Pandemic Response: Best Practices in IT Leadership

Jason Davidson
Butler University

The rapid spread of the COVID-19 virus resulted in shelter-in-place orders disrupting business operations and supply chains. IT leadership was faced with the rapid implementation of crisis management and business continuity plans as well as on-the-fly adaptations required to stay operational. Four CIOs from various businesses discussed the challenges of dealing with a rapidly spreading pandemic, strategies to mitigate the loss of business continuity, and lessons learned in the transition to hybrid or fully remote work environments. This paper recounts and analyzes the best practices gained from these interviews. Data was collected through online interviews with CIOs from for-profit and non-profit businesses. The transcripts of the recorded interviews were then analyzed for similar strategic approaches, aspects of success, and areas that needed improvement. The results revealed best practices in dealing with the loss of a centralized work environment, strategies to leverage technology to maintain business continuity, and procedures to incorporate into future pandemic response plans.

Keywords: pandemic resilience, business continuity plan, continuity of operations plan, IT best practice, disaster recovery

INTRODUCTION

Severe acute respiratory syndrome (SARS), Middle Eastern respiratory syndrome (MERS), Bovine flu (BRD), and H1N1 (swine flu) started a global conversation on digital transformation, disaster recovery planning, and business continuity planning (Xue & Zeng, 2018). With over 75 million infected and 7 million fatalities, the COVID-19 pandemic assessed these strategies and reinforced the importance of information technology and its ability to "connect people regardless of social distance" ("How Information Technology Helped Businesses", 2021). The 2019 pandemic forced IT leadership and business executives to make rapid decisions daily. The first major disease event since the Spanish Flu to garner an "urgent global healthcare response," and spanning 4 years, businesses without strong infrastructure and a business continuity plan faced extreme hardship (Patterson et al., 2021).

Global response to the rapidly spreading virus led to sweeping social distancing and shelter-in-place orders culminating with a global shutdown attempting to "flatten the curve" (Nakash & Bouhnik, 2022**)**. While these precautions were necessary, the negative impact on business, global supply chains, physical and mental health were cataclysmic. Four years after the initial COVID-19 outbreak, there is much that can be learned from businesses who successfully navigated the tumultuous time. This research aims to explore IT leaderships response and best practices to the COVID-19 pandemic. Specifically, companies that leveraged technology to remain operational. The goal is to provide documentation of best practices that can help shape modern business interruption mitigation strategies to prepare businesses for any future hardships.

LITERATURE REVIEW

Many comparisons can be made between the COVID-19 pandemic and 1918 influenza, commonly known as the Spanish Flu. Both are viruses that can lead to acute respiratory distress syndrome (ARDS), both potentially originated as illnesses that mutated to infect humans, and both had "significant negative impacts on the global economy" (Liang et al., 2021). Both illnesses reached a global scale by transmission through the movement of people; however, while the 1918 influenza spread mainly through maritime and railroad transport, the COVID-19 virus was able to reach a global scale faster "because of modern international air travel" (Morens et al., 2021). This rapid transmission prompted travel bans and social distancing restrictions, culminating in a global shutdown. While these safety procedures were needed to slow the spread and ease the strain on hospitals, the economic ramifications were severe, yielding a global recession with a magnitude not seen since World War II (Yeyati & Filippini, 2021).

In 2020 the United States, Federal Reserve reported there was a "surge of business exits (death)" with 330,000 business shuttered resulting in 1.2 million jobs lost (Decker & Haltiwanger, 2022). However, by the end of the third quarter, business births recovered and continued to grow into 2021 (Decker & Haltiwanger, 2022). As we emerge from the pandemic, research shows that strategic use of information technology was a key component to "effectively and efficiently" managing the rapidly changing business ecosystem as it reacted to the global shutdown (Pereira, et al., 2022). Companies that "increased investments in technology during the pandemic outperformed their competition" (COVID-19 and the Future, 2023). Additionally, an IBM study found that 60% of business leadership increased their commitment to digital transformation due to COVID-19 (COVID-19 and the Future, 2023).

The impact of IT can easily be observed during the rapid transition to remote work for nonessential employees during the shutdown. Mobile devices, cloud computing, VoIP, and webcams became a part of daily business operations (Nakash & Bouhnik, 2022). While digital communication software like zoom became a household name, these communication mediums utilized in personal nonsecure residences drastically increased the cybersecurity threat vector (Nabe, N.D.). For example, Zoom paid an $85 million settlement over privacy issues, resulting in zoombombing (Stempel, 2021). Additionally, IBM's Security X-Force reported a 6000% increase in phishing emails imitating the small business administration (Vila & Carruthers, 2020). These challenges are amplified by a report from Deloitte which found that 47% of employees are tricked by phishing attempts while working remotely and discovered a 35% increase in unseen malware attacks during the pandemic (Nabe, N.D.). These numbers are also reflected in a 2021 survey by the Society of Information Management that reported that security is the top concern of IT leadership (Kappelman et al., 2021).

METHODOLOGY

This study consists of qualitative interviews conducted in June of 2020 with four chief information officers spanning the fields of healthcare, auto sales, financial services, big box retail, and commercial insurance. The participants were asked to answer three open-ended questions (1) How has your business been impacted by the current pandemic or past epidemic/pandemics? (2) What strategies have you taken to maintain business operations? (3) Moving forward, what best practices, new strategies, or operational techniques will be adopted?

To protect the identity of the participants, they have been labeled as follows.

A – Healthcare provider that operates primary care clinics. The company has 600 employees across 7 offices

B – Responsible for all technical operations for a franchise-based sales corporation

C – Big Box Retail electronics company. The only subject with prior experience in IT management during a pandemic/epidemic

D – Privately owned insurance company. Responsible for two offices with 170 employees in geographically diverse locations

Reflexive thematic analysis was conducted to analyze the data collected (Braun & Clarke, 2006). As "reflexivity involves a disciplined practice of critically interrogating what we do, how we do it, and the impacts and influences of this on our research (Braun & Clarke, 2022). The identified qualitative themes were then compared to the Society of Information Managements (SIM) 2021-2023 IT Trends surveys in the discussion section. (The SIM IT Trends study is an annual survey of business practices which is distributed to its over 10,000 members).

RESULTS

While the four CIOs companies were from diverse industries, thematic analysis revealed the unified themes of preparedness, communication, cybersecurity, and innovation. As the results will show, the first two themes are somewhat common for all business continuity planning, while the severity of a global pandemic directly influenced their views on the latter themes.

Preparedness

Not all businesses have the luxury of a nimble work environment with the ability to quickly pivot operation. A common theme among the interviewees was training and preparedness to allow all impacted employees to act quickly to mitigate down time, reduce the need for excessive supervisor oversight, and ensure employee safety.

> **CIO (A)** "It is important to be nimble, flexible, and to think outside the box. As a healthcare provider we have essential employees and having a business continuity plan was a key component to constant operation during the pandemic. Of our 600 employees 450 were deemed non-essential and were transitioned to remote or hybrid status. I am new to the position and inherited the current business continuity plan, unfortunately due to turnover our employees required on the fly ad hoc training during the remote transition".

> **CIO (B)** "As a corporation that has 150 franchise stores, our business has historically been 100% on premises. The pandemic has challenged some our infrastructure and also highlighted things we have done well. I can't emphasize how important it is to have a plan and be prepared. Be prepared on the technology side but also as an organization".

> **CIO (C) "**I was in this position during the H1N1 pandemic. As a result of H1N1 we drafted a robust pandemic response plan. As part of the plan, the leaderships mission is to maintain all critical operations. Depending on the nature of the emergency we have the task of deciding what we need to do and how we can make it happen. We want to identify the problem, implement the change required to remain operational and disseminate all needed information throughout the company."

> **CIO (D)** "We were fortunate to have the cloud infrastructure in place to switch to remote employment quickly. We had a business continuity plan and disaster recovery plan in place. While our plan was somewhat robust, it was not designed to manage a shelter in place order followed by a national shutdown. From an infrastructure perspective our cloud-based systems remained operational, however, we had to get creative with our workforce as we were not essential workers and had to flip to 100% remote". From a hardware perspective, as we proceed with traditional upgrades, we maintain 40 or so laptops as part of our emergency plan. They were a little dated, but really saved the day".

Communication

"Communication in business is important for fostering relationships between staff and management, improving morale, efficiency, and keeping employees in the loop. Communication breakdowns can be disastrous and have a far-reaching impact" (Nierman, 2022). All four CIOs stressed the importance of clear, consistent, and accurate communication as part of their business operations during the COVID-19 pandemic.

> **CIO (A)** "As a healthcare provider we have a responsibility to our patients, we are also responsible for the safety of our staff. We need to maintain operations, but that has to happen in a way the ensures the safety of our clients and our staff. Our leadership team conducted three status meetings a day and monitored national and local news sources for updates 24-hours a day. We rapidly deployed Microsoft Teams as a constant channel of communication. We sent executive update emails and had to implement ad hoc training on the new system. We had to make on the spot decisions as soon as they were made by the government. We then had to disseminate that information to our 600 employees and our patients. This was compounded by the need to adhere to HIPPA while many of our employees were remote".

> **CIO (B)** "The shutdown was detrimental to our business. If you are sheltered in place, you are not patronizing one of our retail locations. We still had to keep our operations, HR, finance, and accounting departments functioning. We also had to provide updates to our workforce that were unable to work while our franchises were closed. We implemented Microsoft Teams to communicate with essential staff and shared all other key updates via the company's internal portal. Communications included detailed emails as well as prerecorded video updates. I can't emphasize how important a well-managed company portal is during crisis management."

> **CIO (C)** "A 24x7 conference bridge is part of our business continuity plan. Additionally, we physically spread the management team out over several diverse locations. We held weekly discussions to coordinate operations, due to the nature of the emergency our retail stores were initially closed, however, our website remained operational."

> **CIO (D)** "Communication was emphasized by our management team. Not only did we need to manage our employees, we also needed to focus on communication with our clients. As an insurance company we saw a spike in business during the pandemic and while our employees were able to quickly pivot to remote we lacked the same infrastructure for client communications. While we experimented with various methods of communications, it was not a smooth transition. Internally we utilized Teams, however, Zoom was used for external customers due to ease of use. Weekly communication emails were sent from management to our employees. Additionally zoom meetings were used to communicate with clients until the shelter in place was lifted".

Cybersecurity

Concerns with security were among the top issues discussed during this research. The rapid transition to remote workspaces ushered in challenges with both connectivity and security.

> **CIO (A)** "Security was one of our biggest challenges at the start of the lockdown. 450 of our 600 staff members rapidly transitioned to remote opening the door for cybersecurity issues which are multiplied by HIPPA. Two factor authentication was already in place, however, we had to quickly deploy a VPN solution. Additionally, our staff had to complete ad hoc security training to ensure we didn't have accidental HIPPA violations when

> working remotely. Moving forward we would like to strengthen the amount of security training required of remote employees".
>
> **CIO (B)** "Due to the nature of our business a large amount of our employees were unable to work. Those that were able to continue to work remotely were required to use VPN.
>
> **CIO (C)** "Cybersecurity is a big component of our operations plan. We whitelist IP address for BYOD and use VPN for remote access on company devices. We also set up miniature remote offices that are more secure and controllable for mission critical positions. Our systems were already backed up via private cloud".
>
> **CIO (D)** "Security was a challenge for us. For good or bad we had to make a choice between security and productivity and our scale leaned towards productivity. It was a calculated risk. We had the technical aspects covered, however, our issues were with insecure remote locations. Most of our employees have makeshift home offices, and it is very difficult to control the flow of information in these environments. There is nothing to stop a family member from wondering in or even a potential breach due to something as simple as a child's toy that is connected to their home network. Moving forward we need to overhaul our remote policy to include a security checklist for work from home setups".

Innovation

The COVID-19 pandemic accelerated business adoption of technology and commitment to digital transformation (Evans, 2021). This statement is further supported by the 2022 IT Trends report that found IT spending increased from $118 million to $148 million between 2020 and 2021 (Kappleman et al., 2022). A common theme of innovation through technology to continue operations, communications, and maintain safety emerged in the thematic analysis results.

> **CIO (A)** "We had some areas that had not been monitored, such as hardware needed for remote operation, and we have some checks and balance to install moving forward. Fortunately, we were able to roll out upgrades to Windows 10 and Microsoft teams over a 3-day span to get the remote employees operational. In the future we hope to add remote employee configuration to our onboarding process".
>
> **CIO (B) "**We all have to change, if we have another COVID-19 we can't survive economically, the world won't survive. The switch to remote has caused us to evaluate the importance of interpersonal relationships, leadership, and how to enhance emotional intelligence with customer virtually". Since working remote is the new norm, we have implemented training on effective communication in a 2D virtual workspace".
>
> **CIO (C)** "We set up miniature offices in stores, we also had a contract with a facility for emergency workspace. Our goal was to physically spread the leadership team out. We want to spread people out and not have everyone in the same place for safety purposes".
>
> **CIO (D)** "Our business continuity plans were designed for specific challenges such as fires or natural disasters. The national shutdown forced us to get creative. We were able to utilize dead stock hardware for primary user devices. We made the decision to drop ship peripherals directly to our employees. We had TV monitors shipped instead of monitors because they are cheap, we also had printers/copiers etc. shipped as needed. We also experimented with various communication platforms. We experimented with Slack and ended up deploying Teams for internal communication and Zoom for client use. While Teams would have been better for us, Zoom was more client friendly".

DISCUSSION

The WHO detects around 3,000 indications of potential outbreaks a month (Sridhar, 2020). While these threats are published, few could predict how quickly COVID-19 spread from its initial report to national shutdowns. While business resilience to a global pandemic can never be guaranteed, we conclude that preparedness through creating a robust business continuity plan (BCP) alternatively referred to as a continuity of operations plan (COOP) is a key component to navigating this type of crisis. As one of the participants stated, "you can't be more prepared" and "having a plan allows you to be nimble and move quickly when faced with uncertainty" (CIO A). The 2021 SIM IT Trends national survey found that out of 519 respondents, 30.8% lacked a BCP/COOP entering the pandemic.

Additionally, of the 69.2% that did have plans, 53.7% did not have provisions for a pandemic (Kappelman, et al., 2021). This includes participants in our study that stated "we had a plan but it didn't include the inability to access any of our locations" (CIO D). The following 2021 IT Trends study found an increase to 73.6% in 2022 and also reported business continuity planning as a top personal concern of management in the most recent 2023 study (Kappelman, et al., 2021). Along with the creation of a BCP/COOP we suggest regular review, tests, and updates. As SIM reported in 2021 28% of companies with a BCP/COOP had not reviewed or tested the plan and its supporting systems in 24 months (Kappelman, et al., 2021).

Communication was another key theme that the participants of the study emphasized. As Reddy and Gupta write, "responding to COVID-19 requires critical preparedness and response which includes effective communication as an essential strategy" (Reddy & Gupta, 2020). All respondents to our study deployed a shared communication channel for business communications. The goal being reliable and safe communication between management, internal, and external clients. This was a key component as shelter-in-place restricted close personal interactions. As one participant stated "COVID taught us how to work remotely and still communicate effectively". These lines of constant communication were supplemented with weekly videos or lengthy newsletter type emails providing updates and key directives. One challenge noted is that while technology did allow communication, remote work had some disadvantages compared to in person workspaces. These disadvantages Included distractions, reduced relationship building, and a reduced ability to read employees non-verbal communication. It was suggested that while remote work is the "new norm" (CIO B) a hybrid work environment may be more beneficial to moral and collaborative work. We need to "rethink how we engage internally and externally" (CIO B).

Our ingenuity in leveraging technology to keep us mentally and emotionally together while physically apart also increased the security threat vector of remote employees (Nabe, N.D.). Along with inadvertent security issues that can occur when working from home in a cohabitated space, cyber-criminals also increased their intensity targeting everyday people looking for government assistance and work-from-home employees (Lallie et al., 2021). Since the lockdowns were somewhat unexpected, IT leadership had to make compromises in the transition to remote. As CIO D noted "we had to make a choice between security and productivity and our scale leaned towards productivity". This was echoed by CIO A, who noted HIPPA compliance concerns with remote employees with family members sharing work spaces. These sentiments are reflected in the SIM IT Trend survey. Since 2011 SIM reports that cybersecurity is the top concern of IT leadership (Kappleman et al., 2021). While many companies made the same complex decisions as CIO D, an emphasis on cybersecurity must be deployed moving forward. As CIO D noted, the challenges with security revolve mostly with awareness. With a substantial portion of the workforce not returning to the office, it is important that this staff is trained to maintain the highest level of security. This includes training to raise awareness of phishing, malware, and other social engineering scams, secure the physical remote workspace, and reduce instances of shadow IT. This practice is supported by the research that shows "investment in IT awareness training is above the 10-year average" (Kappleman et al., 2022).

Metaphorically it could be argued that every modern business is a tech company (Leonard, 2023). While there are diverse industries, products, and services, the common theme is that technology is leveraged to operate and innovate to supplement physical labor. Technology is the summation of human knowledge allowing us to exceed our physical limitations. As Brady theorizes, we not only leverage existing technology but also “think technology” in our operations as we innovate in life (Grady, 2010). The world’s response to the COVID-19 pandemic is an example of leveraging technology to push past our physical limitations. Digital communications allowed us to safely continue business operations, disseminate information effectively, and ensure employee safety. Alghamdi et., al. summarized our use of technology during the pandemic as hard and soft innovations. Hard innovations were creating new technology such as the COVID vaccine and testing kits. Soft innovations were novel uses of existing technology adding to our knowledge of how the systems could be operated (Alghamdi & Alghamdi, 2022). This study revealed several hard and soft innovations that are worthy of adoption into future BCP/COOP.

A point of emphasis from the participants in this study was the use of cloud computing and the adoption of an open-channel communication platform. Leveraging cloud infrastructure allows more flexibility for remote employment. Those participants still had on premises systems noted that “while some on prem is necessary it was a pain point” (CIO D) that needs attention in future plans. As a healthcare provider, CIO A recounted the importance of physical safety. While most of the company’s staff transitioned to remote, measures had to be put in place for clinic safety. UV lights traditionally used to sanitize medical equipment were adapted to sterilize equipment in the IT department. CIO D leveraged decommissioned equipment, placing it back into service for remote employee use with the understanding it could be discarded before returning to the office. Additionally, Amazon was leveraged to direct ship peripherals to the homes of remote staff to minimize direct contact. In summary, while BCP/COOP must be thoughtfully drafted, assessed, and often revised IT leadership must also plan for the unexpected and accept the challenge of thinking outside the box to innovate during times of crisis. Companies must remain “nimble and flexible in thinking” (CIO A) as every moment of a crisis could reveal a new challenge that must be overcome.

CONCLUSION

“Strategy is about shaping the future” and to ensure resilience during the next global health crisis, companies must start with an evolved approach towards business continuity planning (McKeown, 2023). As Maxwell states, “Change is inevitable, progress is not”, the pandemic has changed our view of work and challenged IT leadership to innovate through leadership methodology and leveraging technology (Maxwell, 2022). The participants of this study highlighted how the COVID-19 pandemic impacted their companies, employees, and future business strategies. They have emphasized the importance of innovation, nimble operations, security, and communication. Best practices such as redundancy through cloud computing, robust VPN, cloud-based communication platforms, and security awareness training have been spotlighted as best practices that must be continued post-pandemic. Future studies could advance this research with follow up interviews to gauge the impact of lessons learned post-pandemic. Additionally, a larger sample size could provide more insight into the industry not interviewed in this study.

REFERENCES

Alghamdi, N.S., & Alghamdi, S.M. (2022). The role of digital technology in curbing COVID-19. *International Journal of Environmental Research and Public Health*, *19*(14), 8287. https://doi.org/10.3390/ijerph19148287

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Braun, V., & Clarke, V. (2022). *Thematic analysis: A practical guide*. SAGE Publications.

COVID-19 and the future of business. (2022). Retrieved from https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/covid-19-future-business

Decker, R., & Haltiwanger, J. (2022). *Business entry and exit in the COVID-19 pandemic: A preliminary look as official data*. Retrieved from https://www.federalreserve.gov/econres/notes/feds-notes/business-entry-and-exit-in-the-covid-19-pandemic-a-preliminary-look-at-official-data-20220506.html

Evans, G. (2021). *The Pandemic Has Forever Accelerated Technology Innovation for Business and Public Safety*. Retrieved from https://www.forbes.com/sites/drgeraintevans/2021/12/23/the-pandemic-has-forever-accelerated-technology-innovation-for-businesses-and-public-safety/?sh=76593f9d6a8e

Grady, W. (2010). *Technology*. Groundwood Books.

IIBA. (2021). *How Information Technology Helped Businesses Evolve During the Pandemic*. Retrieved from https://www.iiba.org/professional-development/knowledge-centre/articles/how-information-technology-helped-businesses-evolve-during-the-pandemic/

Kappleman, L., McLean, E., Johnson, V., Torres, R., Maurer, C., Snyder, C., …Guerra, K. (2021). *SIM IT Trends Study* (2021 report). Society of Information Management

Kappleman, L., Torres, R., McLean, Maurer, C., Johnson, V., Snyder, C., …Srivastava, S. (2022). *SIM IT Trends Study* (2022 report). Society of Information Management

Lallie, H.S., Shepherd, L.A., Nurse, J.R.C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*, 102248. https://doi.org/10.1016/j.cose.2021.102248

Leonard, K. (2023). *The Shocking Truth: Why Every Company Is a Technology Company*. Retrieved from https://www.business.com/articles/why-every-company-is-a-technology-company/

Liang, S.T., Liang, L.T., & Rosen, J.M. (2021). COVID-19: A comparison to the 1918 influenza and how we can defeat it. *Postgraduate Medical Journal*, *97*(1147), 273–274. https://doi.org/10.1136/postgradmedj-2020-139070

Maxwell, J.C. (2022). *The 21 irrefutable laws of leadership: Follow them and people will follow you* (25th Anniversary Ed.). Harper Collins Leadership. Retrieved from https://public.ebookcentral.proquest.com/choice/PublicFullRecord.aspx?p=6998122

Mckeown, J.J.M. (2023). *Strategy book*. Ascent Audio.

Morens, D., Taubenberger, J., & Fauci, A. (2021). A centenary tale of two pandemics: The 1918 influenza pandemic and COVID-19, Part I. *American Journal of Public Health*, *111*(6), 1086. https://doi.org/10.2105/AJPH.2021.306310

Nabe, C. (n.d.). *Impact of COVID-19 on Cybersecurity*. Retrieved from https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html.

Nakash, M., & Bouhnik, D. (2022). The effects of COVID-19 on information management in remote and hybrid work environments. *Journal of the Association for Information Science and Technology*, *74*(9), 1067–1080. https://doi.org/10.1002/asi.24803

Nierman, E. (2022). *Communication Lessons from the Pandemic Are Transferrable to Business*. Retrieved from https://www.forbes.com/sites/theyec/2022/08/17/communications-lessons-from-the-pandemic-are-transferrable-to-business/?sh=213595601054

Patterson, G.E., McIntyre, K.M., Clough, H.E., & Rushton, J. (2021). Societal impacts of pandemics: Comparing COVID-19 with history to focus our response. *Frontiers in Public Health*, *9*, 630449. https://doi.org/10.3389/fpubh.2021.630449

Pereira, C.S., Veloso, B., Durão, N., & Moreira, F. (2022). The influence of technological innovations on international business strategy before and during COVID-19 pandemic. *Procedia Computer Science*, *196*, 44–51. https://doi.org/10.1016/j.procs.2021.11.071

Reddy, B.V., & Gupta, A. (2020). Importance of effective communication during COVID-19 infodemic. *Journal of Family Medicine and Primary Care*, *9*(8), 3793–3796. https://doi.org/10.4103/jfmpc.jfmpc_719_20

Sridhar, D. (2020). COVID-19: What health experts could and could not predict. *Nat Med*, *26*, 1812. https://doi.org/10.1038/s41591-020-01170-z

Stempel, J. (2021). *Zoom reaches $85 mln settlement over user privacy, 'Zoombombing'*. Retrieved from https://www.reuters.com/technology/zoom-reaches-85-mln-settlement-lawsuit-over-user-privacy-zoombombing-2021-08-01/

Vila, A., & Carruthers, S. (2020). *New Study Shows Consumers Could Be Vulnerable to COVID-19 Spam*. Retrieved from https://securityintelligence.com/posts/new-study-shows-consumers-could-be-vulnerable-to-covid-19-spam/

Xue, L., & Zeng, G. (2018). Global strategies and response measures to the influenza A (H1N1) pandemic. In *Research series on the Chinese dream and China's development path* (pp. 15–44). https://doi.org/10.1007/978-981-13-0644-0_2

Yeyati, E.L., & Filippini, F. (2021). *Social and economic impact of COVID-19*. Brookings Institution.