DISASTER RECOVERY

Peter Groucutt *explains why it's so important and why organisations need to keep it font of mind*

As a society we are increasingly dependent on technology to keep businesses running smoothly. While tech has brought many benefits, our reliance on it can mean that any type of incident – whether a premeditated criminal cyber attack, human error, technical glitch or natural disaster – can result in data loss and downtime.

To make sure organisations are as resilient as possible they must have a Business Continuity Plan (BCP) plan in place. Within that plan, comprehensive IT Disaster Recovery (DR) capabilities – to ensure minimal disruption in the wake of an incident – are essential.

Over the last few years there have been hundreds of examples of cyber attacks having a severe impact in both the public and private sector. In 2017, the NHS was seriously affected by what Mikko Hypponen, chief research officer at F-Secure, called: "the biggest ransomware outbreak in history", when WannaCry malware infected hospitals and doctors' surgeries across England and Scotland. This forced staff to turn away patients and even cancel appointments.

The NHS is not the only public service to fall victim to this type of attack, as a recent Freedom of Information request revealed that local authorities and councils in the UK were hit by more than 263-million cyber attacks in the first six months of 2019.

The private sector has suffered in much the same way, with high-profile attacks on global aluminium company, Norsk Hydro in June and shipping services company Pitney Bowes in October. These examples illustrate just how important it is for appropriate BC plans to be in place so operations can continue in the event of a crisis.

For large enterprises with multiple offices in different locations it also highlights why it is essential for seamless and coherent communication between internal IT, security and BC teams. By working together closely and sharing information it is easier to assess the potential risk and therefore coordinate a unified response.

Although cyber attacks are dominating the headlines, more seemingly mundane technical faults can wreak just as much havoc, as the financial services sector has experienced recently. In April last year, TSB suffered a systems migration failure after attempting to move customer records onto its own platform. The company was forced to pay approximately £330-million in fines and suffered reputation damage that forced CEO Paul Pester to resign.

In June 2018, a hardware problem at Visa resulted in around 5.2-million failed payments, affecting customers in the UK, Europe and abroad. Just five months later, a glitch in Barclays' online banking systems meant customers were locked out of their accounts.

These incidents prompted the government to debate the issue as part of its recent Treasury Committee. The committee published a report on the 'unacceptable' number of IT failures across the financial services sector. The report recommends – and rightly so – that in our tech-dependent society, more must to be done to improve operational resilience and accountability. This shows that BC is rising up the agenda, which can only be a good thing.

IT resilience is especially significant in the current era of digital transformation, as organisations increasingly migrate from outdated legacy technology to take advantage of the agility offered by cloud service providers. The cloud services market is an oligopoly, dominated by Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP).

These platforms have revolutionised the way we deploy and manage IT, but relying on a small number of cloud providers centralises risk. You may think you are more resilient now because you use several different cloud services, theoretically reducing the chance of an outage affecting all systems at the same time. However, a large proportion of internet services and business operations could become inactive if one of the main cloud providers suffers an outage.

TIGHT COLLABORATION BETWEEN IT OPERATIONS, CYBER AND BC TEAMS IS ABSOLUTELY VITAL

For example, an AWS outage in February 2017 affected services including Spotify, Dropbox and Trello. Another failure in 2018 impacted Atlassian, Twilio and Slack. AWS services went down again in October 2019, this time due to a malicious DDoS attack.

To make IT resilient and improve the ability to recover from incidents it needs to be clear where exactly DR sits within the wider Business Continuity Plan (BCP). The two terms are often conflated and we prefer to use the term *IT Disaster Recovery* to make the distinction clearer.

Business Continuity is the catch-all term for all aspects of resilience, including people, premises and suppliers. IT Disaster Recovery specifically refers to how an organisation recovers IT systems if it suffers an outage. It can feel like the IT DR is a large slice of the BC pie, and as a result, continuity planning sometimes takes a technology-first approach, but that is a mistake. The problem with technology-centric continuity is that it can produce rapidly recovered servers, but a team unable to use them. It can also encourage over spending on unnecessary capabilities. The best approach is to start with the real BC work first and set recovery objectives before thinking about backup, recovery and replication technologies.

The creation of the individual plans themselves (Business Continuity Plan, IT Disaster Recovery Plan) come relatively late in the 'enacting' stage. Once the team and scope has been decided, the biggest part of BC planning is assessing the risks (Risk Register) and the impact they could have (Business Impact Analysis).

Although cyber attacks dominate the headlines, more mundane technical faults can wreak just as much havoc

Your Risk Register should be changing to reflect a higher likelihood of particular risks such as cyber attacks. It should also be updated to reflect the greater impact of other risks such as the outage of a major cloud provider.

One of the problems many businesses face is creating a joined-up approach to BC. As the cyber threat has grown, so too have cyber teams. In larger organisations, responding to a major incident will require BC, IT operations and cyber security staff working closely together to quickly diagnose, respond and rectify the problem.

Cyber-related incidents demand the unique skillsets of each team because they can be more difficult to recover from than traditional incidents. If there is a flood or fire in a data centre, the IT team can simply fail-over to a secondary data centre or cloud-hosted DR. The flood or fire might still be happening, but it will not affect the DR site and if staff are capable of working remotely, there may only be an IT outage of hours or even minutes.

With cyber incidents, failing over to a secondary site may not help as it carries the problem over. For example, when recovering from a ransomware attack, the IT and security teams may need to carry out several recoveries to retrieve a clean version of the data before the infection.

The cyber team is responsible for detecting attacks and eradicating any infection before operations can be safely restored by IT. Tight collaboration between IT Operations, cyber and BC teams is vital for an accurate understanding of risk and the potential impact of attacks.

The first step in reducing cloud risk is to get a handle on where cloud services are hosted. For Infrastructure as a Service (IaaS), it should be clear which data centres (or regions and zones) the data is hosted from. For Software as a Service (SaaS), investigation may be required to locate where these services are hosted from. They may run from their own data centres, or they too may be hosted in the public cloud with AWS, Azure or GCP.

The next step is to find out the level of resilience built into those respective cloud services. With IaaS, the tools are available to build resilience into every layer of infrastructure, from the data centres themselves, through storage, server and networking. But it is the customers' responsibility. In the early days of cloud computing, many

▶

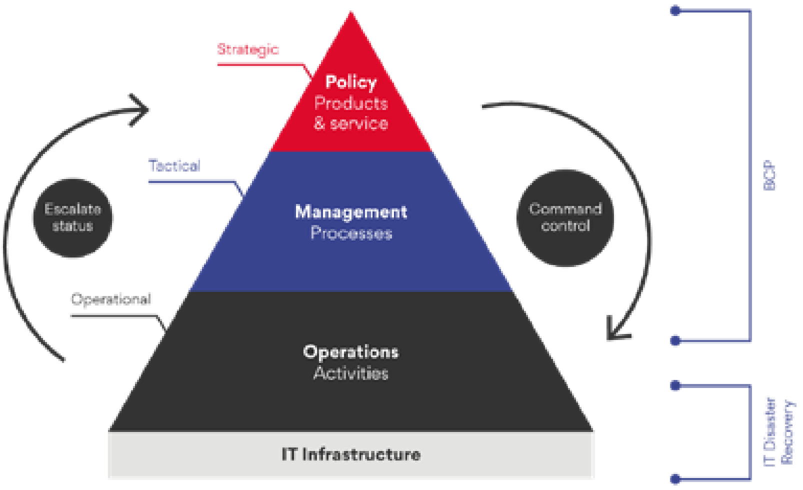
	STAGE	ACTIVITY	
1	Policy	Identify scope of urgent business functions and create the Management Business Continuity Statement	Planning
2	Select teams and determine responsibility	Selection and setting culture, attitude, behaviours	
3a	Determine impact on the business	Business Impact Analysis (BIA) – people, premises, resources, suppliers	
3b	Risk/threat identification	Risk register and matrix	
4	Identify urgent functions (IT & other services)	Service catalogues & technology-service dependency mapping	
5a	Implement mitigation strategies	Put the capability in place	Enacting
5b	Agree activation plans	Writing the runbooks & communication plans	
6a	Exercise & Test	Agree test scenarios, documentation and KPIs	Testing and Maintenance
6b	Ongoing changes and maintenance	Plan exercises, maintain and keep BC & IT DR plans up to date	

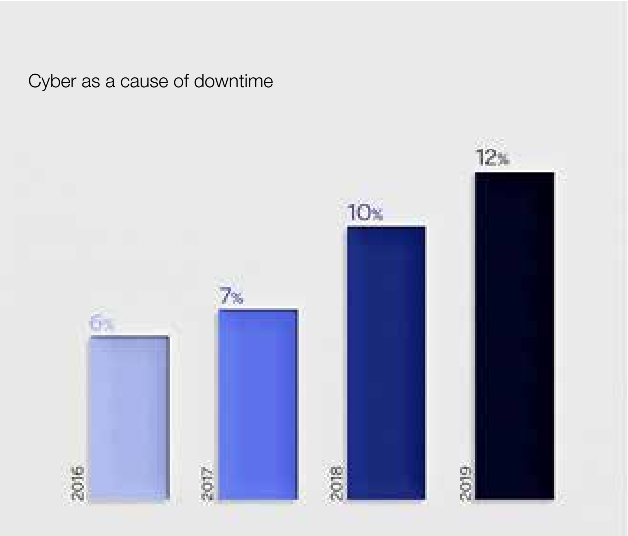
Peter Groucutt, Databarracks' Managing Director, founded the business in 2003 after working in risk management roles in the banking sector. Peter's main focus is to combine technology with a passion for customer service.

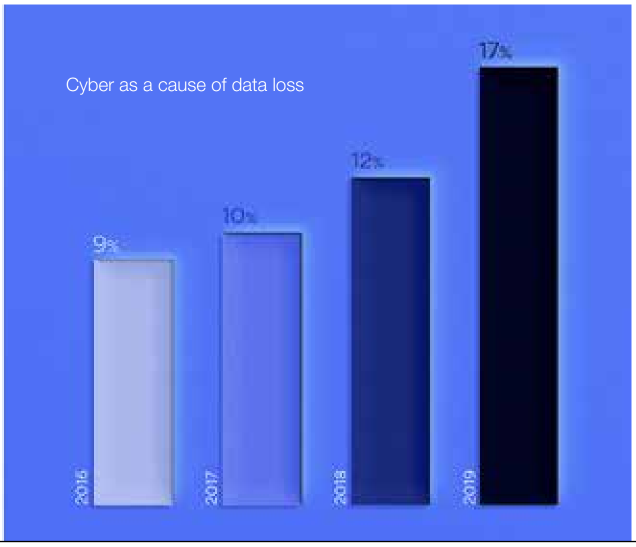
incorrectly assumed that DR was the sole responsibility of the cloud provider, but it actually works on a shared responsibility model. The cloud provider is accountable for some parts of the technology stack while the customer is for others.

Our final recommendation is to diversify risk by using more than one cloud provider. At a minimum, this means keeping a back-up copy of data outside the production cloud. It is also possible to build resilience across multiple cloud providers.

Containers and Infrastructure as Code (IaC) both allow you to build and destroy environments quickly and repeatedly across multiple clouds. The long-term benefits extend beyond resilience, by taking advantage of pricing and performance differences between cloud providers that enables greater freedom of movement ●




Cyber as a cause of downtime


Cyber as a cause of data loss