The past, present and future of business continuity and disaster recovery

By Dr Sandra Bell 4 hours ago

A birds eye view on the past, present and future of business continuity and disaster recovery.

(Image credit: Image Credit: alphaspirit / Shutterstock)

At the time of the Industrial Revolution, merchants would have been concerned with maintaining the supply of raw materials if their ships sank. During the Second World War, businesses would have worried about surviving if they were bombed, or if rationing impacted their supplies. Today, in addition to natural disasters such as hurricane, fires, floods and pandemic and man-made issues such as wars, organisations face other challenges to their operations. A modern business now has to contend with widespread economic and political instability, organised cybercrime and eco-terrorist attacks. Likewise, their vulnerabilities have changed. Disruptive technologies such as AI and the IoT together with hyper-extended supply chains have a created a level of operational complexity where vulnerabilities are hard to detect and even harder to protect.

Yet, regardless of whether it's the 18th or the 21st Century, the cost of operational disruption can potentially be devastating to a business.

- Business continuity - the cornerstone of the build vs. buy debate

The technological revolution and the need for disaster recovery

Planning, investing and committing resources for events that you do not want to happen yet are possible, poses a dichotomy for a business. On one hand it seems prudent to invest based on the costs of the potential downside. But, on the other, it is impossible to anticipate all possible scenarios and therefore investment may prove futile. For many years this dichotomy led organisations to primarily respond in an ad hoc manner to disruptions and it wasn't until the technological revolution of the 1970s that business continuity became a formal discipline.

During the 1970s general purpose computer systems started to become readily available and provided businesses with an integrated single information management system. Improvements in productivity, service, efficiency etc. were realised almost overnight leading to an explosion in innovation and widespread adoption. However, the newness of the systems together with organisation and operator inexperience introduced a systemic business vulnerability.

Due to commercial pressures, organisations started to voluntarily invest in standby systems and critical data backups to reduce their risk exposure. But when information technology started to directly impact the economic wellbeing of citizens by facilitating a variety of operational intra- and inter-bank activities such as Bankers' Automated Clearing System (BACS), Society for World-wide Interbank Funds Transfer (SWIFT) and the development of electronic funds transfer at point of sale (EFTPOS), regulators started to step in, and require disaster recovery planning. One of the first was the US Foreign Corrupt Practices Act (FCPA). Introduced in 1977 to prevent and prosecute instances of corporate bribery of foreign officials, it required organisations to make specific arrangements for keeping and protecting vital company records from destruction. As such records were increasingly stored in electronic form, it thereby necessitated processes for data backup and restoration.

Shift from technical recovery to the continuing operation of a business

The business impact of terrorist events, such as the London Stock Exchange in 1990, World Trade Centre in 1993 and the London financial district in 1992 and 1993, signalled a new threat to organisations and demonstrated that they needed to be able to systematically protect and restore all aspects of value-generating activities not simply protect and recover the IT systems that supported them. Business Continuity emerged as a formal discipline with the aim of preserving

essential customer services, revenue generation, essential support services, customer, shareholder and employee confidence, and the public image of the company.

The formation of the US Disaster Recovery Institute (DRI) in 1988 and the UK-based Business Continuity Institute (BCI) in 1994 helped formalise business continuity as a management discipline with membership criteria, certification standards, and training guidelines.

- Disaster recovery is not a luxury

Post 9/11 – the emergence of rules and automated plans

The terrorist attacks in New York and Washington in September 2001 brought home the possibility of extreme events together with the fact that the resilience of nations is largely dependent on the resilience of the private sector businesses, large and small, that provide essential products and services to the citizens.

Guidelines, standards and regulations snowballed, and what was previously a practitioner-led discipline, where solutions were often ad-hoc and specific needs to the individual business, became an specialist-led discipline with its own language, academics and tailormade solutions such as Work Area Recovery that combined a standby workplace with the IT systems and data necessary to carry on work as normal.

Likewise, the emphasis shifted from culture and awareness to the existence formal plans – the production of which was often automated by one of the myriad of business continuity software planning tools that emerged in the market.

The present - Cyberthreats and other strategic threats

Just like any business, technology doesn't stand still, it is constantly evolving and changing. Likewise, malware such as ransomware and worms are keeping pace with technological advancements, and they pose a real threat. For instance, ransomware attacks skyrocketed in 2017, with WannaCry crippling thousands of businesses, while the Petya crypto-virus knocked out the likes of multinational shipping firm Maersk, British advertising company WPP and pharmaceutical company Merck. The losses from the WannaCry attack have been estimated to be as high as $4 billion worldwide.

Whilst the source of the problem may be with the IT system, and the major disruption to operations, the primary impact of a cyberattack is strategic as you need to be prepared to adapt your response in real time. The attackers will adapt their strategies in response to your defensive moves and therefore if you are not ready, or able, to adapt your plan you are likely to be defeated.

There will also be many stakeholders involved, creating a complex (as opposed to complicated) environment and certain courses of action may have unintended consequences that need to be countered in real time.

It would therefore be easy to say that there is no point having a plan if it is never going to work. However – you need a piste in the first place if you want to go “off piste”, and you never find a sports coach suggesting that there is no point in learning set pieces as the exact situation will never occur in a real game.

The current focus for business continuity is therefore on the process of planning rather than the plans themselves. During the planning process knowledge about how the organisation operates is generated and shared that never normally comes to light. Knowledge about what is important from other people’s perspectives, such as senior management and customers, is also generated.

This knowledge allows the organisation to adapt their plans to the specific circumstances – rather than just simply fold when they face the unexpected.

The future of business continuity

In today’s consumer-driven, complex, always-on world of 24hr news cycles and social media it is almost impossible to have an “isolated incident” as even minor glitches hit social media feeds within minutes of them happening. Likewise, it is a very rare customer that is happy to wait while a disrupted organisation executes a heroic recovery – they are much more likely to turn to competitors.

As the risk landscape in which organisations operate becomes ever more complex, uncertain organisations will increasingly have to be able to display innovation in the face of adversity. However, the innovation process requires people to have the confidence to innovate together with time to think and experiment. The Business Continuity process not only provides clarity on the priority organisational processes, a set of exemplar responses for anticipated scenarios, but, through training and exercise programmes, a safe environment to experiment and practice innovation under stress.

Therefore next time someone says you need to update your BIA or attend a table top exercise don’t think of it as you wasting your time to help the Business Continuity Manager write a plan and tick a compliance box but an opportunity to find out what the business continuity process can do for you.

- GDPR and disaster recovery compliance – who does the buck stop with?

Dr Sandra Bell, Head of Resilience Consulting, Sungard Availability Services