COURION
see risk in a whole new way

Courion White Paper

Access Risk Management: The Key to Protecting Your Business in Today's Mobile, Always-On, Cloud-Based Environment

www.courion.com

Table of Contents

Introduction

In today's mobile, always-on, cloud-based business environment open is not a choice, it's a requirement. Whether you're doing business on premise, in the cloud, on social networks – the complexity of managing security has never been greater... and it's never been riskier.

Openness supports productivity and creates opportunity – but it also creates security and compliance risk. Organizations need to balance exposing data with granting access to employees, partners and customers while simultaneously putting governance controls in place to ensure critical data is secure. Key to this balance is not trying to 'boil the ocean' but focusing on the areas of greatest potential for risk to the business.

With critical information being continually shared, transformed and moved across the enterprise, the web, personal mobile devices and other environments, organizations are constantly facing the challenge of protecting their valuable assets – critical corporate information, sensitive employee and customer data, intellectual property and more – all of which impact their reputations and their bottom lines.

Up until now, the challenge has been knowing which assets may pose the greatest risk to the business, where these assets reside, who has access to them and most importantly – what are users doing with these assets? To protect your business from risk, you need to know this *right now*, in real time – not through periodic reviews once a quarter or once a year.

Protecting and monitoring massive amounts of information in an Identity and Access Management (IAM) system is not only complex, it's mission critical and required by corporate and industry policies and a litany of government regulations. More often than not, it can also be overwhelming and require substantial administrative and financial resources to manage.

A common mistake that many organizations make is that they're primarily focused on passing audits. Their identity and access management strategies are based more on being compliant with regulatory requirements rather than looking at IAM as a business enabler, and a way to protect the entire organization from potential risk to the business. So while audit-focused organizations may effectively demonstrate compliance and manage *known* risks, they have yet to determine how to identify and manage unforeseen risks – leaving the organization exposed and extremely vulnerable.

The Gap Between User Provisioning and Access Certification

Today, it's not unusual for most organizations to merely perform periodic access certification reviews or audits. They provision access for employees and a few months later review that the access is still appropriate. This is the period of time that we've identified as "the gap." Consider it a black hole bookend-ed by provisioning and certification. With this gap between provisioning and certification reviews, there's no way to know what's happening in real time.

Unfortunately, many companies struggle with the gap, typically experiencing a disconnect from what's taking place in their own organizations. They're unable to see what's occurring in real time – so they don't really know if they've had a data breach, or millions of dollars, records or files have been stolen – *and they won't know* until it actually happens. The door is wide open for potential loss of critical information, reputational and financial risk; basically anything that can adversely affect the business.

When organizations don't have the data and the intelligent analysis of that data, they have no way of dealing with potentially risky situations. Without this knowledge, they will always be on the defensive. They need a solution to close the gap without delay; one that gives them intelligent insight into what's happening in their organizations in real time, and on a continuous basis.

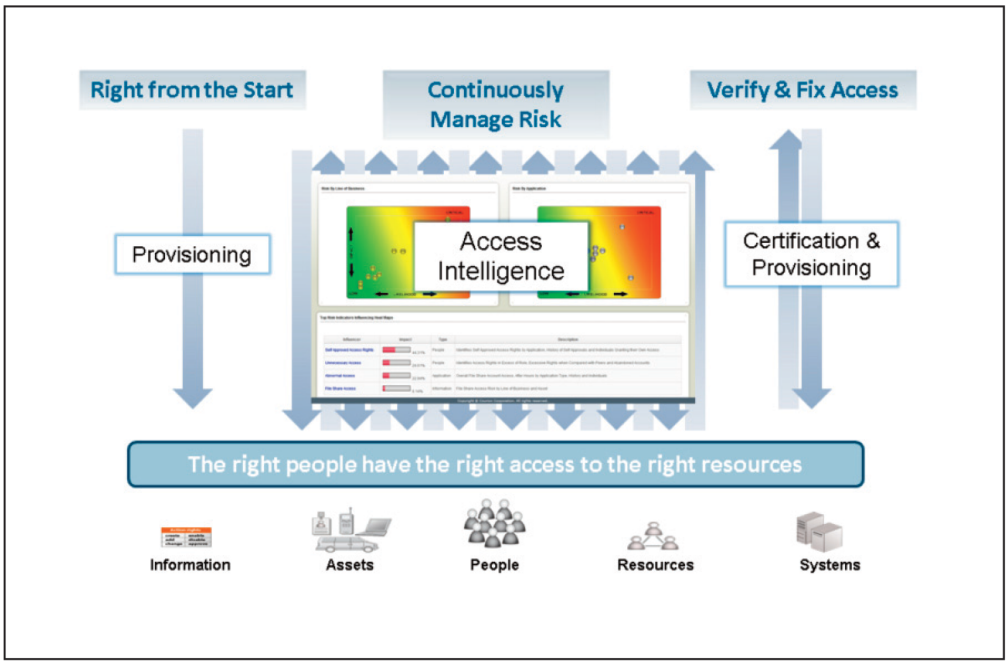

Figure 1. Closing the Gap

Taking Care of Business

A recent study from the IT Policy Compliance Group surveyed IAM programs in 4500 enterprises, reporting on the practices best-performing organizations implement to drive more value and less risk from the use of IT.

"It is the better-managed organizations that are using IT as a competitive advantage to generate more capital to invest in acquiring new customers and markets, reduce capital and operating costs, while significantly reducing operational and strategic risks related to the use of IT."[1]

On the other hand, the study also says that "When it comes to the use of IT, the worst performers are ignoring the risks as well as the rewards, to their own detriment. The average performers are sitting somewhere in the middle of the pack, not ignoring the risks but not adequately reducing risks associated with the use of IT."[2]

What does this really mean? If you want to take care of business, you've got to turn a narrow compliance focus into one that takes a holistic approach to risk – one that looks at managing access risk and potential risk throughout your entire organization.

[1] *How High Performance Organizations Manage IT*, IT Policy Compliance Group, April 2011.

[2] Ibid.

Dealing with *known* risk is one thing, but being unable to identify, quantify and manage the risks associated with information access, leaves the door wide open for access risk. Data breaches (from both internal and external sources) can swiftly compromise your intellectual property, sensitive data and other vital assets – leading to regulatory penalties, loss of reputation and revenue – *directly impacting your bottom line.*

To their credit, many organizations are taking note, and coming to the realization that protecting and securing the organization from access risk is one and the same with 'taking care of business.'

And that's why effective access risk management is critical to protecting your entire organization.

What is Access Risk Management?

Access Risk Management encompasses traditional IAM functions associated with user access administration (password management and user provisioning); Identity and Access Governance (IAG) (role management, compliance management and access certification); and the emerging discipline of Access Intelligence.

Gartner, the world's leading information technology research and advisory company, defines Identity and Access Intelligence as "the process of gathering data about identity and access, and converting it to information and knowledge for action-oriented insight and intelligent decision making in IT and business...Identity and access intelligence elevates identity and access management to a relevant discipline by leveraging business intelligence practices to enhance the usefulness of IAM data."[3]

Access intelligence enables an organization to have visibility and transparency into their IAM system data so they can answer those crucial questions "Who has access to what?" "Who granted that access? And "Is that access being used appropriately?"

Access Intelligence transforms raw data into actionable insight, allowing organizations to make informed decisions about potential business risks based on fact, not assumptions. Access Intelligence strengthens IAG, since IAG becomes more effective when accurate and timely information is available.

What it boils down to is this: an effective access risk management solution analyzes IAM and other security data from IAG and external sources such as Security Information and Event Management (SIEM) and Data Loss Prevention (DLP) systems to identify and quantify real-time access risks to vital information such as intellectual property, personal information and customer data; integrates this massive amount of information into enterprise Governance, Risk and Compliance (eGRC) applications; and provides an overall enterprise view of your access risk. Working together, these functions leverage an organization's existing IAM information to provide insight into where your access risk resides, and the intelligence to determine the level of access of that risk.

The Challenges of IT and the Business

When it comes to protecting the business from risk, most companies face the same *business challenges* – limited resources, regulatory compliance pressures, IT services delivery challenges and

[3] Earl Perkins, *Identity and Access Intelligence: Making IAM Relevant to the Business*, Gartner, Inc., January 14, 2011.

perpetual business change. A by-product of these business challenges is the incidence of access risk; and access risk dramatically increases the likelihood of *business risk*, impacting reputation and the bottom line.

Delving deeper, most organizations encounter similar challenges managing *access risk*: dealing with excess privileges; zombie or orphan accounts; and separation or Segregation of Duties (SoD), not to mention on-going demonstration of regulatory compliance; and non-stop business change.

Take ***excess privileges***. While you wouldn't leave your valuables sitting out on your kitchen table and then announce to the world you were leaving your front door unlocked, neither would you leave your intellectual property or sensitive information inadequately protected and then broadcast it throughout your company. But allowing an individual to possess excess privileges is like giving him an unlimited charge account and the ability to access your valuables…and then letting him take what he likes.

Excess privileges are often accumulated when people move around within organizations – lateral moves, promotions or re-organizations – changing jobs internally. Not only do excess privileges stem from internal movement, they also come from organizations not really knowing who has access to what, and what they're doing with that access.

Meet *John A*. He turns 30 in two months. When he worked in accounting, he needed access to sensitive and confidential files. When John A. transferred into the marketing department, access to those accounting files was no longer relevant to him doing his job. But because his company had no formal or automated process in place, no one removed his accounting privileges.

Today, John A. has excess privileges, aka 'the keys to the castle.' He's retiring at age 30 to a tropical island where he's almost finished building a 10,000 sq. ft. bungalow. Because of his excess privileges, John has been stealing money from his company, unbeknownst to them. Eventually they'll discover millions are missing from the corporate coffers, and that John had the privileges all along to write checks, sign checks and cash checks.

While it sounds far-fetched, it does happen. But by having a process in place to ensure that an individual doesn't have more privileges than he needs to perform his job, you're dramatically decreasing access risk exposure – and keeping the keys to the castle safe.

What about ***zombie*** or ***orphan accounts*** – accounts not associated with valid users. Akin to excess privileges, these accounts are like unlocked back doors, enabling thieves to gain unauthorized access to your most valuable assets – your intellectual property, sensitive data and other critical information.

Meet *Julie B*. She just left her company, but her access to SAP wasn't disabled immediately – so she still had free access to confidential company information. Five days later, a company breach identified Julie's account as still active. Though her SAP access was disabled as soon as the breach was discovered, her former employer is crossing their fingers that Julie didn't steal company confidential information, insert a virus into the system…or worse.

Inaction can be fatal. So the sooner you terminate zombie accounts, the sooner you reduce your access risk. When this process is automated, becoming part of your overall access risk management strategy, you're once again dramatically decreasing your access risk exposure.

Separation or Segregation of Duties (SoD) is a basic internal control used so that no single person has responsibility for initiating and recording transactions, and for the custody of assets. SoD ensures that a single individual is never in a position to engage in fraudulent or nefarious activities without detection.

Here's John A. again. In addition to having excess privileges he's a poster child for why every organization needs to implement SoD controls. Aside from being able to demonstrate compliance to auditors about SoD (especially in the financial world), it's better to uncover SoD violations *before* you find millions of dollars missing or learn that your prime intellectual property has fallen into the hands of a major competitor…or has been leaked to the public.

Regulatory Compliance

When it comes to regulatory compliance, the areas of access risk and the areas of potential loss to the business are one and the same – intellectual property and critical data such as Personally Identifiable Information (PII) and Personal Health Information (PHI).

Remember Julie B.? Her ability to access confidential data following her separation from the company is a prime example of why effective regulatory compliance isn't something to be taken lightly.

Spurred on by highly publicized security breaches, fraudulent reporting and other threats, legislators and industry organizations are bombarding businesses with new laws and requirements that focus on securing critical and sensitive information. Is it any wonder that organizations are constantly under the gun to prove compliance and respond to audit demands in a timely and efficient manner.

Managing Business Change

With business being conducted at an unprecedented rate, organizations need to be agile to stay on top. But with the need for speed and flexibility comes the necessity of managing the inherent risks resulting from business change – Mergers & Acquisitions, corporate reorganizations and, more commonly, employee transfers, promotions and layoffs.

Meet *Joe C.* His company recently went through a massive reorganization. Previously in the Human Resources department, Joe had access to sensitive and confidential data. Now Joe works in Customer Service (and he's not happy about it), but his HR entitlement access was never changed. With this wide open access, Joe could cause a boatload of problems…if he wanted to.

The IT-Business Connection

It's no secret that, in many organizations, IT and business have not been well aligned – they've traditionally communicated on different levels, didn't speak the same language and have often had a *dis-similar* focus on how to keep the organization safe and compliant. Business users primarily think in terms of risk; IT thinks in terms of demonstrating compliance. And, up until recently, the tools used for protecting the business and managing risk have been designed solely for IT, not business users.

To add to the *dis-communication*, in many organizations, much of the information generated from IAM systems is still presented to business users the same way it's presented to IT security teams – as raw data without the benefit of a comprehensible business translation. Providing raw IT-oriented data to business users is like giving a herd of camels surfboards – presenting data that has no business context or meaning, and essentially providing no business value.

All of these challenges result in aggregate risk. Between having to work with a complex mix of application and security models that have been cobbled together over time with little or no integration; and dealing with the language barriers between IT and business, it's no wonder that identity and access management processes have become less and less effective protecting the business from growing business risk. Just think of aggregate risk as the perfect storm – providing unlimited potential for exposing your most valuable assets to ever-present access risk.

Risk — A Business Perspective

Over the past few years, countless organizations, as well as numerous government agencies, have had significant data breaches. From an IT perspective, it's about having sensitive data compromised and the resulting fallout. **But what about risk from a business perspective?** It's not just about fixing the system so it won't happen again; **it's about protecting the organization's potential areas of risk and the potential loss to the business**. We're not only talking about intellectual property, financial information, customer and employee data and PHI, we're talking about reputational and financial risk added to the mix as well. The last time we checked, those things aren't so easily fixed, if at all.

According to Information Week, "A new report from the Privacy Rights Clearinghouse (PRC) notes 535 breaches during 2011, involving 30.4 million sensitive records."[4]

Recent breaches at Sony PlayStation Network, Sony Online Entertainment and Sony Pictures compromised over 100 million user records. Cloud-based email service provider, Epsilon's breach affected data from 75 of Epsilon's clients (and their 60 million customers). Swiss banking giant, UBS, who has experienced several major data breaches, recently lost $2 billion due to unauthorized trading. It cost their reputation a whole lot more.

With news of these notable organizations experiencing data breaches, it has become painfully clear that data breaches can happen to any business, large or small, in any industry. Throwing a few patches on a limping IAM system (and sticking your head in the sand) just won't work.

International Data Corporation (IDC), the premier global provider of market intelligence, advisory services and events for IT, telecommunications and consumer technology markets, reports that worldwide IT spending by financial institutions will reach $394 billion in 2012. Within this context, identity and access management represents a significant part of information security budgets and spending across banking, capital markets and insurance industries.[5]

With organizations experiencing major data breaches on a daily basis, it makes you wonder what they're really doing with all that money they're spending to ensure that the right people have the right access to the right information, and are doing the right things.

Past vs. Present — The Traditional IAM Strategy

The IAM market has been a recognizable segment of the enterprise software market for over a

[4] Mathew J. Schwartz, *6 Worst Data Breaches of 2011*, Information Week, December 28, 2011.

[5] Michael Versace and Sally Hudson, *IDC MarketScape: Worldwide Identity and Access Management 2011 Vendor Assessment*, IDC Financial Insights, January 2012.

decade, evolving from modest beginnings to a significant market with revenues of $ 3.9 billion in 2010.[6]

The traditional way of managing identities and access has always been hard, expensive and time consuming. But while new technologies intended to manage identities and access are sprouting up at unprecedented rates – many organizations are not quite ready for change (whether they want to acknowledge it or not).

Traditional IAM

Traditional IAM has been around for years: relying on manual processes prone to human error; presenting limited deployment options; long and costly implementations and maintenance; endless customization; and requiring significant upfront investments. Like it or not, it was something companies had to endure – and for some crazy reason – still do.

But finally, organizations are waking up to the fact that the traditional way of managing identities and access is just not working for them. It's complicated, expensive and time consuming. And if you're not seeing value for the money you're spending, you need to find a better way.

A Better Way — The Next Generation of IAM

Organizations are slowly but surely re-thinking about how they can best protect the business – how to safeguard the organization as a whole, rather than just being able to demonstrate compliance. So, while traditional IAM methods may have worked well in days long gone, in today's dynamic business environment, it's obvious that the old ways just don't cut it anymore.

Today, the next generation of IAM offers organizations more value than ever before. If an organization is smart, it won't wait before taking advantage of the options offered by Next Gen IAM:

- Clear ROI for IAM security operations
- Fewer audit and security problems
- Faster audits with less effort
- Faster resolution of security and access risk concerns
- Clear tie of security issues to the risk to the business

While managing access risk can be challenging, it doesn't have to be. It requires focus and dedication of services and resources. It requires a commitment from business and IT working together. And it also requires the tools and processes put in place to make it all happen – from the next generation of IAM.

Courion, the leader in identity and access management solutions that effectively and securely manage user access risk, has taken traditional IAM and turned it on its head…with the industry's first Access Risk Management Suite.

[6] Sally Hudson, *Worldwide Identity and Access Management 2011-2015 Forecast: The Three Cs – Cooperation, Collaboration, and Commitment – Are Key for Identity –Driven Cloud*, IDC, June 2011.

Courion's unique solution for managing access risk helps organizations identify, quantify and manage where access risk exists in your organization – even in the most complex, heterogeneous environments. Courion's unique approach to access risk management increases operational efficiency and transparency; strengthens security; and improves compliance, while delivering the industry's fastest time to value and lowest total cost of ownership.

With the Access Risk Management Suite, Courion addresses identity management as a *business issue*, not an IT administrator problem. The Courion Suite provides organizations with a new type of performance and compliance information – information that business can easily use to make accurate and timely on-going strategic and operational decisions.

A Comprehensive Approach to Access Risk Management

Courion's comprehensive approach to access risk management is based on the premise that every organization has a unique, globally distributed environment – on-premise, outside the firewall, in the cloud, and mobile and virtual environments.

The Access Risk Management Suite provides a single platform for managing user access to vital information by automating and integrating key IAM functions such as identity and access governance, user provisioning, and password management.

Courion's approach allows the business to easily manage day-to-day IAM activities and participate in the organization's IAM processes. If business users can actually understand and use the IAM data and information they're looking at, you eliminate many of the roadblocks that keep you from effectively protecting the business.

Taking it a step further, the integration of user provisioning, role lifecycle management, access compliance and password management enables customers to achieve optimal efficiency and the ability to respond immediately and automatically to business changes – using business-friendly tools and processes.

Access Insight™ Leverages Access Intelligence

The Courion Suite leverages access intelligence with Access Insight, the industry's first access intelligence solution. Access Insight is designed to transform operational security tools into real business tools by constantly analyzing IAM and other security data from access governance, user provisioning and password management systems, as well as external sources.

Access Insight is the foremost access intelligence solution that closes "the gap" between provisioning user access and performing access review certification and attestation. It gives organizations intelligent insight into what's happening in their organizations *when* it's happening – allowing them to remediate potentially risky situations in *real time*.

Finally, it's easy to identify and quantify access risks to vital information such as intellectual property, medical records, personally identifiable information and customer data. And all this critical information can be integrated into enterprise eGRC applications as part of an organization's overall enterprise view of access risk. Essentially, *Courion's unique intelligence solution connects identity and access risk management directly to an organization's business risk*.

While other vendors offer limited deployment options. Courion is different. Courion offers both on-premise perpetual license software, as well as a cloud-based subscription model with CourionLive™.

CourionLive, Courion's Software as a Service (SaaS) delivery of Courion's Access Risk Management Suite is a dynamically scalable delivery platform designed specifically to supply enterprise identity and security solutions. The Courion Suite includes everything needed to easily determine and remediate critical access risk in your organization, providing a simple, effective and timely means to see how your access risk impacts your business risk…*and be able to take action*.

Courion's innovative solutions combine out-of-the-box functionality and best practices based on hundreds of successful implementations to provide the intelligence to identify, quantify and manage access risk – ensuring that the right people have the right access to the right information and are doing the right things with that access.

Conclusion

While it's clear that organizations are trying to align business and IT, the longer they wait to take action, the farther they fall behind when it comes to protecting the business. What if organizations could get IT and business to have an on-going, two-way conversation? A real conversation about how IT can provide business users with the tools they need to actively participate in protecting the business. It wouldn't take long for those involved to see how the efficiency of IT Services delivery directly impacts an organization's risk factor. Faster new hire on-boarding means greater user productivity and effectiveness – getting the new hire up and running more quickly with less frustration, and with fewer administrative burdens.

When business and IT align, you begin to eliminate IT administrative overhead; trim audit-related costs and efforts; reduce unnecessary help desk calls; and mitigate your access risk – invariably limiting your business risk.

The recent IT Policy Compliance Group survey about high performing organizations echoes this sentiment. "The best performers post higher revenue, profit, customer attraction and retention levels while also experiencing the least amount of business risk– lowest data losses or thefts, lowest rates of business disruption from problems in IT, and the fewest problems with regulatory audits – using simple approaches to manage more value and less risk from IT and implement specific practices to transform data-driven decision-making into compelling competitive advantage."[7]

So while you're trying to figure out how much longer you can dodge the 'data breach bullet' using only your existing IAM solution, think about this – *It's 10PM. Do you know where your access risk is?*

[7] *How High Performance Organizations Manage IT*, IT Policy Compliance Group, April 2011.

Worldwide Headquarters
Courion Corporation

1900 West Park Drive
Westborough, MA 01581 USA
phone + 1 508 879-8400
fax + 1 508 879-8500

APAC
Courion IT Private LTD

305, Pride Purple Accord
S. N. 3/6/1 Baner Road
Pune, Maharashtra
India 411 045
Telephone: +91(20) 6687-9100

www.courion.com

About Courion

Courion Corporation delivers software solutions that effectively and securely manage access risk. Fourteen million users across more than 500 organizations rely on Courion's access risk management technology to align user access privileges with corporate and regulatory governance policies. Courion's cloud and on-premise solutions provide a full range of identity and access management functionality while demonstrating compliance and achieving quick time-to-value. For more information, visit our website at www.courion.com or contact us at info@courion.com.