# The critical role of identity security in business applications



In recent discussions surrounding the role of identity security in business applications, experts emphasize the increasing dependence on various business software solutions, particularly Enterprise Resource Planning (ERP), Customer Relationship Management (CRM), and Human Capital Management (HCM) systems, to safeguard sensitive data. The discourse highlights the significant risks associated with compromised access, particularly as human capital and client information become more integrated into digital workflows.

These critical business applications often contain personal private information (PII), intellectual property, and financial data, making the management of user access crucial for preserving both trust and business continuity. Access to these applications is typically governed by key personnel such as heads of sales operations or finance, and it is important that they collaborate closely with IT and security teams to effectively manage this access over time.

According to findings presented by the Verizon 2024 Data Breach Investigations Report, approximately 31% of data breaches in the past decade can be traced back to identity or credential compromise. This statistic underscores the foundational importance of protecting enterprise identities and sets the stage for understanding the challenges typically faced by organisations.

One major concern highlighted is the challenge of managing credential access efficiently across multiple applications. Often, enterprise users have unique identities managed through directories like Entra ID or Azure Active Directory, but may lack centralised oversight of their access to business applications. This disconnection can lead to users juggling different usernames and passwords, heightening the risk of credential mismanagement.

The risk is compounded by the issue of excessive permissions. Where a cyberattacker successfully obtains credentials, they can exploit all the permissions associated with that account, which can have dire consequences for an organisation. Challenges arise because many business applications offer limited access levels, often resulting in users possessing more access than their roles necessitate.

Furthermore, businesses must also navigate the complexities associated with the lifecycle of user access, particularly in instances such as employee transitions. When individuals change roles or leave an organisation, there is often a lag in the necessary adjustments being made to their application access. Without timely deprovisioning, users may retain permissions that exceed their requirements, creating further vulnerabilities.

The report also raises concerns over the risks that third-party access can introduce, as contractors may continue to possess access rights long after their work is completed. Ensuring accurate tracking of this access becomes a challenge, especially in organisations that rely on informal communication to manage permissions.

Segregation of Duties (SoD) conflicts also pose significant risks within business environments. As the procedures for IT and application provisioning are often disconnected, companies might fail to identify potential access conflicts, inadvertently opening the door to fraud.

Experts stress the importance of integrated Identity and Access Governance (IGA) solutions, which can help bridge the gap between business application owners and IT security teams. By consolidating access provisioning within an identity security framework, organisations can establish consistent and secure access protocols, enabling the adoption of best practices in identity management. IGA solutions allow for automated provisioning and deprovisioning processes, ensuring that access aligns with the principle of least privilege and reducing reliance on manual processes that are often prone to error.

As the wave of digital transformation continues to reshape the business landscape, the imperative for robust identity security frameworks within business applications becomes ever more critical for protecting sensitive data and maintaining operational integrity.

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.sailpoint.com/products/identity-security-cloud> - This link supports the importance of integrated Identity and Access Governance (IGA) solutions and the need for a unified identity security platform to manage and secure access to critical data and applications.
2. <https://www.techtarget.com/searcherp/feature/The-10-most-common-ERP-security-issues-and-ways-to-fix-them> - This article highlights common ERP security issues such as weak ERP authentication, missing software updates, and web application-specific vulnerabilities, which corroborate the risks associated with compromised access and the need for strong identity security.
3. <https://www.cyberark.com/resources/ebooks/identity-security> - This resource explains the importance of modern Identity Security in managing today's identity sprawl, the inadequacy of traditional access management solutions, and the benefits of a unified identity security framework, aligning with the need for robust identity security in business applications.
4. <https://www.rpic.com/blog/erp-security-best-practices/> - This blog post discusses ERP security risks, including weak authentication, excessive permissions, and the importance of multi-factor authentication, which supports the challenges and best practices in managing access to business applications.
5. <https://www.sailpoint.com/products/identity-security-cloud> - This link details the importance of managing credential access efficiently across multiple applications and the risks associated with excessive permissions, as well as the need for centralized oversight and automated provisioning and deprovisioning processes.
6. <https://www.techtarget.com/searcherp/feature/The-10-most-common-ERP-security-issues-and-ways-to-fix-them> - This article emphasizes the risks introduced by third-party access and the need for accurate tracking of such access, which is a critical aspect of managing user access lifecycle and permissions.
7. <https://www.cyberark.com/resources/ebooks/identity-security> - This resource discusses the challenges of managing the lifecycle of user access, particularly during employee transitions, and the importance of timely deprovisioning to prevent vulnerabilities.
8. <https://www.rpic.com/blog/erp-security-best-practices/> - This blog post highlights the importance of Segregation of Duties (SoD) and the risks associated with SoD conflicts, which can be mitigated through integrated IGA solutions.
9. <https://www.sailpoint.com/products/identity-security-cloud> - This link explains how integrated IGA solutions can help bridge the gap between business application owners and IT security teams, ensuring consistent and secure access protocols.
10. <https://www.cyberark.com/resources/ebooks/identity-security> - This resource underscores the critical need for robust identity security frameworks within business applications to protect sensitive data and maintain operational integrity in the face of digital transformation.
11. <https://www.rpic.com/blog/erp-security-best-practices/> - This blog post reinforces the importance of best practices in identity management, including the use of multi-factor authentication and clear password security guidelines to mitigate various security risks.
12. <https://erp.today/identity-security-for-business-applications/> - Please view link - unable to able to access data