xoriant

The Identity Access Management Handbook

Your Guide to Securing Access to Your Digital Assets

Contents

Welcome to the digital age, where our lives are intricately interwoven with the online world. There is no doubt that just as our possessions offline need protection so does our digital identities.

The cyberthreats we experience online are not limited to the digital realm. They can have a cascading effect on our real lives.

The Cost of Cybercrimes

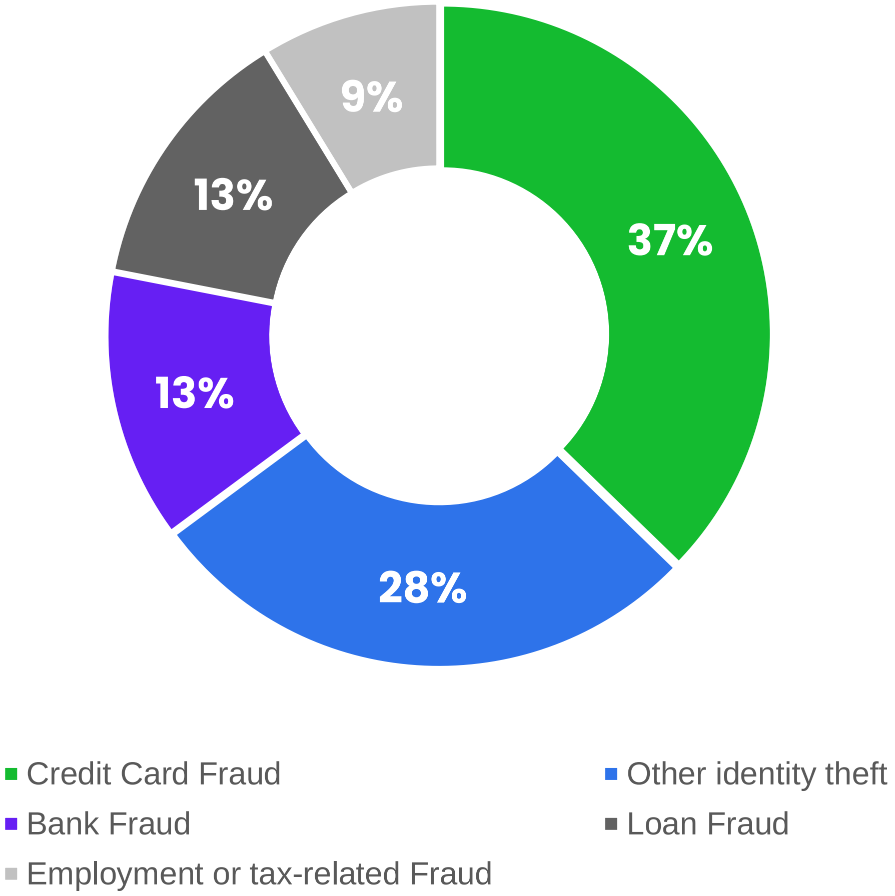
Cybercrimes have become a pervasive and ever-evolving threat, leaving a profound impact on individuals, businesses, and society at large. From data breaches and identity theft to ransomware attacks and online fraud, the consequences of cybercrimes reverberate across all facets of modern life.

At the individual level, cybercrimes can inflict significant financial and emotional distress. Identity theft, for instance, can lead to the unauthorized use of personal information, resulting in financial loss, damaged credit scores, and a loss of trust in digital systems. Moreover, the psychological toll of cybercrimes can be immense, with victims often experiencing feelings of vulnerability, anxiety, and violation of privacy.

353 million

users were affected by data breaches in 2023, according to a Consumer Sentinel Network report.

Most Common Identity Theft



For businesses, the ramifications of cybercrimes extend far beyond monetary losses. Data breaches can compromise sensitive corporate information, erode customer trust, and tarnish brand reputation. The costs associated with investigating and mitigating cyber-attacks, as well as potential legal liabilities, can exact a heavy toll on organizations of all sizes. Furthermore, disruptions to business operations caused by cyber-attacks can lead to downtime, productivity losses, and diminished competitiveness in the marketplace.

Source: Forbes Advisor via Federal Trade Commission Consumer Sentinel Network

The total damages caused by cybercrime is expected to reach a whopping

$10.5 trillion by 2025

- Cybersecurity Ventures

This impact highlights a pertinent question. How does Identity and Access Management (IAM) fit into the big picture? IBM's 2023 report on the Cost of Data Breach reports that the global average of the cost of a data breach is USD 4.45 million, while 82% of those breaches involved data that was stored on the cloud. With the significance of data rising, it's clear that threat surfaces have expanded. One of the keys to reducing attack surfaces lies in limiting access to sensitive resources.

Expanding Attack Surfaces and the Strategic Imperative of IAM

Enterprise Attack Surfaces (EAS) encompass the array of entry points through which cybercriminals can exploit to illicitly access an organization's digital assets. Over the last five years, EAS have undergone significant evolution.
The surge in cloud-based services, the proliferation of connected devices, and heightened reliance on third-party vendors have collectively broadened, multiplied, and complicated these attack surfaces.

Cloud

The shift to cloud-based infrastructure offers organizations scalability, cost efficiency, and agility. However, the rapid adoption of cloud services has highlighted an urgent need for robust vulnerability management strategies to address potential security risks in this dynamic environment.

IoT

The proliferation of IoT devices presents another facet of evolving attack surfaces. While convenient, these devices often lack adequate security measures, leaving them vulnerable to cyberattacks such as botnets and DDoS attacks.

In August 2020, security researchers found FritzFrog, a novel, elusive and highly scalable botnet engineered to operate on compromised IoT devices like routers, diverging from the usual server or computer targets.

Expanding Attack Surfaces and the Strategic Imperative of IAM

Third Party Vendors

Third-party vendors, critical for services like payment processing and data storage, are increasingly targeted by cybercriminals. Unfortunately, these vendors may not be able to maintain the same level of security controls as the organizations they serve.

Supply Chain Attack

The concept of attackers leveraging attack surfaces within third parties to ultimately reach an intended victim

The Business Case for IAM

Here's a quick look at the repercussions of cybercrimes directly correlating with the business case for IAM implementation:

Data Protection and Privacy Compliance

Businesses face increasing pressure to safeguard sensitive data and comply with stringent data protection regulations such as GDPR, CCPA, and others. IAM solutions provide granular control over user access, ensuring that only authorized individuals can access sensitive information. By implementing IAM, businesses can demonstrate their commitment to data privacy compliance, thereby mitigating the risk of costly fines and reputational damage associated with non-compliance.

Prevention of Data Breaches and Insider Threats

Data breaches often originate from compromised user credentials. IAM solutions help prevent unauthorized access by enforcing strong authentication measures, such as multi-factor authentication and biometric authentication. By implementing IAM, businesses can significantly reduce the risk of data breaches and insider threats, thereby safeguarding sensitive information and intellectual property.

Enhanced Operational Efficiency

Cybercrimes can disrupt business operations, resulting in downtime, productivity losses, and increased IT support costs. IAM solutions streamline user access management processes by automating user provisioning, deprovisioning, and access requests. This reduces administrative overhead, accelerates user onboarding and offboarding, and enhances overall operational efficiency.

Protection of Brand Reputation

The fallout from a cybersecurity incident can tarnish a business's brand reputation and erode customer trust. IAM solutions bolster security defenses, instilling confidence among customers, partners, in the business's ability to protect their data. This means, better brand reputation and improved customer loyalty.

Cost Savings and ROI

The financial implications of cybercrimes can be substantial, encompassing expenses related to incident response, legal fees, regulatory fines, and loss of revenue. IAM solutions offer a proactive approach to cybersecurity, helping businesses mitigate the financial risks associated with cyber threats.

Understanding IAM

The cybersecurity sector acknowledged long ago that traditional perimeter security measures were inadequate. With the advent of the COVID-19 pandemic, it's now evident that the concept of an infrastructure perimeter is obsolete. In this new paradigm, identity emerges as the primary perimeter, with identity-centric tools such as Access Management, Privileged Access Management (PAM), and Identity Governance & Administration (IGA) taking the spotlight. These solutions are now pivotal in fortifying organizations' security posture on a global scale.

Understanding IAM

Single Sign-On (SSO): SSO allows users to authenticate once and gain access to multiple systems or applications without the need to re-enter credentials. Popular SSO solutions include Okta, Microsoft Azure Active Directory, and Ping Identity.

Multi-Factor Authentication (MFA): MFA adds an extra layer of security by requiring users to provide multiple forms of authentication, such as passwords, security tokens, biometrics, or SMS codes. Tools like Duo Security, Google Authenticator, and RSA SecurID provide MFA capabilities.

Identity Governance and Administration (IGA): IGA solutions manage user identities, access rights, and permissions across the organization. They help streamline user provisioning, de-provisioning, access request, and access certification processes. Examples include SailPoint IdentityIQ, IBM Security Identity Governance, and Oracle Identity Governance.

Privileged Access Management (PAM): PAM tools manage and monitor access to privileged accounts and sensitive resources to prevent unauthorized access and mitigate insider threats. Solutions like CyberArk Privileged Access Security, BeyondTrust Privileged Access Management, and Thycotic Secret Server fall into this category.

Directory Services: Directory services store and manage user identities and attributes, often serving as a central repository for authentication and authorization processes.

Understanding IAM

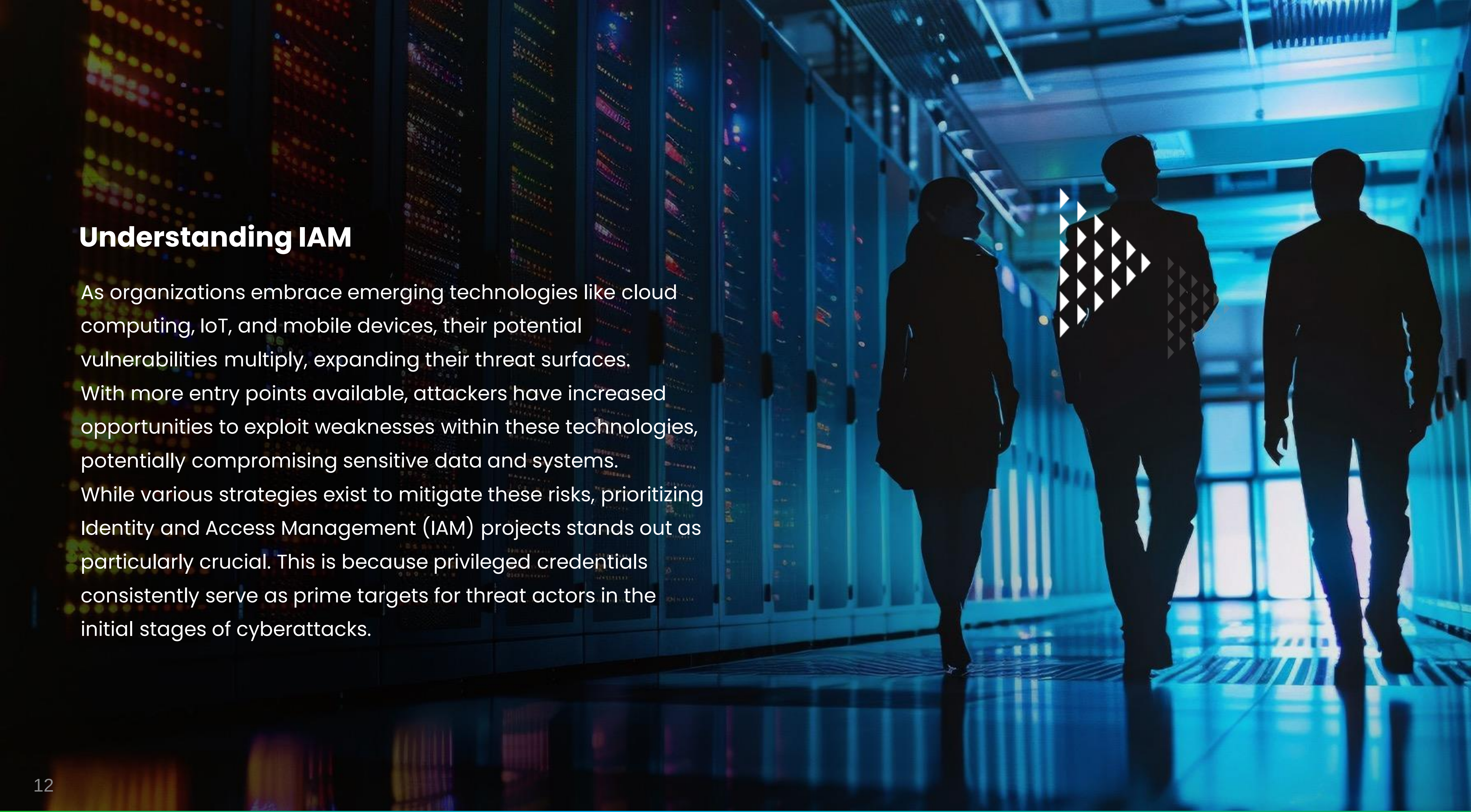
Identity as a Service (IDaaS): IDaaS platforms offer IAM functionality through cloud-based services, allowing organizations to manage user identities and access across various cloud and on-premises applications. Examples include Okta Identity Cloud, Microsoft Azure Active Directory, and OneLogin.

User Provisioning and Lifecycle Management: These tools automate user provisioning and de-provisioning processes, ensuring that users have appropriate access based on their roles and responsibilities. Solutions like Oracle Identity Manager, CA Identity Manager, and Microsoft Identity Manager (MIM) offer provisioning capabilities.

Role-Based Access Control (RBAC): RBAC systems define and enforce access permissions based on users' roles within the organization. They help simplify access management by assigning permissions to roles rather than individual users. Some IAM platforms include built-in RBAC functionality, while others integrate with dedicated RBAC tools.

Access Management APIs: APIs (Application Programming Interfaces) facilitate integration between IAM systems and other applications, enabling seamless authentication and authorization processes. IAM vendors often provide APIs for developers to build custom integrations with their applications.

Audit and Compliance Tools: These tools provide visibility into user access activities, monitor for suspicious behavior, and help organizations meet regulatory compliance requirements. Examples include Splunk, IBM QRadar, and RSA NetWitness.



Understanding IAM

As organizations embrace emerging technologies like cloud computing, IoT, and mobile devices, their potential vulnerabilities multiply, expanding their threat surfaces.
With more entry points available, attackers have increased opportunities to exploit weaknesses within these technologies, potentially compromising sensitive data and systems.
While various strategies exist to mitigate these risks, prioritizing Identity and Access Management (IAM) projects stands out as particularly crucial. This is because privileged credentials consistently serve as prime targets for threat actors in the initial stages of cyberattacks.

Assessing Your Organization's IAM Needs

Strengthen your organization's security posture, mitigate risks, and foster a culture of resilience in the face of evolving cybersecurity challenges.

Unveiling Security Insights

Begin by conducting a comprehensive security audit to evaluate the current state of your organization's digital infrastructure. Assess existing security policies, protocols, and controls to identify potential vulnerabilities and areas for improvement. Evaluate past security incidents, if any, to glean insights into recurring patterns and emerging threats. By gaining a holistic understanding of your organization's security posture, you can lay the groundwork for an effective IAM strategy.

Mapping User Responsibilities

Next, identify and define the various user roles and responsibilities within your organization. Collaborate with key stakeholders across departments to map out the different roles and their corresponding access requirements. Consider factors such as job functions, hierarchy, and the principle of least privilege to ensure that users have access only to the resources necessary to perform their duties. By establishing clear user roles and responsibilities, you can streamline access management processes and minimize the risk of unauthorized access.

Assessing Your Organization's IAM Needs

Unraveling Existing Control Complexities

Evaluate the effectiveness of your organization's existing access controls and authentication mechanisms. Assess the strength of password policies, multi-factor authentication (MFA) implementation, and access control lists (ACLs) governing resource access. Identify any gaps or weaknesses in access controls that could potentially be exploited by malicious actors. Additionally, examine the usability and user experience of access management tools to ensure they align with organizational needs and security objectives.

Navigating Regulatory Waters

Determine the regulatory and compliance requirements relevant to your industry and geographic location. Identify specific regulations, such as GDPR, HIPAA, or SOX, that impose requirements related to identity and access management. Evaluate your organization's current compliance posture and assess the extent to which existing IAM practices align with regulatory mandates. Establish a roadmap for achieving and maintaining compliance, incorporating necessary changes and enhancements to your IAM strategy.

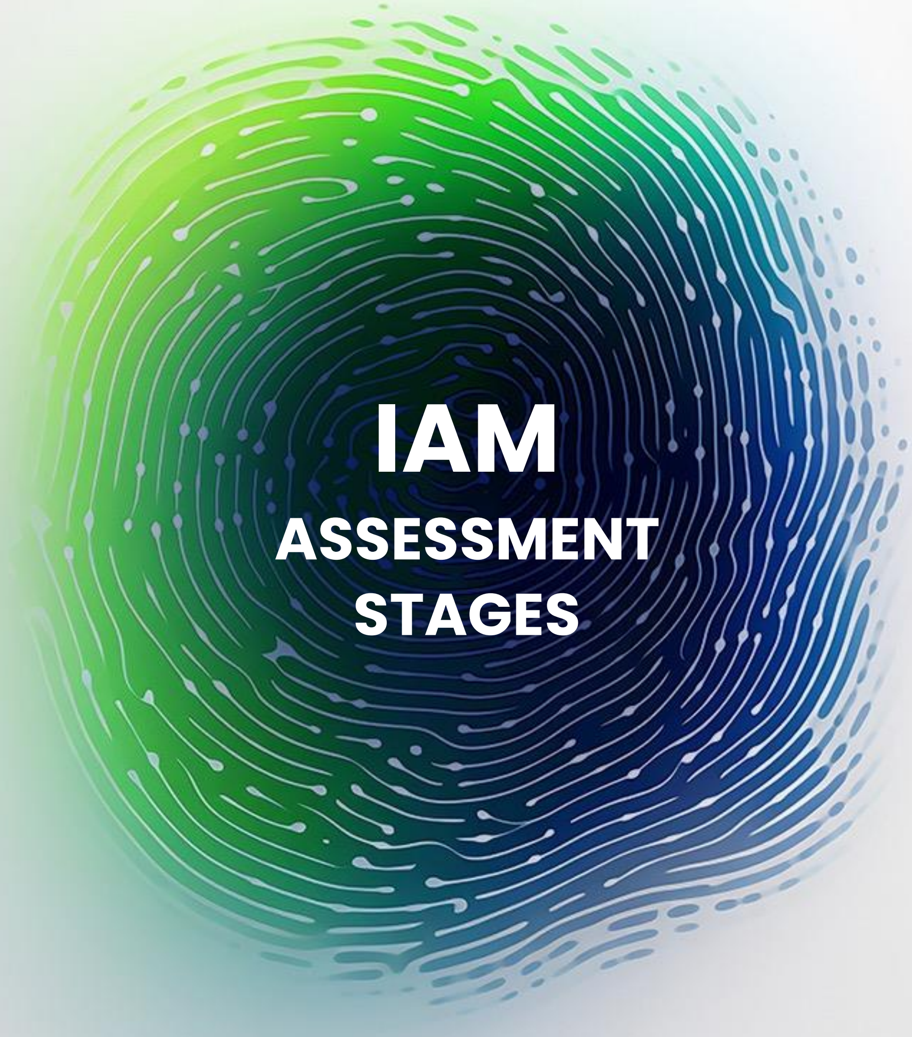
Assessing Your Organization's IAM Needs

WHY

Evaluate network users within the organization and ascertain resource accessibility for each

WHAT

Identify network assets, physical infrastructure, and applications requiring protection.



IAM

ASSESSMENT STAGES

WHERE

Determine remote work locations and out-of-office user connections to assess network accessibility.

WHEN

Define user connection patterns based on work schedules to detect anomalies.

HOW

Analyze procedure effectiveness to meet IAM compliance.

IAM

Best Practices Checklist

Your IAM Best Practices Checklist to help effectively implement IAM, enhance your security posture and mitigate risks effectively.

IAM Best Practices Checklist

Conduct regular security audits to identify vulnerabilities and gaps, ensuring a proactive approach to threat detection and mitigation.

Define clear user roles and responsibilities based on job functions, ensuring that access privileges are aligned with organizational needs and security requirements.

Implement strong authentication methods such as multi-factor authentication, adding an extra layer of security to user accounts and reducing the risk of unauthorized access.

Enforce the principle of least privilege to restrict access to only necessary resources, minimizing the potential impact of security breaches and insider threats.

Monitor and analyze user access patterns for suspicious behavior, enabling early detection of anomalous activities and potential security incidents.

Review and update access controls regularly to reflect organizational changes, ensuring that access permissions remain accurate and up-to-date.

Encrypt sensitive data both at rest and in transit, safeguarding confidential information from unauthorized access and interception.

Establish and enforce strong password policies, including regular password rotation and the use of complex passwords, to enhance the security of user accounts.

Implement automated provisioning and deprovisioning processes for user accounts, streamlining user management tasks and reducing the risk of orphaned accounts.

Stay compliant with relevant regulations and standards, such as GDPR, HIPAA, and PCI DSS, by adhering to industry best practices and implementing appropriate security measures.

Working With an IAM Partner

Embarking on the journey of implementing an Identity and Access Management (IAM) solution can be a daunting task, but with the right IAM partner by your side, it becomes a seamless and rewarding experience. Find out four ways how partnering with an IAM expert can propel your organization towards success.

Working With an IAM Partner

Installation and Configuration

When it comes to the intricate process of installing and configuring IAM solutions, an IAM partner proves invaluable.

With their specialized knowledge and experience, they ensure that the IAM solution is implemented correctly, tailored precisely to your organization's needs. From setting up user authentication protocols to defining access policies, every aspect is meticulously handled to maximize security and efficiency.

Integration with Existing Systems

Seamlessly integrating an IAM solution with your organization's existing systems is crucial for smooth operations.

An IAM partner brings expertise in system integration, allowing them to navigate complexities and ensure compatibility with various platforms and technologies. Whether it's integrating with Active Directory, cloud services, or custom applications, they ensure that the IAM solution seamlessly fits into your existing infrastructure, minimizing disruption and maximizing value.

Working With an IAM Partner

Thorough Testing

Testing is a critical phase of the IAM implementation process, and an IAM partner ensures that no stone is left unturned.

Through comprehensive testing procedures, including functional testing, penetration testing, and user acceptance testing, they validate the effectiveness and reliability of the IAM solution. By identifying and addressing any potential issues or vulnerabilities proactively, they guarantee a robust and reliable IAM solution that meets your organization's security and operational requirements.

Addressing Challenges

Despite meticulous planning, challenges may arise during the IAM implementation journey.

Whether it's technical complexities, organizational resistance, or unforeseen obstacles, an IAM partner is well-equipped to navigate through them. Drawing on their experience and expertise, they provide valuable insights, guidance, and support, enabling your organization to overcome challenges and achieve its IAM goals seamlessly. With their assistance, you can confidently address any hurdles and ensure the successful implementation and adoption of IAM solutions within your organization.

The Path Ahead: Securing Tomorrow's Digital Frontier

In conclusion, mastering Identity and Access Management (IAM) is paramount in safeguarding organizations against the evolving threats of modern cybersecurity. Throughout this guide, we've explored key IAM concepts, from user authentication to access controls, highlighting the critical role they play in protecting digital assets and data integrity.

As we reflect on the importance of IAM, it becomes evident that it serves as the cornerstone of effective cybersecurity strategies. By implementing robust IAM practices, organizations can fortify their defenses, mitigate risks, and uphold regulatory compliance standards.

However, our journey doesn't end here. In the ever-changing cybersecurity landscape, continuous improvement and adaptation are imperative. As new threats emerge and technologies evolve, organizations must remain vigilant, embracing innovation and staying abreast of emerging trends in IAM.

Shekhar Joshi

CISO

Xoriant's Vice President of Technology and Chief Information Security Officer (CISO), Shekhar Joshi, is a seasoned professional with an impressive track record spanning over 26 years in the realm of technology-driven practice development and delivery. As the helm of Xoriant's Cloud Infrastructure and Security practice, Shekhar holds the responsibility of spearheading cutting-edge advancements in cloud and security delivery while crafting innovative, customer-centric solutions that redefine industry standards.

About Xoriant

Xoriant provides software development, infrastructure modernization & migration, data engineering, and security services for global banks, software product companies and F500 market leading enterprises. Headquartered in the U.S. with 18 global offices and 5000+ engineering professionals, we deliver technology consulting as well as onsite and offshore services. Our industry expertise spans high tech, banking & financial services, insurance, healthcare, pharma, industrial manufacturing, telecom, retail, and automotive sectors. Customers credit technological innovation and delivery excellence for our shared success over three decades.