# An Exploration of Business and Continuity Planning and Disaster Recovery in the 21st Century

Scott Mensch
Purdue Global University
Scott.Mensch@purdueglobal.edu

Michael Pry
Information Sciences and Management,
University of Pittsburgh
mip84@pitt.edu

**Abstract.** In December 2019, the authors of this paper met to discuss the possible impact that corporations would face if a cyber-attack took out the Internet for a prolonged period of time. Specifically, the authors were looking at how well-prepared organizations in the Pittsburgh area and surrounding regions would be if a prolonged Internet outage occurred. It had not occurred to the authors that other variables outside of cyber-attacks could disrupt daily organizational operations the way a terrorist initiated cyber-attack could. By February 2020, the proposed survey instrument was sent to the Institutional Review Board (IRB) at the University of Pittsburgh for approval to conduct the study. Unfortunately, this submission was never completed due to the COVID-19 pandemic. After the University had closed its doors and suspended all IRB submissions, the authors used this opportunity to retool and redesign their survey instrument to also include questions that would capture how well prepared these organizations were in having their employees telecommuting on short notice.

## Disaster Recovery and Business Continuity Planning

While much has been published in the area of disaster recovery planning, most organizations practice sound management in regards to backing up their data and files. However, it could not be determined how well prepared organizations were overall in the Pittsburgh region should a prolonged Internet outage occur. This could potentially force businesses to use past business tools such as mail and fax machines to conduct daily operations. Business continuity planning and disaster recovery planning should both be an integral part of an organization's risk-management plan. "Risk-management as a whole focuses on any event or situation that could negatively affect an organization. It analyzes the relative probability of an event and matches that probability with the impact the event will have on business operations (Cook, 2015)." Disaster recovery and business continuity should be a part of every organizations risk management plan but doing so is not without its challenges. "The main challenge that organizations face while constructing a business continuity and disaster recovery plan is to efficiently prepare, deploy and maintain the plans to avoid the consequences of a disaster (Jorrigala, 2017)." Furthermore, as stated in Sahebjamnia," a recovery tool box should be established to include historical documentation, testing techniques and auditing practices." (Sahebjamnia. 2015)

Hatton presented an alternative view that disaster recovery planning benefits may be overestimated. This connects well with estimating the impact of loss and managing the total cost of risk. "While the concept of, and process for preparing, a business continuity plan is very well established, there is rather less literature examining the actual experiences of organizations utilizing their business continuity plan in a disaster setting (Hatton, 2016)." A study on the preparedness of organizations in regards to business continuity planning can be used by all organizations in the Pittsburgh region, as well as other companies, as they begin to better understand how well they are prepared for external risks and how not being prepared can jeopardize their ability to maintain and complete their daily business functions. "Disaster recovery planning is only important to people right after a disaster but then memory fades of the

importance of planning. There is a tendency to blame modern society on the short-term focus of our collective memory. Yet everyone forgets. This is global and affects all cultures (Landry, 2018)."

As Kandel noted, developing a plan should begin by "the establishment of a governing mechanism and committee, business impact analysis to identify essential services or functions, identifying required skillsets and a staff allocation and reallocation plan, identifying relevant issues and implications, documenting essential services and functions and their action plans (Kandel, 2014)." The use of cross-functional teams in planning for these types of instances is critical as the entire enterprise needs to be addressed and not only specific departments. A committee approach is an optimal way to ensure that everyone's voice within the organization is being heard as each functioning unit may have different requirements if they are forced to work remotely. As Russo noted, companies should have at a minimum a group of professionals who will drive the initiative of preparing the organization for such catastrophic events and to ensure the impact from these events will be minimal to the corporate data and daily business functions (Russo, 2015). This is also extremely important for smaller organizations that may not have the technical or business expertise to plan for such unexpected events to occur. These organizations typically have less financial backing and cannot recover from such a catastrophic event (Sarmiento, Hoberman, Jerath, & Jordao (2016). Wieteska proposes an interesting viewpoint related to how supply chain risks should be part of a disaster recovery and business continuity planning and how suppliers affect the organization. "It is recognized that a manufacturing company can be disrupted not only by supply risks and demand risks but also by operational (internal) risks and other risks that come from the external business environment, which can also influence business partners (Wieteska, 2018)."

Historically, much research has been done on cyber-attacks and financial impact that organizations have had to endure from these types of activities. Over the past decade, the United States has seen countless numbers of security breaches that have impacted large Fortune 500 companies such as Facebook, Target, Uber, Tesla, and Marriott. While we seem to focus on records are compromised each year. The financial impact of these breaches is far-reaching as the dollar amounts lost can run into the millions of dollars. A recent study found that "the average cost of a breach is US$3.86m. Verizon reports that 1,000 records breached results in total costs ranging from US$52,000 to US$87,000, while 10 million records breached results in total costs ranging from US$2.1m to US$5.2m. While researchers have different methods of calculating the average cost of a data breach, it is clear that breaches have the potential for severe financial impact (Phillips & Tanner, 2018)."

## Conclusion

The authors of this study have received approval from multiple Chamber of Commerce locations surrounding the Pittsburgh area to distribute the survey instrument to their members. This organization is the world's largest business organization that represents companies of all sizes and sectors surrounding the Pittsburgh region. The Chamber of Commerce was chosen by the authors as this will provide the best method to survey multiple different organizations in various business sectors regardless of how many employees are at the company or how large the

company may be. Once the survey results have been gathered, a second publication will be conducted to share the survey results in the analysis from the data gathered.

## Survey Instrument

The following 24 Survey Questions are part of our Survey Instrument.

**1)** What is your age?

a) Under 24

b) 25-30

c) 31-40

d) 41-50

e) 51+

**2)** Which of the following best defines your INDUSTRY?

a) Manufacturing

b) Retail

c) Information Technology

d) Education

e) Healthcare

g) Banking / Financial

h) Construction /Landscaping

i) Other

**3)** What is your gender?

a) Male

b) Female

c) Not to be disclosed

**4)** Does your organization have a documented disaster recovery plan?
(Definition of a disaster recovery plan - "A *disaster recovery plan* (DRP) outlines how an organization responds to an unplanned event, but the process involves much more than writing the document.")

a) Yes

b) No

c) Not Sure

**5)** Does your organization have a documented business continuity plan?
(Definition of a business continuity plan – *"Business continuity planning* (BCP) is the process involved in creating a system of prevention and recovery from potential threats to a company. The *plan* ensures that personnel and assets are protected and are able to function quickly in the event of a disaster.")

a) Yes

b) No

c) Not Sure

**6)** How many employees does your organization have?

a) Less than 10

b) 11-25

c) 26-50

d) 51-100

e) 101-500

f) Over 500

**7)** Did the recent COVID19 pandemic force you to telecommute and work from home? If so, how well prepared were you to work remotely from a technology standpoint? (For example: access to files, work material, internal databases)

a) The pandemic did not force me to telecommute.

b) The pandemic resulted in me being laid off.

c) I was very prepared to work from home from a technology standpoint.

d) I was prepared to work from home from a technology standpoint.

e) I was slightly prepared to work from home from a technology standpoint.

f) I was not prepared.

**8)** How well prepared are you with the use of collaboration technologies? (Zoom, Microsoft Teams, Go to Meeting, etc.)

a) I am very comfortable using collaboration technologies.
b) I am comfortable using collaboration technologies.
c) I am slightly comfortable using collaboration technologies.
d) I am not comfortable with collaboration technologies.

**9)** Approximately how many computers does your organization have?

a) Less than 10

b) 11-25

c) 26-50

d) 51-100

e) 101-500

f) Over 500

**10)** Approximately how many printers does your organization have?

a) Less than 5

b) 6-20

c) 21-50

d) Over 50

**11)** Approximately how many fax machines does your organization have?

a) None

b) 1-5

c) 6-10

d) Over 10

**12)** If your business has a fax machine, is it a:

a) Stand-alone fax machine

b) Integrated in with a printer

c) Don’t know

d) Do not have a fax machine

**13)** Does your organization save their data over the cloud/Internet?

a) Yes

b) No

c) Don’t know

**14)** Does your organization run applications and/or programs over the cloud/Internet?

a) Yes

b) No

c) Don’t know

**15)** How likely are you to run regular back-ups of your data (files, forms, etc.) on your network?

a) Always

b) Most of the time

c) Sometimes

d) Hardly ever

e) Never

f) Don't know

**16)** How likely are you to test the back-ups of your data (files, forms, etc.) on your network?

a) Daily

b) Weekly

c) Monthly

d) Annually

e) Never

f) Don't know

**17)** How many hours per week do you use your smartphone for business purposes (Example: email, virtual conferences, texting, security applications, etc.…)

a) 0

b) 1-5

c) 6-10

d) 11-15

e) 16-20

f) 21-30

g) 31-40

h) Over 40

**18)** How many days could your organization function efficiently without access to email and the internet?

a) 0

b) 1-2

c) 3-4

d) 5-6

e) 7 or more

**19)** What would the financial impact be if the internet was out for more than a day?

a) None

b) Minimal

c) Severe

d) Catastrophic

**20)** How important do you think a computer is to your organization when initiating sales / ordering tasks?

a) Very Important

b) Important

c) Moderately Important

d) Slightly Important

e) Unimportant

**21)** How important do you think a computer is to your organization when marketing your organization?

a) Very Important

b) Important

c) Moderately Important

d) Slightly Important

e) Unimportant

**22)** How important do you think a computer is to your organization when managing inventory?

a) Very Important

b) Important

c) Moderately Important

d) Slightly Important

e) Unimportant

**23)** How important do you think a computer is to your organization when initiating HR payroll tasks?

a) Very Important

b) Important

c) Moderately Important

d) Slightly Important

e) Unimportant

**24)** Does your organization have a crisis management response team?
(Definition of a crisis management response team - “Crisis Management Team (CMT) provides

support through management of crisis level issues, managing additional risks, exposures and stakeholder interests in response to an event or disaster requiring the activation of the CMT.")

a) Yes

b) No

c) Don't know

## References


Cook, J. (2015). A Six-Stage Business Continuity and Disaster Recovery Planning Cycle. *SAM Advanced Management Journal*, 23–33

Hatton, T. (2016). Lessons from disaster: Creating a business continuity plan that really works. *Journal of Business Continuity & Emergency Planning*, *10*(1), 84–92

Jorrigala, Vyshnavi, "Business Continuity and Disaster Recovery Plan for Information Security" (2017). *Culminating Projects in Information Assurance*. 44. [Downloaded on October 28, 2020 from https://repository.stcloudstate.edu/msia_etds/44]

Kandel, N. (2014). Is there a business continuity plan for emergencies like an Ebola outbreak or other pandemics? *Journal of Business Continuity & Emergency Planning*, *8*(4), 295–298.

Landry, J. (2018). Leveraging history to improve crisis response. *Journal of Business Continuity & Emergency Planning*, *11*(4), 317–325

Phillips, R., & Tanner, B. (2018). Breaking down silos between business continuity and cyber security. *Journal of Business Continuity & Emergency Planning*, *12*(3), 224–232

Russo, F. (2018). Connecting the disaster dots: The benefits of enhanced collaboration between business continuity and risk management. *Journal of Business Continuity & Emergency Planning*, *12*(3), 277–285.

Sahebjamnia, Navid & Torabi, S.A. & Mansouri, Afshin. (2015). Integrated business continuity and disaster recovery planning: Towards organizational resilience. *European Journal of Operational Research*. 242. 261-273. 10.1016/j.ejor.2014.09.055.

Sarmiento, J, Hoberman, G, Jerath, M, & Jordao, G. (2016). Disaster Risk Management and Business Education: The Case of Small and Medium Enterprises. *Ad-Minister*, 73–90

Wieteska, G. (2018). The Domino Effect - Disruptions in Supply Chains. *Scientific Journal of Logistics*, *14*(4), 495–506