October 2023

The Role of Identity and Access Management in Enabling Digital Transformation

WHITEPAPER

- IT Security
- Identity and Access Management
- Identity Management Strategy
- Identity Governance Solutions

IT security as a successful concept for digital transformation

In the course of the digital transformation, computers are assigned more tasks and become interconnected. This offers a correspondingly larger potential attack surface and carries the risk of devastating consequences in the event of targeted cyberattacks. Currently, two out of three companies are already under attack, so digitalisation has significantly multiplied the complexity and vulnerability of IT and OT security. There is no simple solution here. Understanding the individual components and systems alone is already demanding, but in combination, an almost unmanageable complexity is achieved.

It is essential to take a holistic view of the company and to know the entire life cycle of security risks in order to create a comprehensive concept as well as a strategy and implementation. This includes end users and their identities, endpoints, remote access, cloud security, data storage locations, human vulnerability and employee awareness of IT security. In the process of creating a digitalisation strategy, companies should include several success factors in the area of IT security such as management support, information security policy and information security education, training and awareness.

In PATECCO latest whitepaper, we will provide you a clear understanding why IAM is a fundamental part of the security of the information systems and how it will ensure a successful digital transition for your company.

The series of articles describe the role of Identity and Access Management in digital transformation which is integral to an organization's overall security posture, adaptability, and resilience against evolving cyber threats. As the digitalisation continues to evolve, IAM will remain a foundational element of that process. It enhances security, simplifies access management, supports compliance, and contributes to the overall success of digital initiatives. An effective IAM strategy ensures that the right people have the right access to the right resources, empowering organizations to innovate, grow, and adapt in the digital age.

Let’s get started!

The reason why Identity and Access Management is the key to digital transformation

The most important investment that can be made in the digital transformation is an investment in technology that supports employee mobility, security and productivity. One such investment is identity and access management.

The core task of digital transformation is to rethink existing business models with the help of technology. It is a significant understatement to say that this discipline has received more and more attention in recent years. Digital transformation has long been at the top of companies' priority lists. It makes sense that digital transformation is receiving this attention. Because most companies are aware of these benefits:

- Digital transformation creates growth opportunities in new markets
- Digital transformation makes it possible to keep pace with constantly changing customer behaviour
- Digital transformation makes companies fit to compete in an increasingly competitive marketplace
- Digital transformation makes it easier for companies to meet increasing legal and compliance requirements.

However, many organisations find it difficult to tackle the transformation process. This is mainly due to a lack of resources and a limited budget.

Investment in organizational culture must come first

To achieve transformation, the company often needs to invest in modern technologies and IT tools. This means allocating large sums of money to cybersecurity, cloud computing, Internet of Things and blockchain technology. At least that's what many people wrongly assume. And yes. Of course, transformation requires investment to get it right. But transformation is as much about rethinking corporate culture as it is about investing in new, highly touted technologies.

The most important technology investments that can be made as part of digital transformation are those that support employee mobility, security and productivity. These are precisely the parameters that form the basis for a successful transformation of the corporate culture and business foundation.

Why Identity and Access Management is the key to digital transformation

One of these investments is automated user management - identity and access management. And it is an indispensable discipline when implementing a digital transformation project. An identity and access management platform is essential to ensure that employees always have access to the right resources and data - securely and efficiently. This has a massive impact on the overall productivity of the business.

The need for an identity and access management platform has only been amplified by the coronavirus epidemic. During the epidemic - and in the aftermath - all organisations have been working hard to accelerate digital transformation, with the aim of adapting the organisation to new technological requirements, organisational disruption and new ways of working. Identity and access management can help organisations adapt to external disruptions and, most importantly, support and drive digital transformation.

Digitisation begins with secure digital identities

The digital transformation is picking up speed and changing the way business is done. One keyword here, for example, is the omni-channel approach. Cost pressure in global competition requires a level of automation that can only be achieved through digital processes.

Many companies - also in the SME sector - are facing major business challenges today. While digital transformation offers numerous advantages, such as more efficient workflows or more informed decision-making, it also creates areas of tension between fast, simple implementation and the security needs of companies. In addition, government requirements such as the GDPR must be implemented. This requires the introduction of new, suitable structures that increase the level of security. Another aspect is the interaction with customers. It mainly takes place digitally. To communicate successfully, companies must manage digital customer identities on all channels. Especially in the SME environment, there is a lot of catching up to do. Furthermore, IT security should increase, but the costs for it should decrease as much as possible. In addition, a short time-to-market is critical for opening up new markets.

The solution to these challenges lies in digitalisation and - along with it - the secure and efficient management of digital identities of users such as employees, customers and third parties, administrators and "things" such as machines, applications and AIs.

As a result of digitalisation, digital identities of the three groups administrators, users and things are becoming more and more important, because they represent these groups in cyberspace and from there more and more processes are controlled that have an influence on the physical world. Smooth, innovative processes and security therefore require IT security, which in turn requires the protection of digital identities.

Companies invest a lot of money in IT security overall, but unfortunately mostly in classic endpoint protection. As a result, they neglect the protection of digital identities, which is why serious data breaches occur time and again. According to Bitkom, the damage suffered by German companies as a result of these was 55 billion euros in 2016. In 60 percent of all data breaches, the cause is incorrect authorisation management by current or former employees.

Companies that rely on a modern Identity and Access Management (IAM) system, on the other hand, have a 50 percent lower chance of falling victim to a data breach. So with a modern solution for IAM, companies close countless security gaps and take IT security to a whole new level.

IAM should also play a central role in the IT security strategy of all companies, because in today's digital economy, security and the productivity of the entire company are inextricably linked to the secure management of digital identities and appropriate access management. However, IAM not only ensures access management, but also optimises it: the core task of IT security is to allow

authorised users and prevent unauthorised access. Digital identities make this distinction possible, because they are also linked to authorisations for IT systems, applications and data. They can be used to grant and revoke access easily on a role basis.

IAM also offers other advantages. When onboarding new employees, they quickly get exactly the permissions (and none beyond) they need for their work thanks to IAM. The rapid provisioning of rights, adapted to the role in the company, accelerates the onboarding process. Employees can start their work more quickly and have only the rights they need for it - this ensures more efficiency and higher security.

Since their identity is verified, employees can also manage many things on their own via self-service. This minimises helpdesk queries and relieves the IT department. The right IAM solution also enables companies to integrate all services and applications of their choice - regardless of whether they are obtained from the cloud or hosted in their own data centre. Access governance, on the other hand, enables companies to prove, among other things for audits, which employee had access to what at what time. Single sign-on is also possible via IAM. Employees do not have to constantly log in again, helpdesk enquiries due to forgotten passwords are almost completely eliminated and satisfaction increases.

It is also important to implement strict authentication (multifactor authentication) for some scenarios. Adaptive MFA is recommended for reasons of motivation and efficiency: employees generally work with single sign-on and only have to perform the slightly more complex but more secure MFA if they want to access particularly sensitive systems or if the access seems unusual, for example because it takes place outside normal working hours or from an unusual location.

Thanks to the use of microservices and containers, the requirements of the respective companies can be flexibly addressed, with less adaptation effort than with conventional IAM integrations. The use of DevOps principles enables agile development patterns and thus extremely short development cycles. Instead of "one size fits all", with the "custom-fit" approach customers get individually adapted IAM solutions, managed from the cloud.

In this way, medium-sized companies benefit from the security advantages of a well-customised IAM solution. The occurrence of data leaks despite high spending on IT security shows: Digital identities must be protected with IAM and authorisations must be controlled more precisely. Then the digital transformation can succeed and digital risks can be efficiently contained. Whereas the disadvantages of the two conventional deployment options often prevented a planned integration of IAM in the past, a realistic option is now also available to medium-sized companies.

IoT: Do you have a strategy for Identity Management in your company?

Do you notice when your data is accessed without permission? What is the situation in your company regarding identity and access management and IoT environments?

Do you have an overview of all eventualities? Every device, every application and every interface needs an identity so that it can be accessed securely. Only if you monitor this can you prevent privacy-violating behaviour.

In a world of connected people, systems and things, the Internet of Things (IoT), identity and access management (IAM) is changing rapidly and constantly. The challenge is to manage some and keep others out. Digital transformation, the global enterprise environment and the consumerisation of information technology have put identity and access management at the heart of digital business.Originally a means to manage user identities and access to systems or devices, IAM is now used to uniquely profile users. On the one hand, you need to track their needs and behaviour, and on the other, increase efficiency and engagement.

Digital transformation projects offer considerable added value. However, they can also put more of your resources at risk and increase the attack surface for corporate security. But you have no choice, you have to stay in the game.

The market is divided into provisioning, single sign-on, advanced authentication, audit, compliance and governance, directory services and password management. A powerful IAM platform can play a critical role for all organisations managing customer, business partner and device identities. This is especially true as these continue to grow. Dealing with these identities, protecting sensitive data and end-to-end authentication, can be extremely costly without an IAM platform to manage these complex processes.

It's no wonder that the high level of complexity within multi-level partner and user relationships significantly increases the risk of a security breach. Here are a few crucial facts:

- Every year, one in four companies will suffer a major data breach.
- The average cost of a data breach is $3.6 million, with an average 5 per cent drop in share price.
- Fines for security breaches are expected to increase by 4,500 per cent.
- 53 per cent of data breaches result from human error.
- 34 per cent of cybercrime is committed by an insider.

What security risks do IoT environments pose?

The Internet of Things (IoT) connects about 20 billion devices all over the world, which increases the security risk exponentially. Heterogeneous and fast-paced IoT environments dramatically increase the attack surface that product managers and asset operators must protect. The days of static policies and traditional identity and access management are long gone.

Digital transformation and IoT require new identity and authorisation management techniques that are dynamic, transient and contextual.

What you should pay attention to be able to manage identities better:

- Secure information exchange with a large network of external organisations
- Integrated support for external enterprise constructs and access management at multiple levels
- Cross-organizational delegated administration that supports a multi-level organisational hierarchy
- "Out of the box" support for integration: from the cloud to enterprise WAM and legacy applications
- Ease of use and simple support from a true cloud-native application provider

A sound strategic approach to IAM can lead to real savings and added value. To name a few: Reducing software costs with cloud IAM, reducing the attack surface with a single sign-on (SSO) model, and lowering the cost of potential penalties for compliance breaches.

These are just a few of the benefits that PATECCO has delivered to enterprises for more than 15 years. Our platform is unique in its ability to manage not only the identities of people, systems and things, but also the dynamic permissions to securely share data with each other.

But you have to decide which approach you want to use. Here are some thoughts:

- How do you manage all the external identities that come into contact with your company?
- Do users have access to all those resources they need for the success of the company?
- How do you ensure that all interactions are secure, authorised and compliant?
- How do you remove companies and users when access is no longer needed?
- How much money do you spend each year on fines resulting from data breaches?

The fact is that IAM and IoT is a fast-paced, ever-changing challenge. They cannot afford to lose in this game. But you have no choice: you have to play.

How the Modern Identity Governance Solutions Enhance Security of the Digital Enterprises?

In times of progressive digital transformation, Identity governance is one of the most neglected branches of cybersecurity. That is why it is crucial for the enterprises to adopt or to update their current identity governance. And before implementing or updating such identity management tools, the companies should ask several important questions such as: How they ensure the permissions their users have are appropriate to their roles? Can enterprises prevent users from accumulating unnecessary privileges? How can enterprises improve their visibility into their users' identities?

In case your corporation enterprise doesn't take these questions into account, you may face challenges with external and internal threats. It is critical for the companies to be able to see, understand and govern their users' access to all business applications and data. This turns identity into a business enabler for organizations, helping them to properly secure and govern all of their digital identities at the speed of business today.

Identity is not only a number of employees

When talking about identity governance, enterprises often think only about the individual users operating under their scope: their employees. That's ok, but the corporations must bear in mind their contractors, partners, and other third parties when considering access management and identity governance in 2024. If all these groups of people have access to the network, their permissions should be as strictly controlled and monitored as any of your employees.

Furthermore, your identity governance in 2024 must extend beyond the identities of people including also the identities held by applications and software. These can move through your network and access data in much the same way a human user can. Allowing them free govern in your databases can only lead to serious issues. So, application identity governance tools are only going to become more important as cloud applications and cloud architecture continue to transform enterprises.

Identity Governance could be effectively combined with PAM

In fact, maintaining proper role management through identity governance makes a key assumption. Specifically, the users logging in are the users to whom the account belongs.

Bad circumstances such as password sharing, stolen credentials, and phishing attacks can place your employees' identities at severe risk; this applies doubly if the employees in question have significant administrative powers within the network. By incorporating robust privileged access management with your IGA solution, you can prevent hackers and insider threats from turning

your role management against you. This can include implementing granular authentication, implementing multifactor authentication, and deploying behavioural analysis to observe discrepancies.

The benefits of modern Identity Governance solutions

Nowadays the benefits of modern Identity Governance solutions go beyond security. Modern Identity Governance solutions empower organizations with automated workflows that can streamline access requests, detect permission discrepancies, and handle temporary assignments to help your IT team prioritize other projects, thus, eliminating human errors. Organizations can also manage their non-employee identities e.g. - third-party vendors or partners without disruptions and ensure strict monitoring of their access in the network. Without proper identity access governance, it is challenging for organizations to assign and keep track of the applications and resources that identities have access to. Some organizations have hundreds, even thousands of applications.

Here are several important ways that identity access governance benefits your business:

Visibility

Let's say it right: you can't protect what remains unseen. That is why visibility represents the heart and soul of cybersecurity. Identity governance provides visibility and monitoring over employee and user permissions. Also, it helps IT admins get a high-level view of what's happening across the IT environment, allowing them to quickly make changes and troubleshoot problems that could have easily become worse if left untreated.

Streamlined User Identity Lifecycle Management

When onboarding and offboarding, managers and IT personnel typically had direct physical access to the resources that they needed to manage and change, but now that's not necessarily the case. This means that new solutions need to be leveraged to maintain the proper level of control over users, devices, networks, and other IT resources, and this is where an IGA solution becomes integral.

Enhanced Compliance and Security

Identity governance also helps businesses meet their compliance needs. Almost all IGA solutions provide out-of-the-box compliance reports for easy fulfilment; additionally, it can often fill those reports automatically, alleviating a burden on your IT security team. The modern Identity Governance solution reduces risk and improves compliance and security by managing access control in a comprehensive and streamlined manner. By using tools that streamline user identity lifecycle management, your organization is at less risk for the wrong users having access to confidential information, and you have higher visibility into what different users do and do not have access to.

Risk Management

IGA solutions enable a robust approach to managing and governing access by focusing on three aspects of access. First, they practice least privilege access, eliminating excess privileges and granting access to only those who absolutely need it in order to do their jobs. Secondly, they

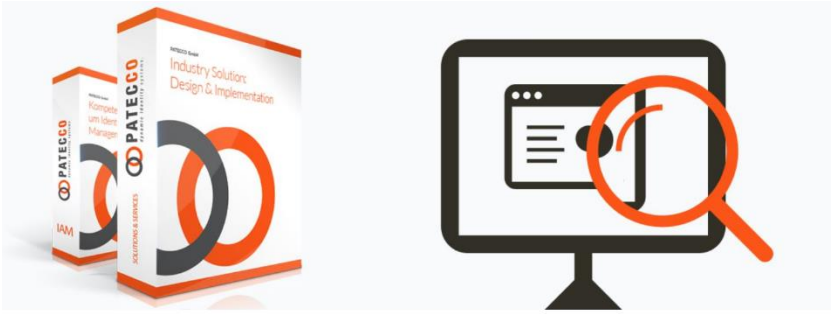
terminate “orphaned” accounts as quickly as possible. These accounts that are no longer being used, either because an employee is no longer with the company, or any other reason, are perfect targets for those looking to breach the environment. Finally, IGA solutions monitor for segregation of duty (SoD) violations. This critical risk management concept dictates that no single individual should be able to complete a task, creating a built-in system of checks and balances.

With these clear, measurable benefits, it’s easy to see why Identity governance solutions are quickly becoming an essential component in many organizations’ security strategy. Identity governance is not a panacea. It must be a part of a comprehensive cybersecurity platform, made of well integrated and well-thought-out solutions

About PATECCO

PATECCO is a privately held German company providing services in the areas of the development, implementation, and support of Identity & Access Management solutions.

The company delivers comprehensive solutions based on latest technologies such as Cloud Access Control, Privileged Account Management, Managed Services, Access Governance, Identity Governance and Intelligence, Role-Based Access Control, Security Information and Event Management, Recertification and Asset Management. Its long-term partnership with IBM, Microsoft and One Identity supports the success in a number of international consulting projects.



PATECCO GmbH

Tel.: +49 (0) 23 23 - 9 87 97 96
Ringstrasse 72 - 44627 Herne
E-Mail: info@patecco.com
www.patecco.com