The Invisible COVID-19 Small Business Risks: Dealing with the Cyber-Security Aftermath

TRACY TAM, ASHA RAO, and JOANNE HALL, RMIT University, Australia

COVID-19 forced small businesses globally to move their presence online to survive. Cyber-criminals have swiftly taken advantage of the chaos wrought by this move. Due to factors ranging from small businesses' inexperience with technology to a global cyber-security skill shortage, policy-based solutions by governments are needed to help ensure that this vital sector in global economies does not fall victim to cyber-criminals. We propose and discuss three measures that governments can take to build up small business cyber-security resilience.

CCS Concepts: • **Security and privacy** → *Privacy protections*; **Economics of security and privacy**; **Social aspects of security and privacy**;

Additional Key Words and Phrases: COVID-19, small business, cyber-security, business risks, governance, policy assistance

ACM Reference format:

Tracy Tam, Asha Rao, and Joanne Hall. 2020. The Invisible COVID-19 Small Business Risks: Dealing with the Cyber-Security Aftermath. *Digit. Gov.: Res. Pract.* 2, 2, Article 23 (December 2020), 8 pages.
<https://doi.org/10.1145/3436807>

1 INTRODUCTION

COVID-19 forced small businesses to adopt digital sales channels. With business and customer data increasingly accumulating, there is a rising concern about the security of these IT solutions. Cyber-criminals, however, have accelerated their attacks, taking advantage of the chaotic time [10, 41]. An urgent effort is needed to support small businesses to manage the cyber-security risks that come with the online move. In this article, we outline the risks facing small business currently and then discuss possible measures that would help protect small business in an online environment.

Small and medium businesses contribute significantly to employment and GDP globally and are a major source of job growth [38]. In the UK, Australia, the US, and China, small businesses form a vital part of the economy and a significant amount of employment [13, 20, 23, 30, 48].

Small businesses traditionally rely on cash reserves to survive unexpected events like COVID-19. However, unlike large enterprises, small businesses tend to have smaller cash reserves. For example, the majority of small businesses in the US purportedly have less than 6 weeks of cash reserve [27]. In Australia, in April 2020, banks provided emergency bridging loans to small businesses to pay their employees' until government support arrived

This research has been supported through the provisions of an Australian Government Research Training Program Scholarship.

Authors' addresses: T. Tam, A. Rao, and J. Hall, RMIT University, 124 La Trobe St, Melbourne, Victoria, 3000; emails: tracy.tam@student.rmit.edu.au, asha.rao@rmit.edu.au, joanne.hall@rmit.edu.au.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

© 2020 Association for Computing Machinery.

2639-0175/2020/12-ART23 \$15.00

<https://doi.org/10.1145/3436807>

Table 1. Impact on Small Business of COVID-19 Key Events

Time	Key Event	Impact on Small Business
February/March 2020	Advice/mandate for people to stay at home took away local “walk-in” traffic [14, 36].	Loss of geographical (local) advantage. Reduction in the proportion of low cost (cash) sales.
February/March 2020	“Non-essential” businesses were ordered shut [21, 23].	Loss of business model.
March-May 2020	Capped patron capacities [44].	Reduction in the potential customer numbers (revenue).
May/June 2020	Extra cleaning tasks are now strongly recommended/mandatory in workplaces [52].	Increased operational costs.

This only takes into account first wave of infections.

5 weeks later [24], indicating similar cash reserves. Hence the viability of small businesses is at financial risk under COVID-19.

To deal with the COVID-19 situation, most actively trading small businesses around the world moved online [22, 29], as evident from increased demand for online platforms and services. Australia Post had a 30% increase in online shopping in April 2020 [4] while Ubereats had a 10% sales boost and an increase in restaurant partners [16].

Protection is paramount for small businesses, with agile cyber-criminals [10, 41] taking advantage of COVID-19 opportunities while the cyber-crime judicial systems globally evolve [19]. As global economies recover from the financial impacts of COVID-19, survivors will need support given their contribution to the economy and employment. Clearly, it is vital that small businesses are supported to defend themselves during this pandemic.

2 THE RISKS FOR SMALL BUSINESSES

Official data on COVID-19 impacts on small businesses are currently unknown and may not be known for many years (e.g., Australian Bureau of Statistics’s business characteristics data covering COVID-19 events is due for release in 2021 [6]). To understand the risks for small business, we first examine the timeline of key COVID-19 events and their impacts on small business, as described in Table 1.

From the first wave of COVID-19, small businesses were suddenly confronted with abruptly changed business models and reduced revenue, amidst a backdrop of rapidly rising costs. These events worked together to present risks that small businesses never previously confronted.

2.1 Businesses (and Staff) under Stress

Extreme stress (as precipitated by COVID-19) is associated with a deterioration in job performance [37]. As small businesses, especially at the sole trader and micro size, are primarily influenced by human business owners [25, 50], a cyber-attack on a small business places additional stress on the human owner and staff. This is in addition to the stress of handling the ever-changing situation of COVID-19.

A situation that combines stress and inexperience with technology is not conducive for cyber-security best practice—where humans play a vital role [15, 49, 51]. Many small businesses already struggle with the fundamental functions of IT [40]. In addition, less than half of the Australian small businesses surveyed received orders via the Internet in 2018 [5], showing a lack of experience in this area. Nearly 50% of surveyed small business admitted that they “need help and know it [about cyber-security]” [7]. A sense of urgency and pressure

play central roles in social engineering attacks and maintenance errors, e.g., unpatched software. Without assistance, this high-stress situation leaves small businesses vulnerable to a range of cyber-security risks.

2.2 Becoming a (New) Target

The increased risk to small businesses from COVID-19 is enabled by the large number of new targets available to cyber-criminals, rather than novel technical attacks. While attack techniques are not new for cyber-criminals, the risk and consequences to be managed are new to the newly digital business. These include:

- **Debilitating Software** (e.g., malware, ransomware): With sales channels moving online, computers have become integral to business functions. The disabling of key business device(s) can cut staff off from critical business functions and data. When combined with a COVID-19 global supply issue of electronic devices [17], small businesses hit with ransomware or malware face a hard and expensive path to recovery.
- **Impersonation** (e.g., social engineering, business email compromise): COVID-19 necessitates a socially distanced society, leading to a lack of social interaction that plays into social engineering techniques.
- **Data breaches** (e.g., blackmail, data exfiltration): Online trading requires the connection of business computers with the internet. These computers, by necessity, contain business-sensitive data. Connectivity and increased use expose this data to theft by a third party, targeted or accidental. With privacy legislation around the world such as GDPR [18], such an incident can lead to serious legal and financial consequences for the business.

These risks represent new aspects of business risks that must be actively managed by small businesses already overwhelmed with new information. Previously, mitigation strategies would have been developed as part of business processes over time. Unfortunately, small businesses were not afforded that luxury during COVID-19.

2.3 Supply Chain

By adopting IT solutions quickly, small businesses increased their reliance on IT suppliers, who were also under increased pressure. COVID-19 has shown that even mature, large-scale IT products contain vulnerabilities, requiring pro-active maintenance and patching. Sudden mass adoption of IT products [39] acts as a catalyst in exposing these vulnerabilities. Without professional support, small businesses run an ongoing risk of these vulnerabilities being exploited.

Ironically, while platform economy services, e.g., UberEats, Etsy, Airbnb, and so on, have enabled business' digital adoption, they have also contributed to supply chain risks for their small business customers from a cyber-security perspective. With increased reliance from their customers, these platforms have effectively become part of the supply chain for small businesses. Unavailability or a breach of these highly visible targets have deep ramifications for the operations and data of the small businesses that utilise them.

2.4 Customer Privacy

The information held by small business grows with each customer interaction via the new digital channels, providing another target to cyber-criminals [9]. Early indications show that some businesses lack awareness of data privacy and controls [54]. As our personal, professional, financial, and digital assets are increasingly tied to our identity, a leak of identity information can have long-lasting implications for victims [2].

Loss of customer information impacts both customer privacy and business reputation. As COVID-19 permanently changes consumer habits [4, 33–35, 53], the reputation of a small business takes on new significance. With assumptions playing a vital role in online interactions [11], a small business involved in a data breach can lose customers very easily to another online offering. As an executive of Unilever pointed out, “They [customers] simply can’t afford to spend money on products they’re not sure of” [53]. The need for customer trust extends to trust in the business itself, and this goodwill has become more important than ever.

These are just selected risks that are new to small businesses forced into a new way of operating due to COVID-19. These risks previously had limited impact operationally due to lack of reliance on IT systems by many small businesses. During COVID-19, these risks need to be managed carefully due to the lack of alternative sales and communication channels. Post COVID-19, these risks, if left unchecked, take on new significance with implications for the viability of the business.

3 INCREMENTAL MEASURES IN A CHANGING WORLD

Implementing multiple incremental changes is a realistic approach in a world that is rapidly changing. The low rate of successful prosecution of computer crimes globally [47] suggests that prevention is the better strategy. As such, our discussion below focuses on incremental prevention initiatives.

3.1 Cyber-security Public Messages

Small businesses operating a digital presence due to COVID-19 are likely to have difficulties with getting professional help. Over half of small businesses in Australia do not have dedicated, qualified IT in-house [5]. This lack of professionals extends to the cyber-security field. In 2019, the cyber-security skills shortage was a recognised issue within the cyber-security industry worldwide [1, 3]. The lack of skilled cyber workers was forecast, pre-COVID-19, to fall short of existing demand. COVID-19 has likely exacerbated the problem.

In the short term, this lack of professional help can be countered, to a degree, by governments up-skilling the general public on cyber-security awareness. Cybersecurity depends heavily on human components, and public messaging will keep the awareness foremost in people's mind. By reminding the public of basic cyber-security measures (e.g., Stop. Think. Connect. [45]), these types of awareness campaigns serve to put the tools to stop attacks in the hands of business owners and staff. When staff are confronted with signs of an attempted attack, e.g., a strange email address, awareness will prompt them to check the authenticity of the request, potentially thwarting the attempt. This vigilance serves to protect the business before it causes damage.

Public messaging has the dual benefits of protecting personal and small business data by equipping owners, staff, and the general public. An example is the Australian Cyber Security Centre's [8] reminder to small businesses of basic cyber-security measures during COVID-19.

3.2 Cyber-security Products for Small Businesses

There is urgent need for investment in cyber-security products catering to small business' unique characteristics. Cyber-security services and information suitable for micro and small business is currently limited. The majority of cyber-security products and standards require a technically literate person to implement, an uncommon resource in small businesses. Given their disparate nature, an effective method of delivering cyber-security to small businesses needs further examination.

A lesson on delivering cyber-security products in a way that is receptive to small businesses can be drawn from online financial services used by over 80% of surveyed small businesses [5]. This is part of an emerging trend of "Platform Capitalism" [43], where large platforms provide services at a fraction of the cost of complete solutions. The platform economy has enabled financial software, such as MYOB, to be accessible to small businesses by lowering the financial and technical threshold for entry. In turn, platforms maintain their profitability by offering their service to many smaller users.

However, platform based solutions in cyber-security have disadvantages. As past platform failures [12, 42] have shown, integrating these solutions into businesses could result in them becoming de facto gatekeepers of key business tasks. A supply chain failure in a deeply integrated platform function like cyber-security would have long-reaching consequences and thus platform solutions need to be implemented with caution, oversight and/or assistance from policymakers.

Society bears the real cost of not offering affordable and usable small business cyber-security solutions. A data breach from a single tax agent [31] is the alleged source of information used to steal AU\$120,000 of COVID-19 early superannuation withdrawals [28] via Australian government systems. The Australian Tax Office (ATO) subsequently suspended the scheme for a short time pending investigations [32]. The investigation and urgent remediation work that ATO undertook delayed legitimate access.

Other industries can provide valuable lessons on how to make cyber-security products accessible to small businesses. Given the cost of inaction to the community, it is an investment that has returns beyond financial rewards.

3.3 Out of Date Identity in a Modern Age

From a long-term perspective, an urgent rethink is required around identity, both the information and the processes involved. Identity theft is in the top three categories of cyber-crime victimisation worldwide [47]. From a small business owner's perspective, this risk is not trivial as running a small business necessitates the exposure of the business owner's personal information, e.g., registration, financial records, and so on. In addition, customer identity can also be affected by cyber-breaches due to the overlap between personal identity and online transaction information.

The traditional method of identifying a natural person based on a same/similar combination of publicly available details, e.g., name, address, birth date, government identifiers, and so on, was based on a model of secrecy. The security of the identity ecosystem was (and still is) contingent on only the identity owner knowing the correct information. The confidentiality assumptions of common information to prove identity are flawed in an age of automated, large-scale information retrieval. Traditional identification information can be easily extracted from publicly available records, past breaches or social media presence.

The core issue is that, unlike a password, personal identifying information cannot be changed easily (e.g., address), if at all (e.g., date of birth), in the case of a breach. As past breaches have shown [46], once information is stolen online, it is easily replicated and reused in perpetuity.

As a solution, the US Internal Revenue Service requires an additional PIN [26] for individuals to change information associated with the COVID-19 stimulus cheques. However, this service is only available to people whose identity is already known to be stolen. There are benefits to extending this service to everyone.

Securing personal identity beyond public immutable identifiers will safeguard both small business and their customers' identity. This allows for business transparency and accountability without risking the small business owner's identity. By extension, removing the identity theft value of customer information also makes small business a less rewarding target to cyber-criminals.

4 CONCLUSION

The reality is that cyber-threats are here to stay, as COVID-19 has ushered in a new digital era for small businesses. Given the many challenges that small businesses are facing due to COVID-19, they need to be supported to lower their attractiveness and ease of access to cyber-criminals. Non-technical policies are worth examining, ranging from making identities harder to steal, increasing small business cyber-security product selection, to increasing the general cyber-security awareness levels in society.

The breach of a small business does not just impact the small business involved—it affects the whole community. The sooner action is taken, however small, the better we can manage the risks.

REFERENCES

- [1] Robert Ackerman Jr. 2019. The Cyber Skills Shortage Continues to Balloon—And Think Tanks Aren't Helping. Retrieved from <https://www.rsaconference.com/industry-topics/blog/the-cyber-skills-shortage-continues-to-balloon-and-think-tanks-arent-helping>.

- [2] Drew Armstrong. 2019. I Lost My Identity to a Fraudster, and It Took Six Years to Clean Up the Mess. Retrieved August 2019 from <https://www.bloomberg.com/news/articles/2019-08-12/i-lost-my-identity-to-a-fraudster-and-it-took-six-years-to-clean-up-the-mess>.
- [3] AustCyber. 2019. Australia's Cyber Security Sector Competitiveness Plan 2019 Update. Retrieved from <https://www.austcyber.com/resource/australias-cyber-security-sector-competitiveness-plan-2019>.
- [4] Australia Post. 2020. Inside Australian Online Shopping, 2020 eCommerce Industry Report. Retrieved from https://auspost.com.au/content/dam/auspost_corp/media/documents/2020-e-commerce-industry-report.pdf.
- [5] Australian Bureau of Statistics. 2019. 8167.0 Selected Characteristics of Australian Business. Retrieved from <https://www.abs.gov.au/AUSSTATS/abs@.nsf/allprimarymainfeatures/C575766838376FA0CA2573E1000E3F2F?opendocument>.
- [6] Australian Bureau of Statistics. 2020. 8167.0—Characteristics of Australian Business, 2018-19. Retrieved from <https://www.abs.gov.au/statistics/industry/technology-and-innovation/characteristics-australian-business/latest-release>.
- [7] Australian Cyber Security Centre and Australian Signals Directorate. 2020. Cyber Security and Australian Small Businesses. Retrieved December 2020 from <https://www.cyber.gov.au/sites/default/files/2020-11/ACSC%20Small%20Business%20Survey%20Results.pdf>.
- [8] Australian Cyber Security Centre and Australian Signals Directorate. 2020. COVID-19: Protecting Your Small Business. Retrieved from <https://www.cyber.gov.au/advice/covid-19-protecting-your-small-business>.
- [9] Australian National University. 2019. Incident Report on the Breach of the Australian National University Administrative Systems. Retrieved December 2019 from https://imagedepot.anu.edu.au/scapa/Website/SCAPA190209_Public_report_web_2.pdf.
- [10] Australian Signals Directorate and Australian Cyber Security Centre. 2020. Threat Update: COVID-19 Malicious Cyber Activity. Retrieved from <https://www.cyber.gov.au/threats/threat-update-covid-19-malicious-cyber-activity-20-apr-2020>.
- [11] Chantal Bacev-Giles and Reeshma Haji. 2017. Online first impressions: Person perception in social media profiles. *Comput. Hum. Behav.* 75 (Oct. 2017), 50–57. DOI : <https://doi.org/10.1016/j.chb.2017.04.056>
- [12] BBC News. 2019. Facebook and Instagram Outage: Business Owners Share Frustrations. Retrieved March 2019 from <https://www.bbc.com/news/world-47568757>.
- [13] British Crown. 2019. Business Population Estimates for the UK and Regions 2019. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/254552/13-92-business-population-estimates-2013-stats-release-4.pdf.
- [14] Craig Butt. 2019. Pedestrian Numbers Drop in the CBD as Pandemic Keeps People Home. Retrieved March 2020 from <https://www.theage.com.au/national/victoria/pedestrian-numbers-drop-in-the-cbd-as-pandemic-keeps-people-home-20200317-p54azk.html>.
- [15] Lijiao Cheng, Ying Li, Wenli Li, Eric Holm, and Qingguo Zhai. 2013. Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Comput. Secur. B* 39, (Nov. 2013), 447–459. DOI : <https://doi.org/10.1016/j.cose.2013.09.009>
- [16] March Chiappetta. 2020. Uber Eats Demand Soars Due To COVID-19 Crisis. Retrieved from <https://www.forbes.com/sites/marcochiappetta/2020/03/25/uber-eats-demand-soars-due-to-covid-19-crisis>.
- [17] Euirim Choi. 2020. Thousands of students could be without laptops. *Wall Street J.* (Aug. 2020). Retrieved on September 16, 2020 from <https://www.wsj.com/articles/laptop-shortage-hits-u-s-schools-as-thousands-face-online-learning-without-device-11598434201>
- [18] Council of The European Union. 2016. GDPR Legislative Act. Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>.
- [19] Cybercrime Programme Office of the Council of Europe. 2020. The Global State of Cybercrime Legislation 2013–2020. Retrieved from <https://rm.coe.int/3148-1-3-4-cyberleg-global-state-feb2020-v1-public/16809cf9a9>.
- [20] Department of Parliamentary Services. 2018. Small Business Sector Contribution to the Australian Economy. Retrieved from https://parlinfo.aph.gov.au/parlInfo/download/library/prspub/6272043/upload_binary/6272043.pdf.
- [21] Luis Ferre-Sadurni. 2020. New York orders schools, bars and restaurants to shut down. *New York Times* (Mar. 2020).
- [22] Natalie Gallagher. 2020. One of KC's best craft cocktail bars adapts with bottled drinks and kits during coronavirus quarantine. *Kansas City Mag.* 2020, Late Edition (Mar. 2020). A.1. Retrieved on March 22, 2020 from <https://www.kansascitymag.com/cocktail-hour-during-coronavirus-outbreak/>
- [23] Laura He. 2020. Small Businesses Drive China's Economy: The Coronavirus Outbreak Could Be Fatal for Many. (February 2020) Retrieved February 29, 2020 from <https://edition.cnn.com/2020/02/14/economy/coronavirus-china-economy-small-businesses/index.html>.
- [24] Georgia Hitch. 2020. Big four banks to speed up loans for businesses applying for JobKeeper amid coronavirus crisis, Josh Frydenberg says. *ABC News* (Apr. 2020). Retrieved on June 18, 2020 from <https://www.abc.net.au/news/2020-04-23/banks-agree-speed-up-loans-for-businesses-waiting-for-jobkeeper/12176632>.
- [25] Markku Ikävalko, Timo Pihkala, and Sascha Kraus. 2010. The role of owner-managers' psychological ownership in SME strategic behaviour. *J. Small Bus. Entrep.* 23, 3 (2010), 461–479. DOI : <https://doi.org/10.1080/08276331.2010.10593496>
- [26] Internal Revenue Services. 2020. Internal Revenue Service IP Pin Service. Retrieved from <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

- [27] JP Morgan. 2016. Cash Is King: Flows, Balances, and Buffer Days—Evidence from 600,000 Small Businesses. Retrieved from <https://institute.jpmorganchase.com/content/dam/jpmc/jpmorgan-chase-and-co/institute/pdf/jpmc-institute-small-business-report.pdf>.
- [28] Paul Karp. 2020. Early access to superannuation paused as police freeze \$120,000 in allegedly stolen funds. *The Guardian* (May 2020). Retrieved on June 20, 2020 from <https://www.theguardian.com/australia-news/2020/may/08/early-access-to-superannuation-paused-as-police-freeze-120000-in-allegedly-stolen-funds>.
- [29] Jessica Longbottom. 2020. Coronavirus Forces Businesses to Adapt to Survive the COVID-19 Pandemic. (March 2020) Retrieved on March 22, 2020 from <https://www.abc.net.au/news/2020-03-19/how-businesses-adapting-to-survive-covid-19-coronavirus/12068696>.
- [30] Adela Luque, Renuka Bhaskar, James Noon, Kevin Rinz, and Victoria Udalova. 2019. Nonemployer Statistics by Demographics (NES-D): Using Administrative and Census Records Data in Business Statistics. Retrieved from <https://www2.census.gov/ces/wp/2019/CES-WP-19-01.pdf>.
- [31] Pat McGrath and Alison McClymont. 2020. Check Your Super Balance. Australians Scammed out of Thousands via the Coronavirus Early Release Scheme. (June 2020) Retrieved on June 20, 2020 from <https://www.abc.net.au/news/2020-06-01/scammers-stealing-thousands-through-coronavirus-super-scheme/12301010>.
- [32] Tom McLroy. 2020. Super early access frozen amid AFP fraud investigation. *Financ. Rev.* (May 2020). Retrieved on June 20, 2020 from <https://www.afr.com/politics/federal/super-early-access-frozen-amid-afp-fraud-investigation-20200508-p54r1z>.
- [33] McKinsey & Company. 2020. Survey: Australian Consumer Sentiment During the Coronavirus Crisis. Retrieved from <https://www.mckinsey.com/business-functions/marketing-and-sales/our-insights/survey-australian-consumer-sentiment-during-the-coronavirus-crisis>.
- [34] McKinsey & Company. 2020. Survey: UK Consumer Sentiment During the Coronavirus Crisis. Retrieved from <https://www.mckinsey.com/business-functions/marketing-and-sales/our-insights/survey-uk-consumer-sentiment-during-the-coronavirus-crisis>.
- [35] McKinsey & Company. 2020. Survey: US Consumer Sentiment During the Coronavirus Crisis. Retrieved from <https://www.mckinsey.com/business-functions/marketing-and-sales/our-insights/survey-us-consumer-sentiment-during-the-coronavirus-crisis>.
- [36] Alle McMahon and James Hall. 2020. Coronavirus Australia: Uniqlo, Sephora Close as Social Distancing Hits Retail Industry. Retrieved from <https://www.news.com.au/finance/business/retail/coronavirus-australia-big-name-shops-closing-their-doors-as-social-distancing-hits-retail-industry/news-story/be67da936b12997d19c78ac6d212309a>.
- [37] Lori A. Muse, Stanley G. Harris, and Hubert S. Feud. 2003. Has the inverted-U theory of stress and job performance had a fair test? *Hum. Perform.* 16, 4 (2003), 349–364. DOI: https://doi.org/10.1207/S15327043HUP1604_2
- [38] OECD. 2019. OECD SME and Entrepreneurship Outlook 2019. OECD Publishing, Paris. <https://doi.org/10.1787/34907e9c-en>.
- [39] Kari Paul. 2020. ‘Zoom is Malware’: Why experts worry about the video conferencing platform. *The Guardian* (Apr. 2020). Retrieved on June 20, 2020 from <https://www.afr.com/politics/federal/super-early-access-frozen-amid-afp-fraud-investigation-20200508-p54r1z>.
- [40] Rachel Pupazzoni. 2020. Consumer Complaints Jump after Coronavirus Chaos Delayed Deliveries for Toilet Paper Subscription Companies. Retrieved from <https://www.abc.net.au/news/2020-07-10/toilet-paper-subscription-service-consumer-complaints-rise/12439036>.
- [41] Yolanda Redrup. 2020. Beverage maker Lion hit by cyber attack. *Financ. Rev.* (Jun. 2020). Retrieved on June 20, 2020 from <https://www.afr.com/politics/federal/super-early-access-frozen-amid-afp-fraud-investigation-20200508-p54r1z>.
- [42] Camron Slessor and Patrick Martin. 2020. MyBudget System Outage Leaves Thousands of Australian Customers in Financial Limbo. Retrieved from <https://www.abc.net.au/news/2020-05-13/mybudget-system-outage-leaves-customers-in-financial-limbo/12244926>.
- [43] Nick Srnicek. 2016. *Platform Capitalism*. Polity Press, Oxford.
- [44] State Government of Victoria. 2020. Coronavirus (COVID-19) Restrictions Victoria. Retrieved from <https://www.vic.gov.au/coronavirus-covid-19-restrictions-victoria>.
- [45] Stop. Think. Connect. 2020. Retrieved from <https://www.stopthinkconnect.org/>.
- [46] Paul Szoldra. 2016. This Is Everything Edward Snowden Revealed in One Year of Unprecedented Top-secret Leaks. Retrieved from <https://www.businessinsider.in/This-is-everything-Edward-Snowden-revealed-in-one-year-of-unprecedented-top-secret-leaks/articleshow/54367926.cms>.
- [47] United Nations Office on Drugs and Crime. 2013. Comprehensive Study on Cybercrime. Retrieved from http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.
- [48] US Census. 2015. 2015 SUSB Annual Datasets by Establishment Industry—Data by Enterprise Employment Size. Retrieved from https://www2.census.gov/programs-surveys/susb/datasets/2015/us_state_6digitnaics_2015.txt.
- [49] Rossouw Von Solms and Johan Van Niekerk. 2013. From information security to cyber security. *Comput. Secur.* 38 (Oct. 2013), 97–102. DOI: <https://doi.org/10.1016/j.cose.2013.04.004>
- [50] Calvin Wang, Elizabeth Walker, and Janice Redmond. 2007. Explaining the lack of strategic planning in SMEs: The importance of owner motivation. *Int. J. Organ. Behav.* 12, 1 (2007), 1–16.
- [51] I. M. Y. Woon, G. W. Tan, and R. T. Low. 2005. A protection motivation theory approach to home wireless security. In *Proceedings of the 26th International Conference on Information Systems (ICIS’05)*. 367–380.
- [52] Work Safe Australia. 2020. Coronavirus COVID-19 Recommended Cleaning: Supplementary Information. Retrieved from <https://www.safeworkaustralia.gov.au/sites/default/files/2020-05/cleaning-table-covid19-26May2020.pdf>.

- [53] Hanna Ziady. 2020. Our Pandemic Shopping Habits Are Here to Stay. Brands Are Racing to Adapt. Retrieved from <https://edition.cnn.com/2020/05/27/business/consumer-trends-coronavirus/index.html>.
- [54] Mark Zita and Staff. 2020. Privacy Confusion over COVID Safe Checklist Rules for Hospitality Venues. Retrieved from <https://www.abc.net.au/news/2020-06-14/covid-confusion-as-cafes-warned-about-privacy-dangers/12351314>.

Received July 2020; revised September 2020; accepted November 2020