Journal of Cybersecurity Education, Research and Practice

Volume 2022 | Number 2 Article 4

January 2023

Cybersecurity Continuity Risks: Lessons Learned from the COVID-19 Pandemic

Tyler Fezzey
University of West Florida, tnf6@students.uwf.edu

John H. Batchelor
University of West Florida, jbatchelor1@uwf.edu

Gerald F. Burch
University of West Florida, gburch@uwf.edu

Randall Reid
University of West Florida, rcreid@uwf.edu

Cybersecurity Continuity Risks: Lessons Learned from the COVID-19 Pandemic

Abstract

The scope and breadth of the COVID-19 pandemic were unprecedented. This is especially true for business continuity and the related area of cybersecurity. Historically, business continuity and cybersecurity are viewed and researched as separate fields. This paper synthesizes the two disciplines as one, thus pointing out the need to address both topics simultaneously. This study identifies blind spots experienced by businesses as they navigated through the difficult time of the pandemic by using data collected during the height of the COVID-19 pandemic. One major shortcoming was that most continuity and cybersecurity plans focused on single-axis threats. The COVID-19 pandemic resulted in multi-axes threats, pointing out the need for new business strategies moving forward. We performed multiple regression analysis and constructed a correlation matrix to capture significant relationships between percentage loss of revenue and levels of concern for different business activities moving forward. We assessed the most pervasive issues Florida small businesses faced in October 2020 and broke these down by the number of citations, the total number of impacts cited, and industry affectedness. Key security risks are identified and specific mitigation recommendations are given.

Keywords

cybersecurity, COVID-19, business continuity planning, information security

INTRODUCTION

The COVID-19 pandemic proved to be a global event that damaged economic activity irrespective of the business sector. Many firms were caught unprepared, rushing to form contingency plans that could have been in place years prior. Additionally, cybersecurity is at the forefront of the minds of many organizations following recent highly publicized ransomware attacks. As one delves deeper into the matter, it becomes apparent that human and organizational factors are the principal vulnerabilities for such attacks (Kraemer et al., 2009). As such, organizations must develop a culture of information security awareness (Ahlan et al., 2015) to deal with such issues related to business continuity planning (BCP) and cybersecurity. BCP and cybersecurity are linked through their purpose of managing risk. Burch et al. (in press) suggest three steps to address both BCP and mitigate cybersecurity threats: 1. Successfully identify major threats, 2. Develop a plan to reduce (or mitigate) the impact of these threats, and 3. Train employees on how to execute and test the plan.

These recommendations are not considerably different from what has been recommended in the past. However, there are lessons to be taken from recent events. This article seeks to identify these lessons by comparing how organizations addressed BCP and cybersecurity before and after the COVID-19 pandemic and discusses changes organizations need to implement to successfully mitigate risk going forward (i.e. lessons learned from COVID-19).

LITERATURE REVIEW

Cybersecurity is defined as the "organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace enabled systems from occurrences that misalign de jure from de facto property rights" (Craigen et al., 2014, p. 13). There is a robust technical side of cybersecurity, but people also play a critical role. For instance, creating a secure organizational culture wherein employees know not to share passwords and adhere to other company protocols is essential (da Veiga, 2019). Building a strong security culture must include considering organizational factors such as policies, communication, and structure (Kraemen & Carayon, 2007). Thus, this article views cybersecurity as one component of an overall organizational risk management framework.

Like cybersecurity, BCP is also a form of risk management. BCP is defined as a plan designed to "avoid, or mitigate, risks: to limit the effect of a crisis: and reduce the time needed to restore operations to a state of business as usual" (Burch et al., in the press). Thus, continuity planning focuses on planning for and/or mitigating a business disruption (i.e., ransomware or pandemic) and moving forward (Torabi et

al., 2016) with all components of a security culture. Kraemer et al. (2009) discuss the importance of understanding relationship complexities related to security. In this vein, cybersecurity is a part of this risk management process and BCP.

Many businesses lack an effective business continuity response plan. These organizations focus on mitigating risk and their response plan rather than ensuring the organization can function in the interim (Phillips & Tanner, 2018). This is also the case with cybersecurity. We recommend that cybersecurity and BCP be linked together, not function as two separate silos. For instance, what good is cybersecurity so strong it is unusable? This means organizations should bring their cybersecurity staff and BCP staff together and form one cohesive planning team that articulates their response and recovery plan for various risks and periodically tests these plans.

Page and Yeoman (2006) outlined how VisitScotland had emergency plans in place for a possible flu pandemic fifteen years before COVID hit. Rightfully, Page and Yeoman (2006) remarked that the process of business continuity planning is a vital step for many organizations in relation to risk assessment and preparations in the event of a major event that interrupts normal business activity. Although a flu pandemic is not identical to the issues created by the COVID-19 pandemic, a firm that has planned and created operating procedures for a flu pandemic scenario would be much more likely to have successfully weathered the COVID-19 pandemic than those who had not.

PRE-COVID-19 CYBERSECURITY AND CONTINUITY PLANNING

Before the COVID-19 pandemic, BCP and its cybersecurity components functioned under a different paradigm than they do now. Pre-COVID-19 plans focused primarily on potential attacks such as phishing, ransomware, and crypto-jacking that were started by an outsider (see Phillips & Tanner, 2018). Following the pandemic, the flux of workers to remote environments, and the increase of business performed online, attacks are now often multipronged and connected to insider threats and poor cybersecurity practices (i.e., accessing sensitive information on an unsecured network). Before March 2020, the focus for many cybersecurity personnel was on recognizing threats- such reactive attitudes are often the weakest point in an organization's cybersecurity network (Qian et al., 2012). Currently, the majority of energy has been shifted to creating continuity plans and ensuring that employees follow up-to-date best cybersecurity practices. As such, firms must center on creating a security culture that starts in the boardroom and is pervasive throughout the organization.

WHAT WE LEARNED FROM COVID-19

The COVID-19 pandemic was unprecedented in the modern, cyber security-aware world. Up to this point, few organizations saw the need or viewed it possible that a majority of the economies in the world would essentially shut down due to a pandemic (see Page & Yeoman, 2006 for a BCP article that came close). This event resulted in lockdowns, closure of institutions, avoidance of in-person shopping, online service growth, and the explosion of virtual meetings. Government and individual reactions to the pandemic resulted in a tectonic shift in the behavior of almost all societies across the globe.

So how has this social/institutional shift affected BCP and cybersecurity? To answer the question, the environment that organizations function in has changed and now organizations must adapt and plan for this new atmosphere. As such, organizations have already or are shifting from focusing predominantly on threats such as phishing, ransomware, and crypto-jacking. New risks include Zoom bombing, COVID-19 specific phishing attacks, malware, decreased network availability due to suddenly increased traffic (Weil & Murugasen, 2020), and VPN issues (i.e., not turning it on when working from home) are climbing up the ranks of issues prompting new security policies.

Now the focus is on creating a security culture to protect the digital fabric of their organization. This fabric is now used to conduct remote work, address changing customer needs, and comply with governmental restrictions on businesses and citizens alike. Organizational BCP and cybersecurity managers understand this, but it is important to do a better job of explaining this to employees and to be sure to explain why it is important (Parsons et al., 2014).

Effects of COVID-19 on Small Businesses

The impacts of the COVID-19 pandemic present new considerations regarding cybersecurity for small businesses. Many small ventures believe they are exempt from digital attacks and have little regard for cybersecurity. This attitude means that most do not have continuity plans or incident responses to prevent or react to many of the potential risks that come from the global, digital transition COVID-19 thrust upon the world. As such, McCormac et al. (2017) point out the need to clearly explain to individuals (even small business owners) the importance of adhering to security awareness policies.

Small businesses are attractive targets because they have the sensitive information cybercriminals are after, yet lack the security infrastructure of larger corporations (U.S. Small Business Administration, 2021). Experts estimate cyberattacks have increased by more than 20% since 2016, and 66% of small and

medium-sized businesses (SMBs) have experienced a cyberattack in the last 12 months. Another 45% of SMBs globally indicated their organization's security posture was ineffective at mitigating attacks (Keeper Security, Inc. & Ponemon Institute, 2019). This highlights the need for increased security awareness in the SMB community.

Methodology

At the heart of the COVID-19 pandemic (October 2020), the Florida Small Business Development Center (SBDC), the University of West Florida Haas Center, and the Florida Chamber of Commerce Foundations engaged in a joint effort to survey small business owners in Florida. This survey included 4,842 small businesses and asked owners a series of questions about the pandemic and how it affected their businesses. The result is a mixed-methods approach to analysis that includes regression analysis, a correlation matrix, and figures of survey responses that support our suggestion that COVID-19 revealed massive holes in business continuity planning and cybersecurity measures.

Regression Analysis and Correlation Matrix

Businesses self-reported their estimated percentage of lost revenue due to the COVID-19 pandemic and consequential business lockdowns. Additionally, they were asked to report their level of concern moving forward regarding the following:

- Loss of revenue
- Acquiring capital
- Business continuity
- Business cost
- Business revenue
- Economic uncertainty
- Government regulation
- Supply chain
- Workforce quality

We performed multiple regression analysis (Figure 1) and constructed a correlation matrix (Figure 2) for all variables to assess the relationships between each concern and the percentage of revenue lost that the business had already incurred.

Model Summary - Percentage of Revenue Lost

Model	R	R^2	Adjusted R^2	RMSE
H_0	0.000	0.000	0.000	32.536
H_1	0.544	0.296	0.294	27.340

ANOVA

Model		Sum of Squares	df	Mean Square	F	p
H_1	Regression	687959.738	8	85994.967	115.048	< .001
	Residual	1.632e+6	2184	747.471		
	Total	2.320e+6	2192			

Note. The intercept model is omitted, as no meaningful information can be shown.

Coefficients

Model		Unstandardized	Standard Error	Standardized	t	p
H_0	(Intercept)	50.933	0.695		73.309	< .001
H_1	(Intercept)	-3.589	2.467		-1.455	0.146
	Acquiring Capital	3.164	0.530	0.147	5.967	< .001
	Business Continuity	6.521	0.753	0.266	8.663	< .001
	Business Cost	2.076	0.744	0.082	2.790	0.005
	Business Revenue	4.917	0.843	0.181	5.830	< .001
	Economic Uncertainty	-0.346	0.749	-0.012	-0.462	0.644
	Government Regulations	0.811	0.533	0.034	1.520	0.129
	Supply Chain	-1.618	0.533	-0.070	-3.033	0.002
	Workforce Quality	-2.011	0.462	-0.094	-4.354	< .001

Figure 1: Multiple Regression Analysis

Multiple regression showed that just under 30% of the variance ($r^2 = .296$) in the percentage of lost revenue could be explained by the variables chosen in this study. Six of eight predictor variables were significant at the 0.05 level: acquiring capital, business continuity, business cost, business revenue, supply chain, and workforce quality. Economic uncertainty and government regulations were not significant. Economic uncertainty and government regulations might have been significant if other variables were removed since these two variables are significantly correlated to the other six variables used in the model.

Pearson's Correlations

Variable		Percentage of Revenue Lost	Acquiring Capital	Business Continuity	Business Cost	Business Revenue	Economic Uncertainty	Government Regulations	Supply Chain	Workforce Quality
1. Percentage of Revenue Lost	Pearson's r	—								
	p-value	—								
2. Acquiring Capital	Pearson's r	0.414	—							
	p-value	< .001	—							
3. Business Continuity	Pearson's r	0.485	0.635	—						
	p-value	< .001	< .001	—						
4. Business Cost	Pearson's r	0.384	0.596	0.698	—					
	p-value	< .001	< .001	< .001	—					
5. Business Revenue	Pearson's r	0.438	0.546	0.721	0.679	—				
	p-value	< .001	< .001	< .001	< .001	—				
6. Economic Uncertainty	Pearson's r	0.328	0.434	0.568	0.540	0.671	—			
	p-value	< .001	< .001	< .001	< .001	< .001	—			
7. Government Regulations	Pearson's r	0.209	0.352	0.375	0.450	0.382	0.499	—		
	p-value	< .001	< .001	< .001	< .001	< .001	< .001	—		
8. Supply Chain	Pearson's r	0.153	0.355	0.397	0.475	0.358	0.375	0.479	—	
	p-value	< .001	< .001	< .001	< .001	< .001	< .001	< .001	—	
9. Workforce Quality	Pearson's r	0.104	0.321	0.351	0.410	0.315	0.308	0.368	0.523	—
	p-value	< .001	< .001	< .001	< .001	< .001	< .001	< .001	< .001	—

Figure 2: Correlation Matrix of Percentage of Revenue Lost and Levels of Concern

Figure 2 shows correlations between the percentage of lost revenue and all of the predictor variables. All correlations were positive and significant at the .05 level. Concern with business continuity had the strongest correlation (r = 0.485) with the percentage of revenue lost. Economic uncertainty (r^2 = 0.328) and government regulations (r = 0.209) were both correlated (p <.01) with the percentage of revenue lost, even though they were not significant in the multiple regression model. The lowest correlation was between workforce quality (r = 0.105) and the percentage of revenue lost.

Analysis of the correlations between predictor variables indicates the most significant correlation was between business continuity and business revenue (r = 0.721), with the second-highest being between business continuity and business cost (r = 0.698). These two correlations indicate that either business revenue or business cost could explain almost 50% of the change in business continuity. These two factors should become major areas of interest in the development of business continuity plans in the future.

Another area of concern is the government's role in such catastrophic economic events. The correlation between government regulations and economic uncertainty was 0.499. The causal direction here is of importance. One could certainly argue that the economic uncertainty caused the government to react. However, it could also be stated government regulations may have contributed to the economic

uncertainty. These two variables are certainly of interest since they were not significant in the multiple regression but have medium to strong correlations with almost all other variables.

Two other variables of concern are supply chain and workforce quality. These variables were significant in the multiple regression but tended to have the lowest correlation with the other variables. This may be due to the timing of the study. Many business owners may not have felt the supply chain problems and workforce quality earlier in the pandemic period.

Survey Results

The following bulleted list was offered as possible choices to the survey question: Please indicate how COVID-19 impacted your business by selecting from the following list (select all that apply).

- Added expenses to mitigate public safety risks
- Business closure (voluntary or mandated)
- Change of business hours
- Change of business model
- Employee layoffs or displacement
- Enhanced an existing second mode of business operation to sell and deliver products
- Event cancellation
- Loss of revenue
- Off-site working options
- Supply chain disruptions
- None of the above

From this question we analyzed the most common problems faced by SMBs and the relative importance of each problem. We then examined the frequencies of responses and industry-specific results. Based on this analysis, loss of revenue was the highest cited impact of COVID-19 on Florida small businesses (Figure 3). Loss of revenue was followed by additional expenses necessary to mitigate public safety risks and event cancellations. Loss of revenue and added expenses coupled with the need to maintain profitability may lead firms to expand their risk appetite beyond acceptable levels.

Loss of revenue was due, in large part, to forced government closures and changes in customer shopping habits. This resulted in many organizations changing their business model, business hours, or simply closing down permanently out of necessity. As a tourist destination, Florida relies heavily on a face-to-face economy fueled by travel. When restaurants were ordered to close their dining rooms, the

competitive advantage of sit-down eating was lost, and many businesses were now forced to compete with delivery-style or takeout restaurants. Many were forced to shift business models, close temporarily, or close permanently. The same is true for educational institutions as they, generally speaking, are destinations for campus living. The shift to fully online learning (change in their business model) resulted in large revenue losses and placed immense burdens on their existing technology infrastructure.

Other notable cybersecurity impacts include off-site working options, enhancing a second mode of business operations, changing business models, changing business hours, and business closure. These changes forced companies to adjust their business operations to remain competitive or stay afloat, potentially at the cost of cyber safety.

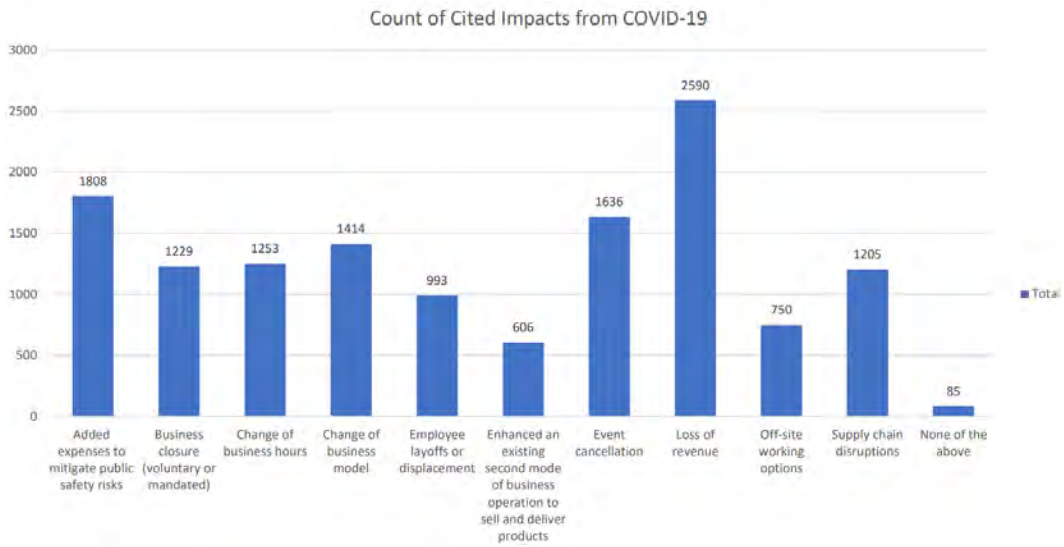

Figure 3: The Number of Businesses Who Selected Each Impact

Figure 4 displays the count of negative impact factors (i.e., problems faced) that each business cited due to the COVID-19 pandemic (a two signifies that a firm selected two answers for the survey question, perhaps "loss of revenue" and "event cancellation"). The most frequent number of issues encountered was four. But most importantly, 344 or 11% of companies reported only one negative consequence, and 540 or 21% reported two or fewer negative effects. This means roughly 89% of respondents reported multiple issues, and 79% reported more than two. This tells us that the majority of Florida small businesses were affected in more than one way by the pandemic.

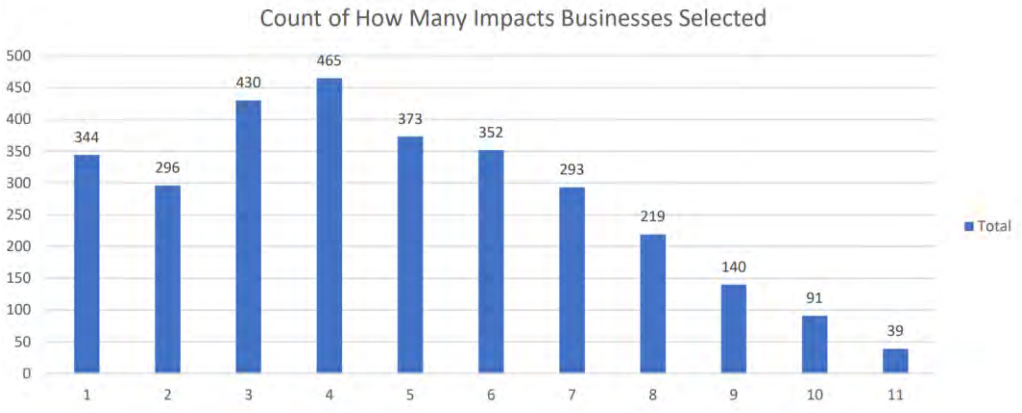

Figure 4: Count of How Many Impacts Firms Experienced During the COVID-19 Pandemic

The effects of the pandemic were not uniform across industries. The accommodation and food services industry cited the highest average count of impacts at 4.4, whereas the utility industry was relatively unaffected, citing only 1.9 impacts (Figure 5). This is likely because of the elasticity of services provided by each industry. More discretionary industries, such as those in food services, arts, entertainment, recreation, education services, and retail trade, were most harmed by COVID-19 because they are funded by discretionary income. These firms were also found to be the most exposed to new cyber risks. Less elastic industries like utilities are much less affected by COVID-19 because their services are not optional (i.e., water, gas, electricity).

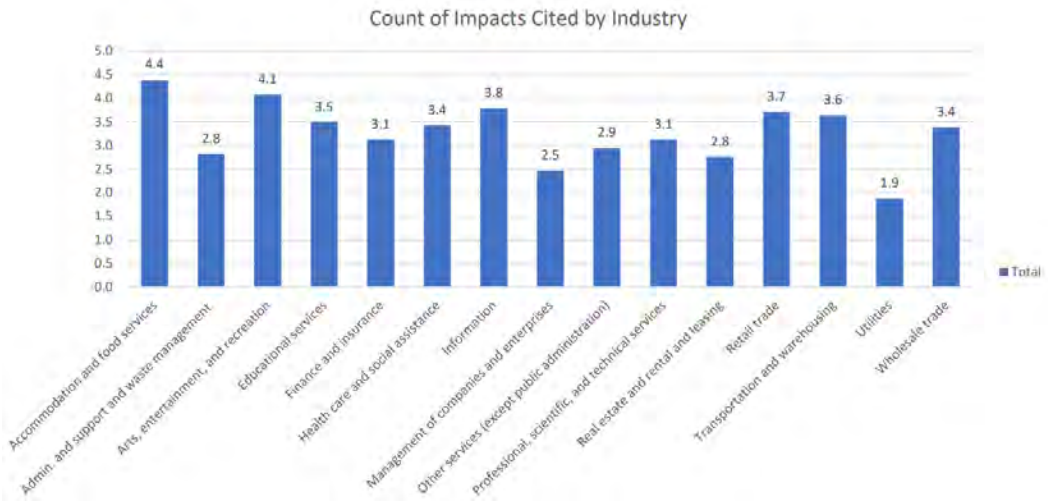

Figure 5: The Average Number of Impacts Cited as Broken Down by Industry

DISCUSSION

Some notable cybersecurity-related impacts caused by the COVID-19 pandemic identified in this study were: off-site working options, enhancing a second mode of business operations, changing the business model, changing the business hours, and business closure. The state of Florida is an ideal situation to study such impacts because of its historical bouts with natural disasters, namely hurricanes. Florida is mostly a coastline peninsula and experiences hurricanes that develop in both the Atlantic Ocean and the Gulf of Mexico. As such, most businesses' continuity planning centers on planning to close for days at a time following a hurricane, then reopening when power and utilities are restored. Others, such as restaurants, run on generators when the power is out. Despite having continuity plans in place for short periods of shutdown, it appeared that Florida SMBs were still unprepared for the long-lasting closures of the COVID-19 pandemic.

From the cybersecurity perspective, the abrupt shift to almost all non-essential, and in some cases essential, workers off-site was a contingency few had planned for. This shift was an unplanned necessity and resulted in many security breaches. Airani (2020) found that 22% of small businesses made this remote work shift without a cybersecurity threat prevention plan. It is unsurprising that this shift led to an increased risk of cybersecurity breaches given that staff are directly connected to financial losses related to data breaches and cybersecurity incidents (Pendergast, 2016) and that many staff members moved to remote work without ever performing their duties online.

Additionally, the unexpected switch meant new software and hardware were abruptly purchased and put into use without proper security audits (Kujawa et al., 2020). Many international employees also returned to their home countries as the pandemic began and worked remotely throughout the pandemic. Some of these employees live in countries with high-security risks and present a higher overall risk to their organizations.

Further, employees began using unauthorized and unprotected personal devices for work. In many cases, remote employees were not using a VPN or even aware of its importance to security. For many organizations, this enhanced vulnerability went unnoticed until after losses occurred (Fichtenkamm, Burch, and Burch, 2022).

TAKEAWAYS

This study's most pronounced continuity and cybersecurity-related finding is that most organizations reported that they experienced multiple impacts from the pandemic at once. Generally speaking, most continuity plans focus on a single incident—for example, phishing or a hurricane shutting down utilities for a couple of days. COVID resulted in multiple pronged attacks on organizations from both a cybersecurity and continuity planning aspect that lasted for a protracted period. The transition to remote work was a substantial new threat with multiple prongs of attack (i.e., increased use of personal devices for work and Zoom bombing) and the continuity issues of abruptly shifting one's business model (i.e., from producing vodka to hand sanitizer). In this study, 79% of respondents reported more than two notable impacts, with four impacts being the most commonly reported number. This points out the need to produce continuity/cybersecurity plans that prepare for worst-case scenarios where multiple threats occur at once. Based on what we have learned in this study, such planning should include a minimum of four impacts. When generating such plans, it is important to bring as many stakeholders to the table as possible, as additional points of view are key to effective informational security (Albrechtsen & Hovden, 2009). Once the plans are generated, it is important to send adequate awareness messaging so that employees understand and act accordingly (Kajzer et al., 2014).

The final lesson learned from this study is that not all industries were affected the same. This study pointed out that the food service and entertainment industries were affected the most, utilities were hardly affected, and the pandemic positively affected the mortgage industry. Forced government closures and fear of going into the public were the culprits for the worst affected industries. Conversely, being stuck at home for long periods caused people to buy new homes or remodel their existing homes, thus increasing the demand for mortgages and refinancing. Although this set of outcomes was pervasive in the COVID-19 pandemic, it does not mean the issues identified here will be the same for the next security issue. For instance, the prevailing "great resignation" wherein thousands of employees are quitting was unexpected and now many organizations are finding themselves floundering trying to adjust. Thus, organizations need to be open-minded and emphasize agility when planning and exploring as many possible detours and disruptions as possible.

RECOMMENDATIONS

Symantec (2014) argues that poorly trained personnel increase the risks of disclosure and loss of sensitive data like Personal Identifiable Information (PII) and

Intellectual Property (IP). A research study from Enterprise Management Associates (Monahan, 2014) reported that 56% of personnel, not including IT and security staff, have never received security awareness training in their organizations. It is clear then that even before the pandemic, cybersecurity was struggling to reach its employees, and that its onset could've only worsened this condition. Rapid changes to business models lead to security risks. Business continuity planning and cybersecurity must, therefore, be intertwined. Table 1 highlights the key security risks viewed during the COVID-19 pandemic.

Internal Security Risks	**External Security Risks**
Remote workers	Supply chain disruptions
Use of personal devices for work-related activities	Event cancellations due to government mandates - i.e. canceling without resource, rent forbearance
Safely switching retail to online	Opportunistic online threats
Onboarding new employees remotely	
Unexpected turnover due to remote working environments	

Table 1: Key Security Risks Associated with Abruptly Changing Business Models

The research herein found that loss of revenue, government mandates/regulations, public safety expense, and business adaptations (model/hours of operation) were the most frequently highlighted aspects of concern during this pandemic. Furthermore, businesses were blindsided by the sheer volume

of obstacles the pandemic caused. These involved continuity planning issues, such as business model changes (i.e., remote work/delivery only) and a myriad of cybersecurity issues ranging from enhanced use of personal devices for remote work to security culture issues (i.e., lack of security monitoring because enforcement is difficult with remote employees). Further, the key factor that separated this pandemic from other unprecedented changes was that organizations were hit with multiple challenges at once. This is illustrated by our study finding that 79% of respondents reported more than two severe impacts. Thus, organizations need to plan not just for one emergency but also for an onslaught of as many continuity/security issues as they can foresee.

To address the general security risks identified herein, we provide the following list of specific actions many organizations failed to implement during the COVID-19 pandemic that made them vulnerable to security threats and continuity issues (Axelos, 2015; Keeper Security, Inc. & Ponemon Institute, 2019; McCarthy et al., 2014). We recommended that organizations actively avoid the behaviors listed in Table 2.

Activities to Avoid	**Why Avoidance Matters**
Failure to back up systems daily	Backing up systems assists in recovering information if systems are compromised
Failure to install or update firewalls and encryption	Firewalls and encryption protect internal information
Using vendor-supplied defaults for system passwords and other security parameters	Serves as an easy in for hackers to reach sensitive information
Using vulnerable, public networks to complete work that uses sensitive information	Public networks such as Starbucks Cafe pose a significant risk of sensitive information being intercepted
Failure to conduct vulnerability tests on networks	Vulnerability tests can catch weak points before they have the chance to be externally exploited

Failure to implement network scanning tools and apps	Utilizing these tools can help companies detect security breaches early and mitigate the damage
Failure to enforce that employees use multifactor authentication in their remote work	Using multi-factor authentication reduces the chances of unauthorized access to networks. According to the Global State of Cybersecurity in Small and Medium-Sized Businesses report, 70% of SMBs reported that their employees' passwords had been lost or stolen in the past year (Keeper Security, Inc. & Ponemon Institute, 2019).
Failure to properly train employees on identifying threats and responding appropriately	Employees are the largest threat to a small organization, and a reported 43% already do not receive regular cybersecurity training; these numbers are likely inflated further by the pandemic rush to remote work (Keeper Security, Inc. & Ponemon Institute, 2019). Training is an essential component of ongoing business continuity planning to prevent security breaches.
Failure to invest in cyber insurance	Cyber insurance helps firms recover financial losses and fund recovery steps like notifying affected parties, attorney fees, investigation, etc. Cyber insurance investment is likely put further on hold due to increased costs to mitigate health risks.
Failure to use properly secured VPNs, patched remote computers, and network perimeter security-protected mobile devices	Using improperly secured VPNs, unpatched remote computers, and mobile devices not protected by network perimeter security can lead to a breach in security.

Failure to follow proper company email and internet protocols	Email and internet misbehavior can create openings for cybercriminals to exploit
Overly depending on a single revenue source (i.e., dine-in service, retail sales, etc.)	This can create a company that is captive to a business line; companies must diversify revenue streams for financial stability
Overly relying on single modality workforce planning	Failing to anticipate employees working from home can create gaps in how to successfully monitor their cybersecurity habits
Depending on face-to-face cultural signals (i.e., security culture signals only conveyed at the workplace)	Remote work lacks face-to-face signals that help enforce cybersecurity culture
Using a single incident continuity mitigation plan	Using a single incident continuity mitigation plan does not prepare employees for a wider set of risk
Failure to train employees on multi-incident continuity planning scenarios	Failing to train employees on multi-incident continuity planning scenarios leaves them unprepared to react
Failure to cross-train key employees	Cross-trained employees are better prepared should a business continuity or incident response plan be activated

Table 2: *Cybersecurity Activities to Avoid*

CONCLUSION

This article used data collected at the height of the COVID-19 pandemic to identify business continuity and cybersecurity blindspots prevalent during the pandemic.

We performed multiple regression analysis and constructed a correlation matrix to assess relationships between loss of revenue and levels of concern for different business activities moving forward. We showed which negative impacts Florida small businesses cited most often, how many prongs of negative impacts hit each business, and which industries cited the most negative impacts. We argued that BCP and cybersecurity should be viewed as intersecting factors for businesses to address, not as separate silos. Thus, for either BCP or cybersecurity planning to be effective, they must be planned simultaneously with input from all involved parties. Another shortcoming of pre-COVID-19 planning identified herein was a predisposition to focus on single-axis attacks/incidents related to one business aspect (such as phishing, ransomware, and crypto-jacking). In this article, we argued that based on the weaknesses identified from the COVID-19 pandemic, businesses should focus on how to mitigate the risks of multi-pronged attacks. We also provided specific recommendations to mitigate such risks.

REFERENCES

Abbate, P. (2020). 2020 Internet Crime Report. *Federal Bureau of Investigation Internet Crime Complaint Center*.

Ahlan, A.R., Lubis, M., & Lubis, A.R. (2015). Information security awareness at the knowledge-based institution: Its antecedents and measures. *Procedia Computer Science*, 72, 361-373.

Albrechtsen, E. & Hovden, J. (2009). The information security digital divide between information security managers and users. *Computers and Security,* 28, 476-490.

Axelos. (2015). Cyber Resilience Best Practices. Norwich: Resilia.

Bisson, D. (2021, May 20). *The State of Small Business Cybersecurity in 2021*. Security Intelligence. https://securityintelligence.com/articles/state-small-business-cybersecurity-2021/.

Bowcut, S. (2021). *Cybersecurity guide for small businesses*. Cybersecurity Guide. https://cybersecurityguide.org/resources/small-business/. (While not cited explicitly, ideas from this article were used throughout the paper)

Burch, G.F., Fezzey, T., Reid, R., & Batchelor, J.H. (in press). Business continuity concerns during the COVID-19 pandemic. *Information System Audit and Control Association Journal* (ISACA).

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, 12(2), 13-21.

Da Veiga, A. (2019). Achieving a security culture. In I. Vasileiou, & Furnell, S. (eds) *Cybersecurity Education for Awareness and Compliance* (pp. 72-100). Hershey, PA: IGI Global.

Escribe, J. (2021). The Changing Trends in Cyber Security. *Information Security Buzz*.

Fichtenkamm, M., Burch, G.F., & Burch, J. (2022). Cybersecurity in COVID-19 world: Insights on how decisions are made. *ISACA Journal,* 2022(2), 1-10.

Kajzer, M., D'Arcy, J., Crowell, C.R., & Striegel, A. (2014). An exploratory investigation of message-person congruence in information security awareness campaigns. *Computers and Security*, 43, 64-76.

Keeper Security, Inc., & Ponemon Institute. (2019). 2019 Global State of Cybersecurity in Small and Medium-Sized Businesses. *Keeper Report*.

Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers and Security*, 28, 509-520.

Kraemer, S. & Carayon, P. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied Ergonomics*, 38, 143-154.

Kujawa, A., Zamora, W., Ruiz, D., Umawing, J., Boyd, C., & Arntz, P. (2020). Enduring from home: COVID-19's Impact on Business Security. *Malwarebytes*.

LeClair, J. (2015). Small Business, Big Threat: Protecting Small Businesses from Cyber Attacks. *Statement for the Record Before the House of Representatives*.

McCarthy, C., Harnett, K., & Carter, A. (2014). A summary of cybersecurity best practices. U.S. Department of Transportation.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, A. (2017). Individual differences and information security awareness. *Computers in Human Behavior*, 69, 151-156.

Monahan, D. (2014). Security Awareness Training: It's not just for Compliance-Research Report Summary. Enterprise Management Associates. EMA.

Network Depot. (2021, March 1). *Top Six Cybersecurity Threats For Your Small Business In 2021*. Network Depot. https://www.networkdepot.com/six-main-cybersecurity-threats-for-your-small-business-in-2021/.

Page, S., & Yeoman, I. (2006). How VisitScotland prepared for a flu pandemic. *Journal of Business Continuity and Emergency Planning*, 1(2), 167-182.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). *Computers and Security*, 42, 165-176.

Penderdast, T. (2016). How to Audit the Human Element and Assess Your Organization's Security Risk. ISACA Journal, 5, 1–5.

Phillips, R., & Tanner, B. (2020). Breaking down silos between business continuity and cyber security. *Journal of Business Continuity and Emergency Planning*. 12(3), 224-232.

Qian, Y., Fang, Y., & Gonzalez, J.J. (2012). Managing information security risks during new technology adoption. *Computers and Science*, 31, 859-869.

Symantec. (2014). Symantec Security Awareness Program: Mitigate information risk by educating your employees.

Torabi, S.A., Giahi, Ramin, & Sahebjamnia, N. (2016). An enhanced risk assessment framework for business continuity management systems. *Safety Science*. 89, 201-218.

Tsohou, A., Karyda, M., & Kokolakis, S. (2016). Analyzing the role of cognitive and cultural biases in internalization of information security policies: Recommendations for information security awareness programs. *Computers and Science*, 52, 128-141.

U.S. Small Business Administration. (2021). Stay safe from cybersecurity threats. https://www.sba.gov/business-guide/manage-your-business/stay-safe-cybersecurity-threats

Virani, R. (2020). Small Businesses, the Flight to Remote Working, & Cybersecurity Report. *Alliant Cybersecurity*.

Weil, T., & Murugasen, San (2020). IT risk and resilience – Cybersecurity response to COVID-19. *IT Professional*, 22(3), 4-10.

Wharton, G. (2019). Hiscox Cyber Readiness Report 2019. *Hiscox*.

Wyss, G., Sholander, P., Darby, J., & Phelan, J. (n.d.). Identifying and Defeating Blended Cyber-Physical Security Threats. *OSTI*.