-optimized security program can reduce the overall cost of developing an application and the business process it enables. The program can integrate security at various layers to mitigate risks that the company or software can face.

One proven and time-tested model is to incorporate security into every stage of the software development lifecycle. The Microsoft Security Development Lifecycle (SDL) is one such comprehensive process that offers an industry-leading software security methodology. The Microsoft SDL embeds security and privacy throughout the software development process.

The SDL delivers real cost savings in the following ways:

- When software development processes include security practices early in the process, the cost to fix vulnerabilities can decrease dramatically.
- A structured approach to security makes the process more predictable, significantly improves its efficiency, and allows the security team to deploy its resources in a heavily leveraged, top- down manner.
- It is cheaper to plan early and have a security requirement than perform a final verification.
- A combination of high-level analysis, low-level review, metrics-based risk management and tools can provide an optimal and measureable ROI.

By following a defined process like SDL, vulnerabilities are more easily found and fixed prior to application deployment. This helps reduce the total cost of software development.

Improving the security of a system makes it more reliable and less expensive to operate in multiple ways. While software security efforts require some resource commitment, a significant ROI can often be achieved with a small initial expense. Careful use of metrics allows the tracking of the effects of the investment, and those same metrics allow long-term improvement of security ROI and overall effectiveness.

Understanding software security problems is a foundational part of building better software. A recent survey conducted by Forrester Consulting noted that none of the company executives who responded selected “lack of time to perform security tasks” as a challenge to implementing a secure development program. Rather, they cited “lack of security expertise”… as a top challenge. So it is essential to know what talent is available in-house and where to look for expert advice.

# Mobile Security with J2ME

With the large number of financial applications that are available for Java-enabled devices, security is of paramount importance. Java 2 Micro-Edition Connected Limited Device Configuration (J2ME CLDC) is the platform of choice when it comes to running mobile applications on resource-constrained devices (cell phones, set-top boxes, etc.). The large deployment of this platform makes it a target for security attacks. The intent of this article is to provide some insight into J2ME security and the common mistakes that occur while developing such applications.

J2ME has fewer features than Java and has a smaller and efficient Java engine designed for small devices. We can divide the security of J2ME into three categories:

- Compile/Runtime Security
- Database
- User awareness

## Compile/Runtime Security

Java compiler and runtime environment through the provision of non-customizable classloaders, pre-verified midlets, protection domain policy and limited/no access to native/reflection API ensures the safety of the mobile devices.

One of the key improvements over the last few years in MIDP is to allow only the trusted application to call the protected API. All trusted API's must be signed. The trusted store in the mobile phone is usually populated with certificates of the manufacturer's choice and not all known CA's root certificates are part of the store. The J2ME permission class cannot be inherited to customize the need. Also the permissions are not really atomic to allow finer control. Once permission is obtained by the application from the user the application is allowed to use the resource in whatever way necessary.

## Database Security

One of the most ignored parts of the J2ME is the RMS database. The database is a simple byte-level file that stores the contents on the local phone. The security of this file is left to the manufacturers and the application developers. Most of the times Application developers are under the belief that the RMS database file is safe to use and is well protected. This is not the case.

A simple way to check is to install the application on a memory card and later on mount the memory card in a computer. You probably can see almost all the files including the RMS file. Application developers must realize that nothing is as secure as or more secure than their application. Application-level encryption is a must to protect the local data in the RMS database.

## User Awareness

Another factor that J2ME developers should be aware of is the knowledge level of the user base. The mobile phone user is not aware of all the computer-related functionality. The fundamental difference in the user base demands a security at a higher level which is also less complicated. The current basic security that is implemented in all J2ME application is the certificate. The expectation that an average user can understand a certificate and invalid applications is questionable. For an average phone user, the trust in an application comes from his interaction with it.

This interaction should be simple enough for the end user to understand. A better user interface design can help the end user understand the messages that he sees on the screen. Companies should take special initiatives to spread the message of security measures.

***Bottom line:*** one should understand that a mobile phone is not better than a laptop; it is pretty much the same from the hackers' point of view. Beware and be Secure!

# Cloud Computing – Security Threats and More

Companies that struggle to maintain their IT infrastructure often look to cloud computing to provide significant cost savings. However, you must look into the clouds and understand what risks are swirling around when it comes to storing your data.

In a recent survey by CIO Research, respondents rated their greatest concerns about cloud adoption. Security was their top concern, with loss of control over data number two:

- Security 45%
- Loss of control over data 26%
- Integrations with existing systems 26%
- Availability concerns 25%
- Performance issues 24%
- T governance issues 19%
- Regulatory/compliance concerns 19%
- Dissatisfaction with vendor 12%
- Ability to bring systems back in 11%
- Lack of customization opportunities 11%
- Measuring ROI 11%
- Not sure 7%

## Is there security in the cloud?

Security is often an afterthought for cloud service providers. It isn't built into their applications and is often added as a plug-in. What's more, if a cloud storage system crashes, millions and millions pieces of information may be lost, often in spite of backup procedures. In contrast, when we are in the thick client world, the information that is lost can be more easily tracked by the number of PCs or notebooks affected or stolen.

## How different should security be in the cloud world?

Business technologies may change, but security fundamentals and lessons learned are still applicable. Some areas to consider for the cloud:

- **Physical security** is a must for any strong security program. The data centre should have a high level of physical security. If sensitive data is being stored, consider deploying biometrics, surveillance cameras monitored by professionals, and very stringent policies for physical access to the system.
- **Authentication** is crucial and whether cloud or corporate individual network the need for authentication will remain the same. Given the processing power of the cloud, you may choose to implement two- factor authentication, one-time passwords or other authentication tools. In spite of a highly secured processing environment, a weak password has the potential to ruin other safeguards. Maintaining password standards is a must.
- **Access rights** are critical for all objects inside the cloud. This part of the security will not change from the user's point of view. There are some changes required to manage multiple corporate accesses inside the single cloud service provider's organization.
- **Strong firewalls** are another integral part of today's security. Even in the cloud, the same rule applies: cloud clients should secure their own networks. The only advantage is they have less information to be secured within their network. The cloud service provider should secure its network with firewalls.
- **Data integrity** is one of the key aspects in security. Today for example, it hard for every notebook to implement a cryptographic checksum or hash. But in cloud service this could become commonplace.

# *Service Oriented Architecture (SOA) Security in the Cloud*

According to Gartner, cloud computing is "a style of computing where massively scalable IT-related capabilities are provided 'as a service' across the Internet to multiple external customers." Service-oriented architecture (SOA), on the other hand, is a collection of services that communicates with each other.

Says David Linthicum, a widely acknowledged SOA expert, "SOA is an architectural pattern, while cloud computing is a set of enabling technologies as a potential target platform or technological approach for that architecture." Therefore, SOA and cloud computing are complementary and not mutually exclusive.

For a while now, companies and business leaders have been interested in moving to a cloud environment to enable growth at lower costs. By combining SOA and cloud computing, it becomes possible to reduce the time taken to implement technology, enhance business performance and expose the existing legacy application over the Internet.

Clouds enable the outsourcing of many or all I of the T functions, making regulatory, operational and baseline compliance difficult. Moreover, the complexity involved in combining data, applications and infrastructure with the cloud requires the securing of the underlying architecture.

The role of SOA in cloud computing is important because a successful cloud solution requires an in-depth understanding of the architecture, the services offered and how to leverage them. Finally, cloud computing becomes part of the architectural arsenal to create a successful SOA.

## *Security considerations for SoA*

The most common security considerations involving cloud-based services include the following:

- **Governance control** – In a governance-free environment, coordinated cloud service planning and monitoring mechanisms, which are required to meet security standards, become difficult. In addition, rogue cloud services could wreak havoc on the delicate trust between providers and businesses. Concerns here include not knowing where data resides, what happens to the data if a decision is made to change services, and how the service provider guards customer privacy.

  Contracts must outline the service provider's responsibility in case of a breach. The cloud is still evolving and as a result, processes do not yet have a standard format. Quality-of-service terms, mechanisms for security and privacy are business continuity issues around failed providers are not well established and regulatory issues raise many questions that have not been satisfactorily answered as yet.

- **Infrastructure Security** – As the cloud's infrastructure and resource pool are shared among multiple users, unified monitoring and control has become almost impossible. Relying on the host's security controls might compromise data, especially as the service provider cannot separate data. The data and the service provider's hosting process are executed and managed in shared environments.

  This requires extending trust to external services and permitting secure data residing on company servers to be moved into a less-secure environment. With a heterogeneous infrastructure, and the more individual technologies and processes in play, the harder it gets to ensure control and consistency. If the service is hosted on a heterogeneous cloud-based platform, managing security or even changing vendors becomes difficult.

- **Communication Security** – As the cloud inherently provides an elastic platform for providing services, there is the need for these services to communicate with each other to perform various tasks. SOA is moving us from User-to-Business communication to Business-to-Business communication.

  This new way of communicating brings in many decoupled software components to interact with each other in a standard format. The lack of trusted authorities and the lack of security in communication protocols could create havoc for the services.

- **Software Security** – Most of the services today are enabled as stateless machines providing optimized solutions for B2B interactions. This has inherent security issues that must be addressed through the entire software life cycle, starting from specification to the release stage.
- **Service Integration** – In a SOA, services integration is often overlooked. "Silo" services have to interact with each other to provide end-user solutions. Hence there is a high need for security in the SOA integration stage.

## *Summary*

Contrary to the popular notion that cloud computing will make SOA redundant, they actually complement each other quite well. In fact, having a strong SOA can make the transfer to cloud-based services easier, less complicated and more secure. Cloud-based SOA is all about delivering services with increased agility and efficiency helping to ensure that companies are competitive and contemporary. To keep up with the new technology, improved security measures, a strong understanding of the cloud plus selection of the right vendor are critical.

# Security threats in the cloud


Security threats can materialize in all forms; let's consider some of them here. In the cloud-based service, the provider decides where your data is stored and how your data is accessed. If your provider offers virtual boxes, a mischievous user can gain control over a virtual box, attack your data and exploit it. Another security threat in cloud computing is the attack on the perimeter of the cloud.

This may be a simple ping sweep to DoS. A cloud service provider must ensure the data of each company is properly isolated and partitioned; if not, data leakage can be expected. Another important factor that must be addressed in the cloud world are the privileges of the power user. How do we handle the administrators and data access? The administrator's rights are not under the purview of the customer anymore; they belong to the cloud service provider. There should be clear transparency and access records to prevent any misuse by an administrator.

Implementing security in the cloud environment is different than what we are used to in a traditional environment. However, remembering the fundamentals of information risk management and the lessons learned along with an understanding of cloud provider risks may help you to weather the storms looming in a dark Cloud.

## Why should the cloud customer implement security?

Though the cloud promises high security, it's essential that the cloud customers implement their own security and maintain standards. An unsecured customer network will attract hackers and is an easy entrance to the cloud.

Data transfer between the cloud service provider and customer should be on a secured connection and the customer should take necessary steps to secure his network from attacks such as the Man in the Middle (MITM).

The applications hosted on the customer network should also be secured. Customers using the cloud to deploy applications should ensure that their software is secured. Unsecured applications can be dangerous for both the cloud service provider and the customer. Cloud security can help very little if there is a vulnerable system unmaintained or not patched. Virus attacks are not going to reduce because you moved your data into the cloud.

## How can you do business securely over the cloud?

Before you decide to buy a cloud service, go security shopping. We usually bargain on price, but that is not enough here. You need to bargain for security rights, transparency and privacy.

The legal agreement is the first level of security that you will always require, no matter where you do business. A well prepared agreement can provide all the legal benefits over your data in the cloud. Make sure to include the ownership of the following:

- Data
- Data backups
- Log files

Your day-to-day business runs on your data. It's essential that the cloud service provider shows transparency in his data centre location, physical security, containment measures, and time taken to recover in case of any catastrophe.

End-to-end encryption is must in cloud computing to ensure the security of data transfer. The customer should demand this capability from the provider.

Authentication and proper access rights must also be secured. Given that you can access the applications in cloud from anywhere, it is essential to block the entire user account to former employees. This has must be an integral part of the customer's HR policies.

Patch management is also very important. Though cloud acts as a versionless world, it is essential that the service provider either informs you about the patches required to access his network or provides automatic patch management. If you use third party clients to access the customer application, you should ensure that these clients are up-to-date with security-related patches.

You should also demand log analysis reports, user accounts and privileges reports, uptime/downtime reports, and penetration test/ vulnerability assessment reports from the service provider on a regular basis. To ensure more transparency, ask that these reports be provided by a third party security company. You should also demand real time security alerts from the service provider.

The last level of security that is often vulnerable is the application security. How secure is the cloud service provider's application? There is no real way of knowing it. There are third party security companies and tools available to certify application security. This should be done on a routine rather than on one-off basis.

Social engineering is another threat that has to be addressed. It is essential for the cloud service provider and customer to be aware of such threats and educate their employees.

Phishing attackers will also target the cloud consumers. Strong phishing filters should be deployed. You may also want to involve third party security companies as partners to verify the cloud service provider's security policies and reports.

## *Summary*

Security should be inbuilt as an integral part of the cloud. This is a must for the cloud service provider to gain trust from its customers. Gaining customer trust is the key to winning the cloud service game. Security is an ongoing measure to protect and deal with everyday threats. No matter where you do business you should secure yourself with the best practices.

# *Identity and Access Management*


Most organizations are growing fast, with many new employees joining weekly. Third-party outsourcing is growing even faster, with more access to company applications and data. Digital identities within an organization possibly are growing the fastest.

The biggest risk most organizations face is access risk or over-access to key applications. In a fast moving organization managing digital access and digital identities is a big concern. This section on “Identity and Access Management” throws light on why companies need to look at why and how organizations need to look at managing identities and access, including converging physical and logical identities and access.

# Understanding the Need for Converged Access Control

According to a study conducted by Carnegie Mellon University – critical system disruptions, loss of customer and/or partner information, loss of confidential intellectual property, brute-force attacks, fraud, reputation risk, etc. were mostly attributed to actions by insiders.

The grave dangers of insider threats, arising from employees retaining their hardware and/or having physical access even after job termination, can be better understood from a shocking incident that took place recently. A US-based water service company auditor, who resigned from his post, sneaked into the company's building and accessed a former coworker's computer to transfer $9 million from the company's fund to his personal account.

Insider threats, in which disgruntled employees or ex-employees, gain access to computer systems or networks of the enterprise, is just one case of improper Identity Management!

## Proliferating Disconnected Identities – Root Cause for Mismanagement of Identities!

In most organizations, it seems that logical and physical identities often multiply like rabbits, making it difficult for the organization to track and manage all the identities effectively.

On the logical side, an employee has one identity within the enterprise HR system, such as a SAP system. That identity typically consists of salary, benefits, insurance and other specific employee details. Then there is a logical identity, for the same employee, within the information technology department's directory software – such as those from Microsoft, Novell, CA, Sun Microsystems, or Oracle. This directory controls the permissions for network, database and software applications for the logical identity.

Within the organizations' Intranets, databases and applications, the user may have still more identities, in the form of different user IDs and passwords or PINs he/she uses to log into each logical resource of organization. Lastly, this employee may have at least one more identity: a physical credential of some sort used for access to organization infrastructure – workstations, buildings, floors, parking garages, warehouses, research labs etc.

Then, there are cases of merger or acquisitions of organizations which often results in more than one brand of Physical Access Control System (PACS) in the organization. In enterprises with more than one brand of PACS and several facilities or areas users must enter, a user may have more than one physical access credential—and therefore, more than one physical identity.

Unconverged identity management systems either result in error-prone manual interventions or security issues!

## The Need for Converging Identities

One of the most important reasons for converging identities is that logical and physical identities multiply when they are disconnected; and it is time-consuming, expensive and inefficient to manage them. This applies across the organizations' domain – IT, physical security, business units and risk managers.

Another equally pressing issue is that security can be more easily compromised when physical and logical identities are separated. A physical identity may appear legitimate to a standalone PACS but it might no longer be trusted by the enterprise network. This is what happens when an employee is terminated in the logical systems but this information isn't immediately relayed to a PACS. If the enterprise has more than one PACS, and they are not integrated with each other, it may take several more steps to ensure all PACS block the ex-employee's credentials.

Physical or logical credentials that are kept alive even after an employee has left the organization can be the cause of a compliance gap and, at worst, can leave the virtual or physical door open to fraudulent attacks. The federal government has acknowledged the importance of converging technologies and has been a significant driver for the development of these technologies. For example, in 2004, the Homeland


Security Presidential Directive -12 (HSPD-12) was passed, requiring the all federal government employees and agencies use a converged physical and logical ID badge. Standards

were to be created on how the badge was to be designed, what identity elements were present inside the card, and how the card was to be used for physical and logical access. This policy was intended to enhance security, increase efficiency, reduce identity fraud, and protect personal privacy.

## Converged Identity and Access Management

Converged IAM (Identity and Access Management) may be understood to be a system which converges disparate physical and logical access control systems together to create a singular trusted identity and one credential to match rights and access them across the enterprise.

Converged IAM cannot' exist without network connections – preferably automatic, software driven ones – between these logical and physical identity systems.

The most typical use-case right now involves the uses of a card reader integrated with an identity management or directory system such the Active Directory of LDAP. Users swipe the access card at the door and use that same access card to log on to network resources.

Logical identity integrations for a user usually begin with links between human resources systems, an IT network component and the enterprise directory. The directory software, such as Microsoft's Active Directory or similar tools based on the Lightweight Directory Access Protocol (LDAP), ensures that all employees have the network, software and database access — the virtual provisions — they'll require to do their job Many large enterprises already use identity management tools from vendors like IBM, Novell, Oracle and Sun, to provision users from the HR system into the directory.

That process is fairly well-automated. The disconnect between logical and physical identity usually appears when it is time to provision a user's physical access rights—at the most basic, when and where that person is allowed to be within the enterprise. In many enterprises, this task is typically still manual: A phone call, e-mail or fax from HR alerts the physical security department to put the new employee into the PACS and create an access badge for him.

Integrating the PACS with the enterprise directory enables enterprises to address the issue of disconnected physical and logical identities. The value for the organization here is that integration allows them to have a better understanding of who has rights to their network and their physical facilities. It allows them to manage access rights and people's responsibilities within the organization more efficiently.

## The Importance of IT Convergence

The IT infrastructure is the backbone of a converged solution, allowing key business data to be shared across systems. For example, a company's physical security system usually does not have critical business data such as employee status, whereas the HR department's IT system does.

Converging physical security with IT security is not easy, but the extra effort it requires can be beneficial, especially for financial, healthcare, and defense organizations. Convergence provides organizations with the opportunity to align security with overall business goals, streamline business processes such as provisioning and investigations, and centralize security operations and policies.

Developing common protocols for managing access to company assets and data allows for more efficient provisioning and management. Different physical and logical security systems should leverage extendable interfaces of identity management solutions and thus stay in sync.

The key benefit is that security personnel can continue to use tools best suited to their jobs and HR personnel can continue to use HR tools. Converged security systems, hence allow users to improve Return on Investment.

## Key Steps for Convergence

To bridge the organizational gap, the physical security department should work directly with the IT security team to identify:

1. Authoritative sources of key data used to determine whether a person has permissions to use a resource or access an area.
2. Compliance or audit needs.
3. Any business or security concerns that are unique or are especially important to an organization.
4. Various business processes such as on-boarding, off-boarding and the responsibilities of different systems.
5. Policies for managing employees who do not have logical accounts, e.g., cleaning staff, caterers, etc.
6. Privacy and security policies that clearly define what personal information is to be collected, how the information will be used, who can access the information, how the information will be protected, and how the individual will control its use and provide updates to the information over time.

## *Effective Convergence through Events Correlation*

With converged access control, organizations can correlate disparate physical and IT security events. For example, it may not seem suspicious that an employee uses a computer. However, physical/ logical correlation might ensure the employee is able to access logical resources, only after he has swiped his ID card at the entry door. Or, a user could be locked out of some of the logical resources as soon as he leaves the premises by using his card at the door.

## *Conclusion*

The convergence of Identity and Access control systems helps enterprises better protect their intellectual property, monitor access to restricted areas and comply with regulations. It improves the operational efficiency of existing physical security systems and resources. How organizations choose to implement this should be aligned with their business strategy and security and compliance requirements.

# More than Password Resets – Identity and Access Management's Real Value


You've probably heard enough about the benefits that an Identity and Access Management (IAM) program can bring to you. Most of the benefits pitched to customers from various vendors revolve around specific features of the products, and are generalizations at best.

For example, password reset is available as a feature, and the obvious benefit is reduced helpdesk costs. There is, however, much more to the story. When you decide to implement an IAM program, this is what you should really set out to do:

## Streamline processes

Setting up an IAM solution forces one to optimize and define processes that carry no ambiguity, because automation cannot be achieved when there is ambiguity. Don't count on the partner who is on keen to migrate your existing processes into the IAM system without questioning the need or sense behind that process.

Example: Quite a few customers insist on having the employee's manager approve the request first, and then send it to a secondary owner for a final approval. When questioned, the response often is, "We don't trust our managers. They may approve just about anything that someone requests, so we need someone else take a look at it." The question we then pose is, "Why has the manager approved something when you don't trust his judgment?" Or "Has the manager approved the requests, but educate the users about the responsibility they carry when they approve something." you get the idea.

## Streamline data across systems

This is an opportunity to bring consistency to how data values are treated by applications across the organization.

Example: The location for a person maybe "SFO" in one application, "California" in another, and "Calif." in yet another application.

Traditionally, each application owner is used to operating in a silo, and comes up with a naming convention designed to suit the needs of the hour and the application. Standardizing the values across applications lets the organization take charge by centrally managing various aspects of user properties, rights, etc.

This change often sees the greatest amount of inertia, but is the one that truly lets organizations leverage their IAM investment. The solution isn't to avoid standardization. The solution (and opportunity) is to strengthen change management.

## Build a platform for future application development

Traditional application development models cater to embedding the authentication and authorization into the core of the application itself. With an IAM program in place, you have the luxury of asking application developers to develop just the business logic in their application. All authentication and authorization related decisions can then be delegated to the IAM platform, resulting in:

- Application developers focused on core business functionality
- A secure, and proven mechanism for authentication and authorization decisions
- A complete view of who can do what in which application

In a nut shell, most IAM programs are about implementing a vision. It is an opportunity to question what has been done for years, to optimize, streamline and strengthen the way the organization functions, and to discard the legacy that has ceased to provide value.

To quote Sara Gates, former VP of Identity Management for Sun Microsystems, "Identity Management is like putting brakes on your car. Why do cars have brakes?" Everyone says, 'So they can stop.' But the real reason cars have brakes is so they can go faster."

# Single Sign-On – Choosing Practical over Paranoid Security

As various business processes are automated in enterprises, the IT landscape gets more and more complex. Multiple applications and platforms require different authentication checks before granting user access. Users need to sign on to multiple systems, each involving a different set of credentials. As a result, accessing systems gets increasingly complicated and frustrating for users and hampers their daily tasks.

Implementing single sign-on (SSO) security functionality can significantly simplify system access. SSO provides a unified mechanism to manage user authentication and implement business rules determining user access. As only one set of credentials are needed to access multiple systems, SSO improves usability, increases productivity and reduces helpdesk expenses, without compromising system security.

SSO also reduces human error, because the user logs in once and gains access to all systems without being prompted to log in again for each, a major component of systems, failure.

## Why is SSO relevant?

- The need for SSO is accentuated by several issues enterprises face including:
- Enforcing strong security and password policies at a central level
- Multiple helpdesks
- Need for helpdesks to engage in more value-adding tasks rather than be consumed by resetting passwords for users
- Management of multiple platforms and application models
- Risk of unsecured, unauthorized administrative and user accounts

## Types of SSO

Two of the most important types of SSO are:

### Enterprise SSO

Enterprise single sign-on (ESSO) systems are designed to minimize the number of times a user must type their ID and password to sign into multiple applications. The ESSO automatically logs users in, and acts as a password filler where automatic login is not possible. Each desktop/ laptop is given a token that handles the authentication.

### Web SSO

This is a single sign-on for web-based applications and a few supported proprietary closed source web applications. It is a browser-based mechanism, with single sign-on to applications deployed on web servers (domain). The main differences between ESSO and Web SSO approaches are given in the table below.

| Enterprise SSO | Web SSO |
|---|---|
| Single Sign On For all kinds Of applications Wed based thick client terminal based and even proprietary closed source applications | Single Sign on for web based applications and Supported proprietary closed source web applications. |
| Password Management Facilities for self service password reset drastically reducing admin intervention. | Extremely limited Password management |
| Windows logon integration No need to Sign in again afer signing on to windows .Can be linked with smart cards Access cards and fingerprint access control. | Windows login interation is kept out of scope. |
| Access from authorized systems only Can also allow remote access. | Deployed when access is to be given from extremely large intranet or internet. Available Wherever browser based apps are available. |
| Quick and straightforwad deployment. | Loang and complex deployment cycles. |

ESSO can provide tangible benefits to an enterprise through:

- **Enhanced user productivity** - users are no longer bogged down by multiple logins and they are not required to remember multiple IDs and passwords
- **Improved developer productivity** - developers get a common authentication framework –and do not have to worry about authentication at all
- **Simplified IT administration** – the administrative burden of managing user accounts is simplified. The degree of simplification depends on the applications since SSO only deals with authentication
- Reduced password fatigue from different user name and password combinations
- Reduced IT costs due to fewer help desk calls about passwords
- Improved security through reduced need to handle and remember multiple sets of authentication information
- Reduced time spent re-entering passwords for the same identity.
- Integration with conventional authentication such as Windows username/password.
- Centralized reporting for compliance adherence like ISO 27001, etc.

Clearly, SSO functionality is a practical approach to security management in an enterprise. However, its detractors protest that once a password is breached through SSO, then other systems become highly vulnerable. Nevertheless, while weighing the pros and cons of the SSO approach, its benefits in the form of lesser maintenance and increased usability far outweigh the disadvantages.

It can even ensure a better protection of the single password, with stronger policies in place, which may not be practically possible if there were multiple passwords to remember. SSO is a good choice for enterprises struggling with the burden of managing multiple accesses.

# *Identity and Access Management – This must be your project, not your partners'!*

Lessons Learned

Having been through numerous Identity and Access Management (IAM) implementations, we see two common denominators in terms of customer expectations that rear their ugly heads rather frequently:

1. Let's integrate everything that we have, and
2. Let's do it all at once

One can understand the excitement we all go through when we contemplate having a solution that allows us to link so many applications, streamline processes with workflow automation and synchronize attributes across the board. While that excitement is infectious and contagious, the sound voice of reason must be heard and listened to.

It is natural for you to want to do as much as you can with a product, and it is human to want all of it done yesterday. Hence, the onus lies on the domain experts to work closely with customers (as partners, not vendors) and develop a deployment plan that gives the customers the most results as soon as possible and additional benefits over subsequent phases.

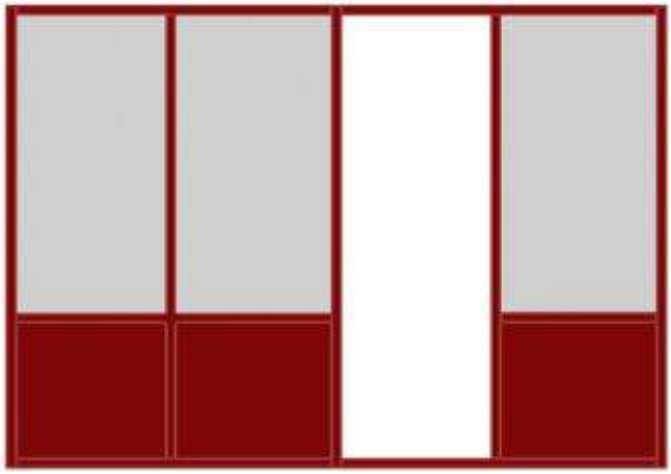
The "good" partner helps the customer prioritize its needs and requirements, and establish plans to achieve those objectives over phases. Strong project management and planning is the key to a successful IAM program. The products from various vendors are unlike those of 5 years ago - they are now mature, stable and scale exceptionally well, unless hacked to death to fulfill a few exotic requirements.

We cannot lose sight of the top benefits of having a robust IAM program:

1. IT systems and applications are constantly compliant with a variety of regulations, and there are very few gaps in access recertification
2. Processes and access governance have been streamlined – business demands, business approves, and business gets – with minimal or no IT intervention
3. Password reset is automated and secure, and helpdesk costs are under control
4. Peace of mind

So next time you want to know whose side the "partner" is on, throw a plan too ambitious at them. While most will try to give you what you demand, you will know during the course of their approach whose interests they have in mind, yours or their own. After all, it is your project and responsibility.

# *Physical Security Controls – What are we Lacking?*



In the world of increasing security threats, we are being attacked at both the physical and the logical fronts. Logical damages hit organizational reputations, goodwill, and the company brand and trust, whereas physical damage at a macro level impacts human lives and the economy. The Mumbai attacks in 2008 (often referred to as 26/11), the London public transit attacks in 2005 (often referred to as 7/7), and of course 9/11, are real life examples that exposed the deficits in physical security controls.

When we examine and measure many of the current physical security controls, we often identify weaknesses and realize that the controls really do not provide the reliance we are looking for. It therefore becomes important for an organization to adopt a layered approach when building its physical security controls.

Many physical security controls are reactive in nature and often the responding professionals may not have the skill levels necessary to follow the standard operating procedure for a response. To address this situation, if the organization implemented a layered approach to physical security controls, response to complex incidents in real-time will probably reduce the risk.

Here is a macro view of a layered approach:

- **Level 1** – Basic controls in place
- **Level 2** – Converging physical security in a single integrated system with automated standard operating procedures
- **Level 3** – Enabling systems on an IP backbone and building strong IT security controls
- **Level 4** – Building a KPI framework for physical security controls

With these levels, we can build a maturity framework for physical security systems, starting with basic physical security controls and followed by the convergence of the same on a single integrated platform that may be accessed, monitored and SOP-enforced on a web interface from any Web-enabled IP device. With this Web advancement it is important to build an IT security layer around physical security controls. This results in a true state where there is convergence of both physical and logical controls.

The benefits to an organization that follows this approach typically include:

- Integration of current hybrid physical security controls in a single unified framework that delivers enforcement of procedures across systems
- Delivery of strong coordination during incident management
- Compliance with regulatory physical security control needs
- Delivery of an audit trail from systems that helps deliver forensic investigation in real-time
- Monitoring and improvement of physical security control operations
- Delivery of real-time incident analysis and operation analysis

Attacks are distributed across the enterprise both at a physical and logical level. For security to be effective, it must be organized to react quickly to resolve issues across the enterprise. There is a definite need for systems that can enable a rapid response to security breaches and prompt investigation of events. Convergence may be the answer.

# About Aujas

*Aujas is a Global Information Risk Management (IRM) company providing consulting and technology life-cycle services in the area of information risk with a presence in Asia, US, Europe and Middle East. The company helps enterprises to manage information risk and enhance value of information through innovation and excellence.*

*Aujas service portfolio includes Information Risk advisory services, Secure Development Life-cycle services, Identity and Access Management services, Managed Information Risk services, Vulnerability Management services and Converged Security services. Aujas has today more than 120 clients globally and it has executed over 250 projects in 15 countries.*

*For more information please visit www.aujas.com or write to contact@aujas.com*


**Karl Kispert**
Vice President
(Sales & Business Development)
+1.973.229.5566
karl.kispert@aujas.com

USA

**Navin Kotian**
Co-founder & President

+91.998.779.9664
navin.kotian@aujas.com

India

**Rajeev Krishnan R**
Vice President
(Middle East & North Africa)
+971.566.940.614
rajeev.menon@aujas.com

Middle East

New Jersey, July 2011

Designed by: Aujas Information Risk Services, New Jersey