Deep Science Publishing
https://doi.org/10.70593/978-93-49910-74-4_6

DeepScience
Open Access Books

Chapter 6: Identity and access management for insurance: challenges and solutions

6.1. Introduction to Identity and Access Management

Insurance organizations are on a digital transformation expedition that seeks to bolster operational efficiency and increase customer satisfaction through enhanced product development and service delivery. This transformation is enabling Insurance organizations to address the constantly evolving expectations of insurers, as well as cater to shifting demographics. In responding to the push for increased access to new-age services, Insurance organizations have partnered with third parties that constitute an extended enterprise ecosystem. However, as Insurance organizations expand, embracing third parties for operations, the threat environment increases. There is also a continued concern that digital transformation drives resilience, not IT risk. With an over-reliance on digital channels to execute new-age transactions now is the time for traditional Insurance organizations to be fully aware of the risk that lies behind the convenience of the easy-to-use digital world (Jøsang & Pope, 2005; Jøsang & Pope, 2005; Bhargavan et al., 2016; Alassafi et al., 2017).

Insurance firms work both for and alongside customers to minimize risk. Insurance organizations that have been in this business for a long time understand that it is critical to put up a vigilant front to cut costs associated with risk and loss. These firms need to be monitored for fraudulent activity and policy abuse and should not only rely on their traditional methods of judgment but are also inclined to use modern technology solutions that help them carry out Identity and Access Management. Today, organizations are faced with identity proliferation due to the influx of users, devices, applications, and systems. This coupled with the untenable risk of data breach and loss posed by connected devices, as well as the new regulatory requirement to reduce third-party risk, have made digital management of user identities, privileges, and authentication methods a critical

priority for organizations. Failure to comprehend and control user identities, particularly the large number of users that have third-party connections to sensitive internal systems and proprietary data, can lead to data leakage and digital disruption (Wazid et al., 2018; Zhao et al., 2020).

6.1.1. Defining Identity and Access Management in a Modern Context

Many terms have been used to mean the same term, for example, authentication, authorization, and account/extranet management are terms used across business disciplines. In the context of Identity and Access Management, we determine authentication to be the process of validating the identity of a person or machine. To "authorize" a person means to verify if they have the right to perform the requested action on the targeted resources. What we mean by authorization goes much beyond "permission". With identity and access management if a person has permission but not the qualifications, they might not receive it.

Fig 6 . 1 : Identity and Access Management Is Important

Also, if a machine commits an action that has been recorded in the logs, there should be a capability to roll back that action and at least have an incident action flagged for investigation. Simply saying that they have permission is not enough. Our third term, account/extranet management, governs the inclusion and maintenance of active users on your organization or organization partner enabled with an IAM system.

Identity and Access Management is a framework of policies and technologies to ensure that the right users have access to the right resources at the right times and for the right reasons. With IAM, you can limit access to sensitive information while ensuring that

authorized users can access all the necessary resources to perform their jobs. IAM can also be used to create, modify, and delete user accounts and permissions to help secure and manage your business. In a broader context, IAM is typically part of a Security Information Management and Security Event Management solution that provides analysis of security alerts generated by network hardware and applications. From this larger definition, IAM would relate to only part of the business process management discussion.

6.2. Overview of the Insurance Industry

The role of the insurance industry in day-to-day life should not be underestimated. Insurance is a mechanism meant to provide a guarantee of compensation for specified loss, damage, illness, or death in return for payment of a specified premium. With its history, the insurance industry is one of the fastest-growing and largest financial sectors. A growing number of people from every background are becoming aware of the necessity of buying life and non-life insurance, not only to protect themselves but also to protect their families from possible hardship. The financial security gained from having insurance in certain areas has become a great aid to many families.

The insurance industry is responsible for taking and holding sometimes colossal amounts of money. The industry requires that all developments in this business be accurately monitored and controlled. There is a continuing need to develop computerized systems to automate the increasingly complex recording, validating, storing, processing, and presenting of insurance data. The emphasis has been on improving the facilities available to all who have a contribution to make to high-quality insurance data. A well-integrated insurance industry is vital to the success of the financial sector, to the overall economic development of a country, and to its continued viability.

At the heart of this insurance industry is a range of customer and corporate data, which are useful for a variety of decision-making and service-delivery functions. These include assessing the risk involved, underwriting insurance, determining the rate of the premium to be charged, offering after-sales service, adjusting any claim on an insurance policy, forecasting and controlling advertising costs, and forecasting future claims experience and reserves.

6.2.1. Industry-Specific Challenges and Opportunities in Identity and Access Management

Identity and access management (IAM) is a foundational area of cybersecurity, with a range of policies, processes, technologies, and safeguards used to assure that the right

individuals have access to the tools, data, and systems they need to carry out their jobs while preventing access that could damage the organization's reputation, cause monetary loss, or expose the organization or its customers to considerable risk. IAM spans the user life cycle, beginning before an individual is an employee, contractor, or partner, creating a crystal-clear identity governing authentication and authorization, and managing roles and access levels throughout the individual's association with the organization. IAM systems also serve a critical function in terms of regulatory compliance, especially in the insurance sector, which is subject to multiple regulations and oversight across both the physical and digital worlds that require a substantial burden of recordkeeping – the opposite of convenience. IAM plays an essential role in meeting specific requirements of some of these regulations, which need to be coordinated with a broader security program and involve massive amounts of sensitive data that could lead to severe penalties in the event of a breach. IAM is also the interface through which many customers or partners interact with the organization and represent first impressions of the organization's brand and customer experience. Regardless of whether engagement is via a mobile app, a website, or other means, the organization's IAM should promote easy yet secure access to the organization's resources.

6.3. Importance of Identity and Access Management in Insurance

Identity and Access Management (IAM) are part of everyday life in today's digital world; this is the reason these concepts are influential and have made their way to the insurance industry. However, is IAM only important for life and health and digital insurance service providers? The answer is no, it is for all insurance sectors, including specialty, general, and re-insurance. Still, it is a key element for all digital service providers. Digital security has a vital role within insurance companies. It protects their clients, businesses, financial data, and company reputation. Security experts have to take care of the privacy of individuals. The theft of information from insurance companies is very dangerous and valuable; there is sensitive and extensive personal information. Insurance businesses also have to take care of governing agencies' regulations and their stakeholders. Insurance businesses should work with an Identity and Access Management system that can help them onboard customers easily. Every KYC regulation should be covered throughout this process. Payments made throughout onboarding should be verified, enabling connection with every payment fraud-detecting tool. Possible risks and frauds should be detected and blocked while maintaining a smooth user ID travel across channels and branches. It is important to have a single view of the customer to be able to respond to KYC questions when needed.

6.3.1. The Vital Role of Identity and Access Management in the Insurance Sector

Much like a castle with a gate protecting its inner treasures, insurance companies need to use security programs to guard against fraud, theft, and cyber attacks. One of the most important tools against fraud is Identity and Access Management. IAM encloses the processes, systems, and technologies that enable the establishment, management, and termination of user accounts and permissions for applications and systems. In layman's terms, IAM covers the inner systems and infrastructures used to protect access to sensitive systems and information of the company from both outside cyber criminals and wrong-doers on the inside of the company.

Insurance companies need IAM not only to lessen the threat from cyber criminals but also because of the regulatory framework in which they operate. A large amount of customer-sensitive data is stored in the IT systems of an insurance company. Therefore, IAM is required to protect such data from unauthorized disclosure and modification. These regulatory requirements are particularly present in the insurance business. Not only do insurers have to comply with the General Data Protection Regulation, which mandates much stricter use and protection of customer-sensitive data, particularly when it comes from children, but also with the Insurance Distribution Directive. Predictably, breaches of data protection regulations can lead to very large fines. For example, in January 2023, the Dutch Data Protection Authority fined two insurance companies $ 1.9 million for deficiencies in their data protection compliance.

6.4. Key Challenges in Identity and Access Management

Identity and access management (IAM) is not only the hot topic of a rapidly growing market, but it is also a challenge to individuals and organizations, including companies in the insurance sector. The reasons are many. IAM is one of the bases of security and privacy and underlies the challenge of trust that has the Internet. IAM is a question of protecting information, data, systems, and business processes. IAM not only protects the assets of the insurance sector, it authorizes employees and authorized external users to perform their respective business process roles. IAM is inextricably linked to compliance with regulations and guidelines wherein IAM is recommended, mandated, or explored. IAM is providing security for an industry that is not only protecting the form of insurance but is also a target due to the value of the information it harbors. Some of the biggest breaches of trust and incidents of loss for financial companies have been thefts or fraudulent activities on the part of insiders.

The insurance sector is under pressure to implement IAM services for both proprietary and third-party purpose-built business applications. There are several reasons why IAM is challenging for the insurance sector. The services need to comply with a variety of

regulations and guidelines, including various standards and their international counterparts. These regulations and guidelines touch on all aspects of IAM services including the collection of identity information, the definition of the policy on information access control, and the actual IAM capabilities for information and systems. IAM for cloud solutions combines the challenge components.

6.4.1. Regulatory Compliance

The growing number of challenges in modern identity and access management (IAM) is tightly coupled with regulatory compliance, which can vary widely based on whose finger is on the policy pen. Recently, the Federal Trade Commission has increased its scrutiny of companies' cybersecurity practices, warning organizations that they could be penalized for security failures if they violate the agency's prohibition on "unfair or deceptive business practices," and there are even entire industries such as finance and medical that are governed by a plethora of regulatory agencies. So, it is a real alphabet soup.

The challenge for IAM is that these various rules often appear to contradict one another, erring on the side of being overbearing and overly prescriptive. If IAM is too strict and cumbersome, it can hamper user productivity on the job, and possibly even discourage employees from doing their jobs since it could become a hindrance to that productivity, as many roadblocks do. Conversely, rules that are too loose can create vulnerabilities — like weak passwords, and inadequate two-factor authentication policies — that can easily be exploited maliciously by an external attacker. Policing IAM to ensure that it remains compliant with all agency recommendations takes a not-insignificant investment of time and dollars, and the penalties for non-compliance could be nearly bank-breaking. But some companies just can't help but do what they can to skirt those rules.

6.4.2. Data Privacy Concerns

While regulatory compliance is one of the foundational elements in addressing data privacy, privacy concerns go beyond compliance and protection of citizens' data. Privacy is a major consideration in the purchase as well as use of insurance by customers. Insurers have to balance the extensive customer data gathering and analytical capabilities that drive differentiation against privacy and trust misgivings. An essential part of the trust equation is access control, ensuring that employees accessing sensitive customer data have the need and right to do so.

Insurers are expanding their use of third-party vendors to improve customer-targeted personalization, deliver predictive analytics, and streamline back-office processes and

functions. These vendors typically have access to customer-sensitive information ranging from call logs, social media data, and social security numbers to family member information and credit history. The need for password-free frictionless experiences on one hand and the increasing volume of vendor data access requests and associated risks, on the other hand, make it imperative for insurers to institute a zero-trust approach to authenticating vendors accessing enterprise resources and the data flowing across the resources. To address vendor privacy and security concerns effectively, insurers have to begin with a comprehensive identity-aware risk assessment covering all aspects of the organization's business ecosystem, both internal and external. This includes data shared across the ecosystem, the devices accessing the data, users accessing the ecosystem's resources as well as applications, and networks connecting the users, devices, and resources.

Once the assessment is completed, organizations will be able to develop a set of enterprise policies and catalog assets supporting efficient risk mitigation. Based on the asset catalog, insurers will then be able to create a set of tasks for each asset, user, and vendor. These tasks can then be continuously monitored to enable rapid preemptive business process enforcement before damage can be inflicted. This approach allows insurers to establish trust and verify without requiring the asset owner to be explicitly trusted.

6.4.3. Legacy Systems Integration

Many insurers still rely on in-house developed legacy systems for their core applications. In many cases, these solutions are workhorses, remaining in place for too long. The lack of open interfaces or closed APIs keeps innovation in adjacencies very difficult. The permanent conversion of new insurtechs into insurance partners and the permanent opening up of core backend systems via innovative API management solutions is paramount for innovation in many adjacent topics. In many cases, customers do not have an understanding of the impact of mitigating risks in adjacent areas. Digital customer journeys require frontend solutions that are increasingly decoupled from backend systems. Heavily customized legacy front office systems are strained as they are simultaneously expected to serve as backend transactional systems while also orchestrating complex commerce processes. Many insurers are forced to implement partial policyholder view, new agent portals, new document creation without new templates, and others as a workaround through specific external projects instead of offering robust local execution commercial capabilities front office solutions powered by their core engine. Alternative vendor solutions are difficult to integrate closely with legacy systems that serve as backend transactional systems because these systems manage labor-intensive, high-volume, and low-margin transactions. Choosing and

investing in flexible API management tools and integrated data intelligence and data analytics tools can help both legacy and external solutions serve as components of a multi-channel solution. Emerging technologies, such as artificial intelligence, machine learning, and predictive analytics, will continue to evolve and help insurers analyze, integrate, and leverage internal and external data. Insurers have been cautious about embracing emerging technologies for many good and prudent reasons. There are many claims across cross-industry players touting return on investment via the operationalization of these technologies across many operational areas.

6.4.4. User Experience Issues

Separately from the basic requirements of security, the user experience and the services' usability, especially in the insurance sector, are also becoming important. Still today, the majority of users associate insurance processes with a high level of inefficiency and a subpar user experience even if online services are provided as self-service portals for selling insurance products and managing insurance policies. For transactions that are difficult to understand, such as claims management, or for high-risk transactions, such as loss reporting on the self-service platform, a complicated authentication process can lead to a negative user experience, especially in cases of urgency.

The often scarce willingness of customers to manage transactions alone through a digital interface depends closely on the types of services offered. Balancing the login and identity proofing requirements with the service type is a major challenge on the user experience side. Services that require a high level of fraud protection may see users drop out of the transaction, whereas for those that only present a low level of user risk an efficiency-centered authentication strategy could be of help to increase the user experience. An example of such a case is the possibility for the service provider to offer users who have never utilized the service before while modifying the insurance policy online an easier login process since they are already known. Such an approach only works if the service cannot be used for any losses or frauds.

6.4.5. Fraud Prevention

While fraud is a concern across all verticals, it is especially dangerous for insurers and can represent a surprising percentage of the total cost of insurance. Insurance fraud is estimated to cost United States consumers between $300 Billion and $600 Billion every year. In 2021, 72% of respondents in a different survey stated that they faced increasing pressure to prevent losses caused by insurance-related fraud schemes, including payment fraud, identity theft, auto glass fraud, and property fraud. Compounding the problem is the fact that emerging technologies, ranging from artificial intelligence to biometric

authentication systems, are increasing both the capabilities of fraudsters to execute fraud and the capabilities of organizations to stop fraud.

Fig 6 . 2 : Fraud detection and prevention

But while these technologies are helping fraudsters, they are also helping organizations. For instance, machine learning-based predictive analytics are enabling organizations to catch fraud quickly and accurately, and artificial intelligence-enhanced customer and device profiling is providing organizations with intelligence that helps them determine who is who and their intentions. These technologies are automatically collecting terabytes of data with little to no human intervention, searching that organized and prepared data for patterns that precede fraud events, and then escalating the transaction to be reviewed for further investigation. In addition to machine learning algorithms and artificial intelligence, involving the user through multi-factor authentication, modal authentication, behavioral analytics, and other technologies is also becoming increasingly important for preventing fraud.

6.5. Technological Solutions for Identity and Access Management

The solutions for Identity and Access Management (IAM) can be divided into two categories. Processes that require a technological implementation include directory services, Secure Access Module solutions, and Public Key Infrastructure implementations. In addition, organizations have to decide the level of dependency on third-party providers and may choose to partner with specialized vendors or deploy in-house IAM services, in particular for verification services. Business process development includes the definition of procedures for user provisioning and de-provisioning, the extensibility of the IAM solution to internal users (employees and business partners) and external users (clients in particular), the classification of business resources, security policies, and credential life cycle management.

Multi-Factor Authentication

Multi-factor authentication solutions first require the user to prove his or her identity with a “something you know” factor, typically a password or passphrase. In the second phase, “something you have” solutions, such as hardware tokens, smart cards, or mobile telephone verification, add a layer of security. If a sophisticated attacker wants to impersonate the user by intercepting and cracking these two types of factors, they will have to face an additional hurdle – biometric authentication. Commercial offerings provide various combinations of multi-factor authentication technologies to increase the security and usability balance for their customers and must also take into account specialized requirements from the banking and insurance verticals.

Single Sign-On Solutions

A single sign-on solution allows companies to reduce their support costs by implementing a single credentials solution across most (if not all) of their application vendors – internally developed, middleware vendors, and commercial off-the-shelf vendor applications. Two categories of commercial solutions have emerged: those that collaborate with application software vendors to implement security and sign provisioning services in the application code and those that build an in-house directory service, extendable to legacy applications, and deploy proprietary in-house security and single sign-on authentication capability. A key aspect of the success of single sign-on offerings is their capacity to integrate with external IAM services. These offerings not only facilitate administration but also allow banks to share IAM tasks and user credentials with their business partners. A defined set of identifiers and demographics would allow issued cards and business transactions to be shared easily by companies A and B if these organizations were engaged in an enterprise transaction for specific customers.

6.5.1. Multi-Factor Authentication

In today's digital world, we are tasked with managing more passwords than ever before. Protecting all of those credentials seems to only get more difficult. People tend to use easy-to-remember passwords, which are also easy to crack, and they often share passwords across multiple devices, applications, accounts, organizations, and services. Each one of these accounts adds another point of vulnerability. It's not surprising that we're also dealing with more breaches than ever before. Multi-factor authentication (MFA) is a great way to add another layer of security to your logins. Think of it like this: Your password is the online equivalent of a house key. If someone gets their hands on it, they can break in and steal all your valuables. But what if you could also lock the door and install a security system to alert you if someone attempts to enter without your permission? That's MFA: an extra layer of security to further confirm someone is who they say they are.

MFA requires more than one form of verification before granting access to sensitive data. Organizations build confidence that a user is authentic with multiple identities. Typically, these identities fall into three categories. Something you know, which includes passwords, PINs, and other common entryways to user accounts. Something you have, which includes the types of mobile devices used for authenticator apps, smart cards, one-time-password tokens, and other devices used for generating or providing secure access codes. Something you are, which includes biometric identifiers such as fingerprint scans, facial recognition, iris patterns, and other user attributes unique to individuals.

More and more organizations rely on MFA to restrict access to only authenticated users and deny unauthorized logins. Banks already use it as standard safety practice to keep money secure. However, requiring a password for every login is burdensome for employees and customers. Security teams want to provide a better user experience without compromising security. That's where new technologies, such as passwordless MFA, come into play.

6.5.2. Single Sign-On Solutions

Another way to diminish the burden of users who need to memorize many different credentials is the implementation of Single Sign-On (SSO) solutions. SSO can be defined as an authentication process that allows a user to log in once and gain access to different applications or services without being required to log in again. SSO is a subset of the broader concept of Identity Federation and relies on the implementation of a centralized Authentication Service. Enterprises normally use SSO when they have multiple applications such as Microsoft Exchange, SharePoint, Windows File Sharing,

and more. These applications may require users to authenticate regularly by entering their credentials. With SSO, organizations can centralize and simplify the authentication and authorization processes.

Within an enterprise, the benefits of SSO are clear, but the users are also able to find advantages in its adoption. These are primarily related to the reduction of the number of recurring logins and password inputs and the possibility of establishing a stronger password policy. It is clear that reducing the number of times a user must log in helps overcome “login fatigue”. Organizations can also enforce a “strong password” policy requiring users to create a strong password that is only used with the “trusted” SSO. Users can then create different accounts with strong passwords for each application without the fear of forgetting them. In addition, account lock-outs will usually decrease because the only account that locks a user out is the SSO account.

6.5.3. Identity Federation

Traditional identity and access management solutions and strategies only support access to applications and services in one administrative domain. Identity and access management in heterogeneous environments involving multiple service providers and application resources requires identity federation technology and services. Identity federation allows users' identities and how these identities are supported and used in different domains to be federated, or linked across multiple domains. With identity federation, authentication, identity management, and data flows no longer remain in a single federating identity management environment. Insurance services will increasingly span multiple service providers, including commercial companies and self-service tools, third-party service providers and partners, and infrastructure as a service, platform as a service, and software as a service service. The need to manage and support user access across multiple service providers in this federated environment has become an increased priority for business executives in information technology and the enterprise. New trends in enterprise business strategies and business management require new approaches to how identity management and federated identity management are supported. Privacy and trust are critical factors influencing how identity management and federated identity management models and security controls are established and implemented. Federated identity solves issues associated with access due to dissuasive user actions such as multiple user credentials being needed before accessing federated resources or careless user actions such as reusing the same user credentials in different and unauthorized ways among service providers. In addition, federated identity enhances security at enterprise borders by allowing enterprise security departments to better assert and manage identity provisioning, authentication, and authorization using identity audits, compliant identity data, provisioning, and trusted digital identities between service providers.

6.5.4. Access Control Models

Access control models help to define what subjects can perform what type of access (operation) on what objects (resource data), i.e., the structure of access rights allocation and use in the specific system. There are various models that can be categorized generally into two: discretionary access control and mandatory access control models.

In a discretionary access control (DAC) model, the owner of the protected resources can decide which subjects can have access to what objects and what type of access can be invoked on them. This model is considered flexible, user-friendly, and suitable for accountability in corporate data processing standards. The most common DAC techniques include access control lists and group-based privileges (permissions). Among the disadvantages of the DAC model are the difficulties involved in ensuring that security requirements are consistently defined to avoid risks of data losses through uncontrolled dissemination and that security-sensitive data resources are not compromised by the users because many organizations do not consider it appropriate to restrict subjects from allowing the sharing of sensitive objects with others.

In contrast, in a mandatory access control (MAC) model, an authority manages all the access controls authorized on the resources. The owners are usually not allowed to change the access controls. This model is based on specific security attributes associated with the objects and subjects involved and provides access only if the attributes confirm a match between them. Role-based access control and attribute-based access control are common MAC techniques. These models are strict concerning the determination of access processes, are less flexible than the DAC models, and offer a higher level of protection for sensitive data. This model is used in critical systems such as military and intelligence systems for which security is of utmost importance. Most organizations, due to the complexity and costs of implementing these processes and the risks of technical difficulties, use a combination of both models.

6.6. Best Practices for Implementing Identity and Access Management

Several best practices must be implemented to have a successful Identity and Access Management system for insurance services, which I would like to highlight and emphasize herewith below.

Implementing risk assessment and management is a vital practice for Identity and Access Management in the insurance sector. Risk assessment helps formulate strategies that reduce or eliminate risk and its potential damages. Risk management prioritizes the right assets and checks the likelihood of each risk factor, estimating the damage each risk could potentially cause. Special emphasis should also be put on prioritizing the protection of sensitive Identity and Access Management data and those of the clients.

After a correct risk assessment is made, companies can decide to transfer the risk, manage it via specific guidelines, mitigate it by applying controls, or accept it when appropriate.

User training and awareness is another vital best practice for implementing an Identity and Access Management system in the insurance sector. Data breaches are not always due to a failed Identity and Access Management system; employees could also bypass the workflow for various reasons. In these cases, proper training and awareness are key for data protection, as employees allow the data breaches to happen unconsciously or not. Insurance companies should therefore invest in employees' education and training programs so that employees are aware of the possible consequences of data breaches, making them more likely to report any unusual activities that could alert cybersecurity experts to malicious attacks. Cybersecurity models can always be expanded and improved, and employees play the most important role for insurance companies.

Regular checks on the system are another important best practice for Identity and Access Management systems. Just because the employees were trained and instructed to follow the rules and procedures stated in the guidelines doesn't mean they will follow them every time. Particularly sensitive operations should be checked regularly; for example, user access review, role contention, and segregation of duties. Regular system checks also help highlight any holes in the cybersecurity workflow and give administrators the possibility to revise it.

6.6.1. Risk Assessment and Management

A robust Identity and Access Management environment requires due diligence in assessing the risk posed to all organizational stakeholders by failure to control identity, credentialing, and access management in the organizational environment. Risk Assessment and Management practices include performing enterprise-wide risk and threat assessments whether internally, externally, or as directed by the regulator. It is important not only to identify the threat landscape around IAM but also to help identify the specific threats to the organization and its technology environment. This threat landscape needs to be dynamic and adjusted routinely based on new technology introductions as well as updates to organizational policy or standard procedures.

Enterprise-wide risk assessments should expand on typical internal loss and breach assessment considerations around IAM operations that are usually driven by changes in regulatory guidelines or standards, technological risk assessment, reviews of IAM product weaknesses and failures, considerations around all IAM personnel, and normal IT security variances. Best practice guidelines for conducting enterprise internal IAM risk assessments focus on employing a risk-scoring model while ranking maintenance

functions based on the level of overall risk they pose. The higher the overall risk associated with a particular IAM project, action, or operational task, the more stringent a security approach should be. Assessing IAM risk throughout requested, authorized, and outsourced execution can help form an ongoing feedback loop that can help organizations more effectively identify IAM risks and promptly prevent security problems.

In addition, not only should enterprise-wide risk considerations be taken into account, but also certain specific user risks considered by employing a risk-based model. Organizations could implement risk-based identity policies on a formal basis by assigning higher security and privacy risks to enterprise support users and functions and, indeed, extending the risk-based assignment rules to external service providers accessing the business environment.

6.6.2. User Training and Awareness

It is estimated that the majority of security compromises are due to social engineering attacks. Either a user accidentally activates malware that compromises the insurance system or a user exposes themselves to phishing or spear phishing attacks. Insurance organizations need to build a culture of security within their organization. Users need to be trained on information security, social engineering attacks, password security, email awareness, and specialized training on any security-aware technologies that the organization implements. Users need to be regularly reminded of the importance of security training. Security awareness signage and information security newsletters should be used to advertise current issues and other best practices to reduce the likelihood of an incident.

Consider the following examples. An employee recently lifted a company policy from the shared drive to prepare for an upcoming meeting. The employee left the computer unlocked while running to speak with a colleague. A visitor to the insured's building noticed the unlocked computer, closed the lid, and returned to the front desk. An observed insider information thief simply grabbed the employee credentials previously entered into the computer and used the information to log into their account after working hours. The visitor was able to see the policy which was now conveniently saved as a PDF in the employee’s company Dropbox.

6.6.3. Regular Audits and Monitoring

Regular audits and monitoring are critical components of an effective IAM program, as they enable organizations to assess the effectiveness of existing controls and processes,

identify areas for improvement, and ensure continued compliance with relevant regulations. Auditing user access control regularly helps teams better understand access level needs and correct privileges where they exceed user needs. Organizations should ensure that access control policies are scalable to help meet growing user base and changing business team objectives. Regular IAM audits help organizations optimize performance, identify holes in security, validate access requests, and ensure quick response to all IAM processes and incidents. In addition, IAM audits help organizations experience quicker incident response times, quickly detect unwanted activities, and provide appropriate assurance to anyone reviewing an organization's implementation of access controls. Specifically, auditors need to substantiate their review of identification and authentication, logical and physical access controls, and other areas affected by IAM controls. Additional monitoring controls must also be implemented as designed in the IAM processes. Reports often exclude IAM element-related controls, increasing the risk that identified deficiencies or incidents may go unnoticed until the next audit.

6.7. Conclusion

In conclusion, our work has covered a range of important themes within the broad topic of Identity and Access Management in the insurance sector. An analysis of the challenges and solutions studied reveals that today, more than ever, insurance companies need to innovate to survive in their sector. Technology is providing the intermediary tools for such transformation. However, it was also shown that due to regulatory constraints, insurance companies typically offer a customer experience that is less flexible than the one offered by banks. Protecting customer data has a direct impact on a company's trustworthiness, and any incident having a direct impact on the data of the company's numerous policyholders must be avoided at all costs, including by technological means. Therefore, the procedures proposed in the area of IAM need to be built on the highest industry standards or, if they can't be, their limitations should be communicated clearly to the customer. Dealing with IAM for a mass customer is difficult, but not impossible. Less flexibility is possible provided that it can be translated into reliability. This is where the acquired knowledge of customers needs to be coupled with decision capabilities and computational power, to provide a trustworthy experience that makes insurance companies stand out from their competitors in other sectors. On the other hand, due to compliance obligations imposed on the sector, together with the level of investment made by these organizations, IAM knowledge is forged as a strategic internal competency for insurance companies. As, for now, the move to the public cloud may not involve all these companies' applications, and there are still several critical and or sensitive applications that are only available locally, cybersecurity measures must be imposed not only internally, but also on every partner linked to the IAM services or synchronizing or redirecting access to IAM in the cloud external service.

Fig 6 . 3 : Identity access management spending

6.7.1. Summary of Key Insights and Future Directions in Identity and Access Management

Directed Towards:

The insurance sector is presented with new opportunities to create business value through the implementation of digital technologies as they migrate towards a customer-centric business model. Moving to a digital strategy is, however, not without its challenges. Our discussions in the essay point to the increasing levels of cybersecurity threats and attacks making front-page news with alarming frequency. Maintaining market, client, and employee trust will rely on effective identity and access management. Strengthening digital trust by increasing security, smooth enrollment, and security of data and transactions will ensure that the new digital offerings are as desirable.

IAAM threats to the insurance sector are expected to grow in step with the anticipated growth of IAM technology and service offerings. Specifically, we expect that identity fraud will continue to increase while insurance claims identity management or risk can be stored away. An increased uptake of IAM technology and service will, however, serve as a considerable deterrent and prevent or reduce the consequences of future attacks.

Indeed, widespread awareness of the value of identity and access, especially by insurance and cybersecurity media, researchers, and policymakers will create increasing compliance and demand, thus increasing growth. As such, while the IAM technology and service offerings are expected to become pervasive the investments in IAM will enable the technological development, thus increasing resilience. The supporting role of IAM is also clear. Appropriately securitized data exchanges, especially for personal data, will enable post-Covid-19 contactless transactions to spur economic recovery. Further research would be required, however, into the performance metrics used to evaluate and implement IAAM planning and service.

References

Zhao, G., Liu, J., Tang, Y., & Sun, J. (2020). Identity and Access Management in Cloud Environment: Mechanisms and Challenges. Future Generation Computer Systems, 109, 320–329. https://doi.org/10.1016/j.future.2018.06.006

Bhargavan, K., Delignat-Lavaud, A., & Pironti, A. (2016). Verified Implementations of the Identity Federation Protocols. ACM Transactions on Information and System Security, 19(4), 1–36. https://doi.org/10.1145/2960009

Alassafi, M. O., Alharthi, H., Walters, R. J., & Wills, G. B. (2017). Security Risk Assessment Framework for Cloud Computing Environments. Computers, 6(1), 8. https://doi.org/10.3390/computers6010008

Jøsang, A., & Pope, S. (2005). User-Centric Identity Management. In: Proceedings of the Australasian Information Security Workshop, 77–86. https://doi.org/10.48550/arXiv.cs/0501039

Wazid, M., Das, A. K., Odelu, V., Conti, M., & Kumar, N. (2018). Design of Secure User Authentication and Key Agreement Protocol for Cloud Computing Using ECC. Future Generation Computer Systems, 71, 437–457. https://doi.org/10.1016/j.future.2016.11.017