Enemy at the gates
What executives need to know about the keys to the organisation’s front door
Executive summary

The potential for unauthorised access to sensitive data and intellectual property presents a constant, pervasive threat to the brand equity, competitive posture, and reputation of any enterprise. Many organisations are aware of the enemies lurking just outside their gates and Identity and Access Management (IAM) solutions have long been an integral element of any risk-mitigation or fraud-prevention strategy.

But with the threat landscape evolving and regulations pertaining to data protection in a transformational state, traditional, time-tested IAM technologies may no longer be sufficient. As a result, corporate leadership – including senior business executives, IT stakeholders, and board members – are rightly concerned about the potential impact an incident can have on the organisation, its business relationships, and customers.
Pressure is mounting on organisations to do whatever is required to not only detect, but, more importantly, prevent threats before they affect critical business processes or sensitive data. Fortunately, help is on the horizon. Next-generation IAM solutions built around advanced risk-based authentication techniques promise to help companies effectively safeguard critical assets against today’s threats.

The availability of these mature solutions is a positive development. But, to maximise the effectiveness of these new technologies, organisations must take steps to determine what implementation best aligns with their specific requirements. To this end, business and IT leaders must work together to analyse current IAM capabilities, understand the implications of various forms of risk, review available options, and adopt a new approach – one that lays the foundation for better security, both now and into the future.

Many organisations have already invested in an IAM infrastructure. Those in regulated industries have worked through regulations and requirements to build somewhat mature and holistic IAM systems. There are, however, many sectors where IAM implemented in an ad-hoc manner and inconsistent across the enterprise.

IAM technology is fundamental to addressing various security risks and challenges, such as mobility, access to sensitive data, third party challenges, etc. As an illustrative example, Deloitte’s 2012 Global Security Study’s for the TMT and FSI industries found IAM being foundational and at the core of each of the top five security threats identified and among the top three initiatives for 2012.¹

---

### Why is access management a concern for senior executives?

What makes effective user access management so important? One only needs to look to recent headlines for an answer:

**Global Electronics and Media Company**

Hackers gained access to over 100 million records, including 12 million unencrypted credit card numbers. The breach also included customer purchase histories, billing addresses, and password questions.

**Email Service Provider**

50 to 60 million customer e-mail addresses were breached, and as many as 250 million e-mails across 75 corporate clients were also exposed.

**Healthcare Services Company**

A computer containing 3.3 million patients’ medical details, including their names, addresses, phone numbers, e-mail addresses, and health insurance plan information, was stolen.

**Managed Care Organisation**

Personal information about 1.9 million current and former policy holders was stolen from a corporate server, compromising names, addresses, healthcare information, Social Security Numbers, and financial data.

**Government Department**

The names, addresses, and Social Security Numbers – and, in some cases, the drivers licenses and dates of birth – of 3.5 million people were inadvertently left on a “publicly accessible” server for over a year.

Breaches such as these can burden organisations with serious, negative repercussions, including:

- Loss of current or future business due to declining customer trust
- Brand impact
- Lawsuits
- Credit monitoring
- Additional expenses associated with investigating the incident, recovering IT systems and data, and dealing with regulators and/or legal authorities

Source: Privacy Rights Clearinghouse.²

---


Many businesses have grown accustomed to doing only what is required to meet audit and compliance requirements, but a key line of defence in protecting company data, business-critical systems, and corporate intellectual property is to confirm the identity of the information requestor using a formalised authentication methodology. Not only does this process have a direct impact on the organisation’s security posture, it is also instrumental in complying with a number of key regulations and standards, such as Sarbanes-Oxley (SOX), the Payment Card Industry Data Security Standard (PCI DSS) and Privacy legislation.

Yet all too often, the processes in place to monitor access – such as requesting and confirming the user’s login credentials – are inconsistent, manually centric, and unreliable.

While this approach may have been adequate in the past, increasing regulatory scrutiny and highly sophisticated threats have rendered traditional authentication methods insufficient – leaving the organisation exposed to significant security threats. Due to the inherent weakness of basic username and password authentication, as well as the need to comply with such requirements as the Federal Financial Institutions Examination Council (FFIEC), some organisations have started implementing “strong” or “multi-factor” authentication techniques. While the approach may differ by organisation, the end-goal is the same: Confirm a user’s identity using two or more unique, hard-to-replicate criteria.

**The basics of strong authentication**

Typically, strong, multi-factor authentication presents two or more challenges to any individual requesting access to a specific resource. These are usually based around three fundamental areas:

1. **Something they know** – Such as a password or PIN
2. **Something they have** – Such as a one-time key from a token, or a security card
3. **Something they are** – Such as a biometric check, including a retina or fingerprint scan
Advanced and evolving threats introduce a new era of risk

As discussed, newer, more sophisticated attacks have become increasingly successful at overcoming traditional security measures.

In particular, the rise of social media and the frequency with which personal information is readily shared online gives hackers better opportunities to understand the individual they are targeting and use this knowledge to guess the answers to password challenge questions. And once they pick the right answer, they are free to change the password and assume an individual’s identity. Add to this the fact that many users employ the same password across many systems, and a single, successful hacking attempt can quickly expand outward and affect a large number of applications and data.

And even though some companies have adopted more robust authentication techniques, such as those based around the use of security tokens, the risk of a breach remains. In fact, a recent compromise of security tokens required a widespread recovery response and forced some organisations to rethink their strategies for safeguarding sensitive information assets.

In light of the way today’s threat landscape is changing, and the inability of established controls to keep pace, one question remains: Do organisations know if and when an unauthorised individual is accessing their critical systems and information? The answer, more often than not, is “no.”

Key terms

- **Identity and Access Management** – A group of services that support the management of users and their authorised access.
- **Authentication** – The methods used to verify a user’s identity prior to granting access to systems or data.
- **Authorisation** – An access-enablement methodology based upon an individual’s pre-approved access rights and other factors.
- **Provisioning** – The management of the user identity lifecycle, including granting and removing approved IT accounts and authorisations.
- **Role-Based Access Governance (RBAG)** – An enhanced approach to sustaining visibility of user roles across the enterprise thus enabling optimal enterprise-wide user and role life-cycle management.
- **Role-Based Access Control (RBAC)** – An enhanced provisioning process that utilises business language and roles to streamline the management of user access.
- **Access Certification** – The processes supporting the periodic review and confirmation of a user’s access rights to IT systems.
- **Single Sign-On** – A family of ease-of-use technologies that allow users to authenticate themselves without having to re-enter credentials for each system being accessed.
- **Federation** – Solutions that authorise access for trusted, external business partners.
Although the sophistication of today’s threats may make it seem as though organisations have no effective means of defending themselves, new techniques designed to combat these attacks are emerging. Specifically, the strongest next-generation solutions will help organisations prevent illegitimate access by leveraging advanced risk-analytics techniques.

Such solutions do so by developing a risk score, which is used to measure the possibility that an access attempt is fraudulent. This score is then weighed against the relative level of risk tolerance assigned to a particular IT asset. This risk tolerance level for a particular IT asset is called a “risk-threshold”. If the risk score when attempting to access this asset is beyond this risk threshold, then authentication controls are automatically elevated to provide a higher level of authentication. Access is ultimately granted or denied based on whether or not the risk score associated with the access attempt exceeds the established threshold (and if it does, whether step up authentication needs are successfully passed).

For example, sensitive applications, such as financial systems, should receive a lower risk score threshold, denying access at the slightest hint of fraudulent activity. On the other hand, less critical resources, like a spreadsheet listing company holidays, would not be subject to the same level of scrutiny and so have a higher risk threshold.
Information security breaches can burden organisations with serious, negative repercussions

Advanced risk-analysis techniques process large amounts of information to produce a risk score.

- **Lawsuits**
- **Loss of business**
- **Brand impact**
- **Loss of consumer confidence**
- **New product launch delays**
- **Loss of intellectual property**

### Login trends
A user historically logs in around 8.30 a.m. Pacific Time, logs out at 6 p.m. Pacific Time, and logs in again around 9.30 p.m. Pacific Time

### Login duration
The user’s evening login typically lasts no more than 15 to 30 minutes

### Geographic Location
The user typically logs in from either Palo Alto, or Sunnyvale, California.

### Usage context
The user routinely accesses the organisation’s systems in the daytime via a company-issued computer

### IP address
A user typically logs in from one of three unique I.P. addresses.

### Device fingerprint
The user typically accesses corporate systems through a company-issued laptop or desktop computer

The goal of the risk score is assign a threshold beyond which access will not be granted.

If the Risk Score is less than the Application Sensitivity threshold the user is granted access.

If the Risk Score is greater than the established Risk threshold, controls are elevated using step up authentication techniques to determine whether access should be granted.
**Use case 1:**

Legitimate employee attempts to log in from office location in Centurion using work computer at 11 a.m. and tries to access the corporate finance system.

**Upon access to corporate advanced authentication system:**

The advanced authentication solution checks the attempt for:
- User ID
- Password
- PIN
- Device Fingerprint
- Geographic Location
- P Address
- Usage Context
- Login Trends

**Current Pattern**
- Entered successfully
- The company issued laptop and in line with pattern
- One of the company locations in Sunnyvale, California and in line with pattern
- Legitimate
- Corporate finance systems and in line with pattern
- During working hours from 8 a.m. to 5 p.m., and in line with pattern

**Outcome:** Pass. User gets access to Corporate Finance system.

**Result:**
- Risk score assigned to attempt: Very Low
- Criticality: Corporate Finance: High || Risk Threshold: Low
- Outcome: Pass. User gets access to Corporate Finance system.

**Use case 2:**

Legitimate employee attempts to log in from OR Tambo International Airport using work laptop at 7 p.m. and tries to access the list of company holidays stored on an internal benefits system.

**Upon access to corporate advanced authentication system:**

The advanced authentication solution checks the attempt for:
- User ID
- Password
- PIN
- Device Fingerprint
- Geographic Location
- P Address
- Usage Context
- Login Trends

**Current Pattern**
- Entered successfully
- The company issued laptop and in line with pattern
- Not one of the standard locations of Palo Alto or Sunnyvale, but close by from a geographic perspective
- Legitimate
- Corporate holidays. Pattern is few times a year
- After working hours working from 8 a.m. to 5 p.m., and not in line with pattern

**Outcome:** Pass. User gets access to Corporate Holiday Calendar page.

**Result:**
- Risk score assigned to attempt: Medium
- Criticality: Corporate Holiday Calendar page: Low || Risk Threshold: High
- Outcome: Pass. User gets access to Corporate Holiday Calendar page.

**Use case 3:**

Hacker attempts to log in from Belarus or Shanghai at 3 a.m. and tries to access the designs for company’s new product stored on an internal development server.

**Upon access to corporate advanced authentication system:**

The advanced authentication solution checks the attempt for:
- User ID
- Password
- PIN
- Device Fingerprint
- Geographic Location
- P Address
- Usage Context
- Login Trends

**Current Pattern**
- Entered successfully
- Unknown device and in not line with pattern
- Not one of the standard locations of Palo Alto or Sunnyvale, and from a higher risk location
- Legitimate
- Product design. Pattern is never
- Outside of working hours or access from home hours and not in line with pattern

**Outcome:** Fail

**Result:**
- Risk score assigned to attempt: Very High
- Outcome: Initial test fails. Additional authentication is requested (e.g., entering one time code sent to the employee’s phone). Since the hacker does not have access to this (phone in this example), additional authentication fails and access is denied. A legitimate user would be able to provide the appropriate information and get access. Outcome: Fail
What the data says

The top security treats in 2012

- Mobile devices (34 percent)
- Security breaches involving 3rd parties (25 percent)
- Employee errors and omissions (20 percent)
- Faster adoption of emerging technologies (18 percent)
- Employee abuse of IT systems and information (17 percent)

Leading drivers and priorities

- The leading drivers for financial institutions to protect the privacy of their client’s information are:
  - Privacy regulatory requirements (79%)
  - Reputation and brand concerns (70%)

- The top three information security priorities of financial institutions are:
  - Security Regulatory Compliance
  - Data Protection and Information Leakage
  - Access and Identity Management

Key Findings

Research show that organisations:
Haven’t changed substantially in their approach to information security ...

However, significant change is noted regarding heightened attention overall for Threats to information security

Figure 1: How often did your organisation experience an information security breach in the past 12 months?

Data taken from a recent 2011 Security Study:
The newest generation of risk analytics leverages various types of information and patterns to build a risk score.

<table>
<thead>
<tr>
<th>Information source</th>
<th>Baseline</th>
<th>Possible deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login trends</td>
<td>User historically logs in around 8.30 a.m. Pacific Time, logs out at 6 p.m. Pacific Time, and logs in again around 9.30 p.m. Pacific Time.</td>
<td>Does the current login attempt follow these timing trends?</td>
</tr>
<tr>
<td>Geographic location of previous login attempts</td>
<td>User typically logs in from either Palo Alto, or Sunnyvale, California.</td>
<td>Is the current login attempt occurring at, or between, these locations?</td>
</tr>
<tr>
<td>Devices used in previous authentication attempts (device fingerprint)</td>
<td>User typically accesses corporate systems through a company-issued laptop or desktop computer.</td>
<td>Is the current attempt originating from one of these known devices?</td>
</tr>
<tr>
<td>Applications or data being accessed</td>
<td>User’s job function requires working with four specific business applications.</td>
<td>Is the she currently attempting to access these, or something unrelated to her organisational role?</td>
</tr>
<tr>
<td>I.P. address usage</td>
<td>User typically logs in from one of three unique I.P. addresses</td>
<td>Is the current login attempt originating an I.P. address outside of the normal set, even if it is coming from a known device?</td>
</tr>
<tr>
<td>Login duration</td>
<td>User’s evening login typically lasts no more than 15 to 30 minutes.</td>
<td>Is the user currently logged in for a duration that is well beyond his average range?</td>
</tr>
<tr>
<td>Usage context</td>
<td>User routinely accesses the organisation’s systems in the daytime, via a company-issued computer.</td>
<td>If a different, though recognised, device is being used for a daytime login attempt, does this indicate that an intruder is trying to access organisational resources from the user’s home?</td>
</tr>
</tbody>
</table>

In addition to the information described in the above table, organisations should consider such additional data points as:

- Is the user typing around the same rate of speed he has in the past, or is it suddenly faster or slower?
- Is the user downloading large volumes of information, when his normal activities would involve looking at a limited number of records?

Based on the risk score derived from this data, the user’s current attempt may fall within a threshold that grants access to a less-sensitive system, but not one that is more critical in nature. Additionally, an organisation may elect to allow certain applications of lower importance to be accessed, despite a login attempt generating a high risk score.

And to prevent legitimate individuals from being denied based on false positives – such as when a user tries to check e-mail using an unknown device during her vacation – offline communication channels can be utilised for a one-time confirmation. This could come in the form of a text message containing a single-use password granting the user the access she needs. This is an example of a “step-up” authentication technique used as illustrated in use case 3 (page 8).
Implementing Role Based Access Governance (RBAG) as the context within which risk based access control is used strengthens the governance of the user lifecycle. However, successful RBAG is only possible with excellent analysis of business and system roles, privileges, connection origins, user activity logs, nature of access, information resource classification and system type.

Advanced risk-based analytics (ARBA) represent an emerging and evolving solution set. Thus far, only those companies on the leading edge of RBAG adoption have implemented these technologies. This trend needs to change – and now. Many of these solutions are not yet mainstream and should not preclude organisations from researching what RBAG and ARBA solutions are currently available and choosing an option that best fits their needs.

One of the worthwhile advanced methods of risk based analytics is the use of Artificial neural networks like Self Organising Maps (SOMs) which can represent a high number of variables (dimensions) into a visual map where similar observations are plotted next to each other. Applying this type of artificial intelligence to the logs and incidents from your IAM data can generate insights that wouldn’t normally be obvious from a manual review of such data.

In order to ensure that critical applications and data, as well as brand reputation, are secured for the long term, executives must determine the organisation’s current level of risk exposure and the value that is provided by their existing IAM solutions. Meeting with the IT leaders in charge of these technologies to answer to the following questions is in order:

- Do we have the right metrics in place to identify risks around access and authentication?
- Can we recognise patterns around user access behaviour? If so, how are we currently using this information?
- What risk-mitigation techniques do we have in place to respond to these advanced threats?
- What is our timeframe for deploying an advanced risk-based authentication solution?

These questions are important to organisations that have already implemented IAM technologies, as they present opportunities to improve and optimise existing solutions. Organisations that do not currently have the most robust measures in place can use this conversation as a way to gain a competitive advantage over companies operating legacy risk profiles, and presents an opportunity to skip a generation of technology and get on board with what is fast becoming the new baseline.

Examples of SOMs include:

Understanding whether issues are pervasive to the IT environment or limited to a specific application can not only focus response efforts but also significantly enhance early detection and possibly reduce response times to security incidents.

Finance Application

Figure 2: IAM Issues that are centred around a specific application

Providing a view on IAM issues that affect a single user versus issues that affect larger groups of users. This type of intelligence can direct your responsive efforts to the critical areas.

Figure 3: IAM issues affecting a single user
Decisions should be made in a measured manner that considers a number of variables. However, the rapid proliferation of smartphones, tablets, and off-premise, cloud-based systems and infrastructures mean the need for robust trust and authentication measures have never been greater. As such, the earlier executives start having these conversations with IT leaders, the better suited they will be to gain an understanding of their existing risk profiles and current ability to handle threats.

Executives should challenge their teams to:
1. Assess: Determine your business need and where your applications stand towards supporting these. Build a strategy and prioritise applications by importance. Understanding the Business Value of a system and comparing this to its technical soundness can provide a strong indicator for systems that should be covered by the IAM (Refer Figure 4)
2. Evaluate: Investigate the available solutions and determine how each can address the evolving threat landscape.
3. Pilot: Perform a pilot with the solution that best meets the needs based on the evaluation and confirm fit for the enterprise
4. Expand: Apply lessons learned from the pilot and expand the solution to applications in a phased manner based on prioritisation.

Challenges – and their requisite solutions – vary from company to company, and there is no one-size-fits-all approach. The key is for business and IT leaders to work together to find the right fit for the organisation. While every solution must reflect operational and regulatory requirements, some standard approaches do apply:
- Smaller organisations with relatively low risk profiles may elect to move forward with the technologies available today, or implement additional layers of security as they wait for solutions to mature or become more economical
- Larger institutions that carry a greater amount of risk may not be able to wait this long, and instead, should consider developing custom solutions that fit their needs

Regardless of the size of the organisation or the approach it adopts, one thing remains clear: Decisive action must be taken before the enterprise is breached.

Figure 4. Using advanced analytical methods to graphically clarify complex issues such as system views
Contacts

Dave Kennedy
Service Line Leader – Risk Advisory
Deloitte South Africa
Cell: +27 (0)82 780 9812
Email: dkennedy@deloitte.co.za

Cathy Gibson
Director – Risk Advisory
Deloitte South Africa
Cell: +27 (0)82 330 7711
Email: cgbison@deloitte.co.za

Shahil Kanjee
Director – Risk Advisory
Deloitte South Africa
Cell: +27 (0)83 634 4445
Email: skanjeer@deloitte.co.za

Navin Sing
Director – Risk Advisory
Deloitte South Africa
Cell: +27 (0)83 304 4225
Email: navising@deloitte.co.za

Derek Schraader
Director – Risk Advisory
Deloitte South Africa
Cell: +27 (0)79 499 9046
Email: dsschraader@deloitte.co.za

Marius Alberts
Director – Risk Advisory
Deloitte South Africa
Cell: +27 (0)82 450 7387
Email: maalberts@deloitte.co.za

Etienne Ward
Director, Risk Advisory
Deloitte South Africa
Cell: +27 (0)82 416 3519
Email: etward@deloitte.co.za

Jens Kock
Partner, Risk Advisory (Namibia)
Deloitte Namibia
Tel: +264 (0)61 285 5003
Email: jkock@deloitte.co.za

Julie Akinyi Nyangaya
Risk Advisory (East Africa)
Deloitte Kenya
Tel: +254 20 423 0234
Email: nyangaya@deloitte.co.ke

Tricha Simon
Risk Advisory (Central Africa)
Tel: +263 4 74 6248
Email: tsimon@deloitte.co.zw

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (DTTL), a UK private company limited
guaranteed, and its network of member firms, each of which is a legally separate and independent
entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte
Touche Tohmatsu Limited and its member firms.

This communication is for internal distribution and use only among personnel of Deloitte Touche
Tohmatsu Limited, its member firms and their related entities (collectively, the “Deloitte Network”). None
of the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies
on this communication.

© 2013 Deloitte & Touche. All rights reserved. Member of Deloitte Touche Tohmatsu Limited

Designed and produced by Creative Services at Deloitte, Johannesburg. (806185/sue)