Barriers to Single Sign-On (SSO) Adoption for Small and Medium-Sized Businesses: Identifying Challenges and Opportunities

Publication: May 2024
Cybersecurity and Infrastructure Security Agency

Table of Contents

1 Problem Statement

This study explores barriers and challenges to Single Sign-On (SSO) adoption by small and medium-sized businesses (SMBs). The study also identifies potential ways to overcome these challenges, which in turn improve an SMB's level of security.

SSO is a user authentication and access control system that allows users to access multiple applications, tools, and systems with just one set of credentials. By centralizing the authentication process, SSO streamlines identity management and simplifies the user experience by only needing to remember one username and password for all accounts. SSO can help bolster security measures as it decreases the frequency of users having to input their login credentials. Furthermore, SSO can reduce password duplication across various platforms, consequently reducing the potential for password leakage.

As part of this study, the Cybersecurity and Infrastructure Security Agency (CISA) engaged with various stakeholders involved with SSO. These include SSO vendors, experienced managed service providers, non-profit organizations dedicated to improving cybersecurity, and SMBs that have experience with adopting SSO and migrating across SSO platforms. Based on these discussions, CISA found that despite the benefits of SSO, the adoption of SSO capabilities for identity management remains low, particularly among SMBs. There are numerous obstacles to successfully implementing a workable SSO solution. These include cost, technical hurdles, and a lack of awareness and resources.

Small enterprises often opt for manual passwords and hands-on approaches to manage access and identities as opposed to the SSO option. These methods tend to be more cost-effective in terms of the purchasing cost, which does not include the hidden cost associated with administrative overhead. Often, a primary reason for the difference in the purchasing cost is that SSO is often only available as a premium enterprise-level service, which comes with custom pricing that is significantly higher than essential services. A premium enterprise-level service with SSO can cost more per user than a lower-tier service without SSO. In addition to a higher cost per user, this premium pricing model typically requires a minimum number of users. This additional incremental cost, which can significantly raise the total cost per user compared to a lower-tier service without SSO, can be a substantial financial barrier for many organizations. The price difference often results in SMBs selecting cheaper, lower-tier services lacking SSO features.

Additionally, setting up the advanced SSO features often requires specialized technical knowledge and expertise as well as a time commitment. The combination of extra costs, the need for technical skills, and the time needed leads many businesses to continue relying on manual methods, such as spreadsheets, to handle user access to various applications and systems. To encourage the adoption of SSO by SMBs, SSO providers must address their concerns and offer comprehensive technical support and solutions tailored to SMB needs and priorities.

This study is organized as follows: Section 2 presents the key findings related to the advantages of SSO, the challenges SMBs face in terms of SSO adoption, and the role government can play in encouraging SSO adoption. Section 3 describes what SSO is and how it works. Section 4 identifies benefits of SSO adoption. Section 5 presents an overview of the literature on how SMBs adopt technology in general and describes how it may be applicable in the case of SSO adoption. Section 6 presents the results of CISA's engagement with SSO stakeholders by identifying key factors and considerations influencing SSO adoption and highlights how vendors and customers have differing views. Section 7 summarizes the study's findings regarding the benefits of SSO adoption, challenges SMBs experience in implementing SSO, SMB needs, and typical vendor practices. Section 8 provides recommendations on how to help ensure a smooth and successful implementation with the aim of encouraging SSO adoption by SMBs. Finally, the appendix presents a brief description of the research method used in the study and associated stakeholder engagement process.

2 Key Findings

Below we describe the advantages and challenges associated with SSO adoption as well as the role government can play in addressing some of those challenges.

Advantages of SSO Adoption

According to Chang and Lee (2012), SSO is designed with a primary focus on security and user experience, distinguishing it from other access management solutions such as individual usernames and passwords. SSO improves user experience, making it more likely that users will properly implement security measures. Users can easily enable and disable the capability to enter multiple systems, platforms, apps, and resources. Also, it may effectively resolve the problem of password-related downtime and reset expenses. When properly implemented and configured, SSO technology offers numerous advantages to SMBs in terms of improving cybersecurity. Cusack and Ghazizadeh (2016) and D'Costa-Alphonso and Lane (2010) agree that SSO reduces disclosure, human error, and cybersecurity risk. SSO also ensures the termination of an Identity Provider session as soon as the user signs out of all the services authenticated by the Identity Provider (Ramamoorthi & Sarkar, 2020). This reduces the risk of events like Cross-Site Request Forgery attacks (Armando et al., 2013).

Considering the recent cyber incidents related to SSO services (e.g., the Okta cyber incident; Bradbury [2023], Bracken [2023], Newman [2023]), digital forensics and incident response experts recommend not locking cybersecurity tools under SSO. If sufficient expertise and dedicated resources are available, a more differentiated and closely monitored approach for cybersecurity tools may be warranted. Nevertheless, cybersecurity analysts perceive the benefits provided by SSO capabilities to outweigh potential risks, even in the context of the most recent Okta cyber incident.

Although long confined to a supporting role, information technology (IT) in general, and cybersecurity specifically have now become an essential part of the strategic behavior of any firm seeking greater competitiveness. In some cases, cybersecurity maturity and adoption of advanced IT is an essential element of a firm's corporate strategy and can serve as a potential factor in product or service differentiation.

SSO Adoption Challenges Faced by SMBs

SMBs represent over 90% of all firms globally and are projected to grow 6.1% annually between 2020 and 2025 (Quirt et al., 2022). SMBs face the hurdle of dealing with numerous logins and passwords needed for web applications. These challenges can create difficulties in password management for end users (Komorowski et al., 2016). While new technology that can streamline access and identity management may sound attractive to SMBs, implementation could be challenging.

SMBs are often reluctant to adopt technology based on a very few published articles that explain the advantages technology can bring to an organization but do not properly explore the cost implications (Fink, 1998). For some SMBs, the lack of conclusive information on SSO from reliable sources reduces their willingness to implement it. Even if they are informed, SMBs often need clarification on where to acquire a viable SSO solution (Riches, 2007).

Due to organizational structure, the willingness to upgrade to other secure and efficient sign-on forms, like SSO, might not be a top priority when profit is crucial for some SMBs. The idea of SSO adoption may be appealing, but external market forces may significantly impact adoption decisions by SMBs. Cybersecurity is inherently a business support function and is dominated by business priorities such as attracting new customers, retaining existing customers, securing financing, complying with regulations, and attracting talent. SMBs tend to be constrained in resources and expertise when it comes to managing new technologies. Thus, the cost of SSO implementation coupled with a lack of requisite technical expertise to configure and deploy the solution properly further hinder SSO adoption among SMBs.

Government Involvement

The government can play a significant role in encouraging SMBs to embrace policies and implement new technologies. Support services in the form of financial incentives or grants may increase adoption of particular measures, but constraints on the use of funds tend to discourage SMBs from accepting government support services.

Through its collaboration with private and public sector entities, CISA can contribute to government initiatives such as promoting positive cybersecurity outcomes (e.g., a higher rate of SSO adoption). CISA can provide technical publications, training support and resources, and instructional materials. In addition, its partnerships serve as effective and credible channels for disseminating accurate and actionable information while also increasing awareness, outreach, and engagement. Furthermore, potential joint collaborative efforts between the government and SSO stakeholders offer an opportunity for key SSO service providers, organizations representing the SMB community, and managed service providers to come together and explore ways to enhance SSO service offerings that are more accessible and affordable for SMBs.

3 SSO Basics

The primary purposes of an SSO service are to efficiently and effectively manage the user and organization identity, create one centralized location to access a system, and establish cohesive log files documenting all instances of use. Connecting all business and operational applications under centralized identity management can improve effectiveness and yield efficiencies. However, the current pricing structure and other challenges described in more detail in Sections 5 and 6 significantly hinder SSO adoption. Organizations are unable to realize the advantages of SSO and instead rely on manual identity and access management practices (e.g., tracking and managing passwords using spreadsheets). An example of this is when individuals depend on spreadsheets or collaborative documents to keep track of their passwords or when administrators opt for a spreadsheet to manage all the passwords associated with IT services. These shared spreadsheets may also contain data regarding bugs, travel and expenses, time tracking, and customer support portal details. Relying on manual spreadsheets for identity, credential, and access management come with notable difficulties and potential risks. The current manual access and identity management practices are illustrated in Figure 1.

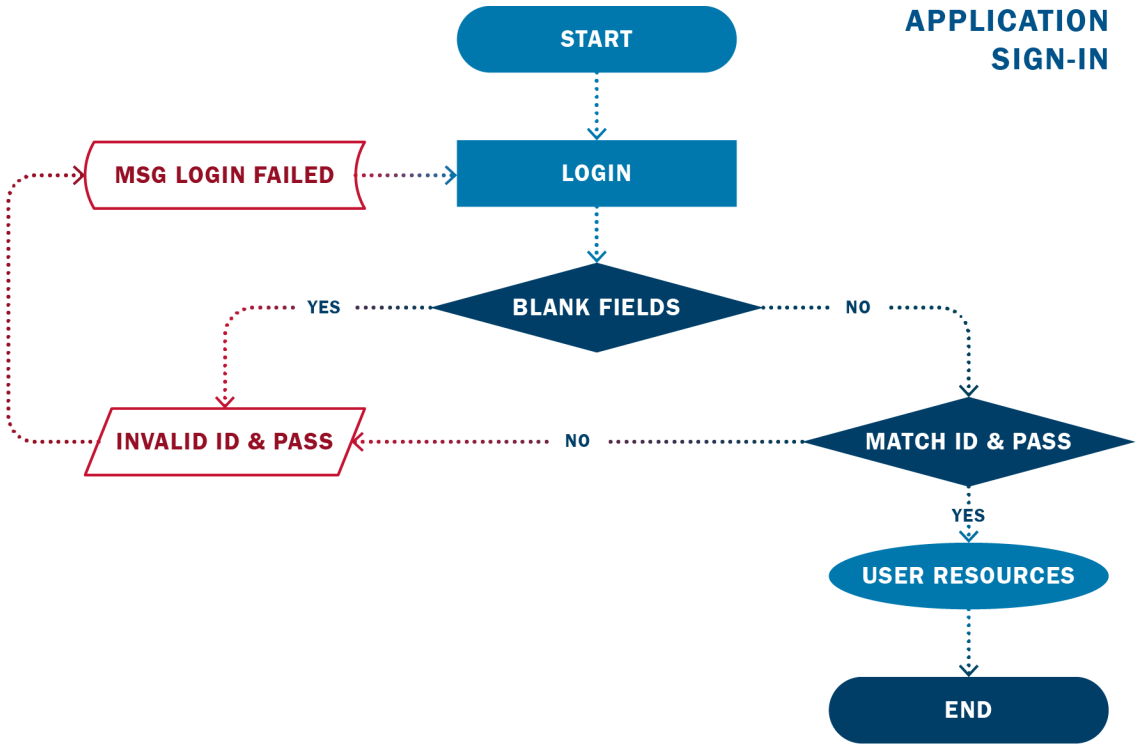

Figure 1: Password-Based User Authentication

During a standard login procedure, users are required to enter their credentials, such as a user ID and password, into the designated fields of the application. Once the user's authentication is successful, they are granted access to the desired resources. However, if incorrect credentials are provided, an error message is

displayed, prompting the user to re-enter the correct credentials. This process occurs independently for each of the applications requiring an individual to sign in, with a separate set of unique credentials per application, and with the administrator manually tracking lists of authorized users for each application.

In addition, another layer of responsibility and administrative burden is associated with managing each stage of the user account lifecycle for each of the applications. Figure 2 illustrates the user account lifecycle, which is briefly described below.

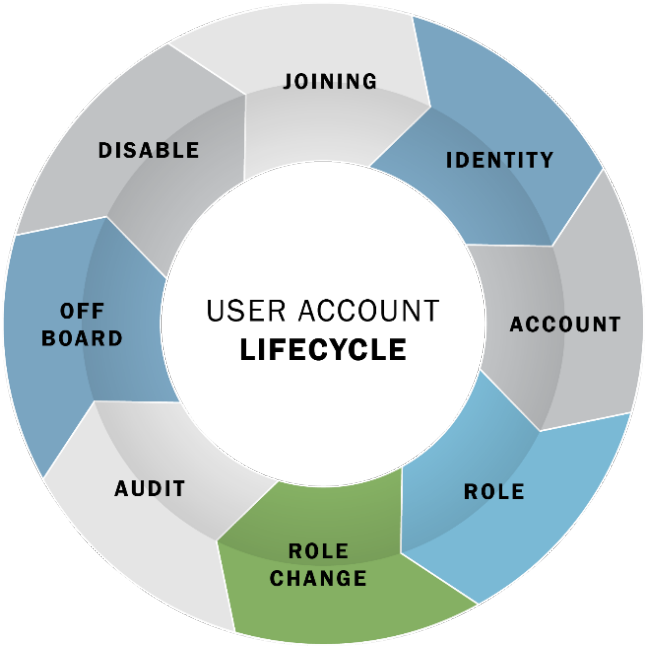

Figure 2: User Account Lifecyle

The administrative burden associated with managing user accounts starts with establishing a new user identity and spans a specific set of activities up to disabling accounts for staff leaving the organization. In larger more mature organizations, once a candidate has accepted a job offer and their identity has been confirmed, the human resources system will notify the IT department to initiate the onboarding process. This involves creating a new user account specifically tailored to the new employee's position within the company, with corresponding privileges assigned accordingly. However, SMBs may not have a separate HR system or an IT department, where an ad-hoc access management is combined with other duties. As employees advance in their careers within the organization, their privileges may be adjusted to align with any role changes. Organizations should conduct periodic audits to evaluate different roles and associated privileges to grant only necessary permissions. Inactive accounts pose potential risks; therefore, when an employee departs from the company, their account is promptly disabled in order to mitigate these risks effectively.

The companies facing the challenge of signing into separate applications with different sign-in credentials and manually managing user account lifecycle are the ones that would benefit from SSO the most. This is especially relevant for SMBs, and even more critical for SMBs below the cyber poverty line. The cyber poverty line is a point of divide that signifies the difference between organizations who can and should perform cybersecurity functions and those that cannot and should not.

SSO provides an integrated unified tool for user management. The user account lifecycle can be managed from a centralized location, reducing management overhead and preventing stale accounts. Figure 3 depicts the SSO process to access multiple applications.

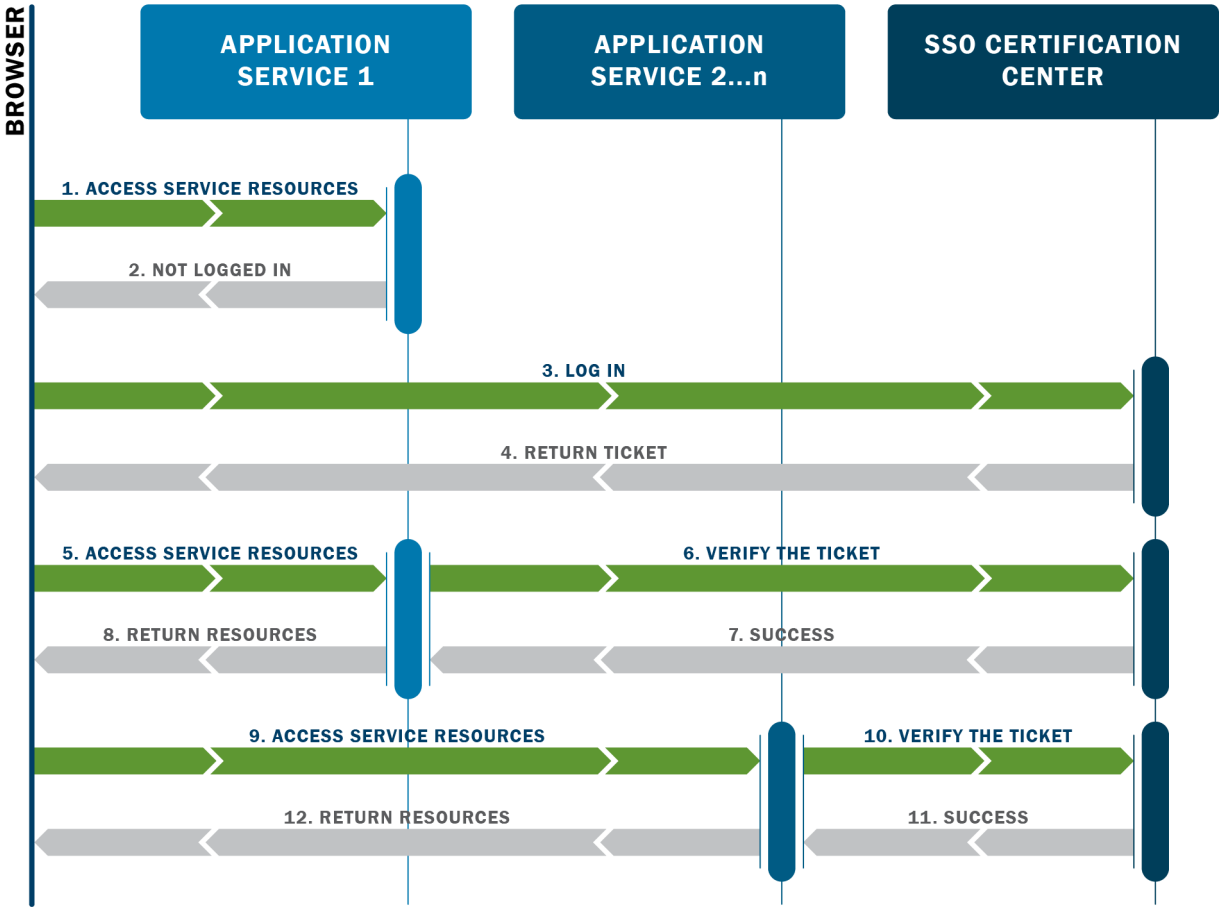

Figure 3. SSO Process for Multiple Applications

The SSO process consists of several steps. Initially, when a user requests access to a specific application service, the service will notify the user that they are not logged in and need to provide their login credentials. The user then provides the necessary login credentials to the SSO Credentialing Center. The SSO Credentialing Center issues a ticket to the user, confirming their legitimacy. The user will then repeat their initial request to access the application service. The application service verifies the user's credentials by checking with the SSO Credentialing Center. The SSO Credentialing Center responds, confirming that the user has been properly authenticated. Once the application service receives this confirmation, it can provide the desired resources to the user. This process can be repeated for additional application services. The key advantage is that the user only needs to provide their credentials to the SSO Credentialing Center once to access multiple application services.

4 SSO Benefits

Unified access management with a single set of credentials has multiple operational benefits and positive cybersecurity outcomes. SSO adoption can result in increased security and privacy, a simplified and improved login and user experience. In addition, SSO may help facilitating e-commerce and IT adoption, with more robust cybersecurity practices potentially serving as a factor in product or service differentiation. These benefits are briefly described below.

Security and Privacy

SSO can improve authentication security (Chang & Lee, 2012; Joshi et al., 2018). SSO mechanisms improve the overall security of distributed computer networks by consolidating user authentication and reducing the need for multiple passwords. By reducing the risk of unauthorized access and data breaches, SSO provides a more

secure environment for users and businesses. SSO deployment can also protect user privacy by reducing the amount of personal information shared between service providers. Such privacy protection can increase user trust and encourage the adoption of SSO solutions (Urueña et al., 2014).

SSO can also address shortcomings in the sign-out process by logging users out of all connected services. By providing a secure and efficient sign-out process, SSO can enhance user trust and satisfaction with SSO systems.

Simplified and Improved Login and User Experience

Improved user experience is a major advantage of SSO since it simplifies the login process by enabling users to access multiple services with a single set of credentials (Ramamoorthi & Sarkar, 2020; Komorowski et al., 2016). In addition to reducing support costs associated with password management, streamlining the user experience can lead to increased productivity and user satisfaction. SSO adoption can make it easier for users to consume media content across different platforms (i.e., cross-media content). This can lead to increased user engagement and a more cohesive media consumption experience.

Facilitated E-Commerce and IT Adoption

In addition to direct benefits of improving cybersecurity, SSO adoption may have auxiliary benefits. SSO systems could encourage electronic transactions among SMBs by simplifying the login process and enhancing security for online businesses. Improved user experience, increased security, as well as internal process improvement that increases operational efficiencies and reduces burden on staff may lead to a more optimal use of time and resources, which in turn can result in increased revenue and growth opportunities for e-commerce SMBs (Esmaeilpour et al., 2016; Govindaraju & Chandra, 2011).

In addition, SSO helps reduce barriers to IT adoption for SMBs by streamlining user authentication and access to various applications and services (e.g., cloud services). SSO features can improve organizational efficiency and enhance their competitiveness in the global marketplace (Santini et al., 2023; Vu et al., 2022; Blili & Raymond, 1993; Nguyen, 2009; Fink, 1998; Ghobakhloo et al., 2012).

5 Barriers and Catalysts to Technology Adoption by SMBs

CISA conducted a literature review to identify general barriers and catalysts affecting technology adoption and innovation diffusion within SMBs. This section presents only a brief overview of available literature (including vendor marketing literature) that attempts to explain such barriers and catalysts. The objective of summarizing the most recent research on this topic is to augment the SSO-specific findings presented in Section 6, which were obtained as part of the focus group discussions. Literature review enhances these findings with a deeper contextual understanding of a much larger set of factors and considerations that may trigger a favorable adoption decision and explain the rationale. These findings are directly applicable and broadly generalizable to adoption decisions for any cybersecurity technology or practice. Below, we discuss how they relate to SSO adoption in particular.

How SMBs Buy Technology

According to Riches (2007) and as confirmed by CISA's recent SSO discussions with SMBs, SMBs are hesitant to pursue early adoption of new technologies as their main goal is to maximize profits. However, they often face challenges in determining which technologies to invest in, assessing the benefits of these investments, and finding reliable vendors that offer reasonable prices. Riches found that SMBs could enhance their purchasing decisions by conducting thorough market research and engaging in multiple discussions with software developers or product vendors. Doing so can help SMBs identify solutions that align with their existing IT roadmap and account for their scalability needs.

When SMBs collaborate closely with vendors, SMBs may find it easier to adopt, implement and operates SSO solutions, which can lead to a better user experience and favorable messaging for potential adopters. Moreover, the level of education and support vendors provide following the adoption of their SSO solution may create a strong desire among SMBs to seek additional services offered by the vendor. The availability of different pricing options and tiers, tailored to suit various business models, also significantly influences SMBs purchasing decisions.

Anecdotal evidence shows government incentives have also helped some IT adoption by SMBs. Dreyer and Nygaard (2020) included examples of various forms of government support (e.g., grants, loans, free online platforms, and consulting and advisory services) that were provided during the COVID-19 pandemic. Examples of direct financial support include the Irish government offering grants to eligible SMBs of up to €2,500 to develop e-commerce or online trading platforms or the Japanese government providing subsidies for sustainability, manufacturing, and IT introduction via the Small and Medium-Sized Enterprise Productivity Revolution Promotion Project. With incentives like these, more SMBs were able to afford technologies prescribed for them, although sometimes with little consideration to the technology's impact on them. For example, such incentives would not address non-financial hurdles faced by SMBs (e.g., the lack of technical expertise needed to implement a technology). If properly designed, incentives may be able to improve the likelihood of the desired outcomes, while avoiding unintended and unfavorable consequences. For more details about the relative effectiveness, efficiency, and equity associated with various incentives aimed at promoting cybersecurity investments, please refer to a comprehensive study of incentives conducted by a U.S. Department of Homeland Security Integrated Task Force (2013).

Factors Influencing the Adoption Decision

The need to increase productivity while facilitating access to the work environment drives the decision to adopt SSO. Santini et al. (2023) conducted a meta-analysis of 59 studies on IT adoption among SMBs and found that resources and market forces were the main predictors of IT adoption. Resources include "human and technological infrastructure that supports the technology implementation (e.g., technology competence, IT infrastructure, technology infrastructure)" (Santini et al., 2023, p. 637), while market forces include changes in technological growth, shifts in client preferences, and the amount of capital a business has.

Reluctance to adopt new technology is driven not only by the concerns of adding on the new platform, but also the need for more knowledge on how to implement such technology properly. Many SMBs do not have in-house cybersecurity expertise. Some SMBs outsource support on an ad-hoc basis only. If in-house expertise is available, many chief information security officers in SMBs wear multiple hats, with sometimes only a fraction of their time allocated to cybersecurity and implementing new technologies that would make the working environment safe. In summary, affordability, awareness, scalability, education, compatibility, and ease of integration drive buying decisions.

One barrier preventing SMBs from adopting SSO solutions stems from a lack of technical knowledge. To fully reap the benefits of implementing SSO, it is important for SMBs to have a clearer understanding of the information required for adoption. Moreover, even if the prominent vendors provide needed information, the technical know-how and the basic operating modalities must be learned by SMBs. Many SMBs avoid this challenge as it requires additional resources and carries a significant opportunity cost.

Technology Adoption and Innovation Diffusion Models

Various theories and models explain reasons behind decision-making surrounding the adoption of IT. In the field of quantitative marketing, several classic adoption theories can be applied to understand how SMBs adopt SSO or new technologies. The following paragraphs provide a brief overview of these models.

The first broad adoption theory that can be applied to SSO adoption is the Diffusion Theory of Innovation. This theory asserts that innovation diffusion is the process by which an innovation is communicated through certain channels over time among the members of a social system (Rogers, 2010). Contextual research with a Diffusion Theory of Innovation perspective was more common in the information systems field to evaluate the value of enterprise resource planning systems (Ruivo et al., 2012) and to investigate the technological innovation process (Mamun, 2018).

The second set of classical adoption theories that can be applied to SSO includes the Technology Acceptance Model (Davis et al., 1989) and the Unified Theory of Acceptance and Use of Technology (Venkatesh et al., 2003). Both theories have limitations when analyzing whether a firm would adopt SSO since the theories are focused more on whether an individual user within a firm would use a new technology and not whether the firm itself would adopt a technology that would be used firm-wide (Davis et al., 1989; Venkatesh et al., 2003).

Also, the factors that lead to technology adoption at the firm level are more individually driven by the firms. The Technology Acceptance Model investigates technology acceptance from a user's perspective (Yousafzai et al., 2007). From this perspective, users tend to adopt new technologies for two main reasons: perceived usefulness and perceived ease of use (Davis et al., 1989). In contrast, the Unified Theory of Acceptance and Use of Technology asserts that technology adoption is influenced by effort and performance expectations, social influences, and facilitating conditions (Venkatesh et al., 2003). Most of the research on the Technology Acceptance Model has been applied to intentions about engaging in e-commerce for SMBs (Hoque et al., 2015; Herzallah & Mukhtar, 2015, 2016). Salimon et al. (2023) used the Technology Acceptance Model and the Unified Theory of Acceptance and Use of Technology to investigate Malaysian SMBs' technology adoption, of which SSO is a part.

Other studies have identified additional factors beyond those highlighted in the above theories. Some studies point to institutional pressures as an essential antecedent of company-level IT adoption, as companies adopt new technologies to better secure their IT environment (Chwelos et al., 2001; Sila, 2013). Another theoretical perspective proposes that the institutional environment, organizational structures, and practices affect IT adoption (Goodstein, 1994). Teo et al. (2003) associated IT adoption with gaining social legitimacy; responding to formal or informal pressures such as governmental regulation, and meeting the environmental needs of suppliers, customers, and businesses. This study is based on panel discussions and limited literature review.

Sutanonpaiboon and Pearson (2006) found that IT adoption by SMBs was related to financial and technological resources. They also note that various types of SMBs may face external pressures to integrate technological devices into their organization. Govindaraju and Chandra (2011) found that human resources and information sources were the most critical barriers to IT adoption in Indonesian SMBs. The Ghobakhloo et al. (2012) study investigated the manager's role in adopting e-commerce in small companies. In this case, the authors used the Diffusion Theory of Innovation as a basis for a theoretical model. They found that usefulness, ease of use, compatibility with an SMB's specific need, risks, and complexity are determinants of IT adoption by SMBs. Esmaeilpour et al. (2016) applied the Technology Acceptance Model to investigate the attitudes and intentions of IT use in SMBs. They found a positive effect of usefulness and ease of use on attitude and behavioral intention.

6 The Perspective of the Vendors and Customers

Despite the operational benefits and positive cybersecurity outcomes of the unified access management with a single set of credentials provided by SSO described in Section 4, its uptake remains slow, particularly among SMBs. To gain a deeper understanding of the most influential barriers to and catalysts of adoption beyond what we were able to learn from the literature review, CISA engaged with vendors, experienced managed service providers, non-profit organizations dedicated to improving cybersecurity, and SMBs that had experience with adopting SSO and migrating across SSO platforms. In order to provide a balanced perspective of the market dynamics, this section discusses the market from both the perspective of SSO vendors and customers.

CISA conducted several focus groups and held technical discussions with various types of stakeholders involved in the SSO market. Participants included SSO vendors, experienced computer network auditors, and SMBs, who all have a significant interest in encouraging SSO adoption and have experienced both barriers and catalysts first-hand. A brief description of the research method used in the study and associated stakeholder engagement process is presented in the appendix.

A summary of the key factors and considerations influencing the SSO adoption rate based on CISA's engagements are presented below. Overall, there are significant discrepancies between vendor perception and customer experience and expectations on numerous issues. Some of the most frequently cited discrepancies between vendor and customer views include such topics as the benefits of adopting SSO and its priority level relative to other business considerations, costs and resource constraints, technical challenges and technology awareness, and difficulties associated with vendor selection and upgrading legacy systems to accommodate SSO technology.

Adoption Benefits and Prioritization

Concerning the benefits of SSO adoption, perceptions among vendors and customers differ substantially. SSO vendors recognize an urgent need for organizations to adopt SSO due to increasing identity theft and improving

levels of threat intelligence for SMBs (i.e., information that helps organizations better protect against cyberattacks). Customers, however, tend to view the adoption of SSO with less urgency. While customers recognize the urgency of addressing security-related issues quickly, they tend to prioritize security concerns that could be addressed with SSO only once an incident occurs, as such an event can force customers to recognize the significance and benefits of adopting SSO as a preventive measure. Increasing customer awareness about potential risks and advantages associated with adopting SSO—particularly, stressing the need for proactive security measures even before any incidents arise—could encourage SMBs to adopt SSO sooner than they otherwise would.

SSO adoption priorities also often vary between vendors and customers. Whereas vendors might view adoption of SSO as both essential and a priority, customers may not view it as such given their assessment of the potential service disruption risks and associated costs (e.g., the opportunity cost of time and lost productivity due to business interruptions). Given their assessment, they may not prioritize investing in SSO over other business objectives such as gaining new customers, retaining existing customers, and complying with regulations.

Cost Implications and Resource Constraints

Cost perception varies significantly between vendors and customers regarding SSO implementation. SSO and application vendors believe the price tag justifies itself. Vendors may bundle services together to reduce overall expenses and appeal to customers with varying budgets, thereby shifting focus from cost to value. Tiered pricing options exist to accommodate different budgets and business sizes. Some customers, however, feel they are subject to what is commonly referred to as an "SSO tax" because they perceive SSO as being excessively costly due to the higher cost of the premium-tier service that includes SSO as compared to the lower-tier service that does not include SSO coupled with a requirement to subscribe for a minimum number of seats that may exceed the actual number of users. Customers also feel they pay for redundant packages or are charged for extra options that are neither wanted nor needed and do not provide value for the money paid. The National Security Agency and CISA (2023) explain this aspect in their joint guidance on Identity and Access Management as follows:

> In numerous [relying party] applications, SSO capabilities are bundled with other high end "enterprise" features in such a way to make them inaccessible to small and medium organizations. This business practice deprives these organizations of the security benefits of [multifactor authentication] and other critical capabilities that come from adoption of SSO and is based on a flawed assumption that SSO is an "enterprise" feature. In today's market, SSO is a table stakes feature for organizations of all sizes and should be included in any pricing plans that are targeted at business customers, regardless of size. (p. 9)

Resource constraints can also result in an unfavorable SSO adoption experience. Customers frequently need more dedicated staff to implement an SSO solution. Those who are unable to meet their staffing needs must rely on overworked and undertrained staff, which may result in difficulties during implementation. Vendors, however, typically assign dedicated resources to an SSO adoption project and may not be aware of the difficulties the customer is experiencing and perceive that the implementation is progressing as planned.

Vendors are interested in encouraging SSO adoption; however, they sometimes make a business case for SSO that does not always accurately reflect SMBs' constraints and objectives. There is an inherent incentive to convince SMBs to adopt technologies at the level of service that may not necessarily benefit the SMBs. Such upselling practices involve embedding or bundling tiers of unnecessary packages or services alongside a few that may be useful to the businesses purchasing them. Some vendors will bound some SMBs to their selected tier of service even if it is underutilized. Such information and negative adoption experience impact adoption decisions by other SMBs.

Technical Know-How and Awareness

Vendors feel confident that they offer sufficient training materials and how-to guides to support customers in effectively deploying SSO technology. They believe organizations should be able to overcome any technical hurdles associated with its deployment; however, customers have different perceptions and user experiences. They see SSO as a complex solution with numerous moving parts that may impede its successful deployment,

thus becoming a potential barrier to adoption. These challenges related to implementation need to be addressed before customers consider adopting it.

In addition, customers have varying degrees of satisfaction with the accuracy and completeness of the provided support materials and instructions. Even some of the more experienced and technically savvy users have reported the need to submit numerous support tickets and engage in multiple interactions with their vendor's customer support staff to fill the gaps or resolve inaccuracies and omissions. For SMBs with limited resources, the opportunity cost of that time makes the pursuit of proper SSO implementation prohibitively expensive and results in a negative user experience from the very start.

Regarding technological awareness, vendors often see SSO as a minimum standard security practice that all organizations should follow regardless of size or industry. They emphasize its benefits beyond security (e.g., potentially reducing cyber insurance costs for SMBs). However, customers have differing perspectives. Some see it as adding value that improves their security posture, while others view it as an unnecessary expense that does not deliver significant operational improvement and commensurate returns. The latter view may reflect a lack of awareness of all the benefits SSO may provide and highlights the need for clear messaging regarding its advantages.

Vendor Rivalry and Legacy System Challenges

The market for SSO solutions is highly competitive. As such, vendors provide different service offerings and technologies that allow flexibility. They attempt to streamline the selection process by publishing marketing data and technical details. Customers, however, may feel overwhelmed during this process. They often rely on unreliable customer reviews or recommendations for solutions that do not align with their needs. They may make judgments based on biased, unverified information, and not wholly on sound vendor trade-off analysis that accounts for their business needs and peculiarities.

Compatibility of SSO and its interoperability with legacy systems is also a challenge. Clients may have existing platforms that need help to accommodate the new SSO technology offerings. In order to adopt SSO, these customers must first invest in upgrading the legacy systems. Customers also often rely on older standalone apps built with outdated technology and see SSO implementation as disruptive and high-risk, given the significant upgrades needed on existing technologies.

Such customers may need accurate and conclusive evidence of SSO benefits and descriptions of its actual operational performance and user experience provided by prior SSO adopters via a trusted and reputable information dissemination channel. Such information can help them assess whether the long-term benefits of adoption outweigh the temporary discomfort SSO implementation might cause. Furthermore, adoption may also depend on an SMB's ability to secure financing. Reliance on significantly outdated legacy systems is often a consequence of constrained financial circumstances over a prolonged period. Thus, even with a favorable cost-benefit analysis, an upgrade that requires a significant initial capital outlay may not be attainable.

At present, many SMBs are using outdated systems for their day-to-day operations. Unfortunately, some platforms do not have the necessary technology to support a modern and scalable sign-on solution. To implement an SSO solution, it might be necessary to dismantle parts, or all of the existing IT environment. This type of upgrade might be perceived as involving a slow rollout that would place an unnecessary burden on the organization's day-to-day operations. The reluctance to undertake a significant overhaul of the environment might bring delays or hamper the adoption of SSO and any other new technology (Teo et al., 2003).

7 Conclusion

Both the literature review and CISA efforts that included focus groups and follow-up technical discussions identify several sets of benefits, challenges, and other considerations associated with the SSO adoption by SMBs.

Benefits of SSO

To fully leverage the advantages of SSO, SMBs should understand that it enhances productivity by minimizing the number of login attempts required to access multiple systems. Additionally, SSO strengthens security measures by reducing the exposure of passwords. Typically, individuals tend to reuse the same password across various

systems, which is considered a risky behavior. Such behavior can be addressed by implementing SSO. SMBs can also reap the benefits of an SSO solution by effectively managing user accounts from a centralized location, streamlining user management, and minimizing the risk of unmanaged accounts. Furthermore, SSO is an enabler for other technologies and e-commerce. It simplifies the process of managing end-user identities online. For many SMBs, e-commerce applications can translate into an additional source of revenue.

SMB Challenges with Implementing SSO

Implementing SSO solutions can be quite challenging for SMBs. Both financial costs and non-financial burdens associated with switching to a new technology solution serve as key obstacles hindering SSO deployment. The cost of entry is a significant factor as it involves a high initial investment. Training poses an additional challenge for many SMBs that need more technical expertise to manage an SSO solution independently. Furthermore, some of the SMBs that have already committed to a long-term or locked-in contract with a specific vendor may find it difficult to switch providers without penalties or integration issues. Lastly, the lack of technical knowledge among SMBs can impede the implementation of an SSO solution, particularly when ensuring interoperability with existing infrastructures.

Vendor Business Practices

Various vendors provide discounts to entice customers to purchase multiple software programs and services. One effective strategy is to offer tiered discounts based on the bundled services. Additionally, vendors aim to establish a Customer Relationship Management system to enhance the satisfaction of SMB clients. By analyzing the data collected through a Customer Relationship Management system, vendors can gain deeper insights into the specific needs of SMBs and provide tailored solutions accordingly.

SMB Needs

SMBs are on the hunt for specific attributes in an SSO solution. It needs to be scalable so it can accommodate additional users as the SMB expands. Affordability is crucial for SMBs in the short and long term, so a low initial cost is considered important. SMBs highly value user-friendliness in an SSO solution, as they often need more skills to manage it. SMBs ranked customer support as one of the most significant features in SSO solutions. As SMBs typically have limited technical experience, they prefer to avoid tinkering with the solution and rely on vendor for guidance and assistance during the initial SSO implementation phase.

8 Recommendations

Based on what CISA learned from this study, CISA has identified general recommendations for SMBs, SSO vendors, government agencies, and non-profit organizations aimed at encouraging SMB adoption of SSO solutions by helping to ensure a smooth and successful implementation while providing enhanced security and streamlined user access.

Recommendations for SMBs

Implementing a systematic approach to SSO will facilitate SSO deployment in SMB environments. We recommend SMBs use an approach such as the following. Start by analyzing the organization's needs, such as the number of users, applications, and security requirements. This assessment will help determine the most suitable SSO solution. Look for affordable options (e.g., cloud-based solutions that do not require extensive infrastructure). Compare the features and compatibility of different SSO solutions provided by the many vendors in the market. Evaluate how well the solutions integrate with existing infrastructure and applications. Conduct a pilot project to minimize risks and test the solution's effectiveness before rolling it out to the entire organization. Train the staff and provide clear guidelines for password management and security practices. Continuously monitor the SSO solution to strengthen the overall security posture.

Recommendations for Vendors

Based on user feedback, vendors can significantly improve their service offerings by implementing the following recommendations. Vendors should (a) gather customer requirements and offer tailored solutions that meet their needs, while eliminating unnecessary services; (b) offer more flexible seat thresholds or requirements; and (c) improve the accuracy and completeness of support materials for their essential set of services such as SSO.

First, basic and essential services such as SSO should be decoupled from bundles with premium services. Vendors should avoid upselling techniques, whereby they sell unnecessary services to SMBs. While product bundling is a recognized pricing strategy to extract maximum consumer surplus, the need for essential cyber services to protect and defend critical infrastructure and cyber-poor, target-rich organizations should not be leveraged to upsell premium services that may not have the same appeal or value-added. Instead, they should encourage customers to request additional services to improve their overall security standing when needed.

Second, vendors should provide a more flexible schedule of seat thresholds or requirements that would allow a meaningful service tailoring based on organization size. Specifically, for SMBs, special consideration should be given for pooling SSO licenses at the managed service provider level or SMB-group level rather than the individual subscriber organization level.

Third, it is crucial that vendors offer SMBs any necessary support and training. To reduce the number of call-ins and amount of technical support required by SMBs to properly implement and maintain SSO, the quality of the instructions given to users upfront should be significantly improved. In their user experience feedback, users consistently emphasized that instructions are incomplete, vague, and often inaccurate. The latter factor is a barrier not only to SSO adoption, but also manifests itself when the existing users attempt to migrate platforms. Jointly these three factors (i.e., the inclusion of SSO in bundles with premium services, inflexible seat thresholds and requirements, and inaccurate and incomplete instructions) result in a negative user experience, which negatively influences adoption decisions for potential SSO adopters.

Recommendations for Government Agencies

Government agencies such as the National Institute of Standards and Technology, CISA, and the General Services Administration can help highlight best practices, provide guidance, and produce buyer guides related to technologies, such as SSO, that align with current security recommendations. Furthermore, the government could consider providing incentives that would encourage the adoption of security technologies, such as SSO. A comprehensive study of incentives conducted by a U.S. Department of Homeland Security Integrated Task Force (2013) contains detailed discussion of the potential options.

Recommendations for Non-Profit Organizations

Relevant non-profit organizations dedicated to improving cybersecurity (e.g., the Global Cyber Alliance and National Cybersecurity Alliance) can engage with the public on the topic of SSO solutions as a part of their community involvement. These community engagements play a vital role in educating SMBs about the advantages of SSO technology. In addition, during their regular interactions with SMBs, these non-profit organizations gather valuable information about the SMBs' requirements, which can be used to offer tailored services and toolkits to these SMBs.

Appendix – Stakeholder Engagement Methodology

CISA chose a convenience sample[1] of SSO vendors based on the Gartner Magic Quadrant,[2] existing industry relations, and broader market research. The list of participants was extended via snowball sampling, where initial participants identified additional contacts of relevance. CISA used a similar technique for identifying managed service providers, experienced network auditors, and SMBs with SSO adoption experience.

CISA then conducted focus groups with various groups of stakeholders involved with SSO. Participants in these discussions include SSO vendors, experienced computer network auditors, and SMBs, who all have a significant interest in encouraging SSO adoption and have experienced both barriers and catalysts first-hand. This study analyzes factors affecting adoption by examining patterns and trends revealed during these discussions. Stakeholder engagement and technical discussions continued until a core set of considerations were addressed to the point that no new incremental information was presenting itself in subsequent outreach.

Research Design

CISA used a qualitative research design to obtain in-depth knowledge of the catalysts and barriers to SSO adoption. The individual conversations helped CISA obtain participants' insight and understand their experiences through semi-structured discussions that allowed for deeper investigation on specific topics while maintaining a uniform framework across discussions.

Data Collection Method

CISA gathered data through one-on-one discussions with each participant, either face-to-face, over the phone, or via video conferencing, depending on their availability and preference. CISA transcribed the discussions and reviewed the notes for later analysis. CISA synthesized and aggregated the findings in a manner that preserves anonymity and prevents re-identification to the extent possible.

Data Sources

CISA chose participants from diverse backgrounds to gain a broad balanced perspective of SSO adoption. The sample consisted of representatives from SSO vendors, computer network auditors with extensive experience in SSO audits, and SMBs who adopted or contemplating adopting SSO solutions.

Validity and Reliability

CISA used several strategies to enhance the validity and reliability of the findings. First, CISA selected participants with relevant expertise in the SSO domain. Purposeful sampling is a technique widely used in qualitative research for the identification and selection of information-rich cases for the most effective use of limited resources. Next, CISA adopted member-checking techniques, where participants received a summary of the findings with opportunities for feedback or clarification from others in attendance. Furthermore, CISA held peer debriefing sessions among researchers to review the data analysis process and ensure an accurate interpretation of findings. In addition, CISA is planning a follow-up engagement and outreach to the SMB community via the Global Cyber Alliance. CISA plans to conduct roundtables and focus groups to validate the findings of this study with a broader set of current SSO users and potential SSO adopters.

Limitations

This study's reliance on a convenience sample based on voluntary participation has recognized limitations. Namely, as with any voluntary discussion, there is a limited sample of participants with inherent self-selection bias, where statistical inference of the sample results on the rest of the population (beyond the actual respondents) is not appropriate. Therefore, the results cannot be generalized for the entire SMB population. Sample size and composition may not accurately represent all aspects of the SSO ecosystem. In addition, insights gleaned are contingent upon participants' personal experiences, assuming honest and accurate accounts of their experiences with SSO adoption are presented. This study's focus on qualitative data regarding a specific cybersecurity solution (i.e., SSO) could limit generalizability across other contexts.

---

[1] A convenience sample is a type of sample where the first-available primary data source will be used for the research without additional requirements.

[2] The Gartner Magic Quadrant is a series of market research reports published by the IT consulting firm Gartner that rely on proprietary qualitative data analysis methods to demonstrate market trends, such as direction, maturity, and participants (Teixeira et al., 2022).

Referencies

Armando, A., Carbone, R., Compagna, L., Cuéllar, J., Pellegrino, G., & Sorniotti, A. (2013). An authentication flaw in browser-based Single Sign-On protocols: Impact and remediations. *Computers & Security*, 33, 41–58. https://doi.org/10.1016/j.cose.2012.08.007

Blili, S., & Raymond, L. (1993). Information technology: Threats and opportunities for small and medium-sized enterprises. *International Journal of Information Management*, *13*(6), 439–448. https://doi.org/10.1016/0268-4012(93)90060-H

Bracken, B. (2023, November 30). *Okta Breach Widens to Affect 100% of Customer Base*. DarkReading. https://www.darkreading.com/application-security/otka-breach-widens-entire-customer-base

Bradbury, D. (2023, October 20). *Tracking unauthorized access to Okta's support system*. Okta. https://sec.okta.com/articles/2023/10/tracking-unauthorized-access-oktas-support-system

Chang, C.-C., & Lee, C.-Y. (2012). A secure single sign-on mechanism for distributed computer networks. *IEEE Transactions on Industrial Electronics*, *59*(1), 629–637. https://doi.org/10.1109/TIE.2011.2130500

Chwelos, P., Benbasat, I., & Dexter, A. S. (2001). Research report: Empirical test of an EDI adoption model. *Information Systems Research*, *12*(3), 304–321. https://doi.org/10.1287/isre.12.3.304.9708

Cusack, B., & Ghazizadeh, E. (2016). Evaluating single sign-on security failure in cloud services. *Business Horizons*, *59*(6), 605–614. https://doi.org/10.1016/j.bushor.2016.08.002

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science*, *35*(8), 982–1003. https://doi.org/10.1287/mnsc.35.8.982

D'Costa-Alphonso, M.-M., & Lane, M. (2010). The adoption of single sign-on and multifactor authentication in organisations – A critical evaluation using TOE framework. *Issues in Informing Science and Information Technology Education*, *7*, 161–189. https://doi.org/10.28945/1199

Dreyer, M., & Nygaard, K. (2020, June 15). Governments encourage SMEs to adopt new technology. Yale School of Management. https://som.yale.edu/blog/governments-encourage-smes-to-adopt-new-technology

Esmaeilpour, M., Hoseini, S. Y., & Jafarpour, Y. (2016). An empirical analysis of the adoption barriers of E-commerce in small and medium sized enterprises (SMEs) with implementation of Technology Acceptance Model. *Journal of Internet Banking and Commerce*, *21*(2).

Fink, D. (1998). Guidelines for the successful adoption of information technology in small and medium enterprises. *International Journal of Information Management*, *18*(4), 243–253. https://doi.org/10.1016/S0268-4012(98)00013-9

Ghobakhloo, M., Hong, T. S., Sabouri, M. S., & Zulkifli, N. (2012). Strategies for successful information technology adoption in small and medium-sized enterprises. *Information*, *3*(1), 36–67. https://doi.org/10.3390/info3010036

Goodstein, J. D. (1994). Institutional pressures and strategic responsiveness: Employer involvement in work-family issues. *The Academy of Management Journal*, *37*(2), 350–382.

Govindaraju, R., & Chandra, D. R. (2011). E-commerce adoption by Indonesian small, medium, and micro enterprises (SMMEs): Analysis of goals and barriers. *2011 IEEE 3rd International Conference on Communication Software and Networks*, 113–117. https://doi.org/10.1109/ICCSN.2011.6014861

Herzallah, F., & Mukhtar, M. (2015). The impact of internal organization factors on the adoption of e-commerce and its effect on organizational performance among Palestinian small and medium enterprise. *International Conference on E-Commerce (IcoEC) 2015*.

Herzallah, F., & Mukhtar, M. (2016). The impact of perceived usefulness, ease of use and trust on managers' acceptance of e-commerce services in small and medium-sized enterprises (SMEs) in Palestine. *International Journal on Advanced Science Engineering and Information Technology*, *6*(6), 922–929.

Hoque, M. R., Ali, M. A., & Mahfuz, M. A. (2015). An empirical investigation on the adoption of e-commerce in Bangladesh. *Asia Pacific Journal of Information Systems*, *25*(1), 1–24. http://doi.org/10.14329/apjis.2015.25.1.001

Joshi, U., Cha, S., & Esmaili-Sardari, S. (2018). Towards adoption of authentication and authorization in identity management and Single Sign On. *Advances in Science, Technology and Engineering Systems Journal*, *3*(5), 492–500. https://doi.org/10.25046/aj030556

Komorowski, M., Coppens, P., Van den Broeck, W., & Braet, O. (2016). Lowering the barriers for online cross-media usage: Scenarios for a Belgian single sign-on solution. *Telematics and Informatics*, *33*(4), 916–924. https://doi.org/10.1016/j.tele.2016.02.005

Mamun, A. A. (2018). Diffusion of innovation among Malaysian manufacturing SMEs. *European Journal of Innovation Management*, *21*(1): 113–141. https://doi.org/10.1108/EJIM-02-2017-0017

National Security Agency & Cybersecurity and Infrastructure Security Agency. (2023, October 4). *Identity and access management: Developer and vendor Challenges*. https://media.defense.gov/2023/Oct/04/2003313510/-1/-1/0/ESF%20CTR%20IAM%20MFA%20SSO%20CHALLENGES.PDF

Newman, L. (2023, November 23). Okta Breach Impacted All Customer Support Users—Not 1 Percent. Wired. https://www.wired.com/story/okta-breach-disclosure-all-customer-support-users/#:~:text=Okta%20upped%20its%20original%20estimate,%2C%20citing%20a%20%E2%80%9Cdiscrepancy.%E2%80%9D&text=In%20late%20October%2C%20the%20identity,of%20its%20customer%20support%20system

Nguyen, T. H. (2009). Information technology adoption in SMEs: an integrated framework. *International Journal of Entrepreneurial Behavior & Research*, *15*(2), 162–186. https://doi.org/10.1108/13552550910944566

Quirt, B; Singh, P; Sparling, C. (2022). SMBs: The next growth opportunity for high tech. https://www.accenture.com/us-en/blogs/high-tech/smbs-the-next-growth-opportunity-for-high-tech

Ramamoorthi, L. S., & Sarkar, D. (2020). Single Sign-On: A solution approach to address inefficiencies during sign-out process. *IEEE Access*, *8*, 195675–195691. https://doi.org/10.1109/ACCESS.2020.3033570

Riches, T. (2007). The challenge of supporting new technology adoption by SMBs. *Database and Network Journal*, *37*(3).

Rogers, E. M. (2010). *Diffusion of innovations* (4th ed.). Simon and Schuster.

Ruivo, P., Oliveira, T., & Neto, M. (2012). ERP use and value: Portuguese and Spanish SMEs. *Industrial Management & Data Systems*, *112*(7), 1008–1025. http://doi.org/10.1108/02635571211254998

Salimon, M. G., Kareem, O., Mokhtar, S. S. M., Aliyu, O. A., Bamgbade, J. A., & Adeleke, A. Q. (2023). Malaysian SMEs m-commerce adoption: TAM 3, UTAUT 2 and TOE approach. *Journal of Science and Technology Policy Management*, *14*(1), 98–126. https://doi.org/10.1108/JSTPM-06-2019-0060

Santini, F. d. O., de Matos, C. A., Ladeira, W. J., Jardim, W. C., & Perin, M. G. (2023). Information technology adoption by small and medium enterprises: a meta-analysis. *Journal of Small Business and Entrepreneurship*, *35*(4), 632–655. https://doi.org/10.1080/08276331.2022.2145787

Sila, I. (2013). Factors affecting the adoption of B2B e-commerce technologies. *Electronic Commerce Research, 13*(2), 199–236. https://doi.org/10.1007/s10660-013-9110-7

Sutanonpaiboon, J., & Pearson, A. M. (2006). E-commerce adoption: Perceptions of managers/owners of small- and medium-sized enterprises (SMEs) in Thailand. *Journal of Internet Commerce*, *5*(3), 53–82. https://doi.org/10.1300/J179v05n03_03

Teixeira, H., Data, A., Kelley, M., Hoover, J., & Guthrie, B. (2022). *Gartner, Magic Quadrant for Access Management*.

Teo, H. H., Wei, K. K., & Benbasat, I. (2003). Predicting intention to adopt interorganizational linkages: An institutional perspective. *MIS Quarterly*, *27*(1), 19–49. https://doi.org/10.2307/30036518

Urueña, M., Muñoz, A., & Larrabeiti, D. (2014). Analysis of privacy vulnerabilities in single sign-on mechanisms for multimedia websites. *Multimedia Tools and Applications*, *68*(1), 159–176. https://doi.org/10.1007/s11042-012-1155-4

U.S. Department of Homeland Security Integrated Task Force. (2013, June 12). *Executive Order 13636: Improving critical infrastructure cybersecurity*. https://www.cisa.gov/sites/default/files/2023-01/19_1115_dhs-eo13636-analytic-report-cybersecurity-incentives-study.pdf

U.S. Small Business Administration. (2023). *Frequently Asked Questions About Small Business.* Office of Advocacy. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjPqMKXvMeDAxUYD1kFHZkHApcQFnoECA4QAw&url=https%3A%2F%2Fadvocacy.sba.gov%2Fwp-content%2Fuploads%2F2023%2F03%2FFrequently-Asked-Questions-About-Small-Business-March-2023-508c.pdf&usg=AOvVaw1q6D9GShZFxP4KyOUe0oEq&opi=89978449

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, *27*(3) 425–478. https://doi.org/10.2307/30036540

Vu, N. H., Bui, T. A., Hoang, T. B., & Pham, H. M. (2022). Information technology adoption and integration into global value chains: Evidence from small- and medium-sized enterprises in Vietnam. *Journal of International Development*, *34*(2), 259–286. https://doi.org/10.1002/jid.3591

Yousafzai, S. Y., Foxall, G. R., & Pallister, J. G. (2007). Technology acceptance: A meta-analysis of the TAM: Part 1. *Journal of Modelling in Management*, *2*(3), 251–280. https://doi.org/10.1108/17465660710834453

Glossary

Access Management- Administering the logins and passwords of users across a range of apps and resources, typically contained inside a single organization.

Authentication- Validating an identity as true or false, generally used to verify that a user is who they say they are. Most commonly achieved through a username and password combination, but the same principle applies to other forms of authentication such as secret questions, secret links, and biometric identification.

Cross-Site Request Forgery- An attack that forces authenticated users to submit a request to a web application against which they are currently authenticated. Cross-Site Request Forgery attacks exploit the trust a web application has in an authenticated user.

E-commerce- Buying and selling goods and services online.

Identity Provider- A website, app, or service responsible for coordinating identities between users and clients. An Identity Provider can provide a user with identifying information and share that information with services when the user requests access.

Information Security (InfoSec)- The practice of protecting information by mitigating information risks. It is part of information risk management.

Information Technology (IT)- The use of computers to create, process, store, retrieve, and exchange data and information.

Single Sign-On (SSO)- An identification method that enables users to log in to multiple applications and websites with one set of credentials.

Small and medium-sized business (SMB) - While Small Business Administration (SBA) has an established definition of a small business, the threshold number of employees and revenue size varies by industry. SBA's Office of Advocacy generally defines a small business as an independent business having fewer than 500 employees[3]. For industry-level small business size standards used in government programs and contracting, see the Table of Size Standards at https://www.sba.gov/document/support-table-size-standards. There is not a set definition for a medium-sized business. However, based on the industry feedback, a business with fewer than 100 employees are generally considered small, while one with 100 to 999 employees is considered medium-sized.

[3] U.S. Small Business Administration. (2023). *Frequently Asked Questions About Small Business.* Office of Advocacy. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjPqMKXvMeDAxUYD1kFHZkHApcQFnoECA4QAw&url=https%3A%2F%2Fadvocacy.sba.gov%2Fwp-content%2Fuploads%2F2023%2F03%2FFrequently-Asked-Questions-About-Small-Business-March-2023-508c.pdf&usg=AOvVaw1q6D9GShZFxP4KyOUe0oEq&opi=89978449