simeio

EBook

Reasons IAM is the Core of

Modern Cyber Risk Management in 2023

Introduction

As cyber threats continue to evolve and organizations become increasingly reliant on digital technologies, Identity and Access Management (IAM) has emerged as a crucial component of modern cyber risk management. In this e-book, we will explore five key reasons why IAM plays a central role in safeguarding businesses from cyber risks in 2023.

1 The Proliferation of Remote Work & BYOD Policies

The reality is well-established that organizations scrambled to maintain operational continuity and adapt to new working conditions amidst the global shift towards remote workforces. The concept of "Identity as the new perimeter" emerged as an attractive and fitting mantra that encapsulated the contemporary workforce and the world we inhabit. It recognized the pressing need for an evolved approach to securing data and applications across fragmented infrastructures where traditional perimeter-based defenses were no longer enough. However, upon reflection, it became evident that IAM rapidly evolved into a central component of modern cybersecurity strategies. Indeed, the world has moved beyond traditional perimeter-based defense mechanisms, and the need for an evolved approach to security has never been more apparent.

In navigating the contemporary realm of cybersecurity risk management, it has become evident that managing cyber risks across an organization has grown increasingly challenging.

The constant emergence of new threats, coupled with the widespread adoption of cloud services, remote work, and Internet of Things (IoT) devices, has added complexity to the already intricate task of safeguarding an organization's digital assets. Indeed, a report found that as many as 20% of digital companies experienced a work-from-home-related breach in 2020[1]. Consequently, the responsibility of risk management and maintaining compliance with ever-changing regulations has become an uphill battle for even the most seasoned professionals.

Cyberthreats have become more sophisticated, and cybercriminals have become more tenacious in exploiting system vulnerabilities. In this context, the importance of Identity and Access Management (IAM) as a risk management strategy for securing a business's assets cannot be overstated. To successfully navigate these challenges, businesses must adopt a proactive approach to cybersecurity risk management, leveraging cutting-edge IAM tools and strategies to stay ahead of emerging threats. By investing in comprehensive security solutions, providing continuous training for their teams, and fostering a culture of IAM maturity, organizations can better equip themselves to tackle the complexities of modern cybersecurity and ensure the safety of their valuable data and resources.

1 20 percent of organizations experienced breach due to remote worker, Labs report reveals, Malwarebytes Labs

> **Identity and Access Management (IAM) is the foundation of cybersecurity, connecting identity, data, and systems to protect valuable assets and shape future strategies. By granting essential access while minimizing risks, IAM empowers a secure and evolving digital landscape.**

2 Identity is Central to Modern Cybersecurity

The realm of identity and access management permeates every facet of security, encompassing elements such as network architecture, risk mitigation, data confidentiality, and the prevention of data leakage. As previously noted, IAM transcends the boundaries of perimeters, a singular product or solution. It represents an essential compilation of guidelines and protocols that are implemented to accomplish a series of crucial business goals. These objectives consist of minimizing operational expenses, mitigating threats to valuable information assets, and enhancing the overall user experience and efficiency.

The significance of data is derived from numerous components, with an emphasis on the association between identity and the data in question. This may involve human identities, machine identities, or other forms of identification. As we examine the current state of cybersecurity, with the majority of firms experiencing a breach[2], it becomes evident that IAM plays a pivotal role. The crux of the matter lies in the connection between identity, data, and systems, as well as the ability to access the necessary resources at the right time and in the appropriate manner without exceeding the required boundaries.

Envisioning the strategy for the future involves establishing limits that grant access to necessary resources while simultaneously restricting access to only those components that are essential. By doing so, the potential threat landscape is minimized in preparation for unforeseen challenges. A robust IAM strategy precisely offers this level of protection, securing various aspects of identity while permitting the appropriate degree of access. The evolution of cybersecurity will ultimately depend on a proficiency in managing identities and regulating access.

2 80% of Firms Suffered Identity-Related Breaches in Last 12 Months, Dark Reading

Integrating Identity and Access Management with the NIST Framework's Essential Cybersecurity Functions

Identify

Create a comprehensive view of their security landscape and identify potential vulnerabilities. IAM plays a crucial role here by identifying users, user groups, and their access levels to various resources.

Protect

Safeguard confidentiality, integrity, & availability of information. IAM contribute to this by implementing access controls, authentication mechanisms, journey-time orchestration procedures, & authorization policies.

Detect

Identify potential cybersecurity events or incidents in a timely manner. IAM systems can help detect anomalies in user behavior, such as failed login attempts, unusual access patterns, or privilege escalation.

Respond

Mitigate the impact of a detected cybersecurity incident. IAM plays a critical role in this process by enabling organizations to quickly revoke or modify user access, reset passwords, or disable compromised accounts.

Recover

Restore systems and services to normal operations following a cybersecurity incident. IAM is essential in the recovery process, as it helps organizations re-establish secure access to affected resources.

IAM practices, systems, processes, and solutions are tightly integrated with the NIST framework's core functions. By effectively managing user identities and access, organizations can significantly enhance their cybersecurity posture and better align with the NIST guidelines for Identify, Protect, Detect, Respond, and Recover.

"Identity and Access Management (IAM): safeguarding assets, empowering response, and driving secure recovery in the realm of cybersecurity."

3 The Ever-Changing State of IAM in the Cloud Era

Digital transformation is ever present anywhere computing is increasingly prevalent. Consequently, IAM has become an essential component of a successful security strategy. But our perspective on identities and their relation to cyber risk management must not be narrow-minded. In reexamining the year 2020, the increase in cyberattacks targeting remote work environments prompted organizations to reassess their approach to identity management, recognizing it as an integral aspect of enterprise risk management[3]. This response has shifted the focus from the traditional defense-in-depth approach, which relied on firewalls and other perimeter-based controls, to a user-centric approach that prioritizes the mature management of user access and authentication.

In this interconnected world, recognizing the importance of identity management and its relationship with data and cloud-based architectures is for organizations to stay ahead of cybersecurity threats and continuously manage risk.

In case you somehow missed it, the present is heavily influenced by the management of identities. Additionally, as we envision the future based on our current understanding, cloud-based IAM architectures will continue to play a significant role.

Taking these two key factors into consideration, it becomes evident that managing entitlements and permissions

Taking these two key factors into consideration, it becomes evident that managing entitlements and permissions in cloud environments is of paramount importance. Just as we strive for seamless management of user identities, it is equally crucial to address entitlements in the cloud without having to individually track them down in every cloud platform. Adopting an integrated model enhances visibility, automation, and policy management, thus streamlining the process and bolstering overall security.

3 Your Remote Workers: A Target for Cybercrime, Association of Legal Administrators

Key Considerations for Leveraging IAM to Manage Risk in the Cloud Era

To effectively manage identities and access in the cloud era, organizations should consider the following:

Scalability

Cloud-based IAM solutions must be able to scale with the growth of an organization's cloud environment, supporting the addition of new users, applications, and resources without sacrificing performance or security.

Flexibility

In the cloud era, IAM systems need to accommodate a diverse range of users, devices, and access scenarios. This requires flexible policies and controls that can be easily adjusted to meet the unique needs of each organization.

Integration

Cloud-based IAM solutions should seamlessly integrate with existing on-premises systems, as well as other cloud-based services, to provide a unified identity and access management experience across the entire IT ecosystem.

Automation

Automating IAM processes, such as provisioning, deprovisioning, and access management, can help organizations maintain security while reducing the administrative burden on IT teams.

Visibility

In the cloud era, having comprehensive visibility into user activities and access patterns is essential for detecting and responding to potential security threats. Cloud-based IAM solutions should provide real-time analytics and reporting capabilities to enable effective monitoring and threat detection.

By treating IAM as the nucleus of security risk management and adopting an integrated approach, businesses can ensure the protection of their digital assets while adapting to the ever-evolving landscape of technology and cybersecurity.

4 Managing Cybersecurity Risk Hinges on How Well You Manage Identities and Access

As cyber threats continue to escalate at an alarming rate, the strength of your security measures is only as robust as the most vulnerable element—frequently, this vulnerability is linked to individuals who have access to your network. These users might include cloud-based systems or gadgets like smartphones, employees with unsuitable access permissions, discontented staff members seeking to harm your organization, third-party vendors needing system access for support purposes, or external adversaries determined to breach your network for the purpose of infiltrating or exfiltrating vital information.

In today's digitally connected world, the cybersecurity risk faced by organizations is directly linked to how effectively they manage identities and access[4]. IAM has become the most critical component of any comprehensive cybersecurity strategy. By implementing robust IAM processes and systems, businesses can significantly reduce their exposure to cyber threats and protect their valuable data and resources.

Key Components of Effective Identity & Access Management

To minimize cybersecurity risks, organizations must focus on implementing the following key components of effective IAM:

1. Least Privilege: Adhering to the principle of least privilege ensures that users only have access to the resources necessary for their job functions. This minimizes the risk of unauthorized access and reduces the potential damage caused by compromised credentials.
2. Multi-Factor Authentication (MFA): MFA adds an additional layer of security by requiring users to provide two or more forms of identification before gaining access to resources. This makes it much harder for cybercriminals to gain unauthorized access, even if they have stolen or guessed a user's password.
3. Role-Based Access Control (RBAC): Implementing RBAC simplifies access management by assigning permissions based on users' roles within the organization. This approach not only streamlines administration but also ensures consistent access levels across the organization.
4. Regular Auditing and Monitoring: Conducting regular audits and monitoring user activities help organizations detect and respond to potential security incidents quickly. Regular audits also help identify weaknesses in the IAM framework, allowing for timely improvements.
5. Identity Lifecycle Management: Managing the entire identity lifecycle, from onboarding to offboarding, is crucial for maintaining secure access. This includes timely provisioning and deprovisioning of user accounts, ensuring that access rights are always up-to-date and accurate.

4 When It Comes To Protecting Your Network, Identity Is The New Perimeter, Forbes

The Benefits of Effective IAM in Reducing Cybersecurity Risk

By implementing a robust IAM framework, organizations can reap the following benefits:

- ·Reduced risk of data breaches: Effective IAM helps prevent unauthorized access to sensitive information, significantly reducing the likelihood of data breaches.
- ·Enhanced productivity: Streamlined access management processes save time and effort for both users and administrators.
- ·Improved compliance: Many regulatory frameworks, such as GDPR and HIPAA, require organizations to implement strict access controls. A mature IAM system can help businesses meet these requirements and avoid costly fines.
- ·Lower cyber insurance premiums: As cyber insurance underwriters increasingly consider IAM maturity when determining risk profiles and premiums, organizations with robust IAM systems can enjoy lower insurance costs.

In conclusion, managing identities and access effectively is a critical factor in determining an organization's cybersecurity risk. By prioritizing IAM and implementing best practices, businesses can significantly reduce their exposure to cyber threats and safeguard their valuable assets in an increasingly connected world.

5 Zero Trust Models are Built Around Strong Identity and Access Management

The zero-trust model represents a transformative approach to cybersecurity, built upon the foundational principle of "never trust, always verify." This security framework fundamentally shifts the traditional perimeter-based security mindset, which often relies on implicit trust within an organization's network. Instead, the zero-trust model operates under the assumption that no user or device, regardless of their location within or outside the network, should be trusted by default.

At its core, the zero-trust model seeks to address the ever-evolving threat landscape that organizations face in today's highly interconnected digital environment. The rapid adoption of cloud computing, remote work, and mobile devices has led to a significant expansion of an organization's attack surface. As a result, conventional security measures have become increasingly insufficient in protecting against sophisticated cyber threats[5].

By implementing a zero-trust architecture, organizations can establish a more granular and dynamic approach to security. This involves continuously validating the identity and context of every user and device attempting to access the organization's resources, regardless of their position within the network. In doing so, the zero-trust model effectively reduces the risk of unauthorized access, data breaches, and other security incidents.

Principles of the Zero-Trust Model

Verify Explicitly
Always authenticate and authorize users and devices before granting access to resources.

Micro-Segmentation
Micro-segmentation: Divide the network into smaller segments with strict access controls.

Least Privilege Access
Limit user access to the minimum necessary for their role or task.

Continuous Monitoring
Continuous monitoring: Continuously monitor and log user and device behavior to identify anomalies and potential threats.

5 4 Reasons Your Business Needs to Implement a Zero Trust Architecture, Akamai

How Zero-Trust Works with IAM

Identity and Access Management (IAM) plays a crucial role in implementing a zero-trust model by managing user identities, enforcing access policies, and monitoring user activities. IAM solutions provide:

1.Authentication: Verify user identities through strong authentication methods, such as multi-factor authentication (MFA).

2.Authorization: Define and enforce role-based access control (RBAC) policies to ensure users have the appropriate permissions.

3.Monitoring: Track user activities and detect potential security threats in real-time.

The Increasing Role of IAM Maturity in Cyber Insurance Risk Management Policies and Premiums

The current IT landscape is facing an unprecedented barrage of cyber threats. As the world shifted to remote workforces during the COVID-19 pandemic, the rate of ransomware attacks skyrocketed. Thus, cybercriminals took advantage of the increased vulnerabilities associated with remote work, such as weaker security measures and employees using personal devices for work purposes. This situation led to a sharp rise in ransomware payouts, which caught the undivided attention of cyber insurance underwriters.

In response to this alarming trend, cyber insurance underwriters began to include policy requirements for more mature IAM processes and systems. They recognized that the implementation of robust IAM frameworks could significantly reduce the risk of ransomware attacks by preventing unauthorized access, improving visibility into user activities, and enhancing overall security posture.

To achieve this, underwriters began to assess the maturity of organizations' IAM processes and systems more closely as part of their risk evaluation processes. Today organizations with higher IAM maturity levels are seen as lower-risk clients, leading to more favorable insurance premiums and coverage.