Five ways to

cut down your business disruption

Five ways to cut down your business disruption

Introduction

More than **550,000 small businesses in the UK have been forced to halt trading due to a disruption in the last two years**, according to 2016 research by small business insurer Direct Line for Business. The average cost of keeping a small business afloat while unable to trade for two weeks is estimated to be £8,775.

Of those companies that have had to cease trading due to business disruption, **the period of shutdown lasted, on average, more than three months**. This will be of particular concern for the one in five small businesses that claim that they would not be able to survive if they had to cease trading for more than a month.

Reduction in profit (48%), reduction in revenue (42%), loss of customers (39%) and putting personal money into the business (32%) were found to be the most common impacts of an interruption in trading on small business owners.

A 2013 study, by the Chartered Management Institute (CMI), found that **organisations without a business continuity plan in place had lost more revenue, more new business opportunities and more customers due to business disruption events than those with a plan**.

The CMI study found that of organisations without a BC plan:

- **55% suffered reduced revenue**
- 29% lost new business opportunities
- 25% lost customers, as a result of a business disruption incident

In all cases those organisations with a BC plan in place suffered fewer losses.

Executive summary

1. **Good planning begins with identifying risk**. Knowing what risks you face as a business is the first step to mitigating them.
2. **Incident specific action plans help you respond more effectively**. When a crisis strikes you need an action plan that you can use in real time.
3. **Ensure you have communication when you need it most**. When your power is down or your network has been hacked, you must still be able to communicate.
4. **Build your supply chain resilience** by including your supply partners within your crises response platform.
5. **Practice makes perfect**. Test and test again, so that when you need it you are ready to respond quickly and effectively.

#1 - Good BC planning begins with identifying risk

Good business continuity planning is above all about identifying and mitigating risks to your corporate environment and, if that fails, **then having an excellent fall back plan in place** that can manage the business disruption event and get your operations up and running again as quickly as possible.

The BC planning process starts with a solid corporate risk assessment process. A good corporate governance structure will have a robust risk assessment process in place that produces a corporate risk register. This will identify the top half-dozen or more risks to the business, based on a combination of their impact on operations and their likelihood of happening. A risk that scores highly on both impact and likelihood will be marked as top priority for attention.

Once the top risks are identified then mitigating actions should be considered and plotted. This means developing a comprehensive set of actions that will significantly reduce either the likelihood of the risk manifesting, or the operational impact if it does happen. For example, installing smoke alarm detectors to alert you to a fire and sprinklers to put it out immediately.

The top risks are then re-assessed in the light of the mitigation planning and a new set of risks or a new priority order may emerge. This risk assessment process needs to be conducted on a least an annual basis and quite probably at a more frequent interval than that, depending on how quickly your corporate risk environment is subject to change.

If you need a starting place for your assessment of risk, there are existing pieces of research available that can help you. One of the more authoritative of these is the annual BCI Horizon Scan. The 2016 report highlighted the top business disruption risks as cyber attacks, data breaches and unplanned IT and telecoms outages.

This is all well and good, but it still leaves you with two situations in which, no matter what plans you lay, a significant business disruption event may occur.

The first situation involves **events that can be more or less predicted, but cannot be avoided or stopped**. Severe weather might be just such an event. You know that bad weather will occur, and you can probably even predict the season when it will take place. But you just can't stop it happening and you can only exercise limited influence over the impact when it does occur, given that you do not control the transport infrastructure.

The second situation involves what might be called a "black swan" event. This is **a disruption event that you cannot predict because it is outside the realm of your knowledge and experience**. A freak weather event, a plane crash or a terrorist attack could all be examples of a black swan event.

What you need to do next is to start scenario planning for your identified risk events, so that you can develop your response and recovery plans should they materialise. And, just as importantly, you can test these response plans with exercises to identify any flaws and adjust them accordingly. By definition, of course, you cannot scenario plan for a specific black swan event. Although you can plan and test your response to a generic unpredictable event that results in a given set of outcomes, such as loss of power, loss of access to your network and loss of access to your office for a set period of time.

#2 – Incident specific action plans help you respond more effectively

Once you have scoped out your risks and looked at the different scenarios that could develop, you are in a great position to plan your response. But you must now beware, because **this is the stage at which most BC plans leave the real world and enter the fantasy world of policy, procedure and backside covering**. Once you enter this fantasy world, then the end result is likely to be an amazing plan that keeps the policy wonks happy, ticks every possible compliance box, reassures the anxious bosses in the C-suite, but is actually completely useless when a real crisis takes place.

When the excrement hits the fan then the last thing you need is an encyclopaedia sized policy document that does not tell you in plain and simple language exactly what needs to be done, who needs to do it and when they need to have completed their tasks. **The most complete and well thought through BC plan is useless in real time if it cannot be used as an action guide**. In this scenario, the most likely thing to happen is that the policy book gets thrown aside and the response team starts to act on gut instinct alone. This would be a disaster.

Far better to have in place a series of short, risk specific, incident standard operating procedures (SOP) that will provide a step-by-step guide to essential tasks in the resolution of and recovery from the incident in question. You should produce at least one of these incident SOPs for each of the identified risks on your corporate risk register, and possibly several of them, segmented by response team, depending on the complexity of your organisation and the risk to be addressed.

Each incident SOP should be clear as to who is responsible for each task or task list, the exact steps that need to be undertaken, the time limit is for completion of these tasks and in what order the tasks should be completed. This might sound ridiculously simple, but **when the chips are down and everyone around you are losing their heads, and blaming it on you, a ridiculously simple set of instructions will help you to keep your head and guide the incident to a quick and effective resolution**.

This real time utility is the philosophy on which Crises Control is based. That is why we have built a library of over 200 potential incidents for our customers to populate and also why we will shortly be launching two new modules for the platform. The first of these is a task manager function with the ability to create a series of incident related task lists and manage the execution of these during a risk event. The second is a unique incident standard operating procedure wizard that will allow customers to create their own bespoke SOPs drawing on best practice and high quality content that is hosted on our platform.

Best practice #3 – Communication when you need it most

When a crisis hits then you need to move quickly to respond to it. **The quicker you respond the more impact you will have in terms of mitigating the event and reducing the short, medium and long-term impact of it**. If you can get your incident response up and running within what the emergency services call the golden hour, then your chances of significantly reducing the damage that is caused to your business and your reputation are greatly increased.

If you can respond quickly and effectively then you will reduce your disaster recovery costs and you stand a much better chance of not losing your customers to your competitors. But to respond quickly you need to make sure of two things.

The first is that **you must have a robust and multi-channel communications system in place with your employees, suppliers and even customers**. Having multiple channels of communications

available multiplies your chances of getting through to those people that you need to contact. Crises Control offers SMS, phone calls, e-mails and push notifications on our mobile app. **This reduces your dependence on either a mobile signal or on internet availability**.

The most common business disruption incident is a power outage. This is very likely to take out your internet communications at the same time. So just when you need it most, your e-mail system may well be unavailable. At that point you need alternatives. **Choose a cloud-hosted communications solution, to ensure that you are not dependant on either your servers or your power source**.

A cloud hosted solution will also come in useful for avoiding the second issue you will encounter. This is that if your incident response plans are hosted on your servers, which are unavailable because of a fire, flood or power outage, then they cannot be used just when you need them most. **To make sure that your incident response plans are available to you when disaster strikes then they must also be cloud hosted and ideally available to you on a mobile device**. You will then be able to manage the incident, using your carefully laid response plans, and return to business as usual as quickly as possible.

Best practice #4 – Building supply chain resilience

In our increasingly interconnected and contracted out world, where corporate supply chains are becoming ever longer, the risk and impact of business disruption at any point along the supply chain is a growing threat. Even the smallest of businesses are now dependent upon cloud hosted providers of data storage, CRM systems and website hosting. Others rely on telecoms, consultancy or utilities suppliers.

The BCI Supply Chain Resilience Report provides some very useful statistics on the problem. The 2016 reports indicates the top sources of supply chain disruption as unplanned telecommunications and IT outages, loss of talent or skills and cyber attack or data breach. **It reports that in the previous 12 months 66% of businesses did not have full supply chain visibility and 70% experienced at least one supply chain disruption**. Of the 70% of businesses who suffered a disruption, 53% incurred increased costs, 40% received customer complaints, 38% suffered damage to their reputation and 37% lost revenue.

There are a number of steps you can take to reduce the threat and impact of supply chain disruptions to your business.

- **Ensure you have full visibility of your supply chain**. Make sure you know exactly who is in your supply chain and whether your suppliers in turn have their own dependencies.
- **Include supply chain partners in your risk assessment process**, to understand what your full risks are. Also include supply chain disruption scenarios in your BC planning.
- Either help your supply chain partners to build their own resilience against disruption or, more likely, **choose suppliers who meet your own resiliency criteria**. Ask about this when you engage them.
- Finally, **include supply chain partners in your incident response planning and within your crisis communications channels**.

Best practice #5 – Practice makes perfect

The best laid plans can come to nothing if they have not been tested. The purpose of this is twofold. First of all, testing will help to ensure that the plan will work in practice. Secondly, testing will greatly increase the chances that the response team will know what they are doing when they are called into action.

There are two different types of test that can be carried out, a desktop/virtual exercise and a real/live exercise.

- A “desktop/virtual” exercise is a paper run through of your plans. This desktop exercise might simply be checking that all of your incident resources are in place, action plans are available, contact numbers are up to date and any physical supplies necessary are in place.
- It might also be a full virtual run through of a test exercise, involving real players and a real scenario that they do not know in advance. This test offers a good workout of your emergency plans, but without committing the resources needed for a live exercise, and so can be conducted on a regular basis, perhaps a couple of times a year.
- A “real/live exercise” is a test that involves your response team, and perhaps employees, in acting out a test scenario in real time and using real resources. The simplest example of this is the fire evacuation test, in which the fire alarm is activated and employees are required to leave the building and gather at the assembly point.
- A more complex version could involve your full response team acting out a live scenario in which they have to physically relocate to your disaster recovery site and open up the facilities there. Because of the resources involved in this, such an exercise would take place less often, perhaps every couple of years.

You should, as a minimum, carry out a desktop/virtual test at least once a year and follow this up with a review meeting in which you assess what lessons you have learnt and implement any necessary changes that you have discovered.

Here at Crises Control we not only encourage you to develop incident specific response plans for all of your identified risks, but we also help you to test these plans virtually with minimum cost and effort. You can use our platform to create a virtual/desktop exercise, and then run a test incident involving multiple locations and teams at the same time that will automatically generate a management report which records all of their response times. You can even schedule a test to start at some future point on time, say every Friday for a fire alarm test, or every six months for a full scale incident desktop exercise.

Our objective is not only to help get you up and running with your business continuity planning, but also to help you test your plans with regular desktop scenarios to see what you can learn before an incident is upon you.

Author

Tim Morris is Director of Marketing for Crises Control. He has worked in the field of corporate communications and disaster recovery for over 20 years. His roles have included the 24/7 press office at New Scotland Yard and being the Head of Communications and Community Engagement at Sussex Police. He has been personally involved in the operational response to a number of major incidents including the Southall rail crash, the Heathrow Terminal One fire and the terrorist bombing of Canary Wharf. He has lectured and conducted research in the field of communications in a variety of academic settings, including the University of the Arts, London and the Chartered Institute of Public Relations.