A System-Based Proposal to Improve Cybersecurity in Construction Organisations

Chua Sin Nee., Muhammad Daniel bin Muhamad Subri., Ng Shi Chun., Oh Jia Min., Ong Yi Ying., Fuziah Ismail., Norhazren Izatie Mohd

Faculty of Built Environment and Surveying, Universiti Teknologi Malaysia, 81300 Johor Bahru, Johor, Malaysia

DOI: https://doi.org/10.47772/IJRISS.2026.10200167

Received: 11 February 2026; Accepted: 16 February 2026; Published: 27 February 2026

ABSTRACT

This study investigates the critical cybersecurity vulnerabilities in construction organizations that manage sensitive project data. The primary weakness identified was reliance on consumer-grade digital tools and single-factor authentication, which exposed the organization to phishing attacks, credential compromise, and unauthorized data access. Although prior research has highlighted the risks of digital transformation in the construction sector, a clear gap remains in the practical integration of unified cybersecurity platforms into operational workflows. A System Development Life Cycle (SDLC) methodology was adopted to evaluate existing security processes, identify system deficiencies, and define technical requirements. Based on this assessment, the study proposed the structured implementation of Microsoft 365 Business Premium as a centralized cybersecurity framework. Key components included AI-driven email threat protection via Defender for Office 365, secure cloud governance through OneDrive and SharePoint, and enforcement of multi-factor authentication. The findings indicate that transitioning from fragmented "Shadow IT" practices to an integrated enterprise-level security environment significantly reduces the likelihood of account compromise and enhances operational transparency. The study offers a scalable, practical framework for strengthening data protection and safeguarding decision-making integrity in construction organizations. Implementing enterprise-grade cybersecurity controls is essential to sustaining client trust and ensuring project continuity in an increasingly digital operating environment.

Keywords: Cybersecurity, Construction Industry, Digital Transformation, Microsoft 365, System Development Life Cycle (SDLC), Data Security**,** Built Environment.

INTRODUCTION

In recent years, the construction industry experienced a significant increase in the usage of digital technologies. Drawings, tender documents, cost data, and project correspondence are now frequently managed using tools such as email, cloud storage, and online collaboration platforms. These digital systems facilitate daily operations and enable teams in professional service firms, such as quantity surveying consultancies, to collaborate more effectively across multiple locations. As a result, many organizations now depend heavily on digital systems to support their daily operations.

However, the way digital tools are used is not always supported by proper cybersecurity practices. It is common for employees to rely on personal cloud storage accounts, basic email services, and simple password-based logins because they are convenient and familiar. These techniques may make daily work easier, but they typically fail to give much control over who can access the information and how it is shared. This makes it more likely that phishing attacks, unauthorized access, and inadvertent leaks of important project and client information will happen (Naqvi et al., 2023).

This study examines how many construction firms persist in employing fragmented and outdated cybersecurity practices that are insufficient for safeguarding digital data in a cloud-based work setting. It is challenging for businesses to keep their data safe and respond to cyber threats when they rely on consumer-grade technologies

and single-factor authentication. Cybersecurity is frequently discussed in general business and technology classes. However, construction companies still lack useful guidance on how to improve their cybersecurity systems in a way that works for their organization.

Most research focuses on explaining the cybersecurity risks or security concepts at a general level. However, fewer people are paying attention to how construction organizations can realistically move from informal digital practices to a more organized and safer system. This gap is important for small and medium enterprises that may not have specialized IT staff to implement complex security measures without clear instructions.

Microsoft 365 Business Premium is the option. It offers productivity apps and strong security features, including multi-factor authentication (MFA), AI-driven threat prevention for email and collaboration, and managed cloud storage (Microsoft2026). L. A. Meyer et al. (2023) found thacorrectly implementing MFA alone can reduce the probability of account breaches by more than 99%.

This paper aims to examine the current cybersecurity practices of construction organizations, identify key weaknesses in digital communication and data management, and propose a systematic implementation of Microsoft 365 Business Premium, applying the System Development Life Cycle method to enhance data protection, strengthen security measures, and facilitate safer digital operations.

Problems Statement

The existing cybersecurity at the Quantity Surveying (QS) company has severe vulnerabilities that pose a risk of unauthorized access, phishing, and confidential data leaks. Since the company relies heavily on email communication and uses conventional password-based authentication and unregulated file-sharing methods, these vulnerabilities place sensitive project-related documentation and client-related information at risk of falling into the hands of cybercriminals. It has been established that phishing is one of the most commonly used attack techniques against organizations, and human errorontinues to feature prominently in successful breaches (Althobaiti & Alsufyani, 2024). This is becoming a major concern for the company, as it has recently encountered many cases involving malicious email use and intruder or hacker logins. These vulnerabilities affect the confidentiality and integrity of tender documents, cost estimates, contracts, and variation claims, which are communicated daily via email and cloud services in a construction and quantity surveying setting.

Other studies also note that, despite visual recognition of a phishing warning, urgent or threatening text in emails can still prompt users to trust malicious emails (McAlaney & Hills, 2020). This is consistent with the problem the firm is currently facing: employees are constantly subjected to spoofed content or fraudulent attachments, but they lack the technological tools to identify or prevent such threats before they fall victim. Phishing attacks may bypass traditional filters and reach employees' inboxes without even using sophisticated email security software, such as artificial intelligence (AI) or sandboxing. Manipulated tender submissions, exposure of commercially sensitive pricing information or unauthorized modification of project documentation can follow a successful phishing attack in this context, resulting in financial loss and contract disputes.

Furthermore, another weakness is that the firms rely solely on single-factor authentication, such as weak password systems. This type of authentication is a target for credential theft because it can be easily cracked. Once they gain access to the account, the thief can obtain open access to the drives, email accounts, and cloud platforms and share or copy the data. This is to reduce the risk of unauthorized access to our data or credential misuse(Mostafa et al., 2023). However, in reality, many firms still do not use MFA, which makes their accounts highly susceptible to credential theft or hacking. Since construction teams often use the same devices and systems across site offices, shared devices, and other remote locations with connected access, leaked credentials could enable attackers to log into numerous projects at the same time without becoming a high-profile target.

Other than that, the usage of unregistered cloud storage applications through online platforms such as Google Drive or Dropbox personal account indirectly generates an unmonitored platform because no one keeps an eye on it at all times, where sensitive data or documents can be easily passed on, moved, copied or saved beyond the authority control or limitations of the organizations. This is a severe threat to data management and does not follow proper data-handling security standards. Unusual activities, such as unauthorized logins by another party

or excessive file downloads, can only be noticed by the user after their account has been breached. That thing happened because there was no real-time data monitoring system or an unusual behaviour-based threat system in place. Research also has shown the importance of combining an AI-based threat system with real-time or continuous data monitoring for early detection of anomalous behaviour and as an early-prevention measure against data breaches(Loh et al., 2024). The uncontrolled use of personal cloud storage is especially important in construction organizations, where drawings, BIM models, and client contracts are frequently exchanged among consultants and subcontractors, which is more likely to lead to the uncontrolled spread of data.

Review Of The Current Approach

Consumer-grade digital tools, Shadow IT, and single-factor authentication (SFA) are the three types of products and practices that significantly influence the organization's contemporary digital environment and daily operations. Because construction teams need quick decision-making, mobile communication, and simple file sharing across scattered project sites, these tools become ingrained over time. Similar findings are highlighted in construction cybersecurity research, where convenience often outweighs formal security governance, as nod by Turk et al. (2022). Sensitive architectural drawings, BIM models, project tenders, and contract data are not protected by these tools, even though they boost productivity and give employees flexibility. A comprehensive examination of each technology shows that the security disadvantages greatly exceed the operational gains as online risks increase across Construction 4.0 settings, according to Tanga et al. (2022).

Though the company relies on consumer-level services for personal Dropbox or Google Drive accounts, Gmail email, and WhatsApp messaging, there are both positive and negative aspects of this approach. The use of consumer-level platforms enhances the company's accessibility, efficiency, and communication among contractor and project teams, which explains why SMEs widely adopt them, as they require less training and lower installation costs for an information management system at the workplace than a business system. Consumer-level platforms mainly rely on personal accounts and file sharing for unofficial use, with no accountability, unlike the business system. According to Sonkor & García de Soto (2021), critical design and project papers are retained and sharedcross multiple devices and communication systems without adequate security measures, making them vulnerable, especially in a construction sector context. Data misuse due to poor personal account protection and a lack of standard data-handling procedures makes these systems prone to loss, unlawful access, and data fraud, which can easily occur without proper data safety despite meeting basic operational requirements. The ineffectiveness of current technological systems to address data safety within a multi-stakeholder construction environment presents a clear weakness that calls for development to address organizational digital insecurity, despite meeting basic operational requirements.

In construction projects, employee use of approved software or cloud services, also known as “Shadow IT,” offers immediate productivity benefits but poses grave risks to project and company information security. Shadow IT enables faster responses to construction project schedules, which are rigid yet flexible within project cycles, compared to approved company IT systems. Shadow IT also arises from insufficient organizational digital systems to supportn-site operational processes, as stated by Yao & García de Soto (2024). However, because it is beyond the IT department's control, it is difficult to monitor data flows, improve security, or ensure compliance with organizational information standards, as compared to organizational IT systems. Shadow IT is one of the main factors driving data duplication and security breaches in the construction industry, as highlighted by Tanga et al. (2022). As a consequence, private documents such as contracts with subcontractors, design information, and cost estimates are often stored in insecure locations, posing a risk of unauthorised access and data breaches. The limitations highlighted here emphasise the importance of pointing out the gap that exists today between information security and work efficiency, thereby supporting the necessity for an organised approach that represents the right compromise between flexibility and governance and control.

Another significant risk involves the use of single-factor authentication. While password-only identification is easy to use, inexpensive, and requires no training, it has been widely recognised as insufficient for today's cyber threats, making it suitable for employees who often travel between project locations. According to research, SFA is highly susceptible to phishing, password reuse, and credential theft. On the other hand, shared tablets, personal mobile devices, and public Wi-Fi are common at construction sites, raising the danger of data breaches. More

recent research on cybersecurity related to Construction 4.0, published by Yao & García de Soto (2024), states that identity compromise is currently one of the greatest risks for construction enterprise attacks. Thus, if SFA is still used, internal systems and project documents are exposed to unwanted access.

When taken as a whole, these tools offer quick communication, cost-effectiveness, and convenience, but they also result in a disconnected and insufficient safety approach. Shadow IT turns off all security controls, consumer products lack management, and single-factor authentication is inadequate to defend accounts against current attacks. The literature on construction cybersecurity repeatedly warns that informal, decentralised technology ecosystems dramatically increase exposure to cyber threats (Turk et al., 2022). The organisation will continue to face increasing risks to information technology security as the use of digital technology in the construction industry increases at a rate that requires no action.

Technological Solution And Available Tools

In the construction organization, the current technological landscape is built largely on consumer-grade tools, unmanaged Shadow IT, and single-factor authentication. These systems were originally adopted because they are cheap, familiar and easy to deploy. However, such arrangements introduce serious security weaknesses into cloud-based environments and undermine formal governance and monitoring mechanisms (Syed et al., 2020). The recent credential-theft incident illustrates how this mix of tools enables attackers to move laterally across email, cloud storage, and collaboration platforms without detection.

Consumer-grade tools, such as personal Dropbox, Google Drive, Gmail and WhatsApp, were selected for analysis because they are the primary channels through which project information currently flows within the organization. The research on privacy and security studies shows that personal cloud-storage services lack centralized access governance, enterprise-level audit trails, and retention control, making it difficult for organizations to track or restrict access to sensitive data since users frequently underestimate the risks of synchronizing confidential material to personal cloud accounts, which can be accessed from multiple unmanaged devices (Floyd, 2019; Syed et al., 2020). Other than that, although effective for rapid communication by using WhatsApp, it operates outside formal document-management and archival systems, which weakens traceability and accountability for project decisions (Abdelhay et al., 2024). Hence, these consumer-grade tools create multiple unlogged channels through which project designs and contracts can leak.

Other than that, shadow IT is selected for analysis because it represents a structural governance failure rather than a purely technical issue. This problem arises when employees introduce unauthorised tools to bypass perceived limitations in official systems, particularly in fast-paced construction project environments, creating new attack vectors and reducing visibility for security monitoring teams. Shadow IT significantly reduces organisational visibility into data flows, as unauthorised systems are not integrated with logging, monitoring, or incident response frameworks (Raković et al., 2020; van Acken et al., 2025). As a result, security teams are unable to detect abnormal behaviour or trace the movement of sensitive information in real time.

Moreover, single-factor authentication using usernames and passwords is analysed because it was the direct enabler of the reported security incident. Password-only authentication is highly vulnerable to phishing and social-engineering attacks, as a single compromised password can provide full access to multiple systems (Alkhalil et al., 2021). In cloud-based project environments, this weakness is magnified because the same credentials often grant access to email, storage, and collaboration platforms simultaneously. Consequently, single-factor authentication undermines both access control and the reliability of identity data used for monitoring (Pöhn et al., 2023), potentially leading to the leakage of design and contract information.

Table 4.1: Comparative Analysis of Existing Technologies and Cybersecurity Implications

Technology	**Strengths**	**Weaknesses**	**Cybersecurity Problem**
Consumer-grade cloud tools	• Easy to use	• Lack of access governance, audit logs,	• Uncontrolled data movement and data

	• Widely accessible • Fast communication • High user adoption	and retention control • No formal archiving • Weak data governance	leakage • Loss of data traceability and accountability
Shadow IT tools	• Flexibility • User convenience	• No integration with monitoring or security controls	• Invisible user activity and unmanaged data flows
Single-factor authentication	• Simple implementation	• Vulnerable to phishing and credential theft	• Unauthorized system access and identity compromise

In real organisational contexts, implementing mature enterprise security tools has been shown to materially improve threat detection and reduce risk exposure. For example, Security Information and Event Management (SIEM) systems, which are widely deployed across industries such as finance, healthcare, and critical infrastructure that provide centralised monitoring, correlation of security events, and real-time alerting, which enhance an organisation's ability to identify and respond to diverse threats compared to environments that lack unified visibility (González-Granadillo et al., 2021). SIEM platforms aggregate security data from endpoints, logs, network devices, and applications, enabling security teams to detect anomalous behaviour, reduce incident response times, and improve overall threat awareness in ways not possible with ungoverned consumer-grade tools alone (González-Granadillo et al., 2021).

Concrete organisational cases illustrate how SIEM-based approaches contribute to improved detection and mitigation outcomes. For instance, when SIEM tools are configured with tailored behavioural analytics and integrated alert correlation, organisations have successfully detected subtle insider threats, such as unusual data exfiltration via email or anomalous login patterns, that would have otherwise remained invisible under traditional logging regimes. However, SIEM-enabled analytics identified a compromised account by correlating disparate login attempts from geographically inconsistent locations, enabling the security team to intervene before sensitive intellectual property was accessed.

These real-world implementations demonstrate that centrally governed enterprise security solutions, compared with unmanaged consumer tools or fragmented log data, can significantly improve detection accuracy and risk visibility, providing evidence that formally validating technology choices based on measurable security outcomes is essential for organisational decision-making.

Enhancement of Data-Driven Decision-Making

The enhancement of data-driven decision-making in the construction organisation requires strengthening the security, reliability, and traceability of all data sources feeding into project reporting and operational insights. At present, the widespread use of consumer-grade tools such as personal Dropbox or Google Drive accounts, Gmail, and WhatsApp disperse critical project information across uncontrolled environments, resulting in fragmented datasets and inconsistent document histories. Studies on cloud storage behaviour confirm that personal cloud accounts lack formal information governance controls, leading totiple uncontrolled copies of project records and weakening the accuracy of data required for decision-making (Floyd, 2019; Ali et al., 2024). Similarly, the use of messaging platforms like WhatsApp for work communication removes project exchanges from official archives, reducing the completeness and integrity of datasets used for analysis and project monitoring. By transitioning to centrally governed enterprise platforms and enforcing unified storage policies, the organisation can consolidate all project data into secure, auditable systems, providing a single source of truth that supports more reliable analytics and managerial decision-making.

Moreover, unchecked use of shadow-IT platforms and reliance on single-factor authentication degrade the fidelity and trustworthiness of behaviour-based data, thereby impairing the organisation's capacity for accurate,

data-driven decision-making. When business units deploy unapproved applications or cloud services outside IT oversight, these systems typically lack integration with central monitoring, inventory and logging frameworks, which makes the full scope of user activity invisible to detection systems (Raković et al., 2020). At the same time, the single-factor, which can be called password-only access, also presents a weak identity dataset which behavioural analytics systems cannot reliably interpret since the compromised credentials appear legitimate, such as forgotten passwords to incorrectly configured fallback authentication methods and bypassing simple passwords undermines the certainty of who is really accessing data (Pöhn et al., 2023). Hence, these gaps mean that user behaviour analytics, anomaly detection and risk-scoring systems are fed incomplete or misleading inputs, which may compromise real-time incident detection and weaken the proactive cyber-risk framework essential for construction project environments.

Proposed System Development

This proposed system uses the System Development Life Cycle (SDLC) to ensure the solution is well-organised and useful. People choose SDLC because it addresses cybersecurity challenges in a single phase, starting with identifying the problems and moving on to analysis and system design. This method ensures the suggested system is built on how the organisation works, not just as a technical idea.

During the development process, the team reviewed their current privacy policies, which rely on consumer-grade products, single-factor authentication, and casual file-sharing methods. These methods showed that controlling cloud documents, managing user access, and securing emails were not particularly useful. A comparative evaluation against alternative enterprise security frameworks and solutions should be undertaken to reduce perceived vendor bias and broaden applicability across different organisational environments. Because of these problems, a conceptual system architecture using Microsoft 365 Business Premium is proposed to address key needs such as enhanced email protection, stronger authentication, and secure cloud document management. The system is built around three main parts: Defender for Office 365, OneDrive for Business, SharePoint Online, and Multi-Factor Authentication with Conditional Access. The proposed approach addresses problems such as reliance on consumer-grade software, uncontrolled shadow IT, and weak security controls. The solution consolidates these security functions into a single platform, making it easier to manage email security, document sharing, and user access across the entire organisation. The financial and operational trade-offs associated with putting the suggested solution into practice, such as licensing fees, training expenses, and anticipated drops in security incidents, must be made clear by a cost-benefit analysis.

Defender for Office 365

Microsoft Defender for Office 365 can identify phishing, spoofing, harmful links, and dangerous files using AI-driven analysis. Safe Links, which rewrite and check URLs in real time, and Safe Attachments, which separate files before they reach the user, are two important features. Clear metrics for gauging efficacy should be found and matched with established standards such as ISO 27001 and the NIST Cybersecurity Framework (NIST CSF) in order to facilitate the methodical assessment of improvement. Figure 1 shows the email security process that Microsoft Defender for Office 365 uses. It shows how new emails are checked before they reach users' inboxes. Moreover, the figure shows that emails undergo multiple stages of security, including phishing detection, spam screening, and attachment analysis. This number indicates that better email security is needed to lower phishing risks. Phishing was identified as a major weakness in the organisation's current practices. The figure makes the case for using an AI-driven email protection system rather than relying on simple email filters even stronger by showing the layered defence process.

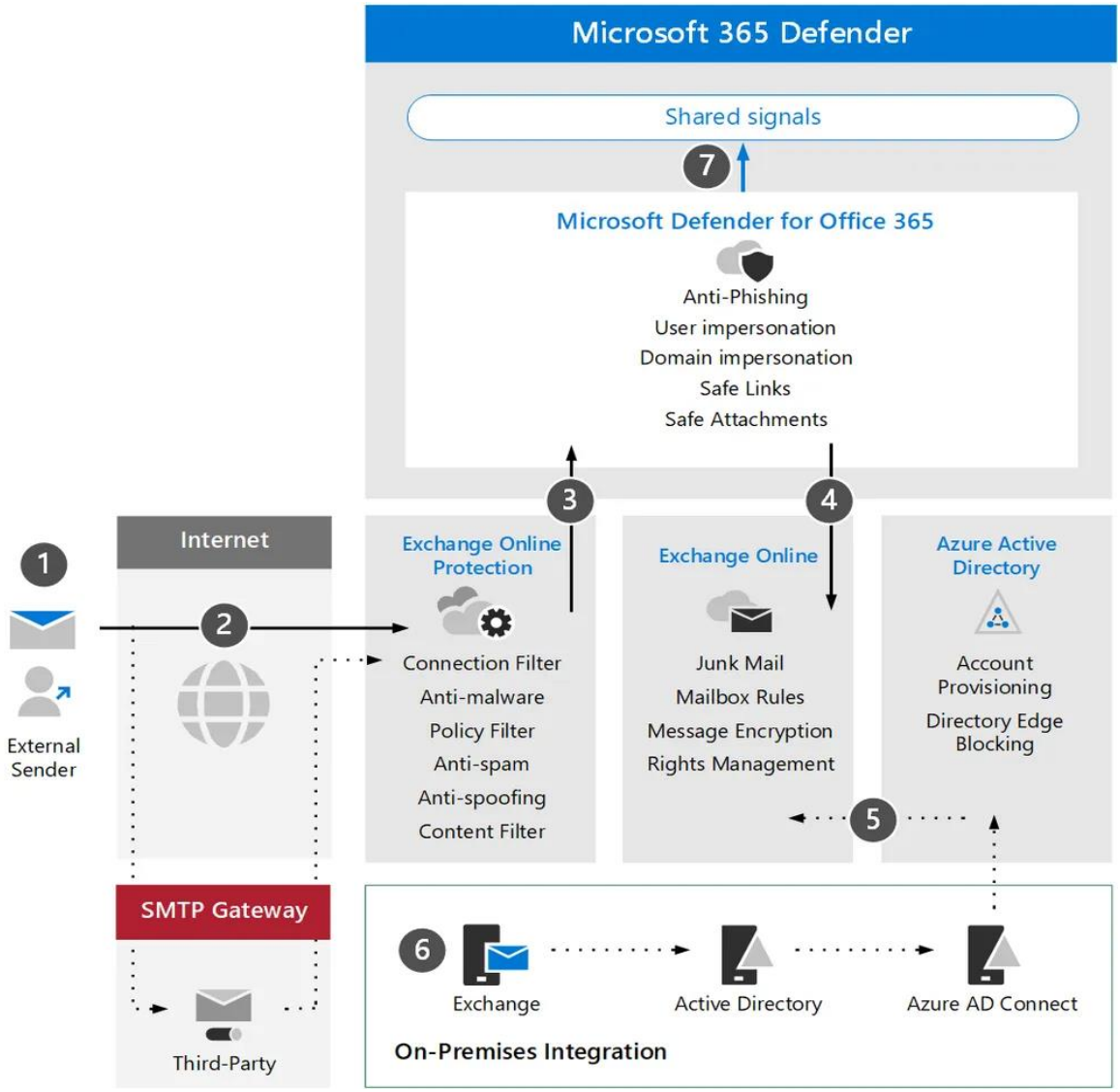

Figure 1: Email Security Workflow Using Microsoft Defender for Office 365

Source: *Microsoft Defender for Office 365 Workflow, Features, and Plans (BlueVoyant., 2026)*

OneDrive for Business (with SharePoint Governance)

The secure file-sharing and cloud storage module utilizes OneDrive for Business and SharePoint Online (both included in Microsoft 365 Business Premium). This module provides enterprise-grade cloud storage with centralized control, encryption both at rest and in transit, versioning, and audit logs. It also allows for policy-driven external sharing restrictions, device access controls, and shadow IT discovery. For organisations that previously allowed employees to use personal Dropbox or Google Drive accounts, this module replaces uncontrolled storage with managed platforms. According to the Business Premium feature map, OneDrive and SharePoint governance are included. They support audit, sharing controls, and data loss prevention workflows.

The company can better control file-sharing activities by using these business platforms. They can see who accesses files, stop people from downloading files that they are not supposed to, and keep an eye on private project papers and client information. This helps lower the risks of uncontrolled data movement and informal sharing practices. Regarding successful implementation, targeted awareness campaigns and onboarding programs should address user adoption barriers including resistance to change and training gaps. OneDrive for Business keeps files in sync by detecting user changes and safely moving them to Azure storage (Figure 2). Before files are sent, they are split into smaller, encrypted pieces. Each piece has its own encryption key to keep it safe. After it is shared, the data is safely reassembled in the cloud. This process ensures that files stay up to date across all devices and that data is safe and accurate when it is sent and stored.

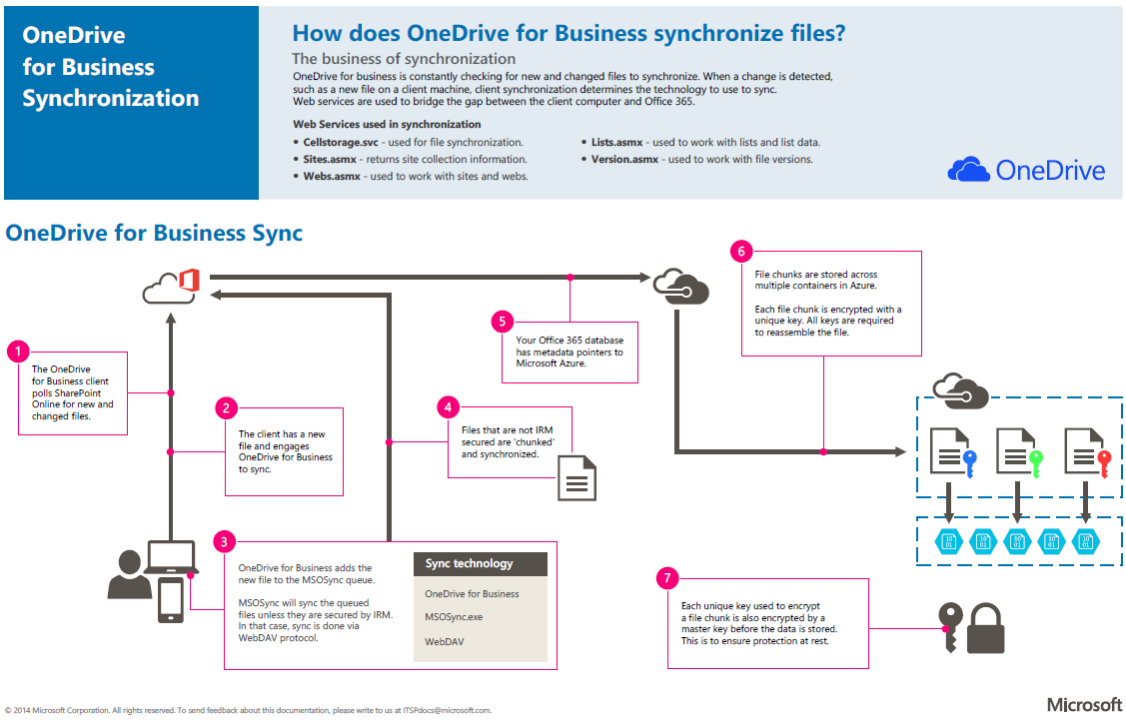

Figure 2: Secure File Synchronisation Process in OneDrive for Business

Source: *Cloud Security Controls Series: OneDrive for Business (Microsoft,2015)*

Microsoft Entra ID Multi-Factor Authentication (MFA)

Microsoft Entra ID (formerly Azure Active Directory) enhances identity and access control by leveraging multi-factor authentication (MFA) and granular access controls. With Microsoft 365 Business Premium, MFA is enabled by default, and Entra ID P1 supports Conditional Access, which adds extra security to the account. This is a big step up for a construction company that used to rely solely on one-factor password security. Many people know that password-only access is weak against identity theft and brute-force attacks. With MFA, you need to take an extra step to access your accounts, so a stolen password no longer suffices. Furthermore, conditional access implements Zero Trust approach that let the company block logins from devices, places, or apps that are not known or that they do not control.

Globally accepted frameworks, like ISO 27001 and the NIST Cybersecurity Framework, improves the security solution's legitimacy and applicability while offering structured control baselines. In order to expand the overall contribution and practical value of this research, future work should seek cost-benefit analysis, implementation challenge assessment, user adoption strategies, empirical validation, and a comparative evaluation against alternative enterprise security frameworks and solutions.

Comparison between Current Process and Proposed Process

The current process offers limited visibility and promotes reactive decision-making because project communications and records are dispersed across personal email, consumer cloud storage, and messaging services. This fragmentation weakens governance and traceability due to the absence of a centralised mechanism to enforce consistent access control, secure sharing practices, retention rules, and audit logging. Consequently, anomalous activities such as suspicious logins, unauthorised downloads, and accidental oversharing are often identified only after damage has occurred. This risk profile is consistent with breach evidence showing that credential compromise and human-related factors remain significant contributors to real-world incidents (Verizon, 2025).

From a control perspective, the current process underperforms against key cybersecurity outcomes: (i) weak governance and accountability; (ii) weak identity assurance due to password-only authentication (single-factor

authentication, SFA); (iii) limited detection and response capabilities due to minimal monitoring; and (iv) inconsistent data management because Shadow IT bypasses approved controls and audit trails. User workarounds and unapproved tools can reduce auditability and weaken consistent enforcement of security practices, particularly when collaboration spans multiple parties (Haag & Eckhardt, 2024).

In contrast, the proposed process reorganises project collaboration around centralised identity, governed information management, and measurable monitoring capacity. Identity assurance is strengthened through multi-factor authentication (MFA) and access policies. These measures reduce reliance on passwords alone. MFA is widely recommended as a high-impact control to reduce unauthorised access when credentials are compromised (Cybersecurity and Infrastructure Security Agency [CISA], n.d.). Beyond authentication controls, the proposed process standardises information governance by introducing role-based access control (RBAC), controlled external sharing, retention policies, and auditable activity logs enhances accountability and supports consistent security decision-making aligned with the NIST Cybersecurity Framework (CSF) 2.0 outcomes (National Institute of Standards and Technology [NIST], 2024) and ISO/IEC 27001 information security management system (ISMS) requirements (International Organization for Standardization [ISO], 2022).

To reduce perceived vendor bias, the proposal is capability-led rather than product-led. Enterprise options should be evaluated against baseline requirements for identity assurance, governance, monitoring, and incident handling, and then mapped to recognised standards such as CSF outcomes and ISO/IEC 27001 ISMS requirements (ISO, 2022; NIST, 2024). Table 5.1 summarises the comparison, while Figure 5.1 visualises the vendor-neutral decision flow.

Table 5.1 Comparison of current process and proposed process (capability-led)

Dimension	**Current process (consumer tools and SFA)**	**Proposed process (enterprise-governed)**	**Standard anchor**
Governance and accountability	Decentralised practices; limited policy enforcement	Defined roles, policies, and central administration	ISO/IEC 27001 ISMS requirements; CSF "Govern" (ISO, 2022; NIST, 2024)
Identity and access	Password-only authentication (SFA)	MFA with access policies	MFA guidance (CISA, n.d.); Authenticator Assurance Levels (AAL) (NIST, 2025)
Data governance	Dispersed records; inconsistent sharing; weak retention	Governed repository; RBAC; controlled sharing; retention policies	ISO/IEC 27001 governance expectations; CSF "Protect" (ISO, 2022; NIST, 2024)
Logging, monitoring, and response	Limited audit trails; delayed detection; ad hoc response	Central audit logs and alerts; consistent incident response	CSF "Detect/Respond/Recover" (NIST, 2024)
Operational efficiency	Version confusion and duplication; higher rework risk	Single source of truth; controlled versioning and traceability	ISO 19650 information management principles (ISO, 2018)

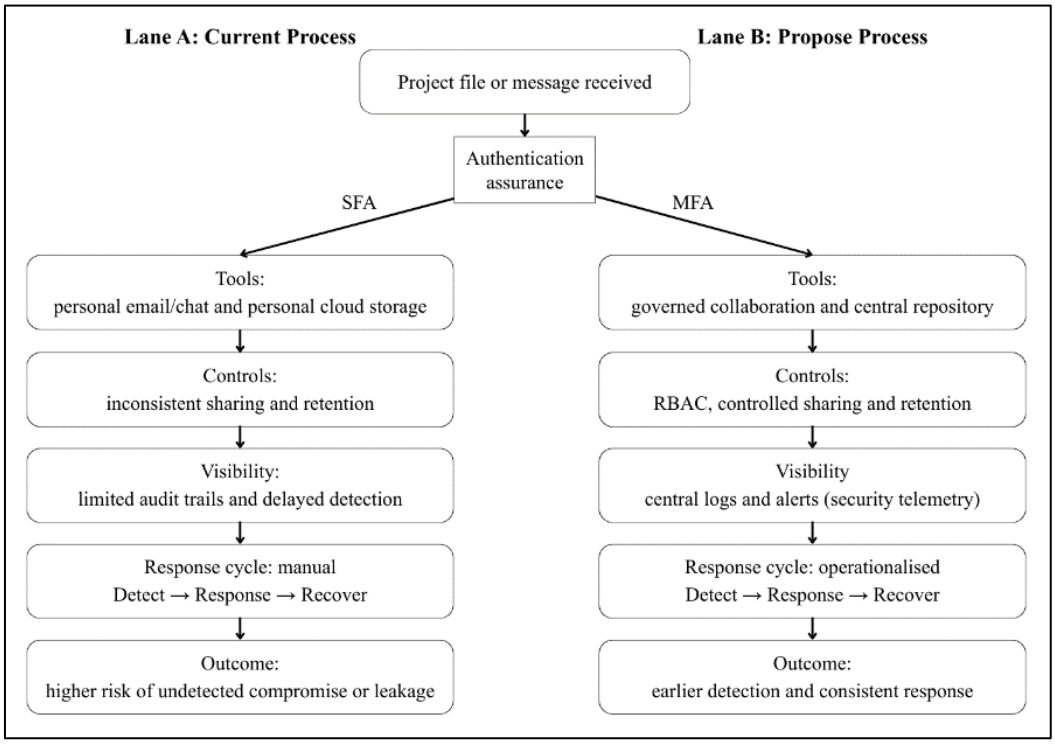

Figure 3 Comparative flow of cybersecurity decision inputs for the current and proposed process.

Benefits of the Proposed System

The proposed system strengthens cybersecurity and operational reliability by consolidating project communication and records within a governed collaboration environment. This is particularly beneficial in construction organisations where information is exchanged frequently among internal teams and external stakeholders, and where inconsistent controls can increase exposure and disrupt project delivery (NIST, 2024; Yao & García de Soto, 2024).

A primary benefit is improved identity assurance and reduced likelihood of account compromise. By moving from SFA to MFA and enforcing access policies, the organisation reduces reliance on passwords and lowers the probability that compromised credentials will enable unauthorised access (CISA, n.d.). RBAC and controlled external sharing also limit access to authorised users and reduce unnecessary exposure of sensitive project information. These measures improve accountability by making access and sharing decisions more structured and traceable (ISO, 2022).

The system also improves detection and response effectiveness by centralising audit logs and alerts, enabling earlier identification of abnormal activity and more consistent incident handling. This directly supports the CSF 2.0 outcomes for Detect, Respond, and Recover by providing the evidence base required for timely triage, containment, and post-incident improvement (NIST, 2024). Over time, these benefits can be demonstrated using clear performance indicators such as MFA coverage, audit-log coverage, external-sharing compliance, mean time to detect, and mean time to respond, which also supports continual improvement consistent with an ISMS approach (ISO, 2022; NIST, 2024).

From a cost-benefit perspective, the proposed system requires upfront and recurring investment in enterprise licensing or subscriptions, administrative configuration and monitoring effort, endpoint readiness, and user training and change management. In return, it is expected to reduce both the likelihood and impact of incidents through stronger identity assurance, tighter governance of sharing and retention, and earlier detection and response enabled by centralised visibility. Operationally, additional benefits include reduced document duplication and version conflicts, less rework caused by outdated information, and improved audit readiness through consistent evidence capture. Although the net financial outcome depends on organisational scale and baseline maturity, these benefits align with recognised guidance that emphasises measurable risk reduction and

improved recovery capability as key value outcomes of structured cybersecurity governance (ISO, 2022; NIST, 2024).

Limitations of the Proposed System

The effectiveness of the proposed system depends on sustained user adoption and consistent day-to-day practice. Even well-designed controls may be weakened if users perceive approved workflows as inconvenient and revert to informal channels for speed or convenience. These workarounds reduce monitoring coverage and weaken policy enforcement, which limits the organisation's ability to maintain reliable oversight of project information flows (Haag & Eckhardt, 2024). To mitigate this risk, implementation should be supported by role-based onboarding, clear communication of expected behaviours, and practical procedures that minimise friction while maintaining governance objectives.

Implementation feasibility may also vary across organisations, particularly among smaller firms and resource-constrained settings. The proposed approach assumes adequate connectivity, suitable endpoint readiness, and ongoing administrative capacity to configure access policies, manage permissions, and review security events. Controls may not be maintained consistently where expertise and resourcing are limited. Over time, this can reduce the effectiveness of the proposed system. A phased rollout can help address these constraints by prioritising identity hardening and governance of critical project repositories. Where necessary, external expertise or managed services may be used to support implementation and operations.

Finally, compliance readiness should not be equated with certification. Although the proposed system can strengthen the consistency of controls and improve evidence capture for audit purposes, ISO/IEC 27001 certification requires an organisation-wide information security management system. This includes establishing the scope, conducting risk assessments, maintaining documented policies and procedures, performing internal audits, and completing management reviews, all of which extend beyond technology deployment alone (ISO, 2022). In addition, to reduce perceived vendor bias and improve wider applicability, future work should compare alternative enterprise security solutions using capability-based criteria—such as identity assurance, governance, monitoring, incident response, and standards mapping, rather than focusing on platform-specific features (NIST, 2024).

CONCLUSION

To conclude, when making an overall evaluation, one can note that the cybersecurity measures the company relied on to secure sensitive project information cannot be used to safeguard that data any longer. The combination of personal cloud storage, single-user logins and passwords, and file-sharing software without any monitoring exposes the organisation to conventional internet threats such as phishing attacks, compromised passwords, and unauthorised access. The research is valuable because it demonstrates how the most frequent cybersecurity vulnerabilities in small-to-medium construction organisations can be identified and addressed systematically using an SDLC-based analysis framework.

Having drawn parallels between the options on the table, one can probably conclude that Microsoft 365 Business Premium is the most likely and reasonable option for advancing the company's security. It can also help the company achieve greater control over its data, facilitate the use of safer personal equipment, and better manage key records through relocation to a single, well-managed system. As a result, it has demonstrated that fragmented application of consumer-grade tools, single-factor authentication, and shadow IT constitute an interdependent risk architecture and represent standalone security concerns in construction project settings.

Microsoft 365 Business Premium minimises the business's susceptibility to most cyber threats and optimises business functions, management, and long-term sustainability in digital services. This study contributes to the current body of literature on cybersecurity by situating cybersecurity risks within the construction and quantity surveying processes, which are often generalised and lack industry-specific specificity. The research measures cybersecurity maturity and supports further planning for digital security.

Finally, the case of Microsoft 365 Business Premium is likely to lead the company to develop a better, more efficient cybersecurity network. Even though it may require certain employees to get used to the new practice, the immediate benefits of new practices, such as ensuring safer information control, reduced cases of security breaches, and improved digital operations, are worth the change. Besides, the upgrade will protect the firm against sensitive project information and will also help the firm expand its more digital workplace.

REFERENCES

1. Abdelhay, S., Draz, A. M. A., Tharwat, W. A. K., & Marie, A. (2024). The impact of using WhatsApp on the team's communication, employee performance and data confidentiality. International Journal of Data and Network Science, 8(2), 1307–1318. https://doi.org/10.5267/j.ijdns.2023.11.004
2. Ali, T., Al-Khalidi, M., & Al-Zaidi, R. (2024). Information Security Risk Assessment Methods in Cloud Computing: Comprehensive Review. Journal of Computer Information Systems, 1–28. https://doi.org/10.1080/08874417.2024.2329985
3. Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. Frontiers in Computer Science, 3. https://doi.org/10.3389/fcomp.2021.563060
4. Althobaiti, K., & Alsufyani, N. (2024). A review of organization-oriented phishing research. PeerJ Computer Science, 10, e2487. https://doi.org/10.7717/peerj-cs.2487
5. BlueVoyant. (2026). Microsoft Defender for Office 365: Workflow, features, and plans. Microsoft Defender for Office 365.
6. Cybersecurity and Infrastructure Security Agency. (n.d.). Multifactor authentication. https://www.cisa.gov/topics/cybersecurity-best-practices/multifactor-authentication
7. Floyd, K. S. , & L. K. (2019). PERCEPTIONS OF CLOUD STORAGE PRIVACY AMONG UNIVERSITY STUDENTS. Issues In Information Systems. https://doi.org/10.48009/4_iis_2019_86-92
8. González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. Sensors (Basel, Switzerland), 21(14), 4759. https://doi.org/10.3390/s21144759
9. Haag, S., & Eckhardt, A. (2024). Dealing effectively with Shadow IT by managing both cybersecurity and user needs. MIS Quarterly Executive, 23(4), 399–412. https://doi.org/10.17705/2msqe.00104
10. International Organization for Standardization. (2018). ISO 19650-1:2018—Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM)—Information management using building information modelling—Part 1: Concepts and principles (Standard No. ISO 19650-1:2018). https://www.iso.org/standard/68078.html
11. International Organization for Standardization & International Electrotechnical Commission. (2022). ISO/IEC 27001:2022—Information security, cybersecurity and privacy protection—Information security management systems—Requirements (Standard No. ISO/IEC 27001:2022). https://www.iso.org/standard/27001
12. Loh, P. K. K., Lee, A. Z. Y., & Balachandran, V. (2024). Towards a Hybrid Security Framework for Phishing Awareness Education and Defense. Future Internet, 16(3), 86. https://doi.org/10.3390/fi16030086
13. McAlaney, J., & Hills, P. J. (2020). Understanding Phishing Email Processing and Perceived Trustworthiness Through Eye Tracking. Frontiers in Psychology, 11. https://doi.org/10.3389/fpsyg.2020.01756
14. Meyer, L. A. , Romero, S., Bertoli, G., & Burt, T. (2023). How effective is multi-factor authentication at deterring cyberattacks? ArXiv Preprint.
15. Microsoft. (2025). (2026). Microsoft 365 for business security overview. Microsoft Learn.
16. Mostafa, A. M., Ezz, M., Elbashir, M. K., Alruily, M., Hamouda, E., Alsarhani, M., & Said, W. (2023). Strengthening Cloud Security: An Innovative Multi-Factor Multi-Layer Authentication Framework for Cloud User Authentication. Applied Sciences, 13(19), 10871. https://doi.org/10.3390/app131910871
17. Naqvi, S. G., Nasir, T., Azam, H., & Zafar, L. (2023). Artificial Intelligence in Healthcare. Pakistan Journal of Humanities and Social Sciences, 11(2). https://doi.org/10.52131/pjhss.2023.1102.0443

18. National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29
19. National Institute of Standards and Technology. (2025). Digital identity guidelines: Authentication and authenticator management (NIST Special Publication 800-63B-4). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63B-4.pdf
20. Pöhn, D., Gruschka, N., Ziegler, L., & Büttner, A. (2023). A framework for analyzing authentication risks in account networks. Computers & Security, 135, 103515. https://doi.org/10.1016/j.cose.2023.103515
21. Raković, L., Sakal, , Marton, Matković, P., & Marić, M. (2020). Shadow IT – Systematic Literature Review. Information Technology and Control, 49(1), 144–160. https://doi.org/10.5755/j01.itc.49.1.23801
22. Sonkor, M. S., & García de Soto, B. (2021). Operational Technology on Construction Sites: A Review from the Cybersecurity Perspective. Journal of Construction Engineering and Management, 147(12). https://doi.org/10.1061/(ASCE)CO.1943-7862.0002193
23. Syed, A., Purushotham, K., & Shidaganti, G. (2020). Cloud Storage Security Risks, Practices and Measures: A Review. 2020 IEEE International Conference for Innovation in Technology (INOCON), 1–4. https://doi.org/10.1109/INOCON50539.2020.9298281
24. Tanga, O., Akinradewo, O., Aigbavboa, C., & Thwala, D. (2022). Cyber attack risks to construction data management in the fourth industrial revolution era: a case of Gauteng province, South Africa. Journal of Information Technology in Construction, 27, 845–863. https://doi.org/10.36680/j.itcon.2022.041
25. Turk, A., Wong, G., Mahtani, K. R., Maden, M., Hill, R., Ranson, E., Wallace, E., Krska, J., Mangin, D., Byng, R., Lasserson, D., & Reeve, J. (2022). Optimizing a person-centred approach to stopping medicines in older people with multimorbidity and polypharmacy using the DExTruS framework: a realist review. BMC Medicine, 20(1), 297. https://doi.org/10.1186/s12916-022-02475-1
26. van Acken, J.-P., Gadellaa, J., Jansen, S., & Labunets, K. (2025). The Unknown Unknown: Cybersecurity Threats of Shadow it in Higher Education. https://doi.org/10.2139/ssrn.5340607
27. Verizon. (2025). 2025 Data Breach Investigations Report: Executive summary. https://www.verizon.com/business/resources/reports/2025-dbir-executive-summary.pdf
28. Yao, D., & García de Soto, B. (2024a). Assessing cyber risks in construction projects: A machine learning-centric approach. Developments in the Built Environment, 20, 100570. https://doi.org/10.1016/j.dibe.2024.100570
29. Yao, D., & García de Soto, B. (2024b). Cyber risk assessment framework for the construction industry using machine learning techniques. Buildings, 14(6), 1561. https://doi.org/10.3390/buildings14061561
30. Yao, D., & García de Soto, B. (2024c). Enhancing cyber risk identification in the construction industry using language models. Automation in Construction, 165, 105565. https://doi.org/10.1016/j.autcon.2024.105565