The Commercial Education Society of Australia

Founded 1910

Journal of Commercial Education

Volume 1, Number 1, August 2025

ISSN 2982-3986 (Online) & ISSN 2982-3978 (Print)

Sponsored By

Elite Education Institute,
The Australian Institute of Technology & Commerce,
The Commercial Education Society of Australia

The journal rests on the assumption that there is a real sense in which every field of education depends on commercial influences in order to flourish.

Postal Address: 8 Quay Street, Sydney, NSW 2000, Australia
Email: journal@commercialeducation.com.au
Web: CommercialEducation.com.au/journal

The Commercial Education Society of Australia

Founded 1910

Australia's First Society of Tertiary Education

Journal of Commercial Education

Volume 1, Number 1

August 2025

ISSN 2982-3986 (Online) & ISSN 2982-3978 (Print)

Sponsored By

Elite Education Institute,
The Australian Institute of Technology & Commerce,
The Commercial Education Society of Australia

Editorial

The **Journal of Commercial Education** marks a pivotal moment for the Commercial Education Society of Australia (CESA), offering a platform that both honours its historical roots and addresses the evolving needs of commercial education in a globalised world. This journal reflects CESA's mission to prepare individuals for careers that not only contribute to the economy but also ensure profitability and sustainability in an increasingly complex and competitive landscape.

Defining Commercial Education

Commercial education is fundamentally associated with equipping individuals with the knowledge and skills to excel in business, commerce, IT, and related fields. It extends beyond traditional notions of business studies, encompassing independent tertiary education, the arts, and social sciences. In today's dynamic world, this includes preparing people for roles that require innovative thinking, practical problem-solving, and the ability to navigate the technological and economic challenges of a global marketplace.

Prime Minister John Gorton captured this sentiment in his congratulatory note to CESA on its 60th anniversary in 1970:

"Over these years the Commercial Education Society of Australia has made a valuable contribution to our commercial and business life. This increasingly competitive and complex world places great responsibilities on those who are in a position to set and influence educational standards. These days there is much glamour surrounding the scientific and technological age, but a nation would not get far without the commercial skills that are the concern for your Society."

This emphasis on the practical and economic importance of commercial education resonates with CESA's foundational goal of preparing individuals not only to enter the workforce but also to thrive in it.

Historical Foundations and Evolution

CESA's origins date back to 1910, when it was first established as the Incorporated Phonographic Society of Australia, reflecting its connection to the Pitman family and their pioneering work in shorthand and commercial training. The influence of Jacob Pitman, brother of Sir Isaac Pitman (the inventor of phonography), left an indelible mark on Australia's commercial education landscape. By the late 1960s, CESA had evolved from an independent shorthand examination board into a leading educational society with a diverse membership spanning typing teachers, university lecturers, chartered accountants, and even senior politicians, such as Sir Eric Archibald Willis, a lifelong supporter.

Its national significance is exemplified through endorsements from Australian leaders, including the Premier of New South Wales and the Prime Minister, as well as international recognition, as evidenced by a telegram from Queen Elizabeth II in 1970. These acknowledgements highlight the Society's role in shaping educational and professional standards.

A Century of International Connections

The Commercial Education Society of Australia has fostered over a century of educational connections with scholars and institutions across the Pacific, Melanesia, Asia, and the Middle East. These connections, established through professional society membership and educational courses—some of which continue to this day—have cemented CESA's reputation as a leader in international educational outreach.

A glance at the Membership Register reveals the diversity of CESA's global network, with members from 33 countries. The back cover of this journal proudly lists the names of 11 Australian Governors-General who have served as Patrons of the Society, endorsing its mission of international collaboration. This global engagement has grown in recent years, with contributions from international scholars to CESA's Periodic Discussion Papers and growing memberships in Associate, Member, Licentiate, and Fellow grades.

Affiliated with the *Société Internationale pour l'enseignement Commercial-International Society for Business Education* (SIEC-ISBE), CESA aligns with evolving global developments while maintaining its unique focus. This journal, while not in competition with SIEC-ISBE, furthers CESA's international outreach, enriching its global partners and welcoming new participants.

A Modern Vision for Commercial Education

In keeping with its tradition of adaptability, CESA has embraced a broader, more inclusive definition of commercial education. The field now extends into IT, creative industries, and even the arts and social sciences, recognising that the principles of commerce—such as efficiency, profitability, and strategic thinking—are applicable across virtually all sectors. The journal seeks to champion this modern understanding by publishing innovative research, practical insights, and abstracts of theses that advance the boundaries of commercial education.

The recent influx of young academics and students from diverse countries has brought renewed energy to CESA. This journal aims to capture their enthusiasm and expertise by providing a platform for original ideas and research related to commercial education and its many intersections. Given the pervasive influence of commerce, the journal also invites submissions that explore how these principles are applied across different fields of education. In this issue, there are two articles which relate to Cybersecurity; these are by young IT graduates, and there is a related letter by an older CESA Fellow.

Honouring the Pitman Legacy

The journal also honours the historical contributions of the Pitman family, whose influence laid the foundation for commercial education in Australia. The original Pitman's Journal of Commercial Education, published in the 1920s, serves as an inspiration for this modern iteration. By incorporating archival materials and reintroducing key historical works now in the public domain, the journal bridges CESA's rich history with its forward-looking vision. Indeed, Sir James Pitman was a former Vice-President of CESA and Mr Alfred Pitman was previously a Patron of CESA. In fact, it is worth noting that Sir Isaac Pitman, invented Shorthand in the English-speaking world in 1837, and his grandson, John Hugh Pitman was invested as an *Officer of the British Empire* for his services to vocational education. Thus, the Pitman contribution to international education in general and to CESA in particular makes it appropriate for this attempt to revive their commercial education journal.

A Platform for the Future

CESA's commitment to maintaining relevance in an ever-changing world is evident in its embrace of new ideas and emerging voices. By publishing contributions from young academics and experienced professionals alike, the journal ensures that commercial education remains a dynamic and responsive field. It also aims to educate stakeholders about the contemporary definition of commercial education, focusing on training individuals not only for jobs but also for entrepreneurial and leadership roles that drive economic growth.

Conclusion

The Journal of Commercial Education is both a tribute to CESA's century-long legacy and a bold step into the future. By promoting research, sharing innovative ideas, and championing the evolving definition of EDUCATION in commercial education, it ensures that CESA continues to be a leader in setting and influencing educational standards in Australia and beyond.

Gratitude is expressed to Professor Engin Özkan of Tűrkiye and Dr Mathew Hillier of Australia for detailed and generous proof-reading of papers in this number of the JCE.

Tony Shannon
Editor
Journal of Commercial Education

Time For Higher Education Chancellors and Governance Bodies to Take Ownership of Their Roles and Responsibilities

Dr Lorraine Bennett

Lorraine Bennett Teaching & Learning Consultancy

Natasha Bita's article in the Australian Higher Education on 04/06/2025, raised two red flags. Firstly, it conveyed the view that it is acceptable to treat international students as the goose that laid the golden egg, and second, that the practice of funnelling windfall funds from international students to further fatten excessive salaries for vice-chancellors and senior executives is ethically defendable.

I felt sure that the next week would carry an article challenging the integrity and wisdom of both these practices. Bita (2025) refers to "padding the pay packets" of vice-chancellors and senior executives by citing annual salaries ranging from the high $700,000s to over $1.2 million, the exception being the University of Divinity, where the vice-chancellor receives a fair and reasonable salary of around $220,000 per annum - more of this as a responsible benchmark later.

A review of Mission Statements across Australia's 44 universities and another 188 registered Private Higher Education Institutions consistently refers to themes of providing high-quality teaching and student-centred learning, engaging in innovative research, focusing on building community and industry engagement, and broadening cultural awareness. Common values cited are commitment to excellence, integrity, and accountability; respect and inclusion for students from all cultures; and sustainability and social responsibility through ethical policies and practices.

The practice of allowing the salaries of vice-chancellors to escalate to such exorbitant levels grates against the mission statements and values purported by the universities. It is time for University chancellors and councils to reflect on their University's mission and values and align their deliberations and decision-making accordingly.

Let us imagine an alternative allocation of the windfall from international student fees. Instead of inflating the vice-chancellors' salaries to unjustifiable levels, some of the funds could be used more productively by investing in innovative course development, teaching, and research activities. Bringing vice-chancellors' salaries to a fair and reasonable level would enable a university to employ an additional three to four tutors, early career academics, and experienced lecturers. If the staff were recruited strategically, their skills and expertise could be used to develop new courses in areas of need, such as AI generative technologies, cybersecurity, neuroscience and learning, mental health, blockchain systems, entrepreneurship, and the application of AI in engineering and medicine. With careful planning and support, these programs could become exemplars

in the sector and attract talented students, which in turn, would grow student enrolments and increase income from student fees, reducing the need to inflate and rely on over-priced international student fees. By offering innovative, relevant, quality courses, the university would be better positioned to build its domestic and international reputation and foster greater opportunities for industry partnerships and internship programs.

Consider the positive impact of redirecting the lucrative income from international student fees to recruit a mix of three to four research assistants and an experienced researcher. This would enable a small cohort of researchers to conduct research on contemporary issues, to apply for research grants, and ultimately to generate income from research outcomes such as commercialisation of inventions, patents and products.

The University of Divinity Council has set the annual salary for its vice-chancellor at around $220,000. Although the University has a low student enrolment compared with many of the Group of Eight Universities, it still requires high-level strategic leadership of a complex network of affiliated religious colleges located over multiple campus sites. The University of Divinity lives its mission and values. Its approach to staffing and leadership might well be a useful benchmark for the broader higher education sector.

For those who regard the University of Divinity as an outlier and a distorted comparison, a cursory examination of similar senior chief executive positions in allied service professions illustrates the largesse of vice-chancellor salaries. In 2023-24, the national average full-time salary was approximately $102,741 per year. The average salary of state premiers hovers around the mid $400,000, the prime minister is paid a little over $600,000, local government CEOs just under $300,000, high school principals average around $160,000, a little less for private schools and hospital CEOs average salaries are just under $400,000. When the majority of our university vice-chancellors are paid 125%- to 200% of the country prime minister's wage, surely it is time to challenge the status quo or at least start to ask some difficult questions.

Of course, now that the 'Genie' is out of the bottle, it will be difficult to turn the ship around. It will require strong leadership from university chancellors and council members. It will require support and backing from the government, perhaps in the form of reduced taxes for vice-chancellor salaries (what a novel thought).

While the task is daunting, the sector has no choice but to rethink its approach if it is to remain a viable and credible institution within the broader education sector. University Councils need to question the current situation where international students are seen as the "cash cows". Over fifty years ago, I had the good fortune to be an international student studying at a prestigious university in the United States of America. I was welcomed with open arms, offered subsidised student housing and a teaching fellowship to support my graduate study experience. At that time, the University believed that international students added to the rich cultural tapestry of the campus and exposed local students to

different ideas and perspectives. This assumption is still valid but has been overshadowed by the need for universities to source funds from a variety of wells, since governments no longer fund universities adequately.

University funding models that rely on international student fees are high-risk and ethically questionable. They are hostage to the whim of a range of geopolitical and environmental events. The 2020-22 COVID-19 pandemic provided a stark wake-up call for the need for universities to become self-sufficient. We need to leave 'greed' to Wall Street and start treating universities not as profit-making businesses, but as important

institutions within society, which provide inspirational leadership, model ethical behaviour, and contribute significantly to the well-being of local communities and global challenges.

Reference

Bita, N., (2025). Universities Reveal Soaring Revenues from Foreign Students. *Australian Higher Education*. April 4.

Artificial Intelligence (AI) and The Teacher

Kathleen McKenzie

President, Commercial Education Society of Australia

My aim as a university teacher is to produce students who value learning, have a thorough understanding of how to solve problems, think creatively, consider options, and value the need for lifelong learning. Many of my overseas students have told me that they are keen to work in international companies, so I want them to understand that organisations need people with skills in critical and innovative thinking, problem solving and research. These all promote better leadership skills. I want my students to be curious and to keep that curiosity forever. I want their parents' money spent wisely and productively.

We all know AI. We all use AI. Almost of our students use it. It is a very useful processing tool. It is here to stay. But as teachers we are concerned about the ethics of students relying wholly on AI and how it impacts on individual learning skills, their working memory with information and ideas and their long-term memory that stores knowledge (AERO, 2023). More important is the longer-term impact on their own learning and thinking.

We all know AI's potential to radically impact education. As teachers, we play a crucial role in preparing them to navigate the future. In today's world, AI is a wonderful tool for helping find information quickly – a machine for processing information. It can be used to complement learning methods. In a lecture session, students have told me that they use AI to find the gaps in their learning, which means that it can challenge their understanding. They like it because it can also help generate ideas and research, create an individual learning plan, and/or help brainstorm and get them started on an assignment question. It can help them with diagrams and graphs.

However, AI can also be used as a substitute for researching and verifying information and critical thinking. The July issue of the Spectator (McKee, 2025) notes that the performance of Australian universities is particularly poor when it comes to reputation with employers. Thirty Australian universities were marked lower for this than for their academic performance.

I agree with Jackson and Wilton (2026) that AI is a useful tool for students to evaluate data and equip them with ideas to tackle tasks and make improvements. Another positive effect is that it can improve their technical proficiency, so boosting their employability competitiveness.

Easy access can lure a student into over-reliance on AI. There are many reasons for this. It could be that they are pressed for time, because they have work/family commitments,

or being a serious learner is not their top priority, or they may simply lack interest in their particular subject.

Although at present AI lack may the subtlety and creativity intrinsic in human reasoning (Luckin et al., 2016), this only highlights our need to take a balanced approach to AI integration. We should ensure that it enhances, rather than replaces, human interaction and the development of critical thinking skills (Wu, 2023). Facione (2020) states that traditional methods of research been the foundation of the educational system for centuries. We also know, as he points out, that teachers can shape the learning experience for students. We often rely on a range of techniques and activities such as questioning, collaboration and course-work (assignments) to enhance students' ability to evaluate, examine and assess information and develop independent points of view.

Some questions that challenge us as teachers are:

- How do we prepare and encourage students to navigate a future shaped by AI?
- How do we encourage students to not rely 100 per cent on AI for all the answers?
- How do our class sessions balance AI integration for students, to ensure that it benefits rather than replaces humans working together?
- How do we ensure that it contributes to their ability to develop the critical thinking skills that are essential to their overall learning experience?
- How do we ensure that students are equipped to use AI in their studies and future careers in a productive and ethical manner?

I do not have the answers to these questions. However, one of the things that I do as I start a new course is to ask students to write one paragraph (50-80 words) on a topic (such as, their hometown, what they like best in Australia…). Students include their name and student number. I collect these so that I can gauge whether some students could perform better in their course with a referral to a university-based learning centre for extra help. This helps me tailor my classes to develop better learning skills combined with the topic.

I use AI through Chat GTP because I want to know how my students are using it. I use it to play Devil's Advocate by asking questions about how the information was verified, where it was found in the textbook, if there were counter-arguments, and what examples has the textbook/Power Point slides provided. In one of my classes, we noticed that some AI models appeared to mix information and found that it was because of the way that different students structured their question. Another reason might be a lack of sources or information that is not completely objective, or because AI, at present, lacks the breadth and creativity of the human mind.

AI is incorporated into translation services accessed by students on their iPhones. Some students use the translator to find words they do not know, but many use it to translate

all the text or the written questions that will be discussed in class. This does not improve their comprehension.

As teachers, we are up against numerous sites such as:

- Undetectable AI
- Word Spinner
- Text humanizer by Just Done.

It is our job to encourage students not to use AI as a substitute for learning methods but as an efficient aid. It is our job to find practical ways to encourage students to actively engage with facts and ideas and master their skills to learn and remember what they have learned. We want this to become their second nature for the future. Practically, it can result in better employment opportunities.

Lodzikowski et al. (2023) emphasised the responsible implementation of AI and ethical regulation of AI use in education. In 2025 it appears that all universities and higher education institutes have clear policies and information available on their websites for students. They run workshops on how to use AI ethically, and most have academic learning skills centres giving individual classes short information sessions. But this is not enough.

We should not approach AI as the enemy, but ask students how they can bring context to what AI lacks by exercising their judgement and contesting ideas. We need to produce a generation of graduates who are reflective and emotionally intelligent and resilient enough to face the challenges of the changing employment marketplace.

There are two approaches, one involving the institution itself – the head of program or subject coordinator. In general, the teacher in the classroom has very little or no input. Institutions, both public and private, are focused on cost efficiency and that affects policy and administration.

Here are my suggestions for universities and higher education institutions to enhance learning beside and beyond AI:

1. Emphasise the realities of employment by inviting more companies to give talks to student – this is cost-effective
2. Re-design the way assessments are set out by breaking them down into small steps
3. Oral assessments can be broken down into small steps
4. Try writing assessments in class
5. Portfolios can be built up, a collection of work over time to showcase problem solving and collaboration
6. Class participation can encourage discussion to show critical thinking and interest in the subject

7. Presentations in class can demonstrate their understanding and communication skills
8. Set one in-class exam at 100 per cent (Aouad, 2025)
9. Give an AI-generated assessment and ask students to point out the mistakes (Aouad, 2025).

My suggestions for us as teachers on how we could lift standards:

1. Starting off on Day 1 of a course by asking each student about their aspirations
2. Give real-life examples of successful businesspeople who have overcome poverty to build businesses and encourage them to read their stories (even as a part of class activity)
3. Show where their studies could take them
4. Encouraging discussion in class to show critical thinking and interest in the subject (both institution and class)
5. Encourage more intrinsic factors such as personal interest and curiosity
6. Focus on student-centred learning that engages them in the learning process as opposed to teacher-centred learning
7. Offer collaborative learning activities relating to their culture
8. Offer praise and rewards
9. Inject humour into the sessions
10. Share expertise and encourage them to apply it
11. Use peer evaluation
12. Appeal to their responsibility to their families

Our challenge as teachers is to create a more flexible, engaging and personalised learning experience that prepares our students for success in the 21st century. Teachers are immortal. The impact we have on students not only lasts their whole life, but often carries on into their children's lives. We will never know how it affects their life or career, but we should strive to make that impact as positive as we can.

References

AERO. (2023). *How students learn best: An overview of the learning process and the most effective practices.* September. The Australian Education Research Organisation. https://www.edresearch.edu.au/sites/default/files/2023-09/how-students-learn-best-aa_0.pdf

Aouad, G. (2025). A Reflection on Exams in Universities based on my humble experience and considering that we are dealing with a digital native… Linkedin (accessed 14 July 2025).

Facione, P. A. (2020). Critical thinking: What it is and why it counts. Insight Assessment. https://insightassessment.com/wp-content/uploads/2023/12/Critical-Thinking-What-It-Is-and-Why-It-Counts.pdf (accessed 20 June 2025).

Jackson, D., & Wilton, N. (2016). Perceived employability among undergraduates and the importance of career self-management, work experience and individual characteristics, *Higher Education Research & Development* 36(4): 1-16, DOI: http://doi.org/10.1080/07294360.2016.1229270 (accessed 28 June 2025).

Justdone. (n.d.). Humanizer AI by JustDone. Techwave Solutions Limited, USA. https://justdone.com/ai-humanizer (accessed 23 June 2025).

Luckin, R., Holmes, W., Griffiths, M., & Forcier, L.B. (2016). *Intelligence unleashed: An argument for AI in education.* Pearson Education. https://www.pearson.com/content/dam/corporate/global/pearson-dot-com/files/innovation/Intelligence-Unleashed-Publication.pdf

McKee, B. (2025). Grim University rankings show Australia is losing where it counts, *The Spectator*. https://www.spectator.com.au/2025/06/grim-university-rankings-show-australia-is-losing-where-it-counts/ (accessed 30 June 2025).

Undetectableai. (n.d.). *Advanced AI Detector and AI Checker for ChatGPT & More*, Undetectable Inc: Boise, ID. https://undetectable.ai/ (accessed 23 June 2025)

Word Spinner, (n.d.). How to Change AI Text and Avoid Detection: A Complete Guide. 24 October. Word Spinner LLC. The Netherlands. http://Word-spinner.com/blog/how-to-change-ai-text-to-not-be-detected/ (accessed 25 June 2025).

Wu, Y. (2023). Integrating generative AI in education: How ChatGPT brings challenges for future learning and teaching. *Journal of Advanced Research in Education*, 2(4), 6–10. https://doi.org/10.56397/jare.2023.07.02

Student Contributions on Topical Issues Facing Commercial Education Institutions

Editorial

Security is an increasing concern for commercial education institutions (CEIs) and this can be acute for smaller providers with more limited resources. Many online systems at smaller CEIs still rely on single authentication methods such as passwords that are increasingly vulnerable to cyber-attack. One method to address this weakness is to adopt multi-factor authentication where by two elements are required to gain access to a resource or system.

The following two papers were produced by students in a commercial education provider who were undertaking an Information Technology program. These two papers offer insights into the importance and use of multi factor authentication that is increasingly being used in commercial education environments.

Comparisons of Multi-Factor Authentication

Samip Manandhar
Samyak Tamrakar
Pratik Pokharel
Sonia Maqsood
Roshna Gurung

The Australian Institute of Technology and Commerce

Introduction

With the continuous development of smart devices and the internet, a growing number of online services have become available worldwide. However, security concerns are increasingly prevalent across various sectors, including banking, government applications, healthcare, and more as data can be accessed or manipulated easily. Thus, authenticating users of internet services has become crucial. “It is good to be wary about publishing your personal information even if other people are happy to post pictures of their house or their contact details – remember what goes online, usually stays online” (Parris-Long, 2012).

Authentication is the process by which a claimant provides proof to verify their identity to a verifier. The verifier then confirms the user’s identity within the information system (IS). Authentication systems address two key questions: (i) Who is the user? and (ii) Is the user truly whom they claim to be?

An increasingly common type of authentications is Multi-Factor Authentication. MFA is an electronic security mechanism that requires multiple forms of identification from independent categories of credentials to verify a user’s identity. Examples are (Australian Signals Directorate, 2022):

- Something you know PIN, Password
- Something you have, Physical token, SMS or email
- Something you are Fingerprint, facial recognition

To ensure secure access to systems and services, a large number of government policies are requiring mandatory multi-factor authentication. However, challenges related to accessibility, outdated regulations, and account recovery processes pose barriers to its broader implementation (Kim & Hong, 2011).

To achieve this aim, the following three objectives were defined:

- To explore various MFA methods and their guarantees
- To identify how they are appropriate and influence non-technical factors such as accessibility of government services, banking, etc.

- To identify the challenges to adopting these as security enhancements more broadly

With the rise of cloud computing, our sensitive data is spread across various online accounts, devices, and cloud storage systems. This expansion has increased the attack surface for both individuals and organisations, creating more opportunities for cybercriminals to breach confidential information (Trevino, 2023). As a result, data breaches have become increasingly frequent. According to Statista, over 1,800 data breaches in 2022 were reported, affecting more than 422 million people in the US (Petrosyan, 2024). These breaches often involve compromised passwords and other sensitive details. Therefore, implementing multi-factor authentication is important as it adds an additional layer of security. Many organisations have opted MFA due to today's security challenges and regulatory demands. With compliance standards such as GDPR and NIST mandating advanced security measures, the adoption of MFA will only increase as it is user-friendly and offers advantages that benefit both employees and IT teams (Okta, 2024, Smallman, 2024).

This group of authors collectively aims to provide a comprehensive analysis of MFA, highlighting its technical and non-technical aspects, to recommend strategies for enhancing security while addressing the challenges of accessibility and outdated regulations. To collect relevant materials efficiently while conserving both time and resources, an electronic database search was conducted. The initial step involved selecting key terms related to Multi-Factor Authentication (MFA); relevant terms were searched across various credible sources, including peer-reviewed journals, industry reports, and authoritative books on cybersecurity and authentication technologies. We also utilised academic databases like IEEE Xplore and Google Scholar to locate recent studies and articles that addressed the security, accessibility, and regulatory aspects of these MFA methods. Additionally, we reviewed industry white papers and guidelines from organisations such as the National Institute of Standards d Technology (NIST) and the European Union Agency for Cybersecurity (ENISA) to understand the practical applications and challenges of MFA in real-world scenarios.

For decades now, passwords have been the standard method of authentication for digital systems. However, as cyber threats become more advanced, relying solely on passwords is no longer sufficient. Even strong passwords are vulnerable to various attack methods, including Phishing, Credential stuffing and Brute-force attacks. So, to avoid this, MFA has evolved significantly with advancements in biometric authentication, password less authentication and risk-based authentication (E-Spin, 2024).

The FIDO (Fast Identity Online), a set of open, standardised authentication protocols, eliminates the use of passwords to make it more effective at protective sensitive information. FIDO uses cryptographic keys, keeping private keys on user's device to eliminate many security risks associated with traditional passwords. FIDO2's

passwordless authentication standard is rapidly gaining traction, providing stronger phishing resistance and ease of use, and is supported by companies like Google, Microsoft, and Apple.

In October 2014, JP Morgan Chase experienced a data breach that affected accounts of 76 million households and 7 million small businesses. The incident involved unauthorised access to the bank's servers, compromising user contact information. The breach underscored the importance of implementing secure web applications. The data exposed in the breach included credit card numbers, expiration dates, cardholder names, billing addresses, and CVV codes (Twingate Team, 2024).

In contrast, companies like Google and Microsoft, have successfully adopted phishing-resistant authentication methods like hardware security keys, which significantly reduced account takeovers. These case studies emphasise the necessity of advanced authentication techniques for securing sensitive data.

According to guidance by The Office of Management and Budget (OMB 04-04), four levels of identity authentication assurance are described where each level describes different degrees of confidence in verifying a user's identity (Bolten, 2003).

- Level 1 Little or no confidence in the asserted identity's validity.
- Level 2 Some confidence in the asserted identity's validity.
- Level 3 High confidence in the asserted identity's validity.
- Level 4 Very high confidence in the asserted identity's validity.

Table 1 : Authentication levels of assurance (OMB 04-04)

The NIST 80063 Electronic Authentication Guideline provides detailed technical requirements for each of these assurance levels, specifying controls for identity proofing, token requirements, and protection mechanisms (Burr, Dodson & Polk, 2015):

Level Identity Proofing Token Authentication Protection Mechanisms

1 Requires no identity proofing. Allows any type of token such as a username or a simple PIN. Little protection against offline attacks or eavesdropping, and only one token is necessary.
2 Requires some identity proofing. Allows single-factor authentication, commonly passwords. Prevention against online guessing, replay and eavesdropping attacks using FIPS 140-2 approved cryptographic techniques.
3 Requires stringent identity proofing. Multi-factor authentication, typically a combining password or biometric factors with a software token, hardware token or OTP device. Prevention against online guessing, replay and man-in-the-middle attack with cryptographic validation at FIPS 140-2 Level 1 overall and Level 2 validation for physical security.

	4 Requires in-person registration. Multi-factor authentication with a hardware crypto token. Prevention against online guessing, replay, eavesdropper, impersonation, and session with FIPS 140-2 Level 2 cryptographic validation overall and Level 3 for physical security.

Table 2: Technical requirements for each level

Evolution of MFA: From Passwords to Passwordless authentication: From the early days of simple passwords, the way we secure access to our digital lives has evolved significantly over the past few decades.

1. Passwords: The earliest and default method of authentication. Passwords were the first widely adopted method of digital authentication. They were easy to implement and provided basic level of security but as the internet grew and cyber threats became more severe, they became vulnerable to various attacks such as brute-force attacks or password guessing. Weakness include:

- Users often choose weak, easily guessable passwords or reuse the same password on across multiple sites. According to studies, 23% of users repeat the same password for many accounts, making them particularly vulnerable.
- Using fraudulent emails and websites, attackers lure people into disclosing their passwords. According to Google, 68% of phishing attempts succeed in deceiving consumers (cybernexa-admin, 2024).

2. Token-based: As online identity threats started to become more complex, strategies to protect digital identities evolved, leading to the development of Multi-Factor Authentication (MFA), a more secure alternative to the password-only model. Token-based security methods added another layer of protection, with hardware tokens like USB security keys and software tokens generating time-sensitive codes that must be used alongside passwords. This significantly reduced the risk of account compromise, as even if a hacker obtained the password, they would still need the token to gain access. While MFA and token-based security improved account protection, they introduced additional complexity and user friction. People now had to manage multiple devices and remember extra steps, creating the need for a more seamless yet secure authentication solution.

3. Biometric Authentication: Biometric authentication marked a major advancement in both security and usability. They offered a nearly impossible-to-forge methods such as fingerprint, face recognition, and iris scanning, to verify identity. When Apple released Touch ID in 2013, and Face ID in 2017, they started to make difference in the world of biometric security. With the combination of new hardware and software capabilities, it enabled fast, secure, and incredibly convenient user experiences. Other technology giants soon followed suit, providing biometric authentication on a variety of devices and applications. Biometrics solved many issues with passwords, as users no longer needed to remember complex passwords or carry extra security tokens. Because biometric data

is unique to the individual and hard to replicate, it provided a far more secure alternative to traditional authentication methods. However, while biometrics worked well for personal devices, businesses and platforms still needed scalable solutions to authenticate users across multiple devices and services.

4. Passkeys: The Future of Passwordless Authentication. With biometrics on the rise, it was now evident that the future of authentication wasn't just more secure, it was completely Password-less. The Fast Identity Online (FIDO Alliance) was founded in 2012 with the goal of developing new standards that would totally eliminate the need for passwords and is more secure and user-friendly authentication. Late, in 2021, these efforts resulted in an innovative authentication method called passkeys. A passkey is a pair of cryptographic keys. The two components are:

1. Private key: Stored securely on the user's device;
2. Public key: stored on the server;

When a user wants to log in, the device uses a biometric factor (facial recognition, fingerprint) to confirm the user's identity. It then uses that private key for session authentication. With the help of passkeys users never need to use passwords and this reduces their vulnerability to phishing attempts, password reuse, and weak credentials (Hasan, 2024).

Issues

While many websites rely solely on single-factor authentication, typically through a password, others require users to verify their identity using multiple authentication factors.

Although verifying biometric factors is impractical for most websites, it is becoming increasingly common to see both mandatory and optional multi-factor authentication (MFA), which often involves combining something you know with something you have. Typically, this requires users to enter a traditional password along with a temporary verification code from an out-of-band physical device they possess.

While an attacker might be able to obtain a single knowledge-based factor, like a password, it is significantly more challenging to acquire another factor from an out-of-band source simultaneously. This is why multi-factor authentication is considerably more secure than single-factor authentication. However, as with any security measure, its effectiveness depends on its implementation. Poorly implemented multi-factor authentication can be circumvented or even completely bypassed, just like single-factor authentication (PortSwigger, n.d.). There are problems, such as:

1. Security Vulnerabilities of SMS Codes: SMS-based MFA is one of the most common methods but also one of the most vulnerable. Attackers can intercept SMS messages as the code transmitted is generated through SMS, instead of being

generated on the device, which opens up the possibility of the code being intercepted. Additionally, there is a risk of SIM swapping, where an attacker fraudulently acquires a SIM card with the victim's phone number. This allows the attacker to receive all SMS messages intended for the victim, including the verification code (PortSwigger, n.d.).

2. Accessibility Challenges Posed by Hardware Tokens: Hardware tokens provide a high level of security but pose significant accessibility challenges. If everyone in your office has a YubiKey, it is easy for them to get mixed up, which would not happen with passwords. Additionally, users must physically carry the token, which can be easily lost or stolen, posing a security risk. Also, it might be difficult for individuals with disabilities to handle the hardware tokens (Eli, n.d.).

3. Slow Adoption of Passkeys Due to Outdated Regulations: In 2023, there was a significant increase in tech companies adopting passkeys, an authentication method that enables users to log in using facial or fingerprint biometrics or a PIN. Password manager Dashlane's CPO Donald Hasson mentioned to Engadget that users log in with passkeys about 20,000 times per month, with usage doubling each quarter. However, despite being more secure than traditional passwords, only a small percentage of users are currently taking advantage of this method due to outdated regulations and compliance requirements that still emphasise older authentication methods like passwords and SMS codes (Gonzalez, 2024).

These problems can be interpreted from different perspectives:

1. Technical Perspective: Each MFA method has its strengths and weaknesses. For example, SMS codes are vulnerable to techniques such as SIM swapping, while biometric data has a high level of security. Hardware tokens are one of the most secure authentications as it is impossible for cybercriminals to steak over the internet but are prone to being lost or stolen. Aside from that, it can be challenging to integrate MFA into existing systems, especially in legacy systems that may not support modern authentication methods.

2. Regulatory Perspective: While biometric technologies have been around for decades, their use is accelerating rapidly with the growth of the digital economy, like taxi booking services, ATMs, online banking, financial services, healthcare, law enforcement, and telecommunications. However, the use of biometric data and technologies has two distinct aspects. On the one hand, they offer significant cybersecurity and privacy benefits, enhancing the security of digital assets, while on the other hand, there are concerns over uses of our biometric data and the increasing threats from cyber incidents, including the serious consequences of unauthorized access to and misuse of this sensitive information (Givoni & Christie, 2023).

3. User-centric Perspective: Some MFA methods can create barriers for people with disabilities. For example, hardware tokens might not be easily accessible to people with physical disabilities, and SMS codes may not be practical for users in regions with unreliable mobile network coverage (NIST, 2023).

Other facets of these problems include;

1. Accessibility: Different MFA methods may be more or less accessible depending on the user's needs and available equipment. Often, MFA steps can be combined with existing accessibility support measures, such as screen readers and custom keyboards. It's crucial to ensure that MFA technology is compatible with user's accessibility tools. Providing one-on-one support to verify that MFA factors work well with these tools can be beneficial. If MFA technology is too cumbersome or incompatible with essential programs like screen readers, users might seek alternative solutions or use unauthorised tools to maintain productivity, potentially creating significant security risks (Lake, 2021).

2. Regulatory Compliance: It is important to recognise that while MFA provides a crucial security layer, it is just one part of a comprehensive security strategy. Successful implementation relies on understanding the specific needs of each compliance standard and integrating MFA smoothly into the organisation's existing processes (Soong, 2024).

3. User experience: MFA can be challenging for users, particularly those who are not tech-savvy, due to its complexity. Setting up MFA tools and navigating various authentication methods can be confusing and overwhelming. Additionally, the need to enter multiple factors each time you log in may be seen as inconvenient and time-consuming, potentially discouraging users from adopting MFA. Many MFA systems also lack clear instructions, which can leave users feeling frustrated and uncertain during both setup and use (Instasafe Marketing, 2024).

An attacker who gains control of an authenticator can often impersonate its legitimate owner. Threats to authenticators can be categorised based on the type of authentication factors involved:

Something you know: An attacker might discover a memorised secret through various means, such as guessing, accessing a shared secret at the CSP or verifier, performing a dictionary attack on a hashed value, observing the entry of a PIN or passcode, finding a written record, or using malicious software like a keylogger. They may also obtain secrets through offline attacks on a password database.

Something you have: An authenticator could be lost, damaged, stolen, or cloned. For instance, an attacker might copy a software authenticator from an owner's computer, steal or duplicate a hardware authenticator, or intercept out-of-band secrets used for authentication.

Something you are: Biometric data, such as fingerprints, can be replicated by an attacker who manages to obtain a copy and create a replica (NIST, 2023).

The primary drawback of MFA is the increased management complexity for both administrators and end users. For example, some MFA methods such as biometric systems or hardware tokens can be difficult for users with certain disabilities. Some users might face challenges in remote or underserved areas because of geographical and technological limitations.

Banks are a significant target for cyberattacks due to the sensitive information and resources, such as personal details and financial records, they handle. As result, banks have adopted MFA widely to ensure the security of these assets and maintain trust and stability in the financial system. Without proper security measures, this data could be exploited by cybercriminals, leading to issues like identity theft, fraud, and other harmful activities. Not just through direct theft, but also from expenses related to remediation, legal fees, and penalties. For example, biometrics and hardware tokens are often used for high-risk transactions while SMS codes or TOTP are frequently used for everyday logins (Smartosc, 2024). For example: The massive cyberattack on JP Morgan Chase in 2014 made the digital infrastructure of financial institutions vulnerable. The historic attack allowed hackers to access 7 million small businesses; and 76 million households; personal data. The bank's reputation took a serious and quick hit. In addition to the immediate financial losses, the hack undermined industry-wide consumer confidence.

The JP Morgan Chase data exfiltration was not caused by a sophisticated, unheard-of hacking method. The attackers got into the server by using the stolen credentials, a common yet critical weakness in digital security. A key solution to mitigate such risks is the implementation of multi-factor authentication, particularly Two-Factor Authentication (2FA), which provides an essential layer of security to protect sensitive data and customers' trust (Amigorena, 2023).

Governments are offering more digital services such as healthcare, social services and tax filing. To keep these personal data secure, MFA is used. But another critical concern is the accessibility. Not all citizens have access to a smartphone or hardware token. In the countries with limited access to technology, government may rely on simpler MFA methods like email or SMS codes, which poses security risks. For example: India's national digital biometric identity system, the Aadhaar system, received criticism for depending primarily on biometrics without adequate fallback options for account recovery. Centralised identity databases like Aadhaar have faced criticism due to security and policy concerns. Data breaches, whether intentional through unauthorised access or accidental due to technical or clerical errors, are ongoing risks. There is evidence that the Aadhaar system has experienced security issues, including accidental data leaks. In early 2017, news reports highlighted how Excel files containing Aadhaar numbers and personal information were mistakenly posted online by various Indian government offices and

could be easily found via Google. One breach exposed the bank details of a million pension beneficiaries due to a programming error. A journalist also discovered thousands of Aadhaar enrolee details, including their Aadhaar numbers, available on several government websites (Dixon, 2017).

References

Amigorena, F. (2023, July 20). Importance of 2FA for financial services. IS Decisions: https://www.isdecisions.com/en/blog/mfa/importance-of-2fa-for-financial-services

Australian Signals Directorate. (2022, October 14). Protect Yourself: Multi-Factor Authentication. Australian Government, Canberra. https://www.cyber.gov.au/protect-yourself/resources-protect-yourself/personal-security-guides/protect-yourself-multi-factor-authentication

Bolten, J. B. (2003, December 16). E-Authentication Guidance for Federal Agencies. George W Bush White House archives: https://georgewbush-whitehouse.archives.gov/omb/memoranda/fy04/m04-04.pdf

Burr, W. E., Dodson, D. F., & Polk, W. T. (2015, August 6). Electronic Authentication Guideline, Technical Series Publications, National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-63ver1.0.2.pdf

Cybernexa-admin. (2024, August 9). From Passwords to Passwordless: The Evolution of Authentication. Cybernexa: https://www.cybernexa.com/blog/from-passwords-to-passwordless-the-evolution-of-authentication/

Dixon, P. (2017, June 14). A Failure to "Do No Harm" -- India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S. *Health and Technology*, 7, 539-567. doi: https://doi.org/10.1007/s12553-017-0202-6

E-Spin. (2024, October 07). The Rise of Multifactor Authentication: Securing the Future of Digital Access. E-Spincorp: https://www.e-spincorp.com/the-rise-of-multifactor-authentication-securing-the-future-of-digital-access/

Eli. (n.d.). Two factor auth with hardware. Anvil: https://anvil.works/blog/two-factor-auth-with-hardware.

Givoni, S. & Christie, A. (2023, March 09). Guide to Understanding the Australian Biometric Privacy Law Landscape. LexisNexis: https://www.lexisnexis.com.au/en/insights-and-analysis/research-and-whitepapers/2023/privacy-law-bulletin-2023-special-issue

Gonzalez, B. (2024, January 23). Passkey adoption lags great expectations but opportunities still growing. Biometric Update.com: https://www.biometricupdate.com/202401/passkey-adoption-lags-great-expectations-but-opportunities-still-growing

Hasan, U. (2024, September 23). The Evolution of User Authentication: From Passwords to Passkeys. TechBullion: https://techbullion.com/the-evolution-of-user-authentication-from-passwords-to-passkeys/

Instasafe Marketing. (2024, July 30). Multi Factor Authentication Zero Trust Blog: https://instasafe.com/blog/refining-your-mfa-user-experience-and-overcoming-usability-challenges/

Kim. J-J., & Hong S-P. (2011). A Method of Risk or Multi-Factor. *Journal of Information Processing Systems* 7(1), 187-198 doi: https://doi.org10.3745/JIPS.2011.7.1.187

Lake, K. (2021, July 29). MFA Accessibility: Evaluating Different MFA Factors. Jumpcloud: https://jumpcloud.com/blog/evaluating-the-accessibility-of-different-mfa-factors

NIST. (2023, October 16). NIST Special Publication 800-63B. National Institute of Standards and Technology. https://pages.nist.gov/800-63-3/sp800-63b.html#sec8

Okta. (2024, June 20). Why Multi-Factor Authentication (MFA) Is Important. Okta: https://www.okta.com/identity-101/why-mfa-is-everywhere/

Parris-Long, A. (2012, February 07). Yahoo! News, UK. https://uk.news.yahoo.com/safer-internet-day--why-every-generation-has-a-role-to-play-in-keeping-the-web-secure-.html

Petrosyan, A. (2024, February 12). Number of data compromises and impacted individuals in U.S. 2005-2023. Statista: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

PortSwigger. (n.d.). Multi-factor. https://portswigger.net/web-security/authentication/multifactor

Smallman, J. (2024). The Effectiveness of Cyber Threat Intelligence in Improving Security Operations. *Journal of Artificial Intelligence General Science*, 21. https://www.researchgate.net/publication/382131714_The_Effectiveness_of_Cyber_Threat_Intelligence_in_Improving_Security_Operations

Smartosc. (2024, July 30). Cyber Security in Australian Banking: Importance, Threats & Challenges. Smartosc: https://www.smartosc.com/cyber-security-in-australian-banking-importance-threats-challenges/

Soong, J. (2024, July 25). Meeting Compliance: Multi-factor Authentication (MFA) Control Requirements. Authsignal: https://www.authsignal.com/blog/articles/how-to-meet-compliance-requirements-for-multi-factor-authentication-mfa-controls

Trevino, A. (2023, June 27). Types of multi-factor authentication. Keeper: https://www.keepersecurity.com/blog/2023/06/27/types-of-multi-factor-authentication-mfa/

Twingate Team. (2024, May 24). JP Morgan Chase data breach. Twingate: https://www.twingate.com/blog/tips/jp-morgan-chase-data-breach

Beyond Passwords: Evaluating Multi-Factor Authentication

Audrey Dale Salang Barangan
Chanikan Polpattanakul
John Rey Mendoza Montejo
Manjusha Thomas
Pravallika Thunga

The Australian Institute of Technology and Commerce

This paper looks at how Multi-Factor Authentication (MFA) can be optimised through evaluation of the cost, security, and user experience, accepting the fact that conventional methods of single-factor authentication are open to more risks than in the past. The study calls for the development of MFA that would help reduce risks attached to cyber threats that threaten organisations and data privacy. Different forms of MFA approaches are discussed in the paper, including the use of SMS codes, email codes, biometric identification, hardware tokens, and application notifications. The advantages, constraints, and applicability of the various approaches are highlighted.

Keywords: Multi-Factor Authentication (MFA), Cybersecurity, MFA Adoption Challenges, Passkeys, Adaptive Authentication, Biometric Authentication, Hardware Tokens, Cost of MFA Implementation

Introduction

Multi-factor authentication is one of the many evolving cyber safety measures instigated so as to reduce data loss and mishandling of pertinent information (be it personal or organisational) and mitigate the risks of being exposed to malicious attacks, thereby maintaining system incorruptibility. This particular authentication requires two or more verification processes to validate a user's identity to access their accounts. Its main objective is to fortify security by incorporating multiple layers of protection. This study aims to disclose the challenges and concerns, particularly the efficiency of the authentication method in terms of various factors like cost, the level of security and user experience.

Like everything in this evolving world, the most straightforward authentication, known as single-factor authentication, is becoming a thing of the past. It involves entering a username and password. Once the user has submitted the details, it will be sent to the server to verify whether the data matches their records. Only if the entries are correct can access be granted. However, because of its simplicity, hackers and cybercriminals can easily guess or crack the password and break into this system (Das et al., 2020). It is imminent that a new method will be developed. The age of multi-factor authentication

has come to its place—it has become mandatory and the backbone of access control for large enterprise companies to protect their system and data (Reno, 2013).

According to Ometov et al. (2018), multi-factor authentication is introduced to enhance security and protect devices from unauthorised access. Multi-factor authentication (MFA) employs two or more credentials, such as biometrics and authenticators, which are automated techniques of recognising people based on their physical characteristics and personal gadgets. It then offers extra protection by identifying the user via numerous criteria.

The implementation of multi-factor authentication is determined by the specific requirements of the user or organisation. Given that passwords are the predominant means of authentication, they can pose significant security concerns. This study will examine the history and evolution of MFA technologies while identifying optimal practices regarding user experience, knowledge, cost, and security levels. Implementing multi-factor authentication is crucial to businesses and other sectors, as mentioned in the background of the issue (Reno, 2013). Currently, cybercriminals are becoming knowledgeable and more equipped by using technology in executing their malicious activities. Therefore, this study is important to evaluate the risks and address the issues associated with applying MFA. For example, in the healthcare sector, people's medical data are considered critical and sensitive. IoT devices collect sensitive information, making this domain vulnerable to attacks without an additional security layer. Multi-factor authentication (MFA) safeguards communication channels against cyberattacks and unauthorised access during data transmission on the server (Suleski et al., 2023). This research gives enterprises and industries the expertise and resources to proactively adopt MFA and safeguard their confidential information.

Cost-effectiveness

Cost-effectiveness incorporates implementation expenses and the advantages they yield. The optimal MFA approach hinges on the equilibrium between security, cost, and user ease. The methods include app notifications, app codes, external and internal security keys, SMS, and phone calls. Based on the information from the table, app-based methods offer a good balance of user experience, level of security, and cost, and they are widely supported. On the other hand, external and internal security keys offer the best user experience and level of security. However, it comes with a price; it is expensive and has limited supported platforms. While SMS and phone calls are widely supported, they have poor user experience and security (Waugh, 2021).

A vital aspect of MFA is the combination of three classes of authentication, namely,

- Knowledge (Password or security question)
- Owned device or account
- Biometric data

Main Issues

At the beginning of the digital age, people used passwords only for authenticating someone. Thus, a single-factor authentication was already enough. However, as technology advances, the days of relying solely on passwords are fading away due to the persistent cybersecurity threats. Using a password is still valid and slightly effective. But the lack of knowledge on how to create a strong password has become a pertinent issue. People who are using weak or simple passwords for their accounts are prone to cyberattacks. Due to the inherent vulnerabilities of outdated single-factor authentication methods, multi-factor authentication (MFA) has emerged as a crucial component of modern cybersecurity defences. According to Reese et al. (2019), the introduction and extensive use of MFA systems present a complex array of difficulties that call for careful research and analysis. However, implementing MFA effectively requires a balance between user experience, cost, and security level. Managing these challenges is critical for individuals and organisations that want to adopt MFA properly. This shows us that the objectives of this particular authentication method are not isolated issues but rather multifaceted aspects. The issue is that we need to understand the best practices of multifactor authentication methods based on the user experience, cost, and level of security. It is also crucial to grasp that the use of MFA comes with its own set of challenges that organisations must be ready to tackle. Solomon (2024) outlined seven key criteria for selecting the right MFA that aligns with the organisation's requirements. These include:

- risk assessment,
- user experience,
- infrastructure and cost,
- accessibility and inclusivity, regulatory compliance,
- technology integration, and security awareness and training.

However, it is a problem for users, especially those with little technological proficiency, to adapt to the supplementary authentication protocols. This may lead to reluctance to change, undermining the intended security improvements. To identify the opinion and understanding of various stakeholders of MFA, we prepared a simple questionnaire so that we would get the feedback and experience from different categories of individuals.

Passwords are knowledge-based authentications that individuals can create according to their preferences. Despite passwords being an accessible method for everyone, they still have several drawbacks, especially their significantly low level of security, which is unacceptable for authentication. It is susceptible to password guessing—the most common form of cyber-attack. The top ten passwords that are commonly used in brute-force or SSH (Secure Shell) attacks were examined by Owens and Matthews (2008). Based on their data, "username"; accounted for 56.9% of the passwords used in these assaults. The passwords "password" (1.4%), "test" (0.8%), and "123456" (3.6%) were among the other passwords that were frequently compromised. The data shows that a significant

portion of the brute-force attempts used common default passwords like “admin” and “passwd” as well as easy-to-guess passwords such as numerical sequences “123456” and “12345” See Table 3 (Owens & Matthews, 2008).

Adhering to regulatory frameworks is essential when implementing MFA, as they differ significantly across jurisdictions. However, the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and the Australian Data Privacy Regulations (ADPR) have distinct criteria for user authentication and data protection. According to Tsakalakis et al. (2019), this highlights the challenges that organisations have when trying to ensure MFA compliance across several regulatory regimes. The efficiency of MFA mostly relies on user acceptance and correct application. Many users of MFA systems believe they are time-consuming and difficult, which helps explain poor adoption rates and attempts to circumvent security policies. Das et al. (2020) results show the conflict between security and usability, as 28% of users disabled MFA on their accounts because they believed it was annoying.

A significant number of organisations encounter difficulties in integrating contemporary MFA solutions with their existing legacy systems. In sectors such as banking and government services, the challenge is particularly acute due to the prevalence of outdated infrastructure. When endeavouring to implement MFA across all of their customer-facing platforms, 63% of financial institutions encountered substantial technical challenges, according to Weir et al. (2009). According to Losinskyi & Sirosh (2024), the reasons given for avoiding MFA are that it is annoying, it is too complicated and it is too slow.

Using a fishbone diagram, we visually depicted and examined the underlying reasons for the difficulties we ran across in our research on issues in multi-factor authentication (MFA). This graph gave us a methodical approach to recognise the influencing elements and their interrelations, thereby helping us to divide the difficulties into main categories. Analysing these domains helped us to understand the fundamental problems influencing the MFA deployment and efficacy. By addressing these core problems, we may increase the overall effectiveness of MFA implementations while balancing user experience, cost, and security.

We examined three major regulatory frameworks—GDPR, CCPA, and ADPR—and their influence on MFA adoption. Our analysis will integrate insights from survey data and other secondary sources, providing a thorough perspective on user impressions and expert viewpoints. Finally, we present diverse interpretations of these challenges from the viewpoints of stakeholders, professionals, and regular users to further our understanding of how MFA impacts various populations. Next we analyse the key criteria for selecting an appropriate MFA: Solomon (2024).

Organisations must evaluate the value of the data they manage in order to determine the appropriateness of implementing an expensive authentication system. According to the Office of the Australian Information Commissioner (OAIC, 2024), the Australian Government, finance, insurance, retail, and healthcare sectors were the most significantly impacted by data intrusions in 2023. User Individuals frequently select authentication techniques according to their experience and familiarity with and comprehension of the relevant technologies. Some MFA systems provide robust security; yet, they might be challenging for numerous users to comprehend and execute, resulting in hesitance towards adoption. A study by Das et al. (2020) indicated that both IT professionals and non-experts recognised their inadequate understanding of the importance of MFA. Furthermore, participants regarded the implementation of MFA as onerous, comparing it to completing a chore.

Every MFA technique has different costs and needs for specific devices. Increased security frequently necessitates large expenditures. Thus, organisations must assess their financial situation while choosing a suitable solution. As per Kinetic IT (2024) and Stytch (2022), hardware authentication, shown by Yubikeys, is the most cost-effective yet highly secure approach. OTPs and TOTPs, on the other hand, provide efficient security at less expense.

Selecting an authentication method that is accessible to all user groups is one of the challenges in cybersecurity. Since each authentication method requires different devices for verification, some phones or computers cannot download a new version of the authentication application. Moreover, not all devices can use biometric authentication. It is the responsibility of security experts to provide multiple authentication options to ensure accessibility for all user groups (Kumar, 2023).

Organisations must also choose MFA solutions that comply with their own policies and regulatory requirements. Comprehending these prerequisites is essential (PCI Security Standards Council, 2017). Multi-factor authentication is crucial for safeguarding digital information and must be a primary focus in cybersecurity. Organisations should require IT specialists and appropriate devices for the efficient adoption of multi-factor authentication (Desk, 2023).

The survey conducted by Das et al. (2020) reveals that numerous persons are unaware of the significance of multi-factor authentication (MFA). This results in cybersecurity concerns. Consequently, companies and enterprises should inform their staff and customers with the significance of multi-factor authentication or authentication procedures. This is evident from the Australian government, which disseminates information regarding MFA on its websites (Australian Signals Directorate, 2023).

Three primary regulatory frameworks impact multi-factor authentication (MFA) policies: GDPR, CCPA, and ADPR. Although these frameworks share similar elements regarding

data protection and security, they all advocate for implementing additional protective measures, such as MFA, for personal data. (Information Commissioner, 2024). The ADPR (Australian Data Privacy Regulation) doesn't require MFA, but it does recognise its importance as a best practice for making data security better. Using MFA is in line with ADPR's focus on protecting personal information and following the rules for reporting data breaches (Donnelley Financial Solutions, 2020).

Pilot Survey Results

Administering a survey, mentioned earlier, was one of the principal methodologies for our research. We assembled 41 volunteers from diverse age demographics. The questionnaire comprised 17 questions, including a section for general comments and ideas. The primary objective was to understand the viewpoints of stakeholders utilising digital services for MFA. We had done a pilot study to validate the quality of the survey prepared. There were 30 responses we have received. To trust in reliable data, we have changed the settings to single response by an individual and modified some of the questions to get more clarity to avoid the bias of data. Below are the analysis and interpretation of the 41 responses: 39% of the respondents were between 25 and 34 years old, while 36.6% were aged 18 to 24. A smaller portion of the respondents were 35 and older, making up 7.3%, 9.8%, and 7.3%, respectively. This highlights that the audience is mostly younger, with the majority being under 34.

Almost half (48.8%) of respondents is employed, while the rest were students, self-employed, or unemployed. This indicates a diverse mix of participants, but with a notable lean toward those actively employed. Most people (75.6%) in the survey knew about Multi-Factor Authentication (MFA). However, 12.2% said they did not know about it, and another 12.2% were unsure. While most were aware of MFA, a small group might need more information or clarification.

Most respondents (73.2%) enable MFA for email accounts, followed by social media and financial services at 53.7%. Work-related systems also see significant MFA usage at 43.9%, with less adoption for platforms like university portals and gaming. When asked about frequency, 41.5% use MFA every time they log in, while 43.9% use it sometimes depending on the account. Only a small percentage rarely or never use it.

Most respondents (68.3%) use an authenticator app like for their MFA codes, while 22% do not use such apps, and 9.8% are unsure. The majority of people in the survey(59.4%) use Google Authenticator for their MFA codes, while 28.1% prefer Microsoft Authenticator. A smaller group, 9.4%, use Okta Verify, and some none. Most people (43.9%) seemed to strongly believe that combining MFA with other authentication methods enhances their account security, with a rating of 5. Another 22% rated it a 4, while 26.8% gave it a 3. Only a small percentage, 4.9%, rated it a 1, showing that very few doubt the added security of using multiple methods.

Most people (56.1%) had never had their account compromised using a strong password. However, 31.7% have experienced an account breach, and 12.2% were not sure if they have been compromised or not. Most people (65.9%) are concerned about security risks like phone number theft, phishing, or bypassing two-factor authentication. Another 24.4% are concerned, 4.9% feel neutral, and only 4.9% aren't worried about these risks. Most people (46.3%) use face recognition to unlock their smartphones, while 24.4% prefer fingerprints. About 19.5% use face recognition and fingerprint, 7.3% do not use any of these methods, and 2.4% use a pattern. There were also issues with loss of smartphone, when they would use their authentication apps.

Regarding updating or reviewing MFA settings, 31.7% of people do so occasionally, about once or twice a year. Another 22% only update them when required by their organisation, while 17.1% rarely update them, and 14.6% either do it regularly every few months or never update them. Almost half (48.8%) of the respondents have trouble receiving SMS or codes for MFA. However, 34.1% haven't experienced any issues, while 12.2% found the process slow or had trouble with biometric authentication.

Suggestions and Recommendations

The most recommended MFA method for enhancing account security is SMS codes, with 34.1% of people suggesting it. Biometrics is also popular and recommended by 22%, while email codes, TOTP (like Google or Microsoft authenticators), and push notifications are each recommended by 12.2%. Passkeys were suggested by 2.4%, and no one recommended hardware tokens. Strong authentication systems become ever more important in more digitised surroundings. The vulnerabilities of conventional password-only systems are becoming increasingly apparent as cyber threats continue to evolve. Multi-factor authentication (MFA) is an essential precaution that enhances the security of private data. Nevertheless, the implications, challenges, and advantages of MFA are not universally understood by all audiences. This is a description intended for technical experts, the general public, and interested parties.

The shift to multi-factor authentication rectifies the deficiencies of conventional password systems. However, research indicates that numerous individuals continue to employ weak passwords, rendering them susceptible to attacks. Organisations must manage the intricacies of MFA by concentrating on criteria such as user experience, regulatory compliance, and integration with existing systems.

Significant technological hurdles exist when integrating MFA across platforms in industries such as banking. Furthermore, user approval is critical, as many people disable MFA owing to perceived annoyance. Research and proficient training are crucial for maximising MFA adoption and enhancing overall security, especially for those who are not very proficient in computers or smart devices. As cyber threats rise, relying solely on passwords to protect online accounts is inadequate. Multi-factor authentication (MFA)

provides an extra layer of security, making it harder for cybercriminals to access personal information. Many people use weak passwords, like "123456," which can be easily guessed. MFA functions like a second lock on your door, offering more protection. It is simple to use—tools like SMS codes or authenticator apps help keep your information safe. By adopting MFA, you take an important step towards securing your online presence and protecting your data. Though there is an available measure in the smartphones, still people need more training and support to use it efficiently.

Concluding Comments

Our study focused on MFA best practices, emphasising their relevance in balancing security, affordability, and user experience. As technology evolves, effective MFA measures are required to safeguard sensitive information from cyber-attacks. Our findings argue for scalable, user-friendly multi-factor authentication methods to improve security while solving uptake difficulties.

i) Security Enhancement:

a. MFA improves security by minimising unauthorised access.

b. Various MFA methods, including biometrics, tokens, and SMS-based authentication, provide differing levels of strength, emphasising the equilibrium between usability and security.

ii) Challenges in MFA:

a. Organisations encounter obstacles such as elevated implementation expenses, regulatory adherence, and technological difficulties, including the integration of multi-factor authentication with legacy systems.

iii) Survey Insights:

a. Adoption trends reveal a growing awareness of MFA; nonetheless, its implementation is inconsistent due to usability challenges.

b. Users frequently express complaints over obstacles such as technical difficulties and perceived irritations.

iv) MFA Methods Comparison

a. Different authentication methods have various strengths and weaknesses. Biometric authentication is gaining popularity, but it requires modern technology to improve accessibility and diversity.

Appendix A: Survey Questionnaire

- Q 1 Which age group are you included?
- Q 2 What is your occupation?
- Q 3 Are you familiar with multi-factor authentication (MFA)?

- Q 4 For which types of accounts do you typically enable multi-factor authentication (MFA)?
- Q 5 How often do you use MFA when logging into your accounts?
- Q 6 Are you using any authenticator app for accessing multi-factor authentication (MFA) code? (E.g., Google or Microsoft Authenticator, Authy, etc)
- Q 7 Which types of multi-factor authentication (MFA)have you used before?
- Q 8 How strongly do you believe that using a password in combination with other authentication methods enhances the security of your data or account?
- Q 9 Have you ever had an account compromised despite using a strong password?
- Q 10 How concerned are you about security risks, such as theft of your phone number, phishing attempts to obtain your login credentials, or bypassing of your two-factor authentication?
- Q 11 Which biometric methods do you use to unlock your smartphone?
- Q 12 If you lose your smartphone, how would it affect your ability to use multi-factor authentication (MFA)?
- Q 13 How often do you update or review your multi-factor authentication (MFA) settings?
- Q 14 Have you ever experienced difficulties using multi-factor authentication (MFA)?
- Q 15 Would you recommend any specific MFA methods for enhancing account security?
- Q 16 Do you have any comments or suggestions?

Appendix B: Survey Responses Summary

- A majority of users either always or frequently use MFA, indicating a strong awareness of security practices.
- A smaller percentage rarely or never use MFA, highlighting a potential security gap among some users.
- SMS and email-based authentication are the most commonly used methods, despite known security risks like SIM swapping.
- More secure options like TOTP and biometric authentication are gaining adoption but still have room for wider usage.
- A significant number of respondents expressed high concern, reflecting awareness of modern cybersecurity threats.
- Some users showed moderate or low concern, which might indicate a lack of exposure to security risks or confidence in existing protective measures.

References

Australian Signals Directorate. (2023). Implementing Multi-Factor Authentication. Australian Signals Directorate, Australian Government, Canberra. https://www.cyber.gov.au/resources-business-and-government/maintaining-

devices-and-systems/system-hardening-and-administration/system-hardening/implementing-multi-factor-authentication

Das, S., Wang, B., Kim, A., & Camp, L. J. (2020, January 7). MFA is A Necessary Chore!: Exploring User Mental Models of Multi-Factor Authentication Technologies. Scholar Space, University of Hawai'i at Manoa. https://doi.org/10.24251/HICSS.2020.669

Desk, O. (2023, December 7). Multi-Factor Authentication: What are its benefits and challenges? OLOID. https://www.oloid.com/blog/multi-factor-authentication-what-are-its-benefits-and- challenges/

Donnelley Financial Solutions. (2020, March 21). Data Protection in Transition: GDPR, CCPA and Comparable Data Protection Laws. https://www.dfinsolutions.com/knowledge-hub/thought-leadership/article/data-protection-transition-gdpr-ccpa-and-comparable-data

European Union. (2016). EUR-Lex - 32016R0679 - EN - EUR-Lex. Europa.eu. Publications Office of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

Kinetic IT. (2024, September 4). What Is The Most Secure Multi-Factor Authentication Method? https://kineticit.com.au/article/multi-factor-authentication-2/

Kumar, S. (2023, April 15). Accessibility Challenges with Digital Security Solutions. DigitalA11Y. https://www.digitala11y.com/accessibility-challenges-with-digital-security-solutions/

Losinskyi, K., & Sirosh, D. (2024, April 18). MFA: Definition, Types, and Adoption Best Practices. Infopulse. http://web.archive.org/web/20240913141241/https://www.infopulse.com/blog/how-to-choose-mfa

OAIC. (2024, February 22). Notifiable Data Breaches Report: July to December 2023. The Office of the Australian Information Commissioner. Commonwealth of Australia. https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-report-july-to-december-2023

Office of the Australian Information Commissioner. (2024). The Privacy Act. The Office of the Australian Information Commissioner. Australian Government. https://www.oaic.gov.au/privacy/privacy-legislation/the-privacy-act

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-Factor Authentication: A Survey. Cryptography, 2(1), 1. https://doi.org/10.3390/cryptography2010001

Owens, J., & Matthews, J. (2008, March). A study of passwords and methods used in brute-force SSH attacks. In USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET). https://lin-web.clarkson.edu/~jmatthew/publications/leet08.pdf

PCI Security Standards Council. (2017). Information Supplement: Multi-Factor Authentication. PSI, Security Standards Council, Wakefield, MA, USA.

https://listings.pcisecuritystandards.org/pdfs/Multi-Factor-Authentication-Guidance-v1.pdf

Reese, K., Smith, T., Dutson, J., Armknecht, J., Cameron, J., & Seamons, K. (2019). A Usability Study of Five Two-Factor Authentication Methods. In *Proceedings of the Fifteenth Symposium on Usable Privacy and Security*. Symposium on Usability Privacy and Security, Santa Clara, CA, USA. USENIX Association. https://www.usenix.org/system/files/soups2019-reese.pdf

Reese, K., Smith, T., Dutson, J., Armknecht, J., Cameron, J., & Seamons, K. (2019). A Usability Study of Five Two-Factor Authentication Methods. In *Proceedings of the Fifteenth Symposium on Usable Privacy and Security*. Symposium on Usability Privacy and Security, Santa Clara, CA, USA. USENIX Association. https://www.usenix.org/system/files/soups2019-reese.pdf

Reno, J. (2013). Multi-factor Authentication: Its Time Has Come. *Technology Innovation Management Review*, 3(8). http://doi.org/10.22215/timreview/716

Solomon, S. (2024, February 7). 8 Multi Factor Authentication Types and How to Choose. Frontegg. Inc., Santa Clara County, California, USA. https://frontegg.com/blog/multi-factor-authentication-types.

Stytch. (2022). Multi-factor authentication: how to choose the right approach for your business. Stytch.com. https://stytch.com/blog/which-mfa-is-right-for-your-business/

Suleski, T., Ahmed, M., Yang, W., & Wang, E. (2023). A Review of multi-factor Authentication in the Internet of Healthcare Things. *Digital Health*, 9(1), https://doi.org/10.1177/20552076231177144

Tsakalakis, N., Stalla-Bourdillon, S., & O'Hara, K. (2016). What's in a name: The conflicting views of pseudonymisation under eIDAS and the General Data Protection Regulation. In D. Hűhnlein, H. Rossnagel, C.H. Schunk & M. Talamo (Eds). *Open Identity Summit 2016*: October 13-14, Rome, Italy (Vol. P-264, pp.167-174). (*Lecture Notes in Informatics (LNI)-Proceedings.* Vol. P-264). *Gesellschaft fűr Informatik.* https://subs.emis.de/LNI/Proceedings/Proceedings264/P-264.pdf

Waugh, A. (2021). The most secure multi-factor authentication methods. 14 March. Push Security. https://pushsecurity.com/blog/which-mfa-methods-should-you-use/

Weir, C. S., Douglas, G., Carruthers, M., & Jack, M. (2009). User perceptions of security, convenience and usability for ebanking authentication tokens. *Computers & Security*, 28(1): 47-62. https://doi.org/10.1016/j.cose.2008.09.008

Letter to the Editor

While I commend the efforts reported in the current discussion paper, the cohort selected can use the internet and other devices to respond to the multi-factor requirements but what about those who have no access to a mobile telephone (or can only use them for telephone connections). Even those who are fairly literate in using the internet sometimes find access impossible. No one over 50 has been included in the study. Why? I believe that if people over 50-80 were included, the results would dramatically change. Think of us older people, after all, we represent 20% of the population and 30% of the wealth.

Dr Ronald Lee Gaudreau *FCES*

Dear Dr Gaudreau

Thank you for your comments:

I do not disagree, as I am 87, but the students are also grappling with the month-by-month advances in Information Technology. I have just returned from a couple of weeks in hospital, following a stroke. If I did not have the HeartBug app on my "smartphone", I would still be there.

The other big issue is cybersecurity, in that those who rob our bank accounts are counting on our ignorance. Banks can be, and are, robbed online these days.

With best wishes

Tony

Doctor of Philosophy Abstract

Learning Writing Collectively via WeChat:

An Investigation of Peer Learning in the Chinese EFL Context

Candidate: Dr Shae Mao
Institution: The University of Sydney
Supervisors: Associate Professor Hui-Zhong Shen and Dr Hongzhi Yang

Abstract: This study explored Chinese (English as a Foreign Language) EFL students' peer collective learning of English writing via WeChat at the tertiary level in mainland China. Based on Vygotsky's sociocultural theory, it focuses on four main ideas: peer feedback, how learners interact, peer support, and the Zone of Proximal Development. The research examined how mobile-assisted language learning (MALL) through WeChat supported collaborative writing, shaped interactional patterns, and facilitated peer feedback. Data were collected through questionnaires, WeChat chat histories, student texts (assignments, feedback, and journals), and semi-structured interviews. The study identified several major findings: Peer scaffolding was most prominent during pre-writing discussions, helping students reach their Zone of proximal development (ZPD). WeChat enhanced EFL learning, peer interaction, and feedback practices overall. The current research brought new insights by offering an extended conceptual framework for investigating peer learning in a WeChat-assisted language learning context. It also contributed to the literature on ESL/EFL learners' peer learning with the aid of technology. In addition, the study clarified and enhanced the analysis of interactional measurement, which could be applied methodologically in both traditional classroom settings and online environments. Lastly, it provided pedagogical implications for mobile-assisted peer language learning, particularly in relation to WeChat-based training sessions and task design.

The Full dissertation is available from Open Access at the University of Sydney library https://ses.library.usyd.edu.au/handle/2123/33951

Purpose of the Journal

Journal: The journal aims to disseminate original ideas related to Commercial Education and cognate fields, including the educational aspects of commerce. It is also interested in publishing abstracts of recently approved research degree dissertations, reports and theses.

Publishing Ethics Policy: The present Publishing Ethics Policy concerns the standards of expected ethical behaviour for all parties involved in the act of publishing in the Journal of Commercial Education. The document aims to provide a clear description and management of situations that may arise if these ethical standards have not been adhered to by the parties while promoting a shared understanding of the responsible publication practices in maintaining the integrity of the scholarly record.

Declaration of Originality and Authorship: Submitted manuscripts must be the original work of the authors**.** Along with the initial manuscript submission, the corresponding author must sign and submit a Declaration of Originality and Authorship that states:

- All authors who have made significant contributions to the work are included in the author list. The author order has been agreed upon by all authors. All authors are aware of the paper submission.
- The work submitted is original and the work of the authors. The work does not include copyright infringements or plagiarism.
- The work in the full text has not been previously published nor is under consideration elsewhere, in either English or other languages.
- State any potential acknowledgements and/or conflicts of interest (such must also be in an acknowledgements section of the manuscript).
- The declaration must be signed (digital signatures accepted) by the corresponding author.

Notes: Partial reuse of other works is only possible a) in amount, justified for the purpose, b) in the context of critical commentary and discussion of the work in question, and c) provided the respective sources are duly quoted and cited.

Use of Generative Artificial Intelligence to produce content or for editing should be carefully considered given the requirement for original work by the authors and in light of the limitations of these tools (see Cossio, 2025 and Hicks, 2024). The editors would prefer authors avoid using Generative Artificial Intelligence to produce content. Authors are responsible for what their submission contains.

Any changes to the author list after submission, such as a change in the order of the authors, or the deletion or addition of authors, must be approved by all authors from the original author list.

Post-publication issues: If in the process of publication, technical errors have been introduced into the article by the hand of a journal staff member, then it is the responsibility of the Journal to correct the errors in a timely manner (in the electronic version of the Journal) or publish respective errata (in both the electronic and printed versions).

- If the Journal's authors discover (technical) errors in their accepted and/or published papers, and request changes from the Editorial Office, then, depending on the timing and impact of the changes, the authors will be given the choice to
    - correct their manuscript prior to publication, or
    - publish a relevant corrigendum.
- For published papers, depending on the respective reviewers' opinions, the authors may be further invited to submit a new follow-up manuscript with substantially new, original results, which informs the readership of the discovered errors and comments on the pertinent corrections.
- In the electronic version of the Journal, these original publications will be linked to the respective errata, corrigenda, or eventual follow-up publications.

If copyright infringements or work not original to the authors become evident post-publication, the Journal may retract (remove) the publication or demand its correction and acknowledgement (in its electronic version), depending on

- the degree of the infringement,
- the context within the published article, and
- its impact on the overall integrity of the publication.

Instructions to Authors

Manuscripts submitted to the Journal of Commercial Education are subject to peer review by three independent referees. The final decision is taken by the Editors-in-Chief in consultation with members of the Editorial Board.

Submitted manuscripts must be the original work of the authors. Papers will only be considered if the content is substantially new and original material that has not been published elsewhere, and has not been submitted concurrently elsewhere, nor is likely to be published substantially in the same form elsewhere.

Copyright: Authors, whose papers are published, retain their copyright under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 licence https://creativecommons.org/licenses/by-nc-nd/4.0/. Authors will grant JCE the right of first publication under this licence. Published papers will be in PDF. Journal readers are allowed to read, download, print, search, or link to the full texts of the papers, share and can use them for any lawful non-profit purpose. Redistribution of remixes/derivatives is prohibited. Commercial use and redistribution of the papers will only be available upon authors' and publisher's written permission.

Peer Review Process

Peer review is fundamental in ensuring the integrity of the scientific publication process and can flag potential misconduct at an early stage.

Each paper submission is sent out for peer review to at least three independent reviewers, whose identities are not released, in a process named single-blind peer review. Papers may, however, be returned to authors without review if the Editors consider that they fall out of the scope of the Journal or fail to meet the basic criteria of scientific presentation, significance, or originality.

Reviewers shall conduct their evaluation in a timely and objective manner, avoiding any personal or unsupported criticisms. Reviewers agree not to disclose any information regarding the manuscript to any other party or to use any part of the content on their own behalf. To guarantee a completely rigorous and unbiased review process, reviewers should not have any conflicts of interest with respect to the research, the authors and/or the research funders.

In case of unavailable reviewers from the Journal's own pool of reviewers, the authors may be offered to propose suitable independent reviewers, who are not directly affiliated with their research unit and are not in any other form of conflict of interest with them. However, the Editorial Office reserves the right to ignore such proposals, if deemed inappropriate, and proceed with its own pool of reviewers.

The final decision concerning the manuscript is taken by the Editorial Office based on the reviewer reports and recommendations. The possible decisions of the Editorial Office are: Accept, Minor revision, Major revision or Reject.

At least two strongly positive reviews are required for a submission to be accepted for publication. The usual review process could take up to four months, but this period may be longer depending on the specifics of the research presented and suitable reviewers' availability in this period.

Editors and reviewers are required to keep confidential all details of the editorial and peer review process on submitted manuscripts. Reviewers will be removed from the Journal's pool of reviewers if it is established that they conducted unethical practices against the authors and manuscripts to which they have been assigned, and have agreed, to review.

Template for submission

Suggested maximum 15 pages in length all-inclusive. Referencing: APA7. Author date, in-text citations. Manuscripts to be in MS Word (.doc or .docx) format. Use A4 page size and 2.54 cm margins on all sides.

You must use the submission template to submit your paper that includes preformatted styles and additional instructions. Obtain the template from https://commercialeducation.com.au/journal-authors. We use open source fonts in the template. The template and the journal authors link has details of where to obtain relevant open source font files. Articles will be published in PDF after acceptance where we will add dates of receipt, acceptance and publication.

Acknowledge any financial support or conflicts in an Acknowledgements section prior to the reference list.

Submission to: journal@commercialeducation.com.au with attachments a) manuscript file in docx (using our template) and b) Declaration of Originality and Authorship signed by the corresponding author.

Processing fee: A non-refundable processing fee of AUD30 is payable on submission to:
Commercial Education Society of Australia: BSB: 062-005; Account: 0000-1925
Payment of the processing fee does not in any way guarantee publication.

Back cover

The Commercial Education Society of Australia

Founded 1910

The mission of the Commercial Education Society of Australia is to provide students of commercial education with the opportunity to raise their standards of education so that they can take advantage of the opportunities for further education through the grades of membership. This is reflected in the Society's motto on its coat-of-arms 'Digne Ambulate' — 'walk worthily' which was granted by the College of Heralds in the United Kingdom.

The Commercial Education Society of Australia was founded in 1910 and incorporated in 1911 as a non-profit company limited by guarantee. In its more than a century of existence it has never been in receipt of any government grants, subsidies, or funding. The Society has a tradition of providing low-cost educational opportunities without discrimination of any kind. Membership is made up of men and women of all nationalities and backgrounds who support its objectives.

Patron of The Society

Emeritus Professor David Barker *AM KCSJ, LLB (London) LLM (Hons) (Cambridge) MPhil DipLocalGovt (Kent) GradDipLegalPrac (Univ Technology Sydney) PhD (Macquarie) FCIS FCIM FAICD FACE FAAL FCES*

Previous Patrons Have Included The Following Governors-General of Australia:

Her Excellency Dame Quentin Bryce *AD CVO DStJ*
Major General The Hon Philip Michael Jeffrey *MC, AC AO (Mil) CVO KStJ*
The Right Rev and Hon Peter Hollingworth *AC OBE*
His Excellency Sir William Deane *AC KBE KVO KC*SG*
His Excellency The Hon William George Hayden *AC BEc LLD (hc) TZO (Latvia)*
His Excellency The Right Hon Sir Ninian Stephen *KG AK GCMG GCVO KBE KStJ*
His Excellency The Right Hon Sir Zelman Cowan *AK GCMG KStJ PC QC*
The Hon Sir John Kerr *AK GCMG KStJ PC QC*
Sir Paul Meerna Caedwalla Hasluck *KG GCMG GCVO PC*
Baron Casey, Richard Gavin Gardiner Casey *MC, DSO, KG GCMG CH PC KStJ*
Viscount De L'Isle, William Philip Sydney De'Lisle *VC, KG GCMG GCVO KStJ PC*

Information can be found in the *CESA Register 1910–2025* of Fellows, Licentiates, Members, Associates.