
This article is © Emerald and permission has been granted for this version to appear here: http://westminsterresearch.westminster.ac.uk/

Emerald does not grant permission for this article to be further copied/distributed or hosted elsewhere without the express permission from Emerald Group Publishing Limited.

The final, published version in Journal of Business and Industrial Marketing, DOI: 10.1108/JBIM-10-2020-0455, 2022 is available at:
https://doi.org/10.1108/JBIM-10-2020-0455

This manuscript version is made available under the CC-BY-NC-ND 4.0 licence https://creativecommons.org/licenses/by-nc-nd/4.0/

The WestminsterResearch online digital archive at the University of Westminster aims to make the research output of the University available to a wider audience. Copyright and Moral Rights remain with the authors and/or copyright owners.

Abstract

Purpose

COVID-19 has affected most business activities, including technology-based business. The higher the business vulnerability rating, the greater the impacts. After identifying three dimensions of vulnerability (exposure, business sensitivity, and response capacity), this research determined the potential components and indicators of the vulnerability of technology-based businesses.

Design/methodology/approach

Using the indicator approach, a comprehensive vulnerability model was developed for assessing the vulnerability of the technology-based business against COVID-19.

Findings

In this study, COVID-19, as a biological threat and an exogenous shock, was considered the exposure dimension. Business characteristics, job characteristics, business owner-manager demographics, product, and supplier characteristics were identified as the sensitivity dimension, while resources, human capital, technological capitals, social capitals, institutional capitals, infrastructures, management capacity, and supply chain capabilities were defined as the adaptive business capability or response capacity. To determine vulnerability and response capacity against exogenous shocks and a pandemic crisis, our framework can act as a useful checklist for managers and owners of technology-based businesses.

Originality/value

Research on the COVID-19, especially in the technology-based business, is still at the emergent stage. This study is a pioneering effort to review the literature on business vulnerability and provide a framework to reduce business vulnerability using the indicator-based approach.

Keywords: Business Vulnerability; Exposure, Business Sensitivity; Business Response Capacity; Indicator-Based Approach
1. Introduction

Detecting business vulnerabilities is one of the main pillars of strategy and public policy (Cowan & Wright, 2016). Business’s vulnerability to crises and disasters, as a growing field, has been concentrated on by researchers and academics, both from theoretical and experimental points of view (Song et al., 2016). Such interest was largely driven by escalating business vulnerabilities; both external, such as legislative and environmental vulnerabilities, and internal, such as financial and internal business-process vulnerabilities (Eltantawy, 2016). Crises and disasters may heavily affect businesses’ various aspects, including direct physical impact, human impact, interruption to lifeline services, delays and increased costs for repairs, reduced delivery performance from suppliers, and potential changes in customer purchasing behavior (Dalziell, 2005).

COVID-19 is unique and unprecedented considering its three simultaneous factors: 1) widespread infection 2) mortality high rate, and 3) lacking cure (Krishnamurthy, 2020). Most countries could restrict this pandemic by limiting human activities, which affected economic affairs negatively (Sharma et al., 2020). Researchers and economists agree that COVID-19 has affected all economies heavily, resulted in recession, and has decreased inter-country product, investment, human interaction, and temporary lockdown (Barua, 2020).

COVID-19 is the “Black Swan” that makes businesses vulnerable to unnatural external forces (He & Harris, 2020). The frequency and intensity of recent events have made studying disasters a necessity, in particular for risk mitigation and rapid recovery of businesses (Morrish & Jones, 2020). To accomplish their mission, owner-managers are forced to regularly assess their business vulnerabilities to potential threats and risks, particularly those who work against vision and object accomplish, and thus make themselves ready for adaptation to external and internal environments using the best possible strategies. According to Angeon & Bates (2015), the factors that increase vulnerability during adverse shocks hamper long-term development.

Up to now, 19,265,000 persons are infected with COVID-19, and 885,000 persons have passed the way (Worldometers, 2020). According to the International labor organization (ILO) forecast, 195M person will lose their jobs because of COVID-19 by the 2020 2nd quarter (ILO, 2020). By April 23, 26.5M worker lost their jobs in the US (Lambert, 2020). Also, according to Global Data, COVID-19, in 2020, will affect the
high-tech sector more than any other sector. In terms of a 17-section report, Global Data have indicated the short- and long-term impacts of COVID-19. One section is devoted to technology, media and communication, and leading companies. The report claims that these sections will be affected negatively, among which the Information Technology (IT) sector will face the darkest long-term horizon (Global Data, 2020).

To save their business against COVID-19, most companies have relied on technology. Meanwhile, its effect on technology-based businesses is delicate since while technology is a widespread sector, the technology-based business isn’t affected similarly (Schaefer et al., 2020). While technological entrepreneurship is gaining momentum and technology-based businesses are getting more attention, research-oriented knowledge is still limited (Bailetti et al., 2012). Considering that technology-based entrepreneurship is still an infant, thus many corners of which aren’t discovered (Peng & Zhang, 2008). Given that in many countries, technological businesses play a major role in economic growth and are encouraged as a competitive advantage and job creation (O’Regan & Sims, 2008), their sustainability and continuity are important. The business should be sustainable in the face of internal and external perturbations and vulnerabilities. Through learning from past experiences of the affected businesses, one can mitigate business vulnerability against future events and disasters, decrease shutdown frequencies, and improve sustainability (Sydnor et al., 2017).

Although vulnerability has been discussed extensively from various spatial-temporal dimensions, there is no universally accepted model or theory (Jamshed et al., 2017). While more researchers are interested in vulnerability assessment methods, they should be modified and integrated into policies (Rana & Routary, 2018). On the other hand, vulnerability is considered an integral element of crises and disasters (Birkmann et al., 2013). The disaster-related literature has disproportionately focused on the vulnerabilities of national and regional analysis units, and the vulnerability of micro-business units has been less focused on (Zhang et al, 2009). Although the vulnerability concept has been embedded in scientific discussions recently, it lacks an accurate clear definition (Lo et al., 2019). Businesses' inadaptability indicates that they are heavily vulnerable to disasters (Davlasherdze & Geylani, 2017). How to define business vulnerability to threats is an open question calling for answers (Song et al., 2016).
Reviewing academic and scientific publications with higher impact factors, it was concluded that vulnerability is an ancient issue, mostly considered by social and natural sciences, while has been embodied to a lesser extent in management, entrepreneurship, and, in particular, tech-based business fields. Also, rare business vulnerability research has focused mainly on climate change and other factors affecting vulnerability. Therefore, to reduce these gaps and due to the COVID-19 epidemic virus, our research seeks to find a framework for the vulnerability of technology-based businesses during COVID-19. Creating a conceptual framework that considers the vulnerability of technology-driven businesses with diverse and complex links is essential to identify policymakers in identifying key components of vulnerability.

This research's first and foremost contribution is designing a model for reducing tech-based businesses' vulnerability, contributing to business survival and sustainability. The proposed framework provides the policymakers and decision-makers with priceless recommendations regarding vulnerability reduction. Vulnerability assessment is a critical component of disaster risk reduction and sustainability field (Zhou et al., 2015). Therefore, this research contributes to sustainability and disaster literature. Given that vulnerability reduction alleviates potential disturbance and promotes resilience (Sheffi, 2005), thus business vulnerability research is linked to resilience literature, which is another contribution of this research. Research objectives are: 1) defining vulnerability and identifying its main dimensions. 2) identifying components related to the vulnerability of tech-based businesses, 3) tech-based business actions to reduce vulnerability, and 4) proposing a conceptual framework for tech-based business vulnerability.

This research begins its work with a vulnerability literature review. Section 2 contributes to the comprehension of the business vulnerability concept and identifies its dimensions. The research methodology is explained in section 3. Reviewing Literature and covering vulnerability-related issues across previous crises and disasters, an indicator approach is employed. Section 4 identifies various components affecting vulnerability's three dimensions: exposure, sensitivity, and adaptive capacity. Section 5 outlines technological entrepreneurial action to reduce vulnerabilities. A conceptual framework is proposed in section 6, based on results obtained in sections 4 and 5. Section 7 presents
the readers with theoretical and practical implications. Undoubtedly, the contributions of this research will pave the way for future research.

2. Literature review of vulnerability

Vulnerability is a concept used in many fields, from economics to psychology, anthropology, and engineering (W. Neil Adger, 2006). The initial tries appeared in risk and disaster management; they were concentrated on engineered structures’ physical resistance, while current works considered vulnerability with characteristics of social and environmental processes (Cardona et al., 2012). The “vulnerability” construct indicates to what extent an organization may be impacted by an event and is defined as how much a natural, economic, or social system is fragile against natural and technological threats (Dalziell, 2005). Vulnerability cannot be regarded independently from hazards. Thus vulnerability is seen as a relative and specific term that always implies vulnerability to a particular hazard (Greiving et al., 2006). Also, Cuevas (2011) defined vulnerability as the extent to which a system is harmed in response to a stimulus. Gallopín (2006) said that vulnerability means a system’s tendency to be affected by harm or potential change or transformation. Many researchers (Turner et al., 2003; Lo et al., 2019; Aleksić et al., 2014; Adger, 2006; Polsky et al., 2007; Smit & Wandel, 2006) consider vulnerability as a tri-dimension system: exposure: to what extent or degree to which systems are exposed to hazard and perturbation, sensitivity: to what extent or degree to which a system is affected or modified, and adaptive capacity: systems capability to adapt to changes and response perturbation.¹

Yan and Zhou (2010) defined vulnerability as a business weakness in quantitative and qualitative aspects or lacking sufficient capabilities to stand any intervention and uncertainty. Perhaps business vulnerability results from the negative impacts, which may affect business responsiveness and its ability to overcome potential barriers (Andrade et al., 2012). The vulnerability construct is defined as a condition that affects a firm’s goal accomplishment dependent upon negative consequences of disturbance (Svensson, 2004). Zhang et al., (2009) presented business vulnerability in four dimensions: labor, supplier, capital, and customer. Also, to define business vulnerability to natural disasters, Song et al., (2016) considered geographical location, economic situation, and critical

¹ - Based on this definition, we worked on our article.
demographic characteristics in terms of tolerating natural disasters. They divided them into four groups: business capital, labor, critical suppliers, and physical location.

The existence of potentially vulnerable points makes the business vulnerable to internal and external threats (Nyanchama, 2005). COVID-19 outbreak, as a global crisis that has affected the globe socially and economically (Giones et al., 2020) has affected technology-based businesses, exploiting their weak points. Dark forecasts, which predict the higher frequency of and more intense natural disasters, focus on local economic activities because small businesses are vulnerable to such events and affect all over the country, given small businesses’ role in job creation (Davlsheridze & Geylani, 2017).

3. Methodology

According to the literature review, to analyze business vulnerability, various metrics were used. To make theoretical concepts operational in the context of vulnerability assessment, three approaches are used for highly diverse systems, as well as spatial and temporal measures: 1) participatory; 2) simulation-model-based; and 3) indicator-based approaches (Nguyen et al., 2016). We used an indicator-based approach in this research.

Indicator-based methodologies are increasingly used in research and studies while being used to support decision-making in terms of disaster risk mitigation (Papathoma-köhle et al., 2019). The indicator approach is useful for monitoring trends and identifying conceptual frameworks (Gbetibouo & Ringler, 2009). It is adopted to create more useful knowledge of the socio-economic and biophysical factors affecting vulnerability (Hebb & Mortsch, 2007).

3.1. Application of the methodology

3.1.1. Reviewing hazards threatening technological businesses

At this stage, by reviewing the existing literature on crises and disasters that have occurred, and the literature on vulnerabilities, one can be aware, to some extent, of the factors that lead to the vulnerability of technology businesses. In this regard, articles related to business vulnerability, improving businesses in times of crisis, as well as articles related to the COVID-19 crisis in the WoS, Scopus, and Google Scholar databases were studied. The criterion for selecting articles was thematic relevance to the present study.
3.1.2. Identifying and classifying vulnerability indicators
By studying the existing literature, indicators of business vulnerability were identified. Then, the indicators were classified into three dimensions of vulnerability (exposure, sensitivity, adaptive capacity) using experts’ opinions.

3.1.3. Weighting to indicators
In the indicator approach, there are two options for weighing indicators. The first option assumes that all vulnerability indicators are of equal importance and therefore gives them equal weights. In the second option, different weights are considered for the indicators. In line with the second option, many methodological approaches have been proposed to compensate for the weight differences of the indicators. Some of these approaches include expert judgment, correlation with previous catastrophic events, and fuzzy logic (Deressa et al., 2008). Given that this study identifies the components of vulnerability and not their ranking, we considered the same weights for the indicators in this study.

3.1.4. Presenting a proposed model
Finally, by reviewing the existing vulnerability models as well as the indicators identified in the vulnerability literature, a proposed framework was presented.

4. Results: Vulnerability Dimensions
According to the literature review, the exposure dimension is caused by environmental-ecological driving forces (Gallopín, 2006; Smit & Wandel, 2006; Greiving et al., 2006; Polsky et al., 2007; Rossignol et al., 2015; Füssel, 2007), social driving forces (Smit & Wandel, 2006; Greiving et al., 2006; Polsky et al., 2007; Füssel, 2007), economical driving forces (Greiving et al., 2006; Füssel, 2007), technological driving forces (Dalziell, 2005; Rossignol et al., 2015, Robertson et al., 2020; Merino, 2016), biological natural driving forces (Dzigbede et al., 2020). COVID-19, in this research, was described as a natural biological threat, and an exogenous shock and other dimensions (social, economic, and technological) won’t be discussed. Two other vulnerability dimensions (sensitivity and response capacity) were divided into the
following components, respectively: 1) sensitivity: business characteristics, job characteristics, owner-manager demographics, product and supplier characteristics, 2) response capacity: resources, human capital, technological capital, social capital, infrastructure, institutional capital, management capacity, and supply chain capabilities.

4.1. Dimension 1: Exposure

Component 4.1.1: Biological Natural Driving Forces - Pandemic Events (COVID-19)

Social distancing, isolation, personal insularity, and travel restriction because of COVID-19 prevalence faced all economic sectors with the labor shortage and deleted many jobs (Nicola et al., 2020). Supply drained and consumption/investment declined led to demand downfall because of the global economic shutdown in anticipation of infection control (Seetharaman, 2020). COVID-19, as a devastating crisis, has affected the global economy (Eggers, 2020) just like previous pandemic infections, including SARS (Pine & Mckercher, 2004) and Flu (Rassy & Smith, 2012), while reviewing SARS and Flue data since 1918, brings us some ideas and information regarding COVID-19 pandemic events, giving weight to the differences, including the following is of grave importance, and will prevent from simple comparison: global prevalence, not being specific to low-middle earning countries, lowering profit rate to its historical minimum, more integration across the world, imposing double effects on supply change, supply and demand decline (Fernandes, 2020). Also, technology-based businesses were affected by these natural biological factors and their exogenous shock. According to Price Waterhouse Coopers (PWC), they experience some difficulties in terms of crisis management, crisis response, workplace, and employees, supply chain and related activities, financial reports, tax and charges, and customers since they didn’t give any point to business uncertainty caused by infection continuance (PWC, 2020). COVID-19, unfortunately, is evolving continuously, the effects of which are unprecedented in terms of speed, intensity, and scope (Yang, 2020).

4.2. Dimension 2: Sensitivity

Component 4.2.1: business characteristics

A business character impacts business function against crisis (Sydnor et al., 2017). Some business characteristics are intangible and are critical for many modern businesses, including tech-driven and knowledge-driven businesses, such that any shortage and
outage makes them vulnerable. Intangible characteristics are brand, organizational
culture, routines, and laws of the important strategic and functional layers (Yan & Zhou,
2010). Business size is discussed extensively as one of the characteristics (Davlasheridze
& Geylani, 2017; Eggers, 2020; Orhan, 2016; Polsky et al., 2007; Song et al., 2016;
Sydnor et al., 2017). While smaller businesses are more flexible and their decision-makers
have closer relationships with their customers and stakeholders such that they have access
to the market’s valuable information, in particular through crises, they face resource
scarcity, including human and financial problems, or even demand decline because of
new competitors. Thus, they will be more vulnerable to internal and external events. So
one can claim that the smaller the business, the more vulnerable it will be to a crisis like
COVID-19 (Eggers, 2020). Compared to the larger companies, smaller businesses
experience greater losses and point to positive dimensions, including irregularity in crises,
of small businesses in developing countries like Singapore. They could implement
recovery strategies after the earthquake because they had their contingency plans.
However, larger businesses are struggling with negative aspects, including a large volume
of business activity, more machinery/tools, and greater expenditure in terms of salary
(Khan & Sayem, 2013). Eggers (2020) counts new businesses as more vulnerable than
older businesses because of lacking confirmed business model, depending on not-totally
known colleagues, and a low rule-observance index. Also, other characteristics include
the number of business locations (Song et al., 2016); economic sectors to which
businesses belong/ industry sector/ type of business/ capital intensity (Song et al., 2016;
Orhan, 2016; Sydnor et al., 2017; Khan & Sayem, 2013; Lo et al., 2019); sales previous/
financial condition before the disaster/ Monthly average income of the firm (Sydnor et
al., 2017; Orhan, 2016; Khan & Sayem, 2013); legal ownership structure/ occupancy
tenure (Sydnor et al., 2017; Orhan, 2016); source of business: inherited-personally
initiated (Khan & Sayem, 2013) are discussed as the important business characteristics
which may be considered to vulnerability.

Component 4.2.2: Owner/Manager/Primary Decision-Makers Demographics

Vulnerability is embedded in the socio-economic trajectories of their primary decision-
makers. Multiple vulnerabilities may arise if the decision-maker's socio-economic
conditions are associated with climate-sensitive business characteristics (Lo et al., 2019).
According to the literature review, owner gender (Lo et al., 2019; Song et al., 2016; Sydnor et al., 2017), education level (Lo et al., 2019; Orhan, 2016; Sydnor et al., 2017), experience, race, ethnicity (Sydnor et al., 2017), manager/supervisor competencies (Yan and Zhou, 2010), and previous disaster experience (Orhan, 2016) are among important factors affecting vulnerability. In experimental models, some are the control, dependent, or independent variables. Some studies claim there is a negative relationship between the female gender and technology entrepreneurial initiative formation (Zapata-Huamaní et al., 2019); according to the OECD, perhaps females are less interested in high-technology than males, while they have a greater tendency to service businesses (OECD, 2012). Facing crises, compared to males, female owners prefer to shut down the business, and to reopen after the crisis disappears. Also, more educated owners continue their efforts and don’t shut the business down, compared to less educated (Sydnor et al., 2017). According to Yan and Zhou (2010), more educated and knowledgeable managers/owners seem to have the quality and efficiency of transferring tacit knowledge to mitigate the business vulnerability, and, thus, a more sustainable business. Given that education level and business preparedness are positively related, thus one can claim that businesses with less-educated owners/managers should gain more knowledge regarding their vulnerability to crises. Also, previous disaster experiences may increase the willingness to engage in preparedness activities, particularly in the long term (Orhan, 2016).

Component 4.2.3: Job Characteristics

4.2.3.1: Job complexity

The complexity of the system is one factor studied by the researchers. Failure is inevitable, whenever the system is complex enough (Robertson et al., 2020). Because of web complexity, portal websites, telecommunication, and e-commerce websites have reported the highest rate of vulnerability across the IT sector, while large and complex systems become more unreliable and more vulnerable through the crisis (Egan, 2007).

4.2.3.2: Interaction between elements of a system

Interaction between elements of a system makes it more vulnerable in crises, such that damage to any element will create a cascade of damages. Also, when new systems are connected, new systems' vulnerability has culminated in the overall vulnerability, and
complexity grows. Thus better management and vulnerability mitigation is accomplished through understanding interaction points and inter-technology/service/system relations (Egan, 2007).

Component 4.2.4: Supplier/Product Characteristics

Repeated and uncommon crises disturb the supply chain and make them more vulnerable to disturbance and greater losses, which can be mitigated through the management of vulnerability-causing factors, including globalization, decentralization, outsourcing, product/process complexity, litigation, sole sourcing, just-in-time manufacturing (Stecke & Kumar, 2009).

Spekman (1988) focused on supplier/product characteristics to strategic vulnerability levels. He considered: product (cost of the service contract, ease of maintenance design, reliability of the product, case of operation, impact on energy utilization, contribution to productivity, warranties); service (amount of pre-purchase information, service response time, dependability, the competence of the salesperson, vendor’s image); experience (experience with a vendor, preferences established by users in the organization, reputation of the supplier, ability to keep a delivery promise); price (price/performance, low price, the total cost of the product); avail (suppliers financial condition, geographic proximity, technical support available, breadth of product lines). Also, Orhan (2016), and Khan & Sayem (2013) focused on the market for the product (regional/local) among the factors affected by the crises.

4.3. Dimension 3: Response capacity

Response capacity stands for a great set of resources, many of which are to a group or nation’s socio-technical and economic development level, that may be turned into either adaptive or mitigative capacity (IPCC, 2007a). Adaptive and mitigative capacities have nearly the same determinants but they differ in their application (Winkler et al., 2007). Mitigative capacity reflects the ability to mitigate the intensity of the natural (and other) disaster (IPCC, 2007a). The adaptive capacity of a system or society indicates its ability to regulate its traits or actions to adapt better to external situation changes (H. M. Füssel & Klein, 2006).
Mitigative capacity depends on viable technological options for decline emissions, policy instruments, institutional structure and the derivative allocation of decision-making authority, the availability and allotment or tools required to ensure their adoption, and the associated opportunity cost of allocating those resources to mitigation, human capital resources, social capital, and the ability of decision-makers to manage information (Yohe, 2001). Adaptive capacity reduces exposure or sensitivity to stresses, whereas mitigative capacity reduces the intensity of the stress itself (Winkler et al., 2007).

Lacking adaptability capacity is an indicator of high business vulnerability to natural disasters (Davlasheridze & Geylani, 2017). Adaptive capacity plays a critical role in the ultimate vulnerability because it defines the size of the effect to a great extent (Moreno & Becken, 2009). Various capital (financial, social, human, knowledge, etc.) affect business vulnerability and resilience (Marshall & Schrank, 2014).

Component 4.3.1: resource unavailability/ scarcity/inability to replace/intense dependency to scarce resources

Previous studies (Eggers, 2020; Miehe et al., 2016; Robertson et al., 2020; Adger & Kelly, 1999) have indicated that resource scarcity is one-factor affecting business vulnerability to crisis. The vulnerability of any group is determined by the availability of resources and, crucially, by the entitlement of individuals and groups to call on these resources (Adger & Kelly, 1999). The negative effect and sensitivity of the community to a crisis depend on the affected resources (Wongbusarakum & Loper, 2011). Across businesses, resource scarcity appears on two levels: 1) no supply, and 2) reduction of supply (Miehe et al., 2016). He also considers the inability to replace the consumed resources as another source of vulnerability. All production and service technological systems depend on viable environmental conditions. User services are condemned to failure in case of unviable environmental conditions and resource unavailability (Robertson et al., 2020).

Component 4.3.2: technology capital

Technology is among those important factors determining a business failure or survival in the face of COVID-19 (Sharma et al., 2020). Technology is one determinant of adaptive capacity to increase resilience and reduce the vulnerability of social systems.
Literature review, following technological items, makes the businesses more vulnerable:

4.3.2.1: New technology/emerging technologies

Emerging technologies, in particular, those in the beta-test stage are vulnerable to failure. Employing new technologies brings about emergent vulnerabilities, or at least prepared the context for unknown consequences, because of mutual unpredictable dependencies. Relying quickly on a novel and emerging technologies makes the larger system, which depends on them, more vulnerable. If the emergent technology tests aren’t completed, making more usage of and depending heavily on them will intensify vulnerability (Egan, 2007). However, using new technologies for higher preparedness for various crises such as COVID-19, hard-working is important (Yang, 2020).

4.3.2.2: Technology development/redundancy

Systems’ new vulnerabilities exist alone with technology evolution (Baek & Kim, 2019). Technology redundancy, as a viable approach to resolving exogenous force-caused challenges, may make businesses more vulnerable (Egan, 2007).

4.3.2.3: Technology maladaptation

Technological shortages make adaptability limited. Thus the more technological challenges, the less the adaptability potential (Cuevas, 2011). Technological adaptation has consisted of two main components: 1) changing the current technologies’ structure, and 2) implementing new technologies. Technological adaptation performed inadequately, threats may enlarge (Merino, 2016).

4.3.2.4: Technology migration

Technology migration is considered one of the technological vulnerabilities and failure points (Robertson et al., 2020).

4.3.2.5: Reverse salient

(Merino, 2016; Robertson et al., 2020; Moreno & Becken, 2009; Thornton et al., 2006; Winkler et al., 2007).
Through crises, the infrastructure of the large technical system becomes critical quickly. Since comprehensive experimenting with services/technologies intended to resolve reverse salient is impossible because of the simultaneous existence and appearance of invention possibility and the need for a social-technical solution (Egan, 2007).

Component 4.3.3: Management Capacity

Managerial measures are one of the adaptive capacity determinants (Egan, 2007; Moreno & Becken, 2009; Polsky et al., 2007).

4.3.3.1: Enterprises’ strategic plans

Enterprises’ strategic plans impact business vulnerability greatly (Yan & Zhou, 2010). Crisis management should be an integral part of the strategic planning processes that companies adopt. To reduce their vulnerability to shocks, business owners need to integrate crisis management with strategic planning processes, prepare detailed contingency plans, define decisional roles and responsibilities, and retain a degree of flexibility. Otherwise, the business is more vulnerable to shocks (Evans & Elphick, 2005).

4.3.3.2: Types of vulnerability management

If the management cannot mitigate vulnerability effectively, damages can’t be identified, evaluated, resolves, and confirmed effectively (Baek & Kim, 2019). According to (Gartner, 2019), the following make businesses more vulnerable: 1-existence of unreported vulnerabilities; 2-trying to fix all identified vulnerabilities; 3-ineffective communication; 4-insufficient remediation resources; 5- fixing only “high” and “critical” vulnerabilities; 6- conceding broad or eternal exceptions; and 7- mitigation without previous planning can be disastrous.

4.3.3.3: Lacking the ability to decide against uncertainties

Entrepreneurs have to make decisions in uncertain conditions since the environment is full of dynamic and uncontrollable forces, and global changes create uncertainty because of which one can act risky (Alvarez et al., 2018). Because businesses are affected by natural forces, including floods and earthquakes, they have to make themselves adapt by
making the right predictions; the entrepreneur, as the owner and manager, should have
the ability to decide against uncertainty (Knight, 1942). Uncertainty affects managers,
founders, and the board of directors’ decision-making, and according to Mintzberg,
anyone who doesn’t understand uncertainty in management can’t comprehend managerial
decision-making (Alvarez et al., 2018). Prevalence of new diseases, such as COVID-19,
as a phenomenon that intensifies uncertainty, makes effective decision making of grave
importance, in particular for mitigating losses caused by uncertainty, since, as noted
(Teece & Leih, 2016), risk-based decision-making is unreal and simple given difficulties
of the global economy. Transformational leadership, behavioral integration, and
comprehensiveness in the decision-making process among members of the top
management team increase the capacity of small entrepreneurial companies to adapt to
environmental changes (Friedman et al., 2016), which absent these factors will reduce
their sustainability and performance.

Component 4.3.4: Financial Capital

4.3.4.1: lack of diverse revenue sources and Flexible business model

If successful companies take their usual path without changing their business model
according to the environment, they will experience failure inevitably (Doz & Kosonen,
2010). While imposing great challenges on all businesses, the COVID-19 crisis gives the
organization a new chance to develop new business models, survive, and decrease
physical contact to the highest possible level through digitalization (Seetharaman, 2020).
Studying business models of fourteen big and prominent firms in the computer and
telecommunication sector, Hacklin et al (2018) identified the business model’s continued
change as one of the success factors of Apple, such that it adapts itself to its environment,
which is full of tension. He continues that some firms try to implement several parallel
models along with the main business model. They will face some challenges; some may
fail since the firm cannot utilize them synergically because the models are operated in
separate firms. In such cases, success requires learning and experimentation.
Implementing parallel models according to previous plans is risky and increases
complexity, utilizing common resources will be more difficult, and, finally, the
organizational function will be hurt (Hacklin et al., 2018). Thus, firms and businesses
should change their business model according to the environmental conditions and crises and consider all aspects of trying to use parallel and secondary models.

4.3.4.2: Lack of financial resources for adapting technology and development

Financial resource availability has been a component of adaptive capacity for investing in developing the primary warning system, adoption-related operations, and technologies (Moreno & Becken, 2009). Creativity and providing customers with novel proposals require financial resources (Eggers, 2020). Emphasizing financial capital and the importance of technology adaption (whether technological systems structure change or implementing new patterns), and also as one factor determining the adaptive capacity of social systems to crises and disasters, Merino (2016): even if technological adaption is possible, it will be ineffective economically without financial resources.

Component 4.3.5: Infrastructure Capital

4.3.5.1: Lack of appropriate infrastructure for digitalization

Digital media usage and distribution grew heavily after COVID-19 (WorldEconomicForum, 2020). Digitalization brings about opportunities for social-economical systems, becoming obvious, especially after the crises and the “Stay Home” protocol (Dannenberg et al., 2020). COVID-19 crisis marked digital communications and services as the elements for social resilience and business survival, for which effective and large digital infrastructure is necessary. Moreover, those companies controlling two or more parts of the value chain by the digital infrastructure are in a better position than specialized independent companies. However, businesses, eventually, will experience lower speeds and greater latency, because of higher demand and, because of which, lower bandwidth quality decline. But supply decline caused by digital infrastructure supply chain disturbance and supplier changes and evolutions makes the situation darker because businesses are challenged (Strusani & Hounghnon, 2020). Thus, the lack of appropriate digital infrastructure makes businesses vulnerable.

4.3.5.2: Damages caused by open innovations and using platforms

four factors make entrepreneurs and entrepreneurship, which act according to open innovations and use open platforms, vulnerable to changes (Nambisan et al., 2018): 1)
business model dependence on platforms and open innovations; 2) access to partner data; 3) access to the creative ideas of others, and 4) apply the acquired strategy on platforms.

Component 4.3.6: Social Capital

Social capital’s role has been considered concerning impact mitigation, adaption, and recovery at individual and collective levels (Meyer, 2018). Social capital facilitates access to various resources through the crisis management cycle; alarming disasters before they occur, information exchange, predicting and procuring tools, financial aids, vulnerability assessment, and other preparedness-related activities. Thus one should consider it as a contributing factor to disaster threats (Han et al., 2019).

Social capital is an effective factor, in particular, for implementing research and development as a strategic network-based capital through explorative learning, which affects technology performance and utilization learning, and finally, business performance. Research and development consortia depend on social capital, given it institutionalizes the mutual common bed over which they interact (Seo, 2020). Research and development coalitions are inevitably vulnerable to many factors, including opportunity seeking, technology shortage, and knowledge protection vs. sharing dilemma which makes costs grow higher (Rauch et al., 2015; Meier et al., 2015; Seo, 2020). The level of discourse-action transition depends on the quality of social networks (Acosta-Michlik & Espaldon, 2008). Social networks should consider this issue.

Against COVID-19 and subsequent stressful and uncertain conditions, Social networks can play a key role in terms of emotional support and information support using modern technologies, all of which can facilitate businesses' performance against the crisis (Giones et al., 2020).

Component 4.3.7: Human Capital

Technologist entrepreneurs can create successful intuitions through their human capital, which leads to fundamental innovations (Marvel & Lumpkin, 2007). Human capital is one of the intangible organizational assets, and is referred to the unique and knowledgeable people of the organization; employing these people can differentiate itself (Johannesson & Jorgensen, 2017). By human capital, we mean explicit and tacit knowledge of organization people; they belong to the company and include experience,
capabilities, learning capabilities, or knowledge creation ability (Delgado-verde et al., 2016). One can define human capital using indicators, including employee capabilities (individual competencies and skills, organization investment in human capital), employee satisfaction (employee’s emotional and sensational expression), and employee endurance (maintaining employees) (Moon & Kym, 2006). Merino (2016) claims academic education, public information, and specialty to be among the important features of human capital. Emphasizing human capital and education level’s important role in accepting and developing technology through the crises, they indicate that deciding on solutions or technological responses or choices is impossible without them.

4.3.7.1: Employee unavailability

Firms losing their human resources need a longer time to recover (Khan & Sayem, 2013). Employee loss is one of the crisis consequences and includes personal and family problems as a result of a crisis, or they may go to work, and considering that employees are critical for organizational success, operational capacity, and also a business improvement, companies will experience great damages if employee loss occurs or absence (Sydnor et al., 2017). Employee replacement easiness, especially during a crisis, is an important factor affecting vulnerability (Lo et al., 2019). Losing key employees, especially leaders who have specialist knowledge, and lack enough good employees (because of infections, death, injury, etc.) influences organizational responsiveness and aftermath recovery greatly. Organizations should know that employees consider themselves, their families, and friends’ security as a priority. Employee availability is plausible only then this need is served (Dalziell, 2005). Failing to serve basic needs will worsen the situation and may continue to collapse (Lazarov, 2020). Since has the public information and specialized experience necessary for technological entrepreneurship and radical innovation (Marvel & Lumpkin, 2007), employing empowered labor will be difficult. Training new employees are time- and money-consuming, especially during crises (Morrish & Jones, 2019).

4.3.7.2: Knowledge, skill, and experience shortage

To accomplish technological entrepreneurship, various kinds of knowledge are required: 1) knowledge of ways to serve markets; 2) knowledge of customer problems;
3) knowledge of markets, and 4) knowledge of technology. At the same time, the experience is of grave importance regarding service/product development for technology-based firms (Marvel & Droge, 2010). Also, Verrest (2013) emphasizes special skills and believes that simpler skills are more vulnerable and that developing special skills requires common education. Regarding COVID-19, Yang (2020) points to the main and important role of specialty in identifying and curing COVID-19 and for politicians and technical elites to distribute and allocate emergency aids. Yang (2020) says lacking the special skills against prevalent conditions leads to more failures.

4.3.7.3: Risk-taking/willingness and ability to change

Willingness to change is one characteristic of adaptive capacity against social systems’ failure, i.e., social vulnerability comes into existence when there is no willingness to change (Wongbusarakum & Loper, 2011). Risk attitude and self-sufficiency play an important role in personal adaptation and mitigation of disaster risk (Poussin et al., 2014). Entrepreneurship (e.x. technology-based firms) can search for new opportunities in the face of uncertainty by employing special actions, including risk-taking and Proactiveness (Runyan et al., 2008), thus they can survive crises.

Component 4.3.8: Supply Chain Capabilities

To reduce vulnerability and increase supply chain resilience to disruptions and crises, supply chain capability is essential (Ekanayake et al., 2020). Supply chain faults become evident in the face of sudden disruptions and events, including political and economic crises or biological disturbances (Ponomarov & Holcomb, 2009). COVID-19, as a crisis, disrupted many supply chains (Kirk & Rifkin, 2020; Sharma et al., 2020).

4.3.8.1: Supply chain disruption

Since the beginning of the COVID-19 crisis, businesses is facing great challenges, including (Sharma et al., 2020):

1- Demand-supply challenges: one of the important challenges some sectors are facing is supply uncertainty. However, technology firms faced demand’s sudden rise.

2- Resilient supply chain challenges: as COVID-19’s power to challenge the supply chain grows, more challenges are revealed regarding the necessity of a resilient supply
Using blockchain-based technologies, artificial intelligence, and collaboration between industries and competitors improve supply chain resilience.

3- Technological challenges along COVID-19: companies differ in terms of technological preparedness. Security breaches, besides technological preparedness, are one of the common concerns.

4- Sustainable supply chain challenges: COVID-19 forced companies to pay more attention to the social, economic, and environmental aspects. Employee welfare and suppliers are important for the company since companies without sustainable approaches cannot fight the virus’s impacts.

4.3.8.2: Financial disruption across the supply chain and customer network

Financial problems, including supplier bankruptcy, are among the factors disrupting the supply chain (Carvalho et al., 2019), which make businesses vulnerable (Song et al., 2016).

4.3.8.3: Consumer behavior-changing

Natural disasters, including earthquakes, storms, and epidemics such as COVID-19, change or modify customer behaviors (Sheth, 2020). Trying to defeat the virus, customers change their behavioral patterns and respond variously to the actions of brands. Future buying decisions are made under the pressure of brands’ reaction to COVID-19, such that some consumers shape their perception of a brand according to how they perceive an inappropriate reaction to the crisis. If customers perceive the brand’s reaction as self-servicing or don’t sacrifice, they will become vulnerable (Kirk & Rifkin, 2020).

4.3.8.4: Dependence on supply chain members

To determine to what extent a business can survive without its supplier, Lo et al (2010) used a variable called Inter-business dependence and introduced it as a factor making business vulnerable. A company faces threats if resource control is passed to its partner, such that it perceives itself as dependent on its partner. The fewer the buyer choices, the more vulnerable the business (Spekman, 1988).

Component 4.3.9: Institutional Capital
Institutional capability as one component of adaptive capacity is effective in reducing vulnerability. Institutional capability is represented by the political leadership and governance structure, and disaster prevention systems (Ludena et al., 2015). As stressful or structural factors affect system flexibility and sensitivity, institutions are important, and institutional structures should be created through conscious efforts, which connect vulnerability analysis to decision-making (Turner et al., 2003). Institutions are fundamental determinants of economic behavior (North, 1990) and exchanges (B. O. E. Williamson, 1998), and affect innovation and technological development directly and indirectly (Arabiyat et al., 2019; Rabelo & Bernus, 2015). Institutional Void occurs when the community’s institutions act inappropriately (Covin & Miller, 2013), after which there will be weak or no institutional support, this factor brings vulnerability with itself. (Cuevas, 2011; H. M. Füssel & Klein, 2006; Moreno & Becken, 2009; Mortreux & Barnett, 2017; Rana & Routray, 2018; T. Williamson et al., 2012).

According to North (1990), human beings have developed institutions to make exchanges disciplined, and mitigate uncertainty; thus, one can conclude that institutions play a greater role in the COVID-19 crisis given its high uncertainty.

Regulatory, normative, cognitive, and conducive aspects of an institution are of grave importance for entrepreneurship support, while innovative firms are more interested in conducive and regulatory aspects (Arabiyat et al., 2019; Stenholm et al., 2013).

1- Regulatory aspect (business freedom, ease of starting up a business, ease of closing a business, property rights, the orientation of the country’s financial system toward entrepreneurship, government policies, and taxes) 2- normative aspect (societal perception of entrepreneurship as a good career choice, the perception of high societal status for successful entrepreneurship, the media attention is given to successful entrepreneurs) 3- cognitive aspect (entrepreneurial intentions, fear of failure, perception of perceived business opportunities, skills for starting a business within the adult population, the percentage of the non-entrepreneurial adult population who knows someone who started a business in the previous two years (networks) 4- conducive (ICT use/ laws, technological adoption, quality of scientific research institutions, university-industry collaboration in R&D, quality of education, availability of venture capital, availability of latest technology).
While COVID-19 affects many economic activities, public support programs prioritize and support established organizations. Unfortunately, they seem to prioritize bankruptcy threat mitigation and job loss, and put innovation or entrepreneurship efforts receive less attention (Giones et al., 2020).

5. Technological entrepreneurial action

Entrepreneurial actions are a response to exogenous shocks that lead to the emergence of entrepreneurial opportunities (Klein, 2008). The final response should be selected according to business capabilities. Researchers, generally point to various response and action mechanisms for vulnerability control and reduction. Based on a review of the literature (Ghedini & Ribeiro, 2009; Turner et al., 2003; Winkler, 2007; Yohe, 2001; Füssel & Klein, 2006), these actions are taken to reduce vulnerability:

1) Coping response: means the system's capability to employ the existing resources to mitigate and manage bad conditions or to promote preparedness for an adverse event. They include predefined policies, autonomous individual actions, and/or an outcome of self-adaptive procedures or learning approaches.

2) Impact response: measures the effect of changes in local and global scales and presents feedback to other parts.

3) Adaptation response: If a significant change has occurred, the systems take an adaptive approach. In this approach, predefined policies and procedures are updated according to negative feedback.

4) Adjustment response: This approach is the same as the adaptive approach, except that it is used when a minor change in the system has occurred. Adaptation/adjustment response is a set of predefined procedures to restructure the business after a response.

5) Mitigation: Füssel & Klein (2006) state that a mitigation strategy is a human intervention to reduce sources of risk. Focusing on mitigation reduces the impact on all stress-sensitive systems, while the potential for adaptation actions is limited for many systems. However, there are some factors that we cannot reduce and therefore the need to use adaptive policies becomes more. IPCC (2007b) defined it as a technological change and substitution that reduces resource inputs and emissions per unit of output. Although several social, economic, and technological policies would produce an emission reduction, mitigation means implementing policies to reduce stressful components.
6. Discussion: Conceptual Framework

Identifying and mitigating vulnerability elements are the main factors decreasing disaster threats (Greiving et al., 2006). According to the literature review, vulnerability has three dimensions: 1) exposure 2) sensitivity of business elements, and 3) lack of response capacity to effects and outcomes caused by internal and external disruptions. Perhaps the greater the three-dimension overlap, the more business is more vulnerable. Business vulnerability includes social-economical responses to social, technological, human, biological, and environmental threats, such that the business will become vulnerable if it becomes sensitive to threats because of lacking response capacity.

To understand the vulnerability process and outputs from quantitative and qualitative viewpoints, vulnerability analysis should be integrated with diverse parameters. In this research, dimensions, components, and corresponding indicators to each dimension were studied using the indicator-based approach. First, potential indicators were identified, then a conceptual framework was developed using a set of factors and connections affecting the vulnerability of technology-based businesses through the COVID-19 crisis (Figure 2).

To analyze technology-based business vulnerability according to the specified indicators, first, the threat should be identified. As you may see in Figure 2, technology-based businesses expose to threats, which in turn may affect sensitivity and response capacity: 1) through various economic, social, technological, and political factors, which we call “other exposure” 2) through businesses’ internal activities, and 3) through a pandemic event like COVID-19. Intensity, frequency, scope, duration, and rapidness of events and crises are determinants of exposure level. Exposure impacts business sensitivity and is related to business vulnerability, in other words, the higher the exposure, the higher vulnerability. The greater the response capacity, the less the potential exposure-caused losses. Exposure and sensitivity create potential impacts if they overlap. The potential impacts are direct/indirect. The response capacity and the potential impacts affect business vulnerability. Response capacity to reduce vulnerability includes two types of capacity, adaptive capacity, and reduction capacity. Vulnerability is related reversely to response capacity, and response capacity is in reverse relation to sensitivity. Response capacity influences sensitivity according to exposure level. If the business is sensitive to stressful factors and lacks response capacity for the related threat, then it is
considered vulnerable. The lower is the response capacity, the higher the vulnerability possibility. An appropriate or inappropriate response to the crisis is associated with response capacity. Vulnerability lowers with an appropriate response, otherwise, it will grow. If businesses are vulnerable to the crisis and fail to take measures to reduce vulnerability, they will eventually collapse.

Insert Fig 2 here

Model variables, classified into three groups of dimensions, components, and measures of components, are shown in Table 1 according to the conceptual framework and literature review.

Insert Table 1 here

7. Theoretical and practical implication

Recently, global change and sustainability literature have focused heavily on vulnerability (Metzger & Schröter, 2006). Assessing small-business vulnerability to disasters helps disaster economy research, establishing a firm foundation for business survival and development policies (Davlashedze & Geylani, 2017). By examining the phenomenon of business vulnerability, several main areas such as risk and crisis management, resilience, development, and sustainability of businesses have been identified as the background of this study. Therefore, this article provides a scientific contribution in the above areas.

Acquiring differential elements of vulnerability is a key precondition for developing and implementing policies, which enhance equitable and sustainable development (Vogel & O’Brien, 2004). Thus, providing a conceptual framework for vulnerability reduction of technological businesses, this research informs and contributes to local, national, and regional decision-makers. Also, identified elements are of great help for policies developed for vulnerability reduction.

Also, this research helps business managers in various ways. First, managers can employ a research model against all crises and disasters, although the proposed model has been developed according to COVID-19 exposure. Second, identified dimensions and components can help managers and owners in vulnerability cognition. Third, the vulnerability dimensions of many tech-based businesses can be determined, compared,
and ranked, using components of all dimensions of vulnerability. Fourthly, owners and managers can develop various indicators and extend vulnerability factors according to their field proficiency, experience, and all related factors, including context and type of business. Fifthly, this research helps managers and owners to develop strategies for shocks, crises, and various disasters about possible internal and external events. And most important, they can prepare themselves for any crisis.

The proposed framework could provide future studies with a useful checklist for developing new approaches to reduce vulnerability and adaptive capacity (mitigative capacity) to shocking events and epidemics.

Researchers, planners, policymakers, and decision-makers can seek solutions and recommendations to overcome shortcomings that reduce the vulnerability of technological businesses and can be feedback to the conceptual framework.

8. Conclusion

This research aimed to design and present a model for high-tech businesses’ vulnerability, and to determine the dimensions, and components of vulnerability. To quantify or review vulnerability, vulnerability management tools need specific patterns. These patterns should be based on all types of vulnerability (Lowis & Accorsi, 2011). Given that business vulnerability is non-linear and includes many interactions, thus taking dynamic perspectives is necessary (Lo et al., 2019). To identify vulnerability levels, we should determine its dimensions and components, and then we can compare and rank a wide range of businesses. Vulnerability assessment is useful only if it can support decision-making processes in real environments (Ghedini & Ribeiro, 2009).

We conclude that analyzing the vulnerability of technology-based businesses should be conducted along four main paths: exposure, business sensitivity, response capacity, and technological entrepreneurial action. Reviewing related literature and a similar situation to the COVID-19 crisis showed informed us that technology-based businesses should always have an eye on environmental dynamics and uncertainty, forecast, and determine what negative outcomes they may bring about. Technology-based businesses have to know their characteristics and components against such crises and consider them as sensitivity components. In this research, we considered Business characteristics, job characteristics, owner/manager demographics, and supplier/product characteristics as the
components of the sensitivity dimension. Thus technology-based businesses should
determine to what extent they are prepared for crises in terms of various levels, including
resources, technology capital, human capital, social capital, economic capital,
institutional capital, managerial capital, and supply chain. Then they have to identify their
weak points and shortcomings to respond adaptively and effectively. This is the only way
they can take to survive and mitigate their vulnerabilities.

Although many researchers are interested in vulnerability assessment, they should be
modified, and then to be inserted into appropriate policies. Also, since vulnerability is
multi-faced and consisted of many components, thus we can’t propose an integrated
method, so we can add more indicators for vulnerability to reflect local requirements
thoroughly (Rana & Routray, 2018). Vulnerability assessment seems focused on
quantitative evaluation, while qualitative evaluation is the key to assessing vulnerability
comprehensively and notifying general policies. Quantitative assessment of vulnerability
requires the ability to provide simple, summary, and standard data. This method needs
little interpretation and provides for a multi-case comparison. To resolve vulnerability
complexity, governmental solutions based on a quantitative-qualitative mix are required,
each of which should be based on participation (Rossignol et al., 2015). In the study a
specific indicator or index was not used, while an indicator-based approach with various
indicators was employed, thus a better view and perspective on business vulnerability was
projected. To assess various businesses’ vulnerabilities, we can use some of the identified
factors.

9. Limitations

This study is not without limitations. Quarantine restrictions and communication
limitations during the COVID-19 did not allow us to interview managers and owners of
technology-based businesses to give different weights and prioritize the indicators, so in
this study, the indicators were identified by reviewing the literature and assumed equal
weight. There is a need for future research. Future research is necessary to validate the
dimensions. The presented study only identifies the indicators. The validation of the
identified findings in a more robust setting with in-depth interviews across a range of
cases in different technology-based business contexts would be desirable. A quantitative/
qualitative survey on a technology-based business is needed to evaluate the empirical
significance of the presented findings based on an indicator-based approach. The comprehensiveness of the cases should be verified by conducting additional focus groups, interviews, and surveys, and additional differentiation dimensions could be identified. And given that cross-sectional designs are not suitable for examining the impact of dynamic changes and discontinuous changes over time on business. It is appropriate to use longitudinal plans to achieve an appropriate model of the vulnerability and ability of businesses to survive. We recommend research on the vulnerability model of technology-based businesses at different levels (individual, group, organizational). Finally, we suggest research in related areas such as business sensitivity, mitigation capacity, and adaptive capacity, as these areas pose similar challenges to the conceptual boundaries of business vulnerability.

10. References


influence of institutional and conductive aspects on entrepreneurial innovation:
Evidence from GEM data. *Journal of Enterprise Information Management, 32*(3),


Bailetti, T., D. Bot, S., Duxbury, T., Hudson, D., McPhee, C., Muegge, S., Weiss, M.,

Barua, S. (2020). Understanding Coronanomics: The Economic Implications of the
https://doi.org/10.2139/ssrn.3566477

Birkmann, J., Cardona, O. D., Carreño, M. L., Barbat, A. H., Pelling, M.,

Cardona, O. D., Van Aalst, M. K., Birkmann, J., Fordham, M., Mc Gregor, G., Rosa, P.,
Pulwarty, R. S., Schipper, E. L. F., Sinh, B. T., Décamps, H., Keim, M., Davis, I.,
Ebi, K. L., Lavell, A., Mechler, R., Murray, V., Pelling, M., Pohl, J., Smith, A. O.,
& Thomalla, F. (2012). Determinants of risk: Exposure and vulnerability. In
*Managing the Risks of Extreme Events and Disasters to Advance Climate Change Adaptation: Special Report of the Intergovernmental Panel on Climate Change*.
https://doi.org/10.1017/CBO9781139177245.005

Carvalho, M., Martins, B., Coelho, J. P., Brôco, N., Ribeiro, A. K., & Magalhães, A.
(2019). Climate change adaptation: a pragmatic approach for assessing
https://doi.org/10.2166/wpt.2018.122


https://doi.org/10.1080/09537287.2020.1732494


https://doi.org/http://dx.doi.org/10.2139/ssrn.3557504


https://doi.org/10.1007/s10584-006-0329-3


https://doi.org/10.1016/j.gloenvcha.2006.05.002


https://doi.org/10.1016/j.gloenvcha.2006.02.004


Global Data. (2020). *While all tech sectors will be negatively impacted by coronavirus, IT services will be hit hardest, says GlobalData*. Https://Www.Globaldata.Com/.


Lambert, L. (2020). Real unemployment rate soars past 20%—and the U.S. has now


Merino, B. humberto hernani. (2016). *Technological Adaptation For Water Storage And Distribution In The Oldman River Basin In Response To Extreme Climate Exposures*. University of Regina.


of Business Research, 117, 443–449.
https://doi.org/https://doi.org/10.1016/j.jbusres.2020.05.035
https://doi.org/10.1016/j.jbusres.2020.05.059
https://doi.org/10.1016/j.gloenvcha.2006.03.008
https://doi.org/10.1007/s11069-016-2652-y
Teece, D., & Leih, S. (2016). Uncertainty, Innovation, and Dynamic Capabilities:
30709, 171–203.


World Economic Forum. (2020). *This is How COVID-19 has Changed Media Habits in Each Generation*.


Figure 1. Methodological approach
Figure 2. Conceptual Framework

Lines A: hazards directly affect the business component of exposure, sensitivity and business response capacity. The greater the intensity, frequency, scope, duration, and rapidness of hazards, the higher the exposure and sensitivity, and the greater the business response capacity needed to reduce the impact of the hazards.

Line B: The component of exposure and sensitivity are directly related. The more exposure a business has, the more likely it is that the business will become more sensitive. This relationship is two-way. The more sensitive a business is, the more likely it is that the business will be exposed to hazards.

Lines C: Exposure and sensitivity have potential effects if overlapped. Potential effects are direct or indirect.

Line D: Business capacity inversely affects component exposure and sensitivity. The higher this capacity, the less businesses are exposed and the less sensitive the business is to hazards.

Line E: Business capacity inversely affects the direct or indirect impact that results from the overlap of sensitivity and exposure, and determines the severity of the business vulnerability.

Line F: Businesses may have current vulnerabilities. These current vulnerabilities affect vulnerabilities in the future and increase the severity of the vulnerability. Therefore, it is necessary to link the business vulnerability to the red rectangle to take into account the current business vulnerability.

Line G: Business response capacity directly affects technological entrepreneurial actions. Businesses decide what to do based on their response capacity. This relationship is two-way. The actions of technology entrepreneurs may increase the business response capacity.

Line H: Technological entrepreneurial actions directly affect the exposure component and sensitivity. These actions, if done correctly, will make the business less exposure or reduce the business sensitivity to hazards.

Line I: Technological entrepreneurial action affect the reduction or increase of business vulnerabilities. This is a two-way communication. The degree of business vulnerability and Business Response capacity determines the actions of entrepreneurs.

Line J: Business will fail if the wrong actions are done and technology entrepreneurs fail to reduce the vulnerability.
Table 1. Dimensions, components, and measures of components

<table>
<thead>
<tr>
<th>Determinants of Vulnerability</th>
<th>Vulnerability Indicators</th>
<th>Measures of components</th>
</tr>
</thead>
<tbody>
<tr>
<td>Biological natural threats:</td>
<td>An epidemic event (Coronavirus)</td>
<td>• Intensity</td>
</tr>
<tr>
<td>exposure</td>
<td></td>
<td>• Frequency</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Location</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Number of people</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Duration</td>
</tr>
</tbody>
</table>

- Business size
- Business age
- the number of business locations
- economic sectors to which businesses belong/ Industry sector

- sales previous
- Legal ownership structure
- Source of business
- Business brand
- Business culture
- Business structure
- Routines/ laws

- Complexity of system
- interaction between elements of a system
- Cascading failer

- Gender (Male/Female)
- Manager’s quality/ supervisor’s competence
- Education
<table>
<thead>
<tr>
<th>Determinants of Vulnerability</th>
<th>Vulnerability Indicators</th>
<th>Measures of components</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• Industry experience</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Previous disaster experience</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Race/Ethnicity</td>
</tr>
<tr>
<td>Supplier/product characteristics</td>
<td></td>
<td>• Product</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Service</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Experience</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Price Price/Performance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Avail</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Number of Exposure Points Raw</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Distance / Time</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Flexibility</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Redundancy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The market for the product</td>
</tr>
<tr>
<td>Technology capital</td>
<td></td>
<td>• New technology / emerging technologies</td>
</tr>
<tr>
<td>Adaptive capacity</td>
<td></td>
<td>• Technology Development / Redundancy</td>
</tr>
<tr>
<td>Human capital</td>
<td></td>
<td>• technology mal-adaption</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Technology migration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Reverse salient</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• availability of employees</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• willingness and ability to change / Risk-taking</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Education</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Skill</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Experience</td>
</tr>
<tr>
<td>Determinants of Vulnerability</td>
<td>Vulnerability Indicators</td>
<td>Measures of components</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td></td>
<td>Knowledge</td>
<td>• Knowledge</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• knowledge of ways to serve markets,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• knowledge of customer problems,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• knowledge of markets, knowledge of technology</td>
</tr>
<tr>
<td>Social capital</td>
<td>• opportunism; technology leakage; and conflict in between sharing and protecting knowledge</td>
<td>• quality of social network</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• R&amp;D consortium performance</td>
</tr>
<tr>
<td>Economic capital</td>
<td>• Income diversity - Business model inflexibility</td>
<td>• Lack of financial resources for technology adaptation and development</td>
</tr>
<tr>
<td>Institutional capital</td>
<td>• Regulatory indicators: Business Freedom, Ease of starting up a business, Ease of closing a business, Property rights, The orientation of the country’s financial system toward entrepreneurship, Economic freedom, Government policies, and taxes</td>
<td>• Normative indicators: The societal perception of entrepreneurship as a good career choice, The perception of high societal status for</td>
</tr>
<tr>
<td><strong>Determinants of Vulnerability</strong></td>
<td><strong>Vulnerability Indicators</strong></td>
<td><strong>Measures of components</strong></td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>Successful entrepreneurship, the Media attention given to successful entrepreneurs</td>
<td>Cognitive and individual aspects:</td>
<td></td>
</tr>
<tr>
<td>Entrepreneurial intentions, Fear of failure, perception of perceived business opportunities, skills necessary for starting a business within the adult population, the percentage of the non-entrepreneurial adult population who personally knows someone who started a business in the previous two years (networks)</td>
<td>Supportive/ conducive indicators:</td>
<td></td>
</tr>
<tr>
<td>ICT use/laws, technological adoption, quality of scientific research institutions, university-industry collaboration in R&amp;D, quality of education, availability of venture capital, availability of latest technology,</td>
<td>Lack of proper infrastructure for digitalization</td>
<td></td>
</tr>
<tr>
<td>Infrastructure capital</td>
<td>Business model dependence on platforms and open innovations</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access to partner data</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access to the creative ideas of others</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Apply acquired strategy on platforms</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Inaccessibility and scarce resources and irreplaceable resources</td>
<td></td>
</tr>
<tr>
<td></td>
<td>High dependence on scarce resources</td>
<td></td>
</tr>
<tr>
<td>Determinants of Vulnerability</td>
<td>Vulnerability Indicators</td>
<td>Measures of components</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Managerial capital</td>
<td>• enterprises’ strategic plans</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Inability to make decisions in conditions of uncertainty</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Types of management of vulnerability</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(1-existence of unreported vulnerabilities; 2-trying to fix all identified vulnerabilities; 3-ineffective communication; 4-insufficient remediation resources; 5- fixing only “high” and “critical” vulnerabilities; 6- conceding broad or eternal exceptions; 7- mitigation without previous planning can be disastrous)</td>
<td></td>
</tr>
<tr>
<td>Supply chain capital</td>
<td>• Financial disruptions in the supply chain and customers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• consumer behavior Changing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Dependence on partners in the supply chain</td>
<td></td>
</tr>
</tbody>
</table>