Contingency Planning: Prioritizing Your Resources

Kathryne Burton, Necole Cuffee, Darius Neclos, Samuel Olatunbosun, and Taiwo Ajani

1 Background

A contingency plan can be described as a proactive and comprehensive backup plan for any business. It is activated in the event of any type of a situational disaster, including natural, technological, or manmade, that may disturb employees, machines, or IT systems. A contingency plan may consist of rerouting data, emergency generators for power, escape routes for employees, and supervisory duties for contingency team members. Plans to get production up and running despite unforeseen circumstances can be the difference between a company that survives a disaster and one that folds [1]. There may be a cost associated with devising a contingency plan and maintaining it, but it could be minimal when measured against the cost of production loss [2].

Developing a well-rounded contingency plan includes analyzing all risks, first. This includes listing all possible events that could disrupt operations [1]. Next, a business should determine the likelihood and impact of all risks and prioritize them. A "risk probability chart" is a resource used to help evaluate and prioritize risks based on the severity of their impact and the probability of the event occurring. Next, businesses must create each event. Creating separate plans will outline the actions that should be taken if the risk occurs. Businesses must consider what must be done in order to resume normal operations after the impact of the event.

K. Burton · N. Cuffee · D. Neclos · S. Olatunbosun (✉)
Department of Computer Science, Norfolk State University, Virginia, VA, USA
e-mail: k.a.burton102699@spartans.nsu.edu; n.a.cuffee@spartans.nsu.edu;
d.j.neclos@spartans.nsu.edu; sbolatunbosun@nsu.edu

T. Ajani
Department of Computer Information Systems, Ferrum College, Virginia, VA, USA
e-mail: tajani@ferrum.edu

H. R. Arabnia et al. (eds.), *Advances in Software Engineering, Education, and e-Learning*, Transactions on Computational Science and Computational Intelligence, https://doi.org/10.1007/978-3-030-70873-3_67

During this step, businesses should also clarify employee responsibilities, timelines that highlight when things should be done and completed after the event, restoring and communications processes, and the steps needed to take in advance to prevent losses when the event has taken place. Lastly, businesses should share, maintain, and execute the plan if necessary. Once the plan is completed, it should be quickly accessible to all employees and stakeholders.

In all, the best contingency plans benefit the company during a disaster. In most cases, a contingency plan helps minimize the loss of production. If implemented correctly, such plans show employees exact roles and responsibilities, while maximizing time and allowing the focus to be solely on the issue at hand. Most importantly, it creates the space to feel more prepared.

2 Literature Review

Technology is only as durable and reliable as it's created to be. It is not exempted from flaws. Indeed, It has a dual nature. It comes with risks in terms of adverse events and potential losses that can be due to several factors and may lead to the disruption of business operations [3]. Examples could be natural disasters, zero-day attacks, outages, etc.

An important factor for contingency planning is to construct that plan as a thorough guideline. According to Yiwen Shi, a reliable contingency plan should be standardized such that each stage adopts the consequence attained from the last stage and extends to a more detailed production [4]. This includes components such as business impact analysis, disaster recovery, and business continuity planning.

There are several methods in creating a contingency plan. No matter the method, the key to a successful contingency plan is to have a consistent flow between stages. A common method used is a rational unified process (RUP). A rational unified process is considered to be a method of iterative development or, in simpler terms, a waterfall methodology [4]. An RUP consists of seven stages, and though each stage is dependent on the next stage, there is space and flexibility to revert back to a previous stage in case new urgent scenarios appear.

Contingency planning should always be viewed as an immediate response procedure. When creating the contingency plan, refrain from attaching resources that will not be immediately available, and in addition, it is best practice to maintain practicality throughout the entire plan to ensure an immediate response [5]. It is important to note that risk assessments and contingency plans coincide with each other. Editor Joseph A. Schafer expresses that contingency planning should only focus on "foreseeable risk [5]." This statement is very agreeable. In today's society, whether it is the provided service or not, technology is the main driver for most companies. No matter the company's complexity, there will be several risks within the company's environment. Creating contingency plans for every risk is not only time-consuming but also costly.

There should only be one main objective when developing a contingency plan, and that involves the ability to continue business operations in the event of any major conflicting situations. Contingency planning should answer many questions, one in particular, “What is the likelihood that this contingency plan will be used?” Most companies create multiple plans in reference to their company’s risks and policies; however, as stated before, every risk does not need a contingency plan. With that in mind, as an information technology and/or information security professional, it is best practice to warrant purpose and necessity within the plan. If the contingency plan is purposeful and holds necessity, the likelihood of using it will be greater and more efficient for the company.

3 Contingency Planning

3.1 Research Design

Research was conducted by entry to mid-level IT professionals. The purpose of this research was to gain an understanding of contingency planning and to explore what the components of a contingency plan are and how they are used. A contingency plan provides procedures on how to recover IT services in the event of a disruption [6]. In the event of a disruption, we will cover when a contingency plan should be implemented and how to overcome such events.

3.2 Research Approach

Various IT professionals agreed to participate in research efforts and were surveyed to assist in data collection. The surveys that researchers compiled included questions geared toward gaining insight on senior-level IT professional experiences with contingency planning as it relates to creating, implementing, and/or reviewing individual plans. The questions included in the surveys were based on the guidelines and recommendations from the NIST Contingency Planning Guide for Information Technology Systems [7].

3.3 Sampling Method

Each survey was completed by a senior IT professional that was currently or had previously been employed by popular IT companies or entities. The companies or entities where professionals were surveyed included but were not limited to IT professionals employed within government sectors, healthcare, and retail. Research efforts took place over the course of 2 weeks with a total of 100 professionals surveyed. Within this timeframe, the participants were provided a four-question survey. The questions are as followed:

1. "Do you know what your company's contingency plan is and what it consists of?"
2. "What is the likelihood that the contingency plan will be used?"
3. "When should a contingency plan be implemented?"
4. "Once a system/service disruption has occurred, what steps are taken to overcome these events?"

3.4 Data Collection Method

Over the course of 2 weeks, the research was conducted in person, online, or by phone surveys. Conducting in-person surveys allowed for interaction and surveying of multiple IT professionals at osne location. The online and phone surveys were made available to individuals that were unable to physically be present or those that had other priorities during the research period. The data collected was based on each individual professional's experience in creating and/or executing contingency plans within their current or previous work environments.

3.5 Data Analysis Method

Data was collected in a qualitative approach. There were no numerical or statistical data to be provided for the research that was administered. The results from each survey were thoroughly examined and grouped together by each company, followed by each individual's recorded response. Each participant provided written consent to participate in the conducted surveys. The identity of each participant, as well as the identity of each company, was kept confidential and remained protected. All data collected was used solely for the intent of this research.

4 Results

Our investigation of contingency planning led us to a few general discoveries. We found that "most contingency plans are rarely carried out as they are detailed on paper." [3] This is important because there are many different possible scenarios each with different variables which by default makes every contingency plan a candidate for repeated testing. Most efficient contingency plans test check for vulnerabilities and/or faults in the process as well as any other inefficient or unnecessary processes. Results reveal that only after thorough testing, contingency plans are needed.

The results have also shown us that while there may be many strategies used to test contingency plans, not all of them count as what are known to be “true tests”. However, they still serve to roughly gauge what policies within the plan need to be updated. Additionally, testing a contingency plan opens the floor for all participating parties to have a discussion surrounding the rehearsal of their part. This then allows for a clearer understanding of roles and responsibilities. The results show that controlled testing is immersive; in addition to this benefit, the testing moderators can actively alter the variables of the scenario which ultimately makes for more efficient testing.

Finally, we discovered that contingency plans had greater success rates when organizations administered multiple “test runs” of each contingency plan component.” [3] If the failure to update these plans was ever to occur, the organization, its information, and various resource changes could decrease the bandwidth to properly handle an incident. This could ultimately result in significant damage to the organization.

5 Discussion

Whenever an organization reviews its strategies, it should adapt over time. Improving plans and rehearsing the revisions are critical to contingency planning. “Each time an incident occurs, the organization should do a detailed review of the lessons learned” [3]. This includes a thorough evaluation of all results.

Additionally, the long-term objective is to implement any discovered changes into an improved set of plans. While doing so, this provides opportunity for constant comparison and evaluation of previous steps from the older plan. In theory, an organization should continue to move forward and improve its contingency plan process so it can strive for an even better outcome.

“Typically, planning for future events is a responsibility reserved for managers in the IT department.” [3] In order for your contingency plan to be considered plausible, it must be supported by the information security department. There are some instances in which organizations have been mandated by law to have contingency plans in place even though it is recommended to not always prepare for every unexpected instance. It is highly recommended that when writing a contingency plan, center it around these four points: business impact analysis, incident response, disaster recovery, and business continuity. A successful contingency planning practice is to have four teams involved with the process. These teams are the: CP, IR, DR, and BC teams.” [3].

Finally, organizations have the choice to either create and/or develop three main planning aspects, or they can choose to individually create three separate elements with intertwining protocols that help with continuity.

References

1. Author Amanda Athuraliya Amanda Athuraliya is the communication specialist/content writer at Creately, Amanda Athuraliya Amanda Athuraliya is the communication specialist/content writer at Creately, A. Athuraliya, Amanda Athuraliya is the communication specialist/content writer at Creately, and View all posts by Amanda Athuraliya →, "What is a Business Contingency Plan: A Step-by-Step Guide," Creately Blog, 19 Sep 2019. [Online]. Available: https://creately.com/blog/business/business-contingency-plan-templates/. Accessed: 30 Apr 2020
2. K. Hughes. How to Make a Contingency Plan, ProjectManager.com, 30 Mar 2020. [Online]. Available: https://www.projectmanager.com/blog/contingency-plan. Accessed: 30 Apr 2020
3. M.E. Whitman, H.J. Mattford, *Management of Information Security* (Cen-gage Learning, Boston, 2019)
4. Yin Li, Yiwen Shi and Chen Li, *Constructing IT contingency planning based on RUP model*, 2008 IEEE International Conference on Service Operations and Logistics, and Informatics (Beijing, 2008), pp. 1017–1022
5. J.A. Schafer, *Policing 2020: Exploring the Future of Crime, Communities, and Policing* (U.S. Dept. of Justice, Federal Bureau of Investigation, Washington, D.C., 2007)
6. M.E. Whitman, H.J. Mattford, *Management of Information Security* (Cen-gage Learning, Boston, 2016). [E-book] Available: Mindtap|Cengage. Accessed 27 Apr 2020
7. M. Swanson, A. Wohl, L. Pope, T. Grance, J. Hash, & R. Thomas. Contingency planning guide for information technology systems recommendations of the national institute of standards and technology, NIST special publication / no. 800, Part 34 (2002) ALL [Online]. Available: https://norfolkstateu.on.worldcat.org/oclc/109238742. Accessed 27 Apr 2020