The Importance of Business Continuity Planning

Written for KAMIND, IT, Inc.

By Ravi Das

Introduction

If we backtrack to December of 2019, many of the Cybersecurity pundits were already making their predictions for what the threat landscape would hold for 2020. Many had agreed that threat variants such as Ransomware, Cryptojacking, Phishing, would all continue in different forms. Another fear that was starting to take some grip revolved around potential attacks on critical infrastructure, and misuse of AI platforms. Little did we ever realize that the whole Cyber world would be turned over upside down as we are seeing it now.

There have been many key lessons that have been learned, and some of them include the following:

- The need to be able to deploy a mobile workforce in the time of crisis, whether it is a Cyberattack or even a natural disaster.
- The need to be able to quickly deploy virtual communications mechanisms so that your workforce can resume productivity in a just a very brief period of time.

But apart from this, many, if not all business is starting to full grasp the importance of having a Business Continuity Plan in place. This is the focal point of this article.

The Differences Between Incident Response, Disaster Recovery, and Business Continuity Plans

There is very often confusion between these plans, and mistakenly, they are used synonymously with each other. But the reality is that these three are quite different from each other, and their variances are as follows:

<u>The Incident Response Plan</u>:

If your company is impacted by a security breach, you need to ACT NOW. How can this be done? It is all done with the IR Plan. This plan exactly spells out what you need to do, whom to notify, and how you will mitigate the threat from proliferating inside your business. In other words, this is your plan as to what you will do at that moment in time, without succumbing to knee jerk reactions which will lead to bad decisions.

<u>The Disaster Recovery Plan</u>:

Once you have contained the threat that has impacted your business, the next step is then how you will resume baseline operations again. Most of the time, this will involve only just implementing those mission critical operations that are deemed to be absolutely necessary. This is where the DR Plan kicks into play. It should exactly spell out what you will do, what those processes are that are deemed to be the most important. This plan can be viewed as a short term one, perhaps lasting for just a few days or even a week.

<u>The Business Continuity Plan</u>:

Once you have established those mission critical operations, the next step is in figuring out as to how you will bring your business back to where it was before you were hit by the security breach. In other words, how will you resume back to being normal again? Well, this is where the BC Plan comes into play. It should spell what your plans will be and how you will evolve yet once again. In other words, this is viewed as a long-term plan, lasting months, perhaps even a year or even longer.

The Benefits of A Business Continuity (BC) Plan

Now that we have examined the above differences, and provided an overview as to what a Business Continuity Plan is at a high level, the next question that you may be asking is: "What are the benefits of such a plan"? Or in other words, what is the sheer importance of having one? Here are some key reasons:

1) <u>It mitigates the risk of future Cyberattacks</u>:

   In today's world, everybody is at risk of becoming a victim. But the key is in how to actually mitigate that risk. The BC Plan can substantially aid in this process because you will be much better prepared in the future in dealing with a security if in the unfortunate chance you are impacted yet again.

2) <u>It can help with audits</u>:

   If you are ever faced with any kind of compliance audit, one of the key things that you will get asked is if you a plan in place to resume business operations after being hit. If you have the BC Plan, you can produce it immediately to the auditor, and avoid facing huge financial penalties.

3) <u>Cost Prevention</u>:

   By knowing ahead of time what you need, you will save a lot of huge expenses down the road if you ever need to restore your business and its associated processes/operations from literally the ground up. This is the exact situation that we are facing with the Coronavirus today. Many businesses were caught off guard by not having a BC Plan in place ahead of time and practicing it. Because of this, a big chunk of them were left scrambling in trying to figure how to best provision their employees in literally just a few days' time.

4) <u>Brand reputation</u>:

   No matter how large or small a business is, there is a common truth to the reality if you are impacted: You will lose your brand and the faith of your customers quickly. The longer your downtime is, the worse it will get. But by having the right BC Plan in place, you can be more or less assured that your business will be up and running in just a matter of hours. Although there could be some damage to your company's image, you should be able to recover it fairly quickly. Remember, it takes a long time to get a customer, but only seconds to lose them to your competition.

5) <u>You will be able to understand your processes much better</u>:

   Part of crafting a BC Plan means that you have to go through each and every process and operation in your business, see how it works in detail, and from there, formulate the steps that are needed when they are down. Although this might sound like a very laborious and time consuming process (and the truth of the matter, it really is), there is a another side benefit to this: You will see which of those processes and/or operations are not running as efficiently, and because of this, you will also have the opportunity to make them more efficient. The bottom line here is that with this, you will see increased productivity, and a positive return to your bottom line.

6) A clearer of the integrations that exist:

When crafting a BC Plan, one of the methodologies that you will most likely be using is what is known as the "Business Impact Analysis", or "BIA" for short. By using this, you will get a much clearer idea of all of the technologies that are housed from within your IT and Network Infrastructure. But importantly, you will also get a detailed view into how they all interact amongst one another. This can help in understanding exactly how the information and data flows into your business, how it is processed inside of it, and also how it is stored in your databases. If there any inefficiencies that are discovered in the integration of your technologies, now will be the time to make the necessary improvements to them.

7) Identify points of consolidation:

In the world of Cybersecurity, the common thinking has always been that the more security technologies you have in place, the better off you will be. In other words, to use the proverbial term, there is safety in numbers. Because of this, many businesses have procured tools from many vendors, which has led to a huge sprawl. Apart from being expensive to maintain, the other downside to this is that by having all of them, you are simply increasing the attack surface for the Cyberattacker. Thus, many CIOs and CISOs are starting to see the value where perhaps it would be far better to have maybe just a fraction of the entire total but place them strategically on the lines of defense where they can offer the most robust protection. Another key benefit of doing a detailed BC Plan is that you will see where all of your security technologies lay at, and thus, you will be offered the opportunity to see where you can consolidate them into perhaps just a few tools. As the CIO or CISO, if you can prove these kinds of cost savings to your Board of Directors, there will be a far greater chance that you will get a bigger Cyber budget.

8) Organizational efficiencies:

By having a rock solid BC Plan in place, you can assure not only your customers, but your outside vendors, and even the all-important shareholders that your business is well structured and organized, and for the most part, will be able to recover from any kind or type of security breach that it may face. But equally important, it will help immensely in getting a good Cybersecurity Insurance Plan in place. In fact, many of the more reputable insurance companies look at all kinds of factors before they will award out an insurance policy. But more importantly, when you have a BC Plan, it will also show them you are not in a high risk category profile, and if and when you file a claim, there is a much greater likelihood that you will get all of your money.

9) Enablement of quick response times:

A critical component of the BC Plan is to not only have a communications sub plan, but also who will be responsible for what. Remember, everything cannot fall onto the hands of the IT Department, because not all of your assets will be digital in nature. Many of them will be physical as well. So therefore, you will need to delegate in your BC Plan who will be responsible for what and rehearse all of these activities at least on a semi-annual basis. It would be preferable to this once a quarter, just to make sure that everybody stays on their A-Game. By doing this (having a BC Plan and practicing it), you will have very quick response times in terms

of getting your business back up and running, and confusion in the communications process will be greatly mitigated.

10) A greater peace of mind:

    If you are the CIO and/or CISO for your business, your day is filled with stomach churning tasks to get done and questions you need to answer to your higher ups. By having a solid BC Plan in place, this is just one less, major thing that you have to worry about, and will let you focus more on what you need to do at the present moment: Fighting off those threat variants. Also, seeing how there is much more pressure being applied to CIOs and CISOs for accountability, you will be one step ahead of this by producing your BC Plan on demand if and when asked for it, whether it be your CEO, Board of Directors, or external auditors.

Conclusions

Overall, this article has examined the importance of having a BC Plan. But keep in mind, although there are many such templates that you can download and use, you need to make your BC Plan specific to your own unique security requirements. A future blog will examine some of the details that need to go into a BC Plan.

Sources

1) https://www.mha-it.com/2017/07/19/benefits-of-a-business-continuity-program/
2) https://www.refreshtech.com/2018/04/04/6-benefits-business-continuity-plan-smbs/
3) https://www.ctgmanagedit.com/6-benefits-of-business-continuity-plan/