Determining the Impact of Cybersecurity Failures During and Attributable to Pandemics and Other Emergency Situations

Maria Clare Lusardi
Department of Electrical Engineering and Computer Science
University of Missouri
Columbia, MO, USA
mclntg@mail.missouri.edu

Isaac Dubovoy
Department of Agribusiness and Applied Economics
North Dakota State University
Fargo, ND, USA
isaac.dubovoy@ndsu.edu

Jeremy Straub
Institute for Cyber Security Education and Research
North Dakota State University
Fargo, ND, USA
jeremy.straub@ndsu.edu

***Abstract*—In emergency situations, such as the current COVID-19 pandemic, less immediate concerns such as cybersecurity and long-term economic impact can fall by the wayside. This paper presents a discussion of the impact of cybersecurity issues that occur during and are attributable to pandemics and other emergency situations. This discussion is facilitated by a simulation tool, the Disaster Vulnerability Threat and Impact Simulator System (DVTISS). DVTISS simulates the network structure, security measures, user characteristics and demographics, data, and devices of an organization or region's computing infrastructure. The system is provided input parameters and performs analysis to identify the combined results of numerous different decisions, which are made in concert, to identify the types of vulnerabilities that may be present and the impact of their exploitation. The impacts of system unavailability are considered. This can aid businesses, governments and others in determining the level of prioritization that should be given to cybersecurity considerations. The simulator can also be used for disaster preparedness and planning, evaluating particular response strategies and the evaluation of laws and policies that impact IT decision making during emergencies. This paper uses the DVTISS tool to consider organizational responses to several example emergency situations. It demonstrates the utility of the tool as well as its efficacy for decision making support. Based on the example emergencies, the paper also discusses key areas of vulnerability during emergency situations and their financial, data and system outage impacts.**

Keywords—pandemic, cybersecurity, simulator, economics, policy

I. Introduction

Emergency response presents organizations with a challenge that they have limited resources and time to respond to. During the COVID-19 pandemic response, businesses, governments and other organizations have had to find methods for sustaining income, maintaining operations, and restructuring their operations model for remote work [1]. Changes such as these, during an emergency, can cause cybersecurity to be treated as a concern secondary to the emergency. Cyber-criminals and others with nefarious motives are demonstrably aware of this and have shown that they can take advantage of emergency situations that create cybersecurity vulnerabilities in myriad ways. Phishing scams and fraudulent vaccine and cure scams have circulated widely and organizations particularly under strain, such as hospitals, have been major targets [2, 3].

In an emergency situation, there are many urgent concerns which often take precedence over cybersecurity and long-term economic impact. However, being less urgent, at the moment, does not mean they can be ignored. Thus, there is a need for research regarding pandemic response. To help quantify the cybersecurity risk, this paper presents the Disaster Vulnerability Threat and Impact Simulator System (DVTISS). This simulator is derived from a pandemic simulator [4] and uses pandemic data, as well as network data, security estimates and user demographics, to estimate how many devices on a network are likely to be compromised by cyber-attacks over a user provided length of time. DVTISS takes many different inputs and can, therefore, be used to model a variety of possible policy scenarios. In this paper, the use of DVTISS to model both a public policy scenario, school closings, and a private policy scenario, business closings, are discussed. With this information, organizations can have a better understanding of the risks they face and plan accordingly.

II. Background

This section provides background in several key areas which provides a foundation for the current work. First, cybersecurity during the COVID-19 pandemic is discussed. Then, policy impact is considered. Finally, the use of simulation for policy analysis is reviewed.

A. Cybersecurity

In the wake of the COVID-19 pandemic, there has been a rush to measure the impact of the disease on all aspects of life, including its impact on computers and computer networks. In late June of 2020, researchers from the United Kingdom [2] performed a study of cyber-attacks in the U.K. that had a connection to COVID-19. They found that many reports had been made of scams where attackers impersonated trusted authorities and organizations, such as the World Health Organization. They also identified attacks against support platforms, and fraudulent advertising for personal protection equipment and COVID-19 cures.

978-1-7281-8243-8/20/$31.00 ©2020 IEEE

These scams have targeted the general public and those who have transitioned to working remotely. Attacks are also often timed to immediately follow major events and policy announcements. [2] Certain types of organizations, which have been put under strain due to the pandemic, have been targeted by cyber-criminals. Hospitals, especially, have been common targets for ransomware. The Washington Post reported that attacks have impacted health institutions all over the world, from the Champaign-Urbana Public Health District in Illinois to a university hospital in the Czech Republic. In some cases, these attacks have halted operations for as long as three days and forced hospitals to pay as much as $300,000. These strains have caused some hospitals to turn away patients [3].

On September 17, 2020, the first death attributable to a ransomware attack occurred when a patient died after being rerouted to a different hospital due to an ongoing ransomware attack at the Duesseldorf University Hospital [5]. A Nigerian cybercrime group, Scattered Canary, has targeted unemployment agencies in several states in the U.S. via fraudulent accounts, stealing social security numbers and other personal information so that they can receive unemployment benefits before the intended beneficiaries even file a claim [6].

Schools that have turned to remote instruction have faced problems with video conferences being hijacked. The FBI reported that it, "has received multiple reports of conferences being disrupted by pornographic and/or hate images and threatening language" [7]. Cyber-criminals appear to be taking advantage of the current crisis to launch especially large attacks, and many of society's most critical institutions are finding themselves unprepared.

B. *Impact on Policy*

Since most decisions during COVID-19 are unprecedented in modern history, decision-makers must be incredibly well-informed. The impact of the virus has affected every sector of the economy; furthermore, the need for research related to the outcomes of different political decisions has not been this great in decades [8]. Only a few disasters are likely to cause as much disruption to both local and global infrastructure as COVID-19 has caused. Efforts to reduce the number of COVID-19 cases have led to drastic policy and societal changes. The closure of educational institutions and businesses should be a cause of concern. Changing major institutions quickly can have unintended consequences if the policies are not carefully considered. For instance, suppose there is an enacted policy that regulates the price of rent, but this policy leads to a decrease in innovation in the community. Therefore, it is beneficial to learn more about potential consequences before enacting policy. The public's health should be of great priority during a pandemic. However, if other aspects of the economy are not pondered, then there could be significant repercussions stemming from new policies.

Simulation can be used to equip decision-makers with information on cybersecurity risk to enable them to craft better short and long-term policy. If there are two policies that appear to have similar results and one of the possible policies leads to a much higher cybersecurity risk, then a policy that was seen as similar to the other policy is in fact clearly different. Analysis enables decision-makers to see what possible outcomes could be before they enact a policy.

C. *Use of Simulation for Policy Analysis*

Simulation can have a key role in preparing for and responding to an emergency situation, such as a pandemic [9]. In many cases, some or much of the information that is required to make decisions in response to a crisis is not be known at the initiation of the response. Crisis response may start with an observation or report. Response, thus, may be triggered by a report of an incident itself or something that occurs because of the incident. For purely cyber incidents, the report may be of abnormal behavior or diminished system functionality. Investigation may be required to determine the incident's exact nature and extent. Initial response activities may be required even during the initial investigation.

Decision making with limited information or possibly inaccurate or changing information is inherently problematic. Ideally, decisions would be made with all of the information and based only on accurate information; however, in many cases the best available information must suffice. When dealing with limited or changing information, decisions should be evaluated under multiple scenarios to make sure that they will perform sufficiently well under multiple possible values of unknown, changing or inaccurate information. Using a probabilistic decision model [10] which may include elements of game theory, adversarial risk analysis [11] and algorithmic game theory [12] aid in making decisions that will work well under multiple circumstances.

Simulation systems can be used to both respond to and prepare for emergency situations. A simulation system can be used to conduct 'table top' exercises by evaluating the results of policy decisions through changing simulator parameters. The Netherlands [13] demonstrated the effectiveness of such a simulation-based exercise with a scenario that had over 100 sub-plots and involved numerous government agencies.

III. Discussion of Simulator

DVTISS works in conjunction with a previously developed pandemic simulator [4], the Decision-Making Support System (DMSS). If DVTISS is used with DMSS, data from DMSS is automatically sent to DVTISS and the user is prompted to input additional data necessary for DVTISS. The input data needed for DMSS and DVTISS, and why it is needed, are discussed in the following subsections.

A. *Explaination of Input*

This section explains the data necessary to operate DVTISS. This data is supplied from DMSS and the user. The accuracy of this simulator, as well as the accuracy of any policy comparisons made with this simulator, heavily depends on the quality of data that is inputted.

DVTISS relies on a considerable amount of data from DMSS. This is depicted in Figure 1. First, DVTISS reads the selected population control method, and work and school restrictions for each age group from DMSS. The population control method can consist of quarantining different individuals based on different factors such as whether a person is symptomatically sick, above a certain age, has a medical

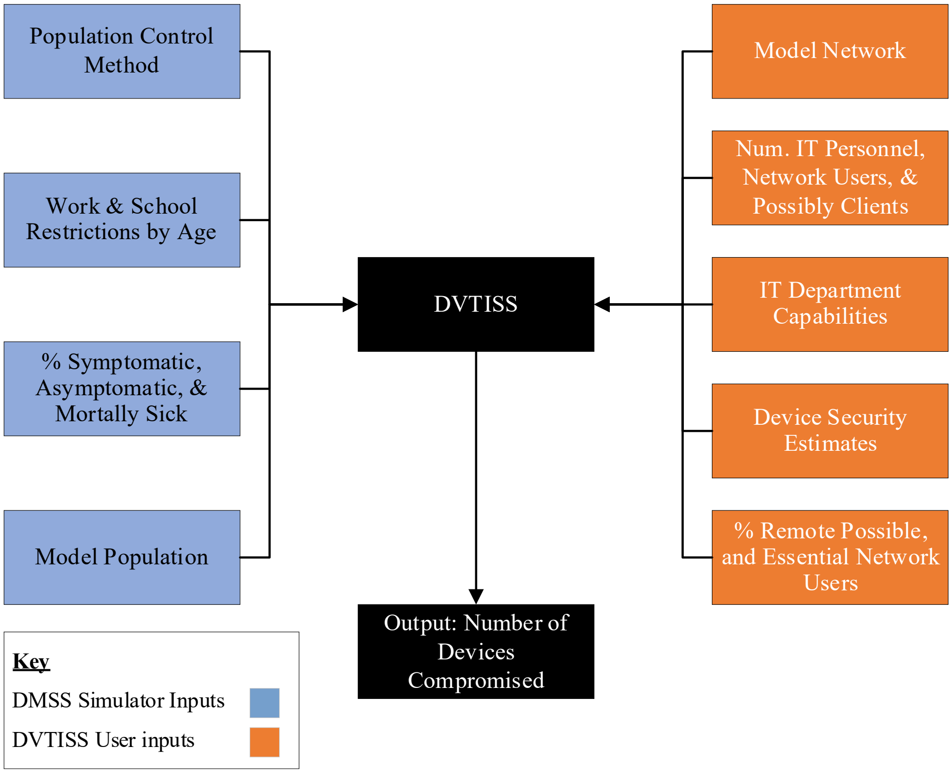
Population Control Method
Work & School Restrictions by Age
% Symptomatic, Asymptomatic, & Mortally Sick
Model Population
DVTISS
Output: Number of Devices Compromised
Model Network
Num. IT Personnel, Network Users, & Possibly Clients
IT Department Capabilities
Device Security Estimates
% Remote Possible, and Essential Network Users
Key
DMSS Simulator Inputs
DVTISS User inputs

Figure 1. DVTSS Inputs Model.

condition, or is generally at increased risk. Population control methods can also be set to affect the entire population with shelter-in-place mode (to simulate complete lockdowns) and reduced contact mode (to simulate social distancing policies). To simulate no change in policy, the no restriction mode can be selected. Work and school restrictions stipulate whether a given age group is allowed to participate in those activities in-person. If that is not allowed, then they will be counted as either remote working, unemployed, or remote learning depending on the particular setting. Altering these values can be used to simulate differences in policy.

DVTISS uses the same user population model that DMSS produces and reads who is infected, mortally sick, and asymptomatically sick during each round of the simulation. This is used to calculate the number of remote workers, the demand on organizations such as hospitals and schools, and the number of people who must be removed from the simulator due to succumbing to mortal sickness. Because of the need for this data, it is impossible to run DVTISS without also running DMSS.

The network model DVTISS uses is entirely based on user input. Users input the number of devices distinguished by type (desktop, laptop, mobile, etc.), platform (Windows, Mac, Linux, etc.), purpose (infrastructure or personal), and ownership (company or private). The user can also supply information on how many company devices can be used remotely, what kind of networking equipment is used to allow remote networks to connect (virtual private networks or a remote control system), and how much time it is estimated that devices spend on home, work, and public networks. This information is used to calculate how much a particular device is exposed and vulnerable to attack.

Security details are another important user input. This includes estimates of the security of individual devices, networks, and the capabilities of any information technology (IT) personnel who work with the model network. Device security can be specified by type, platform, and connection (wired, wireless, or VPN), and network security can be specified by type (company, home, or public). IT capabilities which can be specified include the time spent monitoring the network, and the percent chance an attack will be recognized. IT capabilities can be hampered if the client capacity level setting is exceeded, if there is an excess of remote employees requiring IT support, or if IT members, who are also members of DMSS's model population, become mortally sick and must be removed from the simulation. Together, these estimates project attacks which may be stopped before impacting devices on a network.

Calculating the human effect on cybersecurity requires data from both simulator systems. Members of the model population can play five roles, network user, co-user, attacker, defender, or client.

Network users can be employees, students, or anyone who is using devices that are connected to the model network. Network users have three possible work statuses: in-person, remote, or unemployed.

Work status depends on the population control method and the input percentage of critical and remote possible network users. If unemployed, they are effectively removed from the network user group.

Co-users are those who use devices on the network, but not for the network's intended purpose. An example would be the child or spouse of a remote worker using the worker's laptop for schoolwork or games.

There are many security variables which can be set for network users and co-users. These include percent phishing vulnerability, average rate of downloads, and percentage chance of password breach.

Attackers are those launching attacks against the network. The number of attackers in the simulation and their individual efficiency depends on their work status (in-person, remote, or unemployed).

Defenders are IT personnel for the network in question. Their number and effectiveness also depend on pandemic factors.

Clients rely on the network for services but are not directly connecting to its infrastructure. This number can be set to a default percentage, but in a hospital or school mode the number of clients depends on the number of people symptomatically sick or the number of people participating in school remotely, respectively.

Not all members of DMSS's model population are guaranteed to be part of DVTISS's model population. These security variables allow DVTISS to account for how user habits impact a network's security.

B. *Explaination of output*

The output of the DVTISS simulator is an estimate of the number of devices successfully compromised by cyber-attacks. In the context of the simulation, compromised does not mean the device is completely unfunctional, rather it means that attacks could be launched from it, thus increasing the security risk of all devices connected to it. This information is further broken down by device type, platform, purpose, and ownership. Though the provided numbers are estimates, repeated runs of the simulation at multiple time stages can provide useful data when compared with simulator results from different settings of variables. To demonstrate the simulator, data on population age distribution for different careers was used to compare the cybersecurity risk for a network with younger, average, and older age demographics. Quarantine symptomatic restrictions were used, meaning that any person who is found to be symptomatically sick in DMSS is either remote working or unemployed in DVTISS. Group variables are set to average values based on census data. Phishing susceptibility is set to gradually decrease as age increases (though this is not necessarily an accurate representation of the actual risk levels – other settings will be discussed subsequently). All other values are set to defaults. The simulated time period was two consecutive 90-day periods. The results of this simulation are shown in Table I.

TABLE I. QUARANTINE RESTRICTIONS EFFECT IN TERMS OF THE PERCENTAGE OF DEVICES COMPROMISED.

Time (days)	**Age**		
	Young	***Average***	***Old***
First 90	61%	60%	60%
Second 90	85%	84%	84%

The similarity of the data across all three trials indicates that worker age, under these settings, may not have a great impact on cybersecurity risk. However, this output was generated with inputs that may not be reflective of a particular environment. Altering these estimates could potentially produce very different results.

To illustrate this difference, a second example compares the effects of changing user security variables. In the first condition, phishing susceptibility gradually increases as age increases. In the second condition phishing susceptibility gradually decreases as age increases. In the third condition, all user security variables (percent phishing susceptibility, percent breach chance for passwords, percent unit time online) are set to 100% across all age groups and working statuses. In short, this indicates a near worst possible case for user security. Worker age distribution was set to average values based on census data. All other values are the same as those that were used for the simulation that produced the data presented in Table I. The results of this second simulation are shown in Table II.

TABLE II. USER SECURITY EFFECT IN TERMS OF THE PERCENTAGE OF DEVICES COMPROMISED.

Time (days)	**Security Settings**		
	Condition 1	***Condition 2***	***Condition 3***
First 90	60%	60%	82%
Second 90	84%	84%	95%

The similarity of the data between conditions 1 and 2 shows that any one given variable may not have a very large impact on overall network security. However, changing some inputs or input combinations, as shown in condition 3, can have a considerable effect on the results.

IV. ANALYSIS OF SCENARIOS

To illustrate common impacts of pandemic response, this paper analyzes two policy scenarios, one public and one private, to discuss the effects they have both on policy and cybersecurity. Then how DVTISS could be used to simulate such impacts and provide useful information is discussed.

A. *Public Policy: School Closings*

In the COVID-19 pandemic, the closure of almost all public and private educational institutions, at all levels – from kindergarten to graduate schools – has occurred at various times. The closure of sectors related to education, such as day-cares, tutoring centers, and think-tanks has also occurred. The policy analysis leading to these decisions, as well as their impact on subsequent policies and cybersecurity issues are now discussed.

Policy: Social distancing, the act of separating oneself from other people (usually at least six feet apart), has become commonplace both within societal norms and public and private regulations to reduce the spread of disease [14]. As it is nearly impossible, in the current educational setting [15], to achieve this, educational institutions around the world have either closed completely or transitioned to having students learn online from home. These policies will have a great impact on society for years to come.

At the university level, these closures have impaired the advancement of many areas of scientific research [16]. For secondary schools, closures have increased dropout rates [8]. Dropout rates are proven to cause severe long-term economic impact on the individual, which harms society [17, 18].

For families of primary and secondary school aged children, these closures have required parents to stay home from work in order to care for their children during the day [19]. Parents caring for their children during the day has caused an increase in unemployment, as these childcare responsibilities make it difficult for many parents to continue their jobs [20]. This change is also likely to lead to an increase in child abuse [21], which has been shown to result in an increase of lifetime costs in healthcare, productivity, and education over the course of these children's lives [22]. Therefore, education has been shown to be crucial for the success of the current generation as well as future generations.

Cybersecurity: To effectively educate students remotely, cybersecurity concerns must be addressed. An attack could result in students not having access to instruction, teachers being unable to deliver instruction, or instruction being continuously interrupted via hijacking of online meetings. System insecurity makes effective teaching almost impossible. Simulating this scenario accurately allows school officials to plan for these challenges, thus limiting their impact and enabling students to receive the best education possible under these circumstances. To simulate this, the population control method can be set so that no age groups are permitted to attend school in-person. The DVTISS simulator can also be set to school mode so that all people in the population model attending school remotely will be counted as clients. However, depending on how remote learning is implemented, students could also be considered network users. For example, if a school provides school-owned devices to students and allows students to connect directly to the school's network, it would be more accurate to consider the students as network users rather than clients. User security estimates could also be altered to account for possible vulnerability of younger populations of students. Another possible set of variables to alter would be the number of school-owned vs. privately-owned devices that students use, the amount of time spent on remote learning, and what security measures are put in place.

B. Private Policy: Business Shutdowns

Policy: Social distancing efforts have also led to businesses closing down [23]. Many, if not all, sectors of industry have been affected by this. Arguably one of the most severely impacted industries, since the COVID-19 pandemic began, is the recreation and entertainment sector [22]. The entertainment industry has seen the use of venues that used to hold hundreds, and sometimes thousands of people, become virtually nonexistent. The closure of these venues has resulted in the loss of livelihood for many of those who worked there [20]. The transportation industry, including tourism, has also been forced to alter operations to an extent that has has not been seen since World War Two [20]. The impact of these shifts in industry operations, imposed by policy and societal changes, will lead to a decrease in tax revenue for the government [24]. This decrease in revenue will make supporting the current fedral and local budgets much more difficult. These are just a few examples of the detrimental effects that COVID-19 is having on the economy.

Cybersecurity: A business shutdown can be modeled in DVTISS by adjusting the percentage of workers who are critical and the percentage that can work remotely. DVTISS also takes into account the number of remote-possible devices a company has when making calculations on how many company and privately owned devices are on the network. A cybersecurity failure could cause large numbers of employees to be unable to work. Particularly, a compromised infrastructure device (such as a web server or network equipment) can completely paralyze company operations.

V. Conclusions

COVID-19 has been shown to have numerous detrimental effects on society. The potential economic effects of policy changes show that careful consideration must be given to fields beyond just public health. This makes DVTISS a useful tool, as it provides projections, in this time of rapid change, for evaluating the impact of policy changes on cybersecurity. Making careful considerations not only benefits the short-term economy, but it also benefits society as a whole in the long-term. Further exploration into possible usages of DVTISS and policy changes is needed to ensure multiple perspectives are considered. In this way, negative cybersecurity and economic consequences can be limited while a principal focus on protecting public health remains.

Acknowledgment

This research was partially supported by the United States National Science Foundation (NSF award # 1757659) and the NDSU Challey Institute for Global Innovation and Growth.

References

[1] "COVID-19: 10 tech trends getting us through the pandemic | World Economic Forum." https://www.weforum.org/agenda/2020/04/10-technology-trends-coronavirus-covid19-pandemic-robotics-telehealth/ (accessed Jun. 14, 2020).

[2] H. S. Lallie *et al.*, "Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic," pp. 1–20, 2020, [Online]. Available: http://arxiv.org/abs/2006.11929.

[3] J. Marks and T. Riley, "The Cybersecurity 202 : Hospitals face a surge of cyberattacks during the novel coronavirus pandemic," *PowerPost*.

[4] J. Straub, "Pandemic Simulator Decision Making Support System," Submitted for publication in SoftwareX, 2020.

[5] C. Cimpanu, "First death reported following a ransomware attack on a German hospital," ZDNet, pp. 16–17, 2020, [Online]. Available: https://www.zdnet.com/article/first-death-reported-following-a-ransomware-attack-on-a-german-hospital/

[6] C. Hassold, "Scattered Canary Cybercrime Ring Exploits the COVID-19 Pandemic with Fraudulent Unemployment and CARES Act Claims," pp. 25–27, 2020.

[7] "FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic," *Fed. Bur. Investig.*, 2020, [Online]. Available:

https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic.

[8] M. Nicola et al., "The socio-economic implications of the coronavirus pandemic (COVID-19): A review," International Journal of Surgery, vol. 78. Elsevier Ltd, pp. 185–193, Jun. 01, 2020, doi: 10.1016/j.ijsu.2020.04.018.

[9] J. Straub, "Using Simulation to Understand and Respond to Real World and Cyber Crises," submitted for publication in Information Technology Applications for Crisis Response and Management, IGI Global.

[10] C. W. Chen and C. P. Tseng, "Default risk-based probabilistic decision model for risk management and control," Nat. Hazards, vol. 63, no. 2, pp. 659–671, Sep. 2012.

[11] R. Insua and J. R. & D. Banks, "Adversarial Risk Analysis," J. Am. Stat. Assoc., vol. 104, pp. 841–854, 2009.

[12] T. Roughgarden, "Algorithmic Game Theory," Commun. ACM, vol. 53, no. 7, 2010.

[13] I. Helsloot, "Bordering on Reality: Findings on the Bonfire Crisis Management Simulation," J. Contingencies Cris. Manag., vol. 13, no. 4, pp. 159–169, Dec. 2005.

[14] R. Baldwin and B. Weder, "Economics in the Time of COVID-19," London, UK: CEFR Press, 2020.

[15] E. Dorn, B. Hancock, J. Sarakatsannis, and E. Viruleg, "COVID-19 and student learning in the United States: The hurt could last a lifetime," McKinsey & Company, 2020.

[16] A. J. Salter and B. R. Martin, "The economic benefits of publicly funded basic research: A critical review," Res. Policy, vol. 30, no. 3, pp. 509–532, Mar. 2001, doi: 10.1016/S0048-7333(00)00091-3.

[17] C. R. Belfield and H. M. Levin, "The Economic Losses from High School Dropouts in California," 2007. Accessed: Aug. 29, 2020. [Online]. Available: www.lmri.ucsb.edu/dropoutsPhone:805-893-2683.

[18] H. Lempel, R. A. Hammond, and J. M. Epstein, "Costs of School Closure," 2009. Accessed: Aug. 29, 2020. [Online]. Available: https://www.brookings.edu/wp-content/uploads/2016/06/0930_school_closure_presentation.pdf.

[19] G. Gallacher and I. Hossain, "Remote Work and Employment Dynamics under COVID-19: Evidence from Canada," Can. Public Policy, vol. 46, no. s1, pp. S44–S54, Jul. 2020, doi: 10.3138/cpp.2020-026.

[20] M. R. Keogh-Brown, S. Wren-Lewis, W. J. Edmunds, P. Beutels, and R. D. Smith, "The possible macroeconomic impact on the UK of an influenza pandemic," Health Econ., vol. 19, no. 11, pp. 1345–1360, Nov. 2010, doi: 10.1002/hec.1554.[21] S. Galea, R. M. Merchant, and N. Lurie, "The Mental Health Consequences of COVID-19 and Physical Distancing: The Need for Prevention and Early Intervention," JAMA Internal Medicine, vol. 180, no. 6. American Medical Association, pp. 817–818, Jun. 01, 2020, doi: 10.1001/jamainternmed.2020.1562.

[22] X. Fang, D. S. Brown, C. S. Florence, and J. A. Mercy, "The economic burden of child maltreatment in the United States and implications for prevention," Child Abus. Negl., vol. 36, no. 2, pp. 156–165, Feb. 2012, doi: 10.1016/j.chiabu.2011.10.006.

[23] S. Parrott et al., "CARES Act Includes Essential Measures to Respond to Public Health, Economic Crises, But More Will Be Needed," Cent. Budg. Policy Priorities, 2020, doi: 10.2307/resrep23736.

[24] A. Hevia, Constantino and Neumeyer, "A perfect storm: COVID-19 in emerging economies," COVID-19 in Developing Economies, Apr. 21, 2020. https://voxeu.org/article/perfect-storm-covid-19-emerging-economies (accessed Aug. 29, 2020).