IS5104-P2: Storing Financial Models On a Shared Drive

220034672

March 27, 2024

In small and medium-sized enterprises (SMEs), Excel spreadsheets are the cornerstone of financial management, used by over 80%of businesses[6]. The shift towards shared drives, including cloud solutions—adopted by 97% of SMEs[11]—facilitates collaboration but introduces significant security risks. Surveys show that around 60% of SMEs have 100,000 broadly accessible folders [14], contributing to approximately 25 monthly data breaches [4], highlighting the critical challenge of safeguarding financial information while maintaining operational efficiency. The following sections will explore these risks and propose mitigation strategies.

A secure system safeguards its data and resources from unauthorised access, modification, or disruption while guaranteeing authorised users access [12]. Suppose spreadsheets are on shared drives; permission to whole folders rather than specific files exposes sensitive financial data to users who may alter or view confidential information. Additionally, the absence of solid version control makes the problem of access control even worse. Multiple versions of a spreadsheet may exist, which can confuse users and make them use outdated information. Incorrect data could lead to severe financial losses when used for decision-making processes.

Implementation of document management systems (DMS) can address the issue of access control [9]. DMS granular access controls allow administrators to assign permissions to distinct model sections for specific groups or individuals. DMS often employs role-based control (RBAC) or attribute-based access control (ABAC) models, which grant access decisions based on specific characteristics of users, data, and actions [3]. These models ensure that only authorised individuals may read or write data, lowering the likelihood of breaches and the risks associated with shared drives.

Authentication is essential to determining access rights to data when storing financial spreadsheets in a shared environment. However, data breaches can occur internally if access rights are too broad or if more attention needs to be paid to employee behaviour. If employees use mobile devices to access data, the loss of the mobile device puts the data at risk of being compromised. Further, the enterprise's online sharing platform may provide limited security protection. Attackers can exploit platform vulnerabilities and expose our data.

Two-factor authentication (2FA) is more effective in preventing password attacks than setting a 'strong password'[15]. By using two elements to prove identity, for example, based on face recognition and a one-time code sent via SMS, these systems implement the assumption of behavioural biometric authentication and physiological biometric authentication since the received code is entered by sliding the finger on the screen [1] - effectively preventing remote attacks. Role-based access control (RBAC) assigns users to roles and assigns permissions to roles. Users obtain permissions by becoming members of roles. Only the role currently responsible for the business can obtain permissions, reducing the risk of internal data leakage. Enterprises should choose a trusted sharing platform service provider to store spreadsheets, educate employees on cyber attacks, and implement secure remote device management, such as device encryption. To effectively prevent data threats, enterprises must provide security protection from human and system vulnerabilities.

Financial models are vulnerable to security risks during storage and transmission, exposing them to data leakage and theft threats that can lead to substantial losses. However, these vulnerabilities can be mitigated by implementing robust data encryption and secure transmission technologies that ensure integrity and confidentiality. Companies that do not take these vulnerabilities seriously risk reputational damage and legal liability.

Encryption technology is key to information security, with standard techniques such as symmetric and asymmetric encryption. While encryption technology plays a critical role in safeguarding financial data, it is essential to acknowledge weaknesses. Vulnerabilities such as outdated encryption algorithms or improper key management practices may compromise data security [7]. Additionally, inadequate access control measures may lead to unauthorised access and potential data breaches. Potential attack vectors include malicious actors, malware, and social engineering tactics. Notably, the xSE-ACAS model [13] and hybrid encryption technology [17] are innovative approaches for data protection.

Additionally, secure transmission practices are susceptible to various challenges and issues. For instance, without robust authentication mechanisms, data transmitted over networks may still be vulnerable. Weak encryption protocols or insecure communication channels could expose transmitted data to unauthorised access or malicious attacks, compromising its confidentiality and integrity. The NOSDT algorithm's utilisation to classify nodes, analyse the behaviour of malicious nodes, and select reliable nodes for safe data transmission improves the security and transmission rate [10].

Storing financial data requires a rigorous audit to ensure its confidentiality, integrity, and availability. Auditing is a traceability mechanism that acts as a posteriori and a deterrent to unauthorised data modification and interception. We will design a general system based on [2] that logs the subjects, objects, and actions relevant to security policy violations, such as security level, writes, reads, and temporal and geographical information by ISO/IEC 27001 standards [8]. The log passes state changes to an analyser, where we set rules and axioms - a matrix of permissions for actions, objects and subjects at differing security levels - to identify suspicious activity. These stringent classifications will match the RBAC system, ensuring classification-bound adherence. The notifying system will alert the security team if suspicious activity is detected or alerts security defence systems if the threat is severe.

Naturally, processing everything across all representations and pathways is infeasible, so we suggest an adaptive logging system that aligns with the data's sensitivity classification. Further refinement will operate on a continuous feedback loop operationalising feedback from security incident investigations. We must integrate the discovered audit trails with the current security incident and event management solution for a faster and more robust response. Training will need to be provided to clarify the roles, responsibilities and best practices of the primary and secondary actors within the organisation regarding adherence to the system and, more generally, state laws concerning this environment.

Finally, supply chain attacks pose another threat to the new implementation mechanism. These attacks occur when malicious actors penetrate the software or hardware vendors upstream of the enterprise, implanting malicious code in their products or services, thereby compromising the data security of downstream users. Such attacks may lead to data leakage or ransomware infection, significantly impacting SMEs' finances, reputation, and operations. In 2022, Cloud-Based attacks increased by 48%[5], and 82% of CIOs expressed concerns about the potential negative impact of compromises to their cloud storage service providers[6]. Actual world incidents validate this concern. Despite significant investments in protection by cloud providers, data remains at risk. For instance, in 2019, cloud storage provider Citrix fell victim to a significant supply chain attack, compromising 6TB of internal data[7].

Additionally, office software like Excel faces similar supply chain security issues. Its extensive ecosystem of third-party plugins offers customisation options but also introduces vulnerabilities exploited in cybercrime campaigns, leading to data theft, ransomware, and other cybercrime[8]. Therefore, SMEs should raise awareness of supply chain security and take action, such as supplier risk management and assessing software qualifications, cloud services, and other suppliers. Third-party assessment should be introduced when necessary.

In conclusion, safeguarding financial models in SMEs extends beyond technological fixes to embody a culture of security awareness and proactive risk management. Emphasizing continuous employee education, regular security audits and strong leadership commitment is essential. By integrating advanced security measures with a vigilant organizational culture, SMEs can enhance their defences against evolving threats, ensuring their data's integrity and operational continuity. This holistic approach to cybersecurity fosters an environment where digital innovation thrives alongside robust security practices, positioning SMEs for sustainable growth in an increasingly digital landscape.

References

[1] Bartłomiejczyk, M., Imed, E.F., and Kurkowski, M., [n.d.]. *Multifactor Authentication Protocol in a Mobile Environment*. Available at: https://ieeexplore.ieee.org/document/8879478 [Accessed 24 March 2024].

[2] Bishop, M., 2005. *Introduction to Computer Security*. Boston, MA: Addison-Wesley. ISBN 978032124744.

[3] Chiquito, A., Bodin, U., & Schelen, O., 2023. *Attribute-Based Approaches for Secure Data Sharing in Industrial Contexts* (Vol. 11). Available at: https://doi.org/10.1109/ACCESS.2023.3240000 [Accessed 24 March 2024].

[4] Code42, [n.d.]. *2023 Data Exposure Report*. Available at: https://www.code42.com/resources/report/2023-data-exposure-report/ [Accessed 24 March 2024].

[5] Check Point Research Team, [n.d.]. *Check Point Research flags a 48% growth in cloud-based networks attacks in 2022, compared to 2021*. Check Point Software Technologies Ltd. Available at: https://blog.checkpoint.com/2023/01/17/check-point-research-flags-a-48-growth-in-cloud-based-networks-attacks-in-2022-compared-to-2021/ [Accessed 24 March 2024].

[6] Foley, M.J., [n.d.]. *Forrester: Google still A Distant Office competitor*. ZDNet. Available at: https://www.zdnet.com/article/forrester-google-still-a-distant-office-competitor/ [Accessed 24 March 2024].

[7] Grobauer, B., Walloschek, T., and Stocker, E., 2011. *Understanding Cloud Computing Vulnerabilities*. *IEEE Security & Privacy*, 9(2), pp. 50-57. Available at: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5487489&isnumber=5739630 [Accessed 24 March 2024]. DOI: 10.1109/MSP.2010.115.

[8] International Organization for Standardization, 2013. ISO/IEC 27001:2013 *Information technology — Security techniques — Information security management systems — Requirements*. Geneva: International Organization for Standardization.

[9] Kurteva, K., 2023. *Compliance and Data Security in Document Management Systems*. 2023 XXXII International Scientific Conference Electronics (ET), pp. 1-5. Available at: https://doi.org/10.1109/ET59121.2023.10279617 [Accessed 24 March 2024].

[10] Li, X., and Wu, J., [n.d.]. *Node-Oriented Secure Data Transmission Algorithm Based on IoT System in Social Networks*. Available at: https://doi.org/10.1109/LCOMM.2020.3017889 [Accessed 24 March 2024].

[11] McAfee, [n.d.]. *Navigating a cloudy sky*. Available at: https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-navigating-cloudy-sky.pdf [Accessed 24 March 2024].

[12] Sandhu, R.S., & S.P., 2005. *Access Control: Principles and Practice. IEEE Security & Privacy*.

[13] Thouraya Bouabana-Tebibel, and Kaci, A., [n.d.]. *Parallel search over encrypted data under attribute-based encryption on the Cloud Computing*. Available at: https://doi.org/10.1016/j.cose.2015.04.007 [Accessed 24 March 2024].

[14] Varonis, 2021. *2021 data risk report: Financial services*. Available at: https://www.varonis.com/2021-data-risk-report [Accessed 24 March 2024].

[15] Wiefling, S., Dürmuth, M., and Lo Iacono, L., [n.d.]. *Verify It's You: How Users Perceive Risk-Based Authentication*. Available at: https://ieeexplore.ieee.org/document/9442838 [Accessed 24 March 2024].

[16] Zhang, Q., [n.d.]. *An Overview and Analysis of Hybrid Encryption: The Combination of Symmetric Encryption and Asymmetric Encryption*. Available at: https://doi.org/10.1109/CDS52072.2021.00111 [Accessed 24 March 2024].