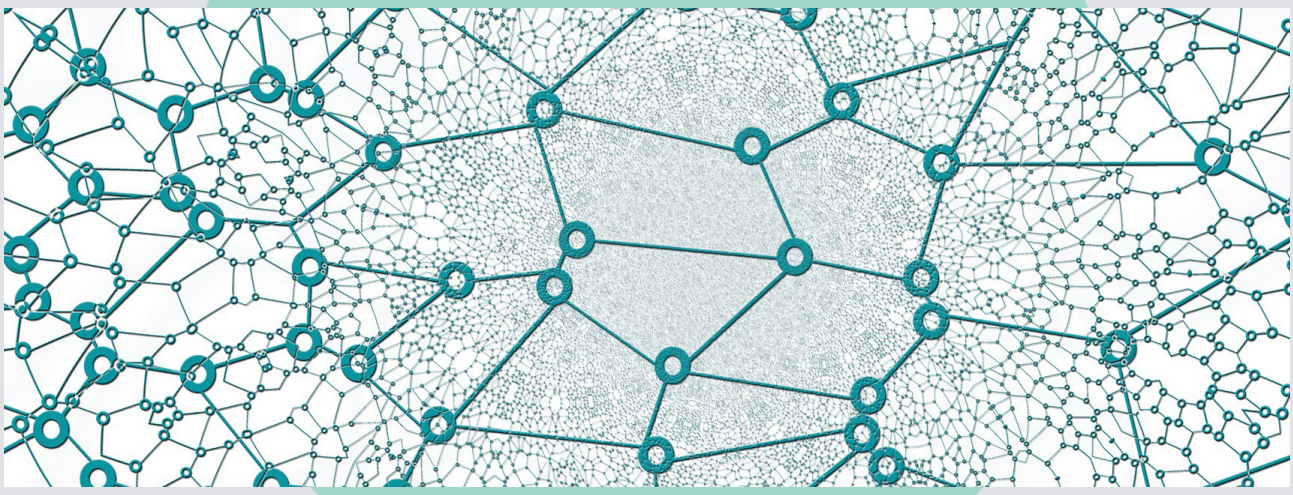
ac3.com.au

Business continuity planning and tech solutions



A guide to business continuity and disaster recovery planning. Why does your organisation need a business continuity plan? What does a comprehensive plan include and how should it be put into effect when the need arises?

AC3

Business continuity planning and tech solutions

For businesses and other organisations 2020 has brought with it some vital lessons. In Australia the year started with the horrific bushfires that covered many parts of the country and then, just as it was starting to recover from that, COVID-19 radically changed the landscape, affecting the lives, well-being and economic statuses of people across the world.

How do enterprises recover from such fundamentally life-changing upheavals and events? Because one of the key lessons of the first six months of the year is the critical necessity of having and executing a business continuity plan (BCP) when an unexpected disruption sends shockwaves through your organisation.

Many companies have had to, temporarily at least, close their doors. For them, business continuity has been about putting usual operations into hibernation and enacting a carefully considered plan of action to ensure they are on the front foot as soon as they are able to reopen and get back in business.

Other enterprises have seen their operations and procedures change radically. In these cases, the steps to business continuity have been more immediate and an absolute priority.

Very few organisations have been completely untouched by the events of the year so far, but even those that fall into this category will now be aware that sudden and unexpected disruption can severely affect any business. They will have realised that if they didn't have a well-conceived and detailed BCP before, it is imperative to ensure that they do now.

Future success or otherwise for all organisations will greatly depend on how prepared they are to negotiate the next unexpected disruption.

Further to this, the advantages of technology in business continuity are only becoming more widely understood and acknowledged, as the right managed services partner can ensure your business has the most fit for purpose processes and systems implemented to respond quickly and effectively to any unexpected disruption or cataclysmic event.

In the following chapters, we will explore how businesses can set up their workforces to reduce the impacts of disruption in times of need and how they can use various cloud tools, products and services to accomplish this.

Who needs a BCP?

In business continuity planning there are broadly two different types of organisations – first, those that must implement plans or execute a level of risk mitigation in order to be allowed to trade and to be compliant with a regulatory body. These companies are legally required to spend money on BCPs. Second, are those companies that aren't forced by law to create a BCP, but really should anyway.

Organisations that fall into the first category include those in industries like financial services and insurance markets – i.e. particularly organisations in those market verticals that are regulated by APRA (Australian Prudential Regulation Authority). The standards around how these organisations conduct their business, their business continuity and, particularly, their information security are extremely stringent. Addressing those business continuity standards means they often require a technology solution to assist them.

Examples of businesses in the second category may be manufacturing companies that have very traditional processes in place. For example, there is a conveyor belt, raw materials are put in one end and the finished widgets appear at the other. The goods go to a warehouse, are picked and packed and sent to the customer. Everything seems very straightforward until either one simple part of the internal process goes wrong or something unexpected happens externally and the system is derailed.

For instance, perhaps there's a label printer on the manufacturing line that breaks down and the supplier explains that the vital parts cannot be shipped for at least a week. If the business is making 1000 products an hour and that label stops printing labels, it becomes impossible to pack the stock as, without labels attached, the RFID (radio frequency identification) machine will have nothing to scan. The stock can't be packed, but is still being produced and in such quantities that there is soon too much to store. Ultimately, the line will need to be shut down, which is the single worst thing that can happen in a manufacturing organisation – costing possibly hundreds of thousands of dollars an hour in loss of productivity and revenues. This is an example of an internal issue.

A clear example of an external disruptor is the COVID-19 crisis. Some organisations may not even realise they need business continuity until, as with the 2020 pandemic, the Government tells them to send all their workers home and they have no idea how to do that. They have found themselves in a situation that they don't know how to tackle, because they have never faced it before and didn't think it would ever happen.

But this is where a good partner can utilise all of their collective knowledge and experience of working with other organisations to solve their disaster recovery (DR) problems and then create a bespoke technology solution for each individual business.

Clearly, meeting statutory compliance isn't the sole reason to ensure that your business has a comprehensive BCP in place. Whatever enterprise you operate, consider how technology comes into play around that part of your business continuity process. Inspect that component of your IT infrastructure and build resiliency into that.

A solid partnership with a service provider can prove invaluable. They will assist you to assess your processes and, even without previous DR preparation, they will indicate the good places to start and show how a few simple steps can immediately improve your position.

It's about continuous improvement and, fundamentally, how technology can support your business to continue operating when there are issues. What are the things you need to consider? What are the things that could happen? How can technology help you mitigate those risks?

Tailored solutions

An important element to remember at this point is that any DR solutions and BCPs should always be tailored to an organisation. There is no such thing as a one-size-fits-all. There may be common elements with other organisations' systems, but the overarching solution is always bespoke to the customer's needs. For example, you may have three different customers who all require a 15-minute recovery point objective (see page 10) as a service level, but they will need three very different solutions to achieve that service level.

Finance

In any DR situation, cash flow is likely to be a priority concern. Your managed service provider can help engineer a financial solution to ensure that you can solve that problem now and pay for it later. For organisations that have been putting off dealing with an issue due to capital expenditure reasons, it may actually be more affordable than first thought.

AC3 partners with HPE on a number of DR related products, whether they be storage, compute, network, Wi-Fi or remote access. GreenLake is a financial construct that allows the purchase of a range of equipment without paying for it all immediately – leading to the potential removal of a barrier to entry for an organisation that is trying to solve a problem, but doesn't necessarily have the ready cash to do so.

Cyber risk

According to the Cyber Risk Index, the top 10 countries that are the most attractive targets for cybercriminals are:

1. **Iceland**
2. **Sweden**
3. **United Arab Emirates**
4. **Norway**
5. **The US**
6. **Singapore**
7. **Ireland**
8. **New Zealand**
9. **Denmark**
10. **The UK**

What are the elements of BCP?

There are two main aspects of BCP:

Consideration of potential things that could go wrong and how to ensure the company survives and thrives

For example, what would a company do if the CEO is stuck overseas, her flights have been cancelled due to unexpected volcanic activity and she can't get to her laptop, the executive team are away on a team building retreat and the payroll is supposed to be delivered? How does that company create and execute plans of action to make sure it delivers business as usual?

What if the emergency has much greater reach and impact? In a situation like the COVID-19 pandemic, how does an enterprise ensure that it comes out of such a crisis as a vibrant entity with a future assured? Answering these overarching questions means breaking down into a series of clear steps the actions that must be taken depending on the nature of the crisis.

The area that many first associate with the term 'business continuity' is disaster recovery (DR). In the digital sphere this can be something as innocent as system failures leading to a production data centre losing power and perhaps needing to be offline for several days. Or there could be something more malevolent at play – company wide hacks or the deliberate disabling of infrastructure by a third party, for instance.

There are different responses required if, for example, your data centre burns down or, on the other hand, if all of your staff laptops become infected by malware. These are both cyber and digital-related issues, but with very different causes and will therefore need different BCPs.

There are, of course, many examples of unforeseen interruptions to business as usual that prompt DR plans – such as extreme weather events (flooding, cyclones, storms etc), bushfires or personnel challenges (key stakeholders unexpectedly leaving the organisation).

Different continuity challenges will require different responses, meaning that action plans will need to be tweaked and amended for the particular crisis in hand.

Some crises, such as COVID-19, will be so all-encompassing they will require BCPs that cover a wide range of areas, from economic and financial fallouts, to physical business operations, and health and wellbeing responses.

Risk assessment

As with many aspects of business planning, much thought and preparation is necessary regarding the likelihood of any of the imagined disasters actually occurring. While it would be foolhardy to set up a business on the coast of central and southern Queensland without planning for a possible flooding event, it could be a waste of resources to make similar preparations in parts of Australia where flooding and cyclones are less common, particularly the southern states, for example.

For an organisation based in Ipswich in Queensland near the Brisbane River, a company may choose to have a subset of staff elsewhere, in a designated DR site, with the capability to carry on business as usual if the floods of 2010 and 2011 are replicated and the primary site is evacuated. This, however, could cost $10,000 a month – so a risk benefit analysis should be carried out. 'We need to spend X amount based on how likely the scenario is.'

Another piece of the plan to consider is, once a back-up system has been implemented, is it accessible? There is no point in having one if it isn't regularly tested, because the day that you lose the data is not the day to find out whether it is actually accessible.

Key risk areas

The top risk factors identified in a Cyber Risk Index survey are:

- Data risk – R&D, financial, company confidential and customer accounts information.
- Cyber risk – phishing, clickjacking, botnets, fileless attacks and denial of service (DoS).
- Operational risk – disruption or damages to critical infrastructure, stolen or damaged equipment, consultancy expenses and productivity decline.
- Human capital or infrastructure risk – inadequate spend on recruitment and maintenance of security IT personnel, organisational misalignment and complexity, negligent and/or malicious insiders, server environment and shortage of qualified staff or education and training resources for employees about security.

Before the disaster

Drawing up the BCP

A BCP or range of BCPs needs to be put together by a number of business stakeholders – the CEO and the rest of the C-suite will be involved, particularly the CIO. But it's also imperative to have input from your managed service partner, human resources and facility managers.

Business continuity planning often requires fundamental changes to the infrastructure, both physical workspaces and the computer network, so the people who look after the environment in which your workforce operates will be integral to any planning. Are there any others who need to be involved? External advisers such as insurers, financial consultants or a preferred relocation company, for example?

Once you have your committee organised, it's time to put your BCP together. A typical BCP could include sections on the following:

- *Repair or replace damaged equipment and infrastructure*
  In a flood or bushfire event, for example, you may have lost vital equipment. How quickly will your business be able to replace or repair, in order to get systems up and running again?

- *Physical location*
  If moving from the primary site is necessary, how does this happen? Do any pieces of furniture or fixtures and fittings need to be relocated? What about computer systems and their servers? Is there a DR site all ready to spring into action? What about rent and other expenses at the primary site? It may be necessary to liaise with landlords to organise rent freezes or reductions during the period of the crisis, while also pausing or ceasing supplies of electricity, gas, water, sewerage or telecommunication systems. Who will oversee this?

- *Identification of critical systems*
  An important part of a DR BCP is pinpointing exactly which parts of the business or operation are the most vital. For example, if your company is running 200 applications in your primary site and there is a disaster that leads to you moving everything across to the DR site, the application that your company uses for people to work out whose turn it is to bring the food on 'sweet treats Monday' is not business critical, so that will not need to be replicated. Even something as important as payroll may not necessarily be a priority if the disaster happens at the beginning of the month and payroll isn't calculated until the end.

  There are not only decisions to be made about which applications need to run or be replicated but also at what capacity. Because speed and capacity also have cost implications. You may take the view that if the DR systems have to be run for a

week at the maximum, it may be bearable to have them running more slowly than usual. It will be a little painful for the staff utilising those systems, but less infrastructure is a way to reduce the cost. If the DR looks like being a long haul process, then any cost benefits of slower systems would be wiped out by the loss of productivity, not to mention the issue of staff grievances and frustrations.

- *Technology continuity*
  This is arguably the major component of any current BCP and the one that will be examined in greater detail in later chapters. If your business is not currently doing so, now would be a good time to partner with the right managed service provider that can advise regarding the implementation of a number of technology products and services that will place your business in the best possible position to mitigate any future disasters.

- *Outsourcing*
  It may be necessary to temporarily outsource or contract some of your operations. If so, what parts of the business can be outsourced and how will this be managed?

- *Human resources*
  Taking care of your employees' physical, mental and emotional well-being in times of stress and disruption is vital. Counselling services may be required. Where will these be sourced and who will oversee them? There may be extended sick or carer's leave required. Will this affect your operations? What provisions will you include in the BCP to ensure that this component is taken into consideration?

- *Communication*
  This is another major and vital part of any continuity planning – covering the everyday communication between team members and customers, suppliers, service providers and any other stakeholders, all the way to media releases and marketing. How will the business communicate effectively with the outside world to explain the current situation and how it intends to continue its operations?

- *Supply chain management*
  A physical relocation will have ongoing effects for many aspects of the business and supply chains may be severely impacted. How will this be addressed and managed?

As part of the planning process, it's also necessary to work out who is responsible for each action and task. Also consider what other resources may be needed.

Storage of the BCP

Once a plan has been developed and checked, and a schedule has been devised for regular testing, another important consideration is where the BCP is stored. For safety have both digital and hard copy versions. For the latter, if it lives in a locked safe in your head office and it's the head office that has just burned down, clearly that isn't going to work.

So, do you have a copy in a bank deposit box you can access quickly? Perhaps you store a copy at someone's home? Preferably this would be one that is close to either your primary or DR site. Or are there multiple copies, including one at your primary site and one at your DR site, but again always accessible?

Digitally, it is easier to have multiple copies available wherever they may be needed, and the safest thing of all is to utilise cloud storage. Storing anything, and especially a BCP, with a trusted cloud partner is much less risky than relying on a hard copy.

Training

One of the most important pieces of any BCP is staff training. This is not a 'set and forget' operation, but an ongoing and essential part of any DR preparation. Part of this training should include a detailed explanation of any BCPs and knowledge of where they're going to be living. This means that when the time comes to execute the plan, staff will not only know where to go to find out what to do, but will very likely have the first 10 steps in their heads already.

Regular risk assessments

As with training, risk assessment is not something that is carried out once and then ticked off and forgotten about. Well-prepared organisations will have a committee that meets monthly or quarterly to assess the changing situation, and consider current risks and potential future ones. They will stay alert as to what is reported in the media or what their competitors and external partners are experiencing. This way, they can recognise if a new risk or potential threat has also been faced by others and, possibly, learn from the way it was addressed or solved.

After the disaster

Before the BCP is enacted there are a number of clear steps to take:

- *Are our people safe?*
  Are there any actual physical threats such as those posed by extreme weather events, bomb threats, bush fires or climate-related emergencies? If so, the first thing to do may be to evacuate the building. Does your team know the safe evacuation points? Have they been paying attention during the regular fire drills? What about their mental and emotional well-being? A viral outbreak like COVID-19 doesn't just threaten the physical health of your staff and associates, but it can also cause great emotional distress, especially if the events are extremely unusual and have never been experienced before. There are many tell-tale signs that people are in a state of trauma – inability to focus on work can be one of them. Consultation with psychological experts may be a necessary but unexpected procedure.

- *Communicate*
  Get the key stakeholders together – the C-Level and, critically, the service providers and key suppliers – to help in the evaluation. Your plan should dictate who these stakeholders are.

- *Evaluation*
  Once it's clear that everyone is out of physical danger and able to resume their work from another location, whether this be a DR site or their own homes, the next step is to evaluate the exact nature and extent of the disaster. From a technological solution aspect, it may actually be unnecessary to execute the BCP.

For example, you may have a BCP that includes bringing up your DR site as your primary data centre, which can take time. From a cost risk perspective, it's necessary to assess whether it's worth making the move. There are two key phrases here: recovery point objective and recovery time objective.

The former indicates the age of the data that you will be recovering. Will it be five minutes,five hours or five days? Usually the smaller the point objective, the larger the cost to achieve it.

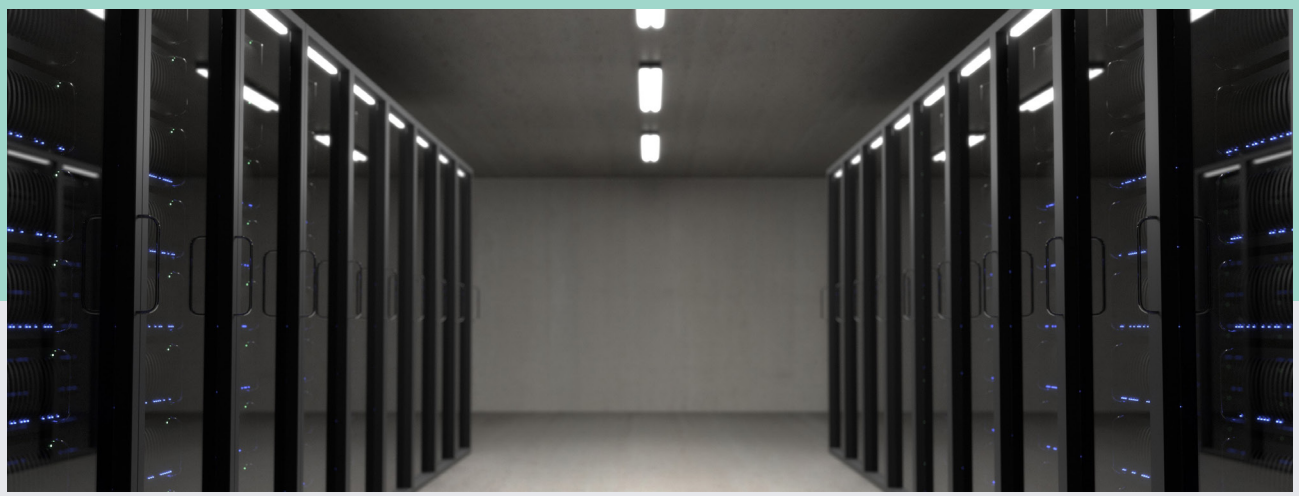
The recovery time objectives relate to the time it takes to bring full operations back up to speed. If there has been a loss of power to your primary data centre, for example, and it's an eight-hour process to get the DR site up to speed, but you've been informed by the supplier that the power will be restored in four hours, there's not much point in kick-starting your BCP, as the problem should be over by then. So, evaluation is a primary consideration as there is always a cost and risk associated with most BCPs.

There is also a cost to the business of rolling back the DR plan to move back to normal production systems – another interruption and outage to pull the data back. This also needs to be weighed up in the cost risk assessment.

- *Enacting the BCP*
  Once the evaluation has determined that it is necessary to execute the BCP, consult the checklist and mobilise the team who will be responsible for overseeing its individual parts – internal stakeholders and service providers, for example. Who needs to be in the communication loop? Who needs to be involved? Get these people on the phone and start running through the checklist.

- *Digital recovery*
  Top of the checklist is ensuring that all staff have everything they need to carry on. Do they all have laptops? Are there VPNs (virtual private networks) in place? Can they safely and securely access the company servers remotely? Are there team sharing and communication protocols set up, such as Microsoft Teams, Zoom etc? Do you have the right firewalls in place? What about anti-virus and anti-malware software? Is this installed across the laptops of the entire team?

Technology



As previously noted, arguably the major component of any business continuity planning today is technology. Here is where the right managed service provider can help you navigate the myriad of products and systems available to ensure that your business has the resilience, flexibility and capability to survive any crisis it faces. And not only survive, but thrive.

Infrastructure to scale

No matter the crisis, for business continuity to be successfully addressed one of the first steps that must be taken is ensuring that your digital infrastructure is able to be scaled to cope with a new or evolving situation. In the case of COVID-19, all of the systems at AC3, for example, were in perfect working order, but the people accessing those systems had to move. Suddenly, like thousands of companies around the world, it was necessary to plan for staff working from home for possibly three or four months ahead or even longer.

So what happens when you have to unexpectedly evacuate the office? After the basics (ensuring all staff have laptops they can use and that remote workers are able to access the corporate systems), data storage and the ability to scale it is a priority. Infrastructure as a Service (IaaS) is a type of cloud computing that provides virtualised computing resources over the internet. It is one of the three main categories of cloud computing services, alongside Software as a Service (SaaS) and Platform as a Service (PaaS). And it is a valuable tool in your arsenal when it comes to DR, offering a cost-effective and scalable solution that is much easier to manage than on-premises options, particularly when it may be the very premises that are the source of the disaster.

Do take into consideration the potential surges in application workloads and unprecedented demand. During the COVID-19 crisis, hundreds of thousands of homes were suddenly requiring Wi-Fi access at much greater magnitude than ever before. With your staff working remotely, will this lead to unusual levels of demand and access requirements? How will this be addressed?

Location

Some organisations take the public cloud approach, but there are considerations to take into account. One thing to consider is the issue of data sovereignty. Some organisations may seek cheaper and more cost-effective ways to replicate data, but they should always perform due diligence. There may be complications around where some of that data is stored. Such solutions may seem cost-effective, but in solving one problem it could well create several others from a regulatory or compliance standpoint.

Also, a core issue is the possible difference in approaches required for current and legacy systems. There are two challenges regarding replicating legacy technology to an alternative location in a specific time-frame.

It's important that you're able to recover legacy systems as quickly as you can recover new parts of your technology environment.

In a new environment, there could be custom or bespoke apps that may or may not be operating in the public cloud. What level of integration do these custom or bespoke apps or boutique, independent software vendors offer with other third-party applications versus mainstream applications, such as any Microsoft-based application, for example?

Hybrid cloud

The key advantage of a hybrid cloud solution relates to the fact that, despite common requirements, each end-to-end technology solution needs to be tailored to a customer's individual environment. You will be working with a multitude of vendors, but a trusted partner will be able to help your business integrate all of those elements together into one DR solution that allows you to move it all over and recover it as needed. They will assist you to work backwards from the types of events you're anticipating. The outcome will be dependent upon what you are trying to achieve and this is again why solutions are different for every company.

Another consideration is location, as requirements can change depending on where an organisation is sited geographically. If, for example, your organisation is operating outside of a major city, where access to data centres may be an issue, you may find it is not possible to run all of your DR environment in completely geographically separate locations, that are far enough away from one another.

When you are pushing data across, you are typically paying for everything by the hour, minute or even second, depending on the cloud. But you don't necessarily need every application turned on.

In a traditional model, you may have a primary and a secondary data centre and you have to replicate all the storage across. Even if nothing is turned on in the secondary centre, you have to have the compute there running, so that the service can run your workloads. But your services provider should be able to organise a leveraged model with two or more customers and won't charge you to manage those virtual machines (VMs) that aren't running, because ultimately this isn't working at the same level as hyper scale providers.

Once you go to a hybrid cloud solution, you have the ability to replicate your storage and pay for it in the public cloud, but the VMs don't get turned on until the minute they are needed – the moment the BCP is implemented. The potential cost savings here can be considerable.

Again, the lesson is to partner with an organisation that can take on this complexity on your behalf and craft a solution that makes it simple.

Data storage in DR

To ensure your business doesn't fall prey to loss of data and productivity, consider how you are going to protect that data and where it is going to be safely stored.

There are a couple of potential approaches. One solution is to have real time or close to real time replication; i.e. replication between storage arrays. So you can have a storage array at one data centre, and one at the other, and those two storage arrays talk to each other and replicate all the data directly across. The potential disadvantage is that, with a simple replication, the storage array at the master site is going to be the exact same size and specifications as the one in the secondary site. This obviously has cost implications.

An alternative approach is to go up a level and have, potentially, your hypervisor or virtualisation layer doing that replication. This way you can stipulate which of your machines you want replicated from one site to another, leading to potentially less storage needed.

Right sizing your environments

An important element to take into account in a DR situation that is specifically around business continuity and should come into the BCP, concerns the length of time the situation will last and so what size of environment you will require. Hopefully, the crisis will be in the hours, days or weeks, rather than months or years, but all of those scenarios have different capacity needs.

Perhaps, normally you have a payroll application supported by four servers. If you need to go to half the RAM and then half the CPU, operations will be slow and and somewhat painful, but everything will still work and be good enough for the short term. The longer the situation lasts, the more unpalatable a smaller size infrastructure

becomes. And moving applications to the cloud may prevent much frustration and loss of productivity.

Cloud economics and demand fluctations

Moving applications to the cloud is where cloud economics really comes to the fore. Traditionally, with a private cloud environment, there will be a lot of fat built into the infrastructure that you may deploy for applications, because you're making a capex (capital expenditure) purchase and you have the hardware sitting on the ground. You need to have that extra capacity so that you can scale up or down as necessary and not find yourself constantly in the position of needing to buy further hardware.

This means, with a private cloud arrangement there will often only be from 30 to 50 percent utilisation and the upper end of that is solely if the user is running the system hard.

With the public cloud, you can use and, importantly, pay for only what you need. It's possible to tune to the amount of memory or CPU, the particular instance size, that an application uses in a matter of seconds. It's simply a matter of popping into a console or management tool and changing the instance size to be larger or smaller as needed.

And you pay as you go, so you can begin by experimenting with the smallest server you imagine may suffice and then scaling up as necessary, maximising the value and not overspending at any point.

Weighing up the pros and cons

In a similar vein it's easy to over or underestimate the costs that may be involved in regard to migration. If you have, for example, an application where if you move it exactly as it is and don't take advantage of any of the native services that the cloud providers are offering – especially if you don't do the right sizing – it may end up costing you more on a public cloud.

However, when you take all the elements into account, you may have an application with a queuing system. Perhaps you have two or three servers to run the queuing system. This is opposed to a native queuing tool in a system like AWS or Azure where you pay a set fee, say 40 cents, per million items sent to the queue.

In this case, there is a substantial cost benefit by doing even small amounts of refactoring or rearchitecturing of your application before doing a large refactor. A few small refactors may give you some really quick wins in terms of savings, whereas a major refactor can be so significant it may even require a capex expense to transform the application.

Depending on the application and how long it's going to live, such moves may or may not be valuable and it may be preferable to simply pay the slightly higher opex (operating expense). It's an application by application decision.

Similarly, there are organisations that are hesitant when looking at the cloud, concerned that they may lose their flexibility,

asking questions like, 'I'm going to run these workloads in AWS today, but what happens if I want to move them to Azure for some reason?' The danger of holding back from being cloud agnostic is that this can end up reducing the architecture of the applications down to the lowest common denominator – just compute and storage. You will be able to do a quick migration from one cloud provider to another, but you will not be able to take advantage of the native tools and get the cost savings.

A far more advisable approach is to keep the cloud that has the right native tool sets and features to give you the best outcome on a workload by workload or application by application basis. Make the decision based on what makes the most sense for what it is you're trying to migrate.

SecOps

Security should be top of mind in both regular operations and DR. It must be a vital component of any BCP. Liz Joyce is the CISO (Chief Information Security Officer) at Hewlett Packard Enterprise (HPE). On the enterprise.nxt web portal she explains how cybersecurity threats have changed in recent years. According to Joyce, the four key things are now: "the scale of an attack, the speed of an attack, the attack's sophistication and the organisation of the adversaries you are dealing with".

She notes how breaches that may have happened on an annual basis are now regular occurrences, with millions of records attacked in a single incident. "It's not an issue of if companies are going to have an incident, it's when they are going to have one," she says. "And it's not only about how you react but also very importantly… is how you recover."

When considering the Security Operations Procedures in DR and BCP the priority is to emphasise the necessity of always being mindful of security in everything the organisation does. The BCP should consider what those security risks may be – data loss, data being encrypted or stolen, for example. When you're implementing any new architecture or design, ensure that the security implications involved have been addressed. Do you have the right firewalls in place? Are any secrets or confidential information being stored in the right way, so that they're not sitting anywhere that is public?

How do you make sure that these places are not accessible? Do you have monitoring in place to know if data is leaking or is secure? It requires a continual security mindset, and constant mitigation of risks.

Holistic approach to SecOps

When choosing technology vendors and/or managed service providers, look for those that can provide you with holistic and unique solutions. HPE is known for its holistic approach and for having the most secure industry standard servers.

The company has developed a secure compute life cycle with a number of standout factors:

- ***Silicon root of trust***
  The company designs its own silicon and firmware, unlike organisations that use off-the-shelf solutions. The essential firmware is anchored within the silicon and this digital fingerprint ensures that the server will simply not boot if the firmware is compromised in any way.

- ***Firmware threat detection***
  This tool ensures that organisations will know on a daily basis if their firmware has been compromised.

- ***Tape supporting GDPR***
  Integral to HPE solutions is compliance with general data protection regulations (GDPR), which demand that organisations fortify their cybersecurity and risk management portfolios.

Staff management

Security awareness training

A culture of SecOps mindfulness is only as successful as the people involved. Staff training should not just be regular but also conducted in the right way. Ensure you're asking the correct questions and educating staff as to the potential traps they should be looking out for.

When you're considering a new vendor, there are many security questions that will be asked. Every time you are having that conversation, you will go through those questions. The right service providers will be able to do static analysis of code and conduct penetration testing.

But on an individual level, especially in a situation where people are suddenly working remotely, it's vital that all devices are protected and all users are informed of any potential hazards. During the COVID-19 crisis, virus related scams were common, so ensure that your employees take precautions when encountering any communications that may seem even slightly suspicious.

In an office environment, it's simple to approach a co-worker to check the validity of an email. If someone is working from home and receives a message that appears to be from their employer but is asking them to transfer money to a specified account, they need to be prepared to query such an instruction and to be on their guard at all times.

Staff productivity and operational resilience

As you move into a cloud environment, this will also have an effect on your staff and their ways of working. You no longer have to worry about running a data centre, as all of this will be taken care of for you. You also will not need to be concerned about running physical servers on physical networks, as most of this will be taken care of too. Whether you choose a hybrid model or a private cloud, using a managed service provider also ensures this is all taken care of for you and you will no longer need to be concerned about travelling to the datacentre.

The difference in the types of operations you will now be running also potentially applies to the difference in staff productivity. Instead of travelling out to a data centre, you're logging into an API and simply ordering a new server, a new type of VM or a new native tool. This again will be taken care of for you if you partner with a managed service provider.

Productivity increases can also be linked to beginning to take a DevOps or Agile approach to projects and deployment, with staff using more modern techniques and tools for solving workload problems.

Always remember that without your staff, there is no business or organisation and the most important piece of your BCP to get right concerns them. Excellent planning and smooth execution of a BCP that puts staff and their tools at the forefront is your best possible chance of success – to ensure that your organisation doesn't just survive in a DR situation, but comes out even stronger than before.

Tools for remote working

To ensure your staff are supported and able to maintain their productivity there are multiple products and services available.

For work-from-home initiatives, pop-up locations, and temporary facilities, HPE can also provide seamless and secure access to corporate resources at scale with Aruba Remote Access Points (RAPs) or Aruba VIA VPN access for single client solutions or IAP-VPN for multiple clients.

Aruba also offers an extensive portfolio of outdoor Access Points (APs) to be used in outdoor pop-up locations extending the corporate network. With these solutions, organisations can quickly deliver secure network connectivity and the office experience to mobile workers and remote offices with plug-and-play access points, zero-touch provisioning, multi-level security, and remote management with robust, highly scalable Aruba VPN, on premises or cloud-based platforms. The experience has been designed to be simple, with Zero Touch Set Up in three easy steps.

Hearing Australia DR platform

The challenge

Government organisation Hearing Australia had a disaster recovery (DR) platform that was in need of an overhaul. The platform worked but was "costly, complex and not optimised" according to the organisation's CTO, Andrew Bakhsh.

The use of multiple different technologies made it difficult to keep it up-to-date and maintain. The issue was not core to the business, but was undeniably an important one to resolve.

The solution

An internal review was conducted, which led to a 'request for a quote' process to identify a managed service provider able to deliver a suitable replacement system.

AC3 was selected due to its considerable experience across local, state and federal government spaces, as well as its flexibility around licensing, options and solutions, as part of the overall technology.

The third vital component was the ability to have a larger computer network to provide Hearing Australia with scalability and room to grow.

AC3 deployed a dedicated project team with in-house specialist engineers and solution architects. The team examined the Hearing Australia environment and developed a hybrid cloud solution, similar to the one used by the New South Wales Government.

The solution brought together major partners including HPE, VMware, Microsoft and Oracle.

The results

Hearing Australia is extremely satisfied with the outcome. The new system has been found to be very secure and "gave us a lot of confidence" says Bakhsh. "It gave us a really all-encompassing solution.

"The results have been astounding," he continues. Benefits include cost reductions and 50 percent improvements in both net recovery point objectives and recovery time objectives.

The system is available 24/7 and is scalable. "It's an effective tool in helping us manage that business compliance risk," says Bakhsh.

"What the team and I have definitely learned is that getting AC3 as a managed service provider has given us confidence that these business critical tasks – which are not core to our business – can be taken outside and we then have the ability to focus on more strategic tasks that add value to the organisation."