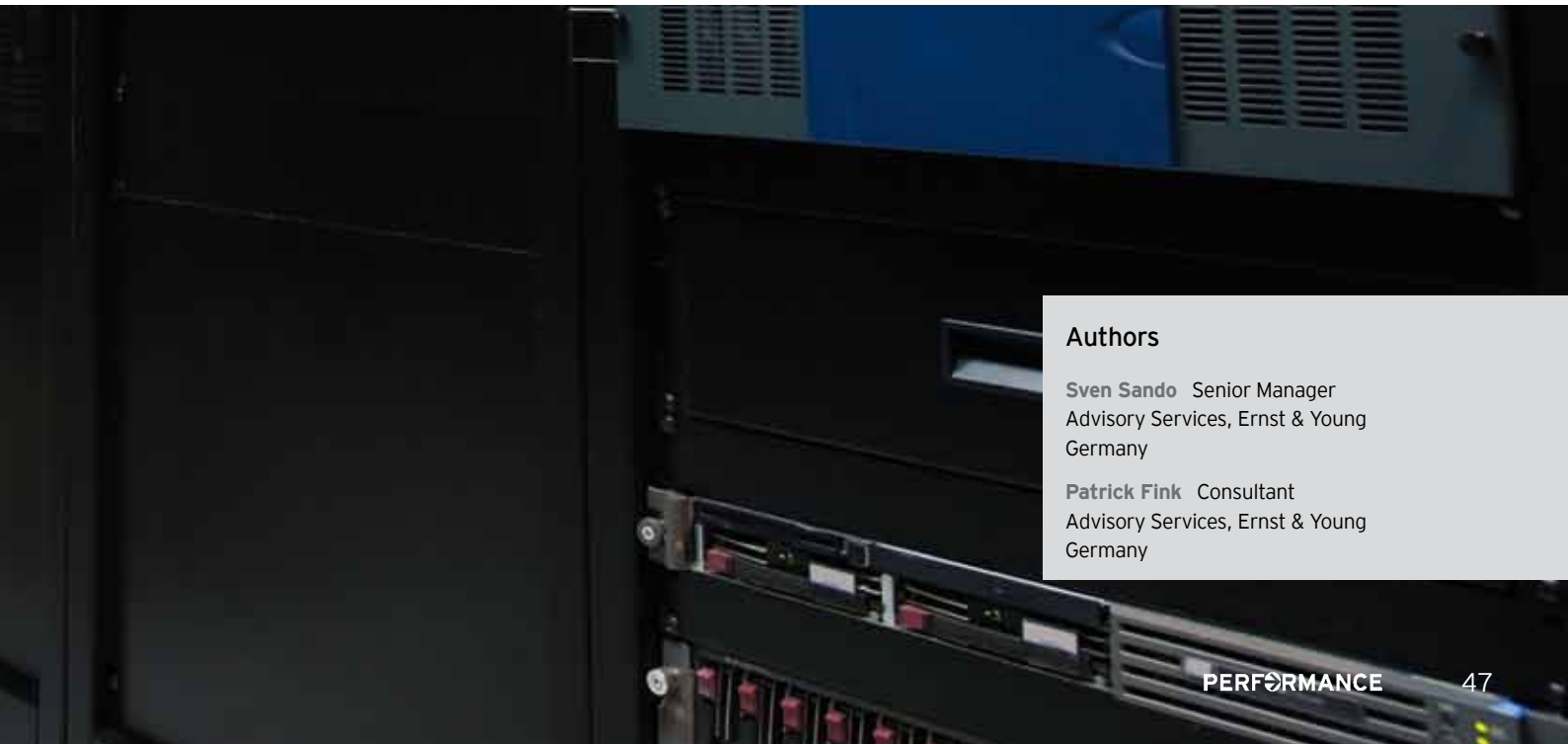
Article

Off limits: controlling the level of information access for employees

In today's corporate environment, protecting invisible assets such as information is just as important as protecting physical assets. Companies should safeguard sensitive information by investing in a good identity access management system that controls employees' data access rights, whether they are working in the office or remotely. For businesses today, looking after their data means looking after their reputation.



Authors

Sven Sando Senior Manager
Advisory Services, Ernst & Young
Germany

Patrick Fink Consultant
Advisory Services, Ernst & Young
Germany

We are moving to a "dual-use environment" in which people use devices, laptops or mobile phones for both corporate and personal use

In most companies, employees work on a need-to-know basis that dictates how much or little they know about the business. Giving them the information they require to perform their duties is considered more than enough. Anything else would be, at best, unnecessary and, at worst, potentially harmful to the business.

Should a secretary tasked with arranging meetings and answering telephones have access to more sensitive information such as company accounts? The general consensus among most managers is no. Not only is this information completely irrelevant to that person's job, but it can also be damaging if unwittingly or knowingly passed on to others within or outside the company.

To limit the chances of sensitive information falling into the wrong hands, most companies have identity access management (IAM) systems assigned to their IT networks. Created by software developers such as Oracle, IBM and Verizon, IAMs are security systems that give employees access via their computers to job-related resources and applications. Restrictions are also in place to prevent workers from accessing information that has no relevance to their specific roles.

In general, employees are assigned usernames and passwords that grant them certain privileges and allow them to use applications or enter specific networks within the business. The access management system is typically linked to a main directory containing the details of every staff member. Through that database, the IAM prescribes levels of access based on a person's job title and status.

For example, a credit controller responsible for chasing invoice payments could view spreadsheets that show how much debt the company is carrying and which clients still owe money. But that same employee would probably have no access to the business' five-year growth strategy – a privilege that is generally reserved for senior executives and directors.

Security is another reason to monitor and restrict the networks and applications that people can either enter or use. Andrew Braunberg, an IAM expert who worked with business network and IT services specialist Current Analysis for more than 11 years, says that disgruntled employees pose the biggest threat.

Problems often arise when a salesperson has been fired or made redundant, according to Braunberg. Some employees will try stealing client information or sales figures – data available to them during their time at the firm – before leaving. To eradicate the risk, companies must have the capacity to block an employee's access to sensitive information instantly.

Visiting clients and guests also have to be accounted for when establishing an IAM system. Business partners or job candidates who wish or need to use the internet, for example, would not be afforded the same access rights as someone working full-time in the company.

Risky business: what happens when companies overlook access management

In our experience, allowing employees to roam freely through a corporate IT system and database is a dangerous exercise. We've worked with a number of companies that have paid the price for not establishing clear data boundaries.

In one example, a human resources employee created a fictitious worker on his company's database. He then added his own bank account details to the non-existent staff member's profile to claim a second monthly salary. The fraudster was authorized to access many company databases, enabling him to carry out the deception.

But it's not just about losing money; the loss of intellectual property is one of the biggest risks facing companies with limited controls on access management.

We recently worked with a large industrial company that had taken an innovative new product to market. Shortly after the launch, a rival business released an almost exact copy with some minor adjustments – it featured a different component and was made from another material.

Just before going to production, the industrial company behind the original tool decided to make a small change to one of the components and used a different material to produce it. The adjustments were never incorporated into the final set of drawings that the rival business managed to get hold of.

Realizing that the designs were slightly different to the industrial company's final product, the rival business could reproduce the tool

from the drawings without breaching any copyrights. This incident provides an important lesson for businesses dealing in intellectual property: without access management restrictions in place, sensitive information, with or without copyright protection, could easily be leaked to a rival organization.

Establishing IAM systems in the banking sector

The level of security that companies apply to their internal networks is often up to them. Other businesses, however, have no choice but to establish IAM systems to satisfy a regulatory requirement.

In Germany, Deutsche Bundesbank and the Federal Financial Supervisory Authority recently introduced new regulatory guidelines for all banks and financial institutions. Among them, industry players must have access management systems in place to control how much internal data employees can view.

Given that German bank databases collectively hold the personal details of millions of customers, it is imperative for financial institutions to have sophisticated IT security. Allowing all bank staff to have access to account holders' details could be disastrous. If such information were stolen or leaked by an employee, the financial institute would face a barrage of questions from its shareholders and the industry regulator. The public relations fallout of such an event would be an additional headache.

In 2011, ING Direct Australia implemented an IAM system to limit the number of employees with unverified access to core banking networks and applications.[1] The issue needed to be addressed so that ING could comply with the Australian Regulatory Authority's regulations covering access rights.

Access management software IdentityIQ was eventually chosen to cover access rights for more than 1,200 users within ING. Some two months after setting out to improve its IAM system, the financial institute was able to control access rights to business policies, manage risk and remove the possibility of a rogue employee gaining access to financial records.

Introducing the software also allowed management to see who within the firm could access banking applications that were generally off limits to most employees.

ING's success illustrates the importance of investing in high-quality IAM software. Not only does it enable companies to comply with regulatory guidelines regarding access rights, it also gives them peace of mind about the security of their data. In an age when information is a company's most valuable asset, maintaining control over it is more important than ever.

1 www.cio.com.au/article/430697/ing_direct_australia_removing_identity_management_risks/

The public is becoming increasingly alarmed about privacy and identity theft, which is affecting business operations

Access management trends

In March 2012, technology research company Gartner identified six trends that will drive the evolution of access and privacy management. In its report, the company said that corporations would increase their focus on identity and privacy within the workplace.

The key trends cited in Gartner's research are tactical identity, authorization, identity assurance, the identity bridge, policy battles and the sea of tokens. What follows is a summary of the issues related to IAM's evolution.

- **Tactical identity**: Budgets for identity management projects will remain constrained. Projects with too broad a scope and a lack of focus on business values tend to fail. To address this, IAM projects will be limited in scope to ensure success.
- **Identity assurance**: Demands for stronger authentication and more mature identity provider infrastructures and practices will intensify. Serious deficiencies in both these areas, and in credential issuers, came to light in 2011. Organizations have to trust IAM software developers to complete a job as instructed. They must also understand the consequences for any service providers that fail to meet their obligations.
- **Authorization**: Regulatory pressure and more complex IT will increase the need for personnel authorization within organizations. Authorization is about creating and enforcing access control, which helps companies monitor what people are looking at. While relatively immature at the moment, authorization will become a first-class business function in most companies.
- **The identity bridge**: A new architectural component is needed to manage the flow of identity information among cooperating organizations. Managing federated identities is a complex task, and the protocols for federated provisioning and management of identity policies and attributes is immature.
- **The sea of tokens**: Identity information has to be transformed by each domain that receives it, and then passed on to downstream domains. Identity information is transmitted via tokens, which are becoming more modular and more flexible.
- **Policy battles**: The public is becoming increasingly alarmed about privacy and identity theft, which is affecting business operations. The business community, law enforcement agencies and national security organizations will continue to wrangle over identification and privacy laws and regulations – and this will continue to drive changes in identity infrastructure.

Legal matters: the laws and regulations surrounding access management

- The growing complexities of modern business are putting increased pressure on an organization's processes and its supporting IT systems. Moreover, companies are duty-bound to meet new requirements and government regulations.
- In addition, organizations need to comply with IT regulations, as well as international and country-specific regulatory frameworks. These include:
  - The minimum requirements for risk management (MaRisk)
  - ISO 27002, Section 10.10, 11-11.3.1.
  - Generally accepted principles of computer-assisted accounting systems
  - IDW PS 330 and FAIT 1
- A series of accounting and corporate scandals involving businesses from around the world has ensured that corporate compliance is now a major global business issue. These scandals triggered a move toward greater corporate governance regulations, controls and anti-corruption laws, such as the Sarbanes-Oxley Act.

Mobile devices: how to control mobile access to information

If necessity is the mother of invention, the rise of mobile devices can be attributed to society's need for constant connection with family, friends and work colleagues. Throughout the Western world, laptops, smartphones and tablets are now as ingrained in people's lives as televisions or desktop computers. Whether by talking, texting or interacting through social media, people now have the means to communicate with one another at any time of day.

In Braunberg's words, we are moving to a "dual-use environment" in which people use devices, laptops or mobile phones for both corporate and personal use. While great for our social lives, mobile devices have created another headache for companies' IT departments. People can now access applications and networks through their smartphones and tablets – something that companies have to account for when setting up IAM systems.

The corporate device of choice is the BlackBerry, which has been around for several years. In that period, companies have had time to establish levels of access for people using BlackBerrys by introducing network management software. But smartphones and tablets are more recent innovations, so IT experts within large and medium-sized corporations are still working out how to apply the same levels of access for people who own such devices.

Several mobile device management and security companies are developing software to address this issue. In the meantime, business chiefs have to decide whether to allow people with smartphones and tablets access to corporate networks.

Taking the health care industry as an example, today's technologically-savvy doctor might use an iPad to record a patient's condition while doing his rounds in a hospital. When in the building, the doctor could reasonably expect to have access to all of his patients' medical records. But Braunberg believes that those same privileges might not be available away from the workplace.

Access would be restricted if the doctor were in a bar or at home, for example. For this to work, an IAM system that governs access to networks and applications, based on an employee's proximity to their place of work, would be required.

Some experts believe creating applications that control whether the mobile device is being used for social or work purposes is the way forward. At work, the phone or tablet would automatically switch to corporate mode, giving employees access to whichever networks they require. Away from the office, the device would operate in social mode, removing all access rights for work-based applications.

Industry players must have access management systems in place to control how much internal data employees can view