Sponsored by

ContinuityLogic

CIR
CONTINUITY INSURANCE & RISK
thinking resilience

Truly resilient organisations need much more agility than traditional business continuity plans may be able to afford. This is the theme of a new series of events being held in the UK to explore the options. CIR went along to listen to the speakers p34

Evolving priorities and organisational change are driving the need for a different approach to business continuity. Paul Gant explains the role enterprise software can play in powering the complex shift from traditional planning to resilience p36

Resilience for thought leaders

ContinuityLogic

Sponsored by

Thinking ahead

Truly resilient organisations need much more agility than traditional business continuity plans may be able to afford. This is the theme of a new series of events being held in the UK to explore the options. CIR went along to listen to the speakers

As headlines frequently remind us and, increasingly, first-hand experience hammers home the message, cyber attacks can have wide-ranging and long-lasting impacts for organisations. Creating resilience to cyber attacks is complex and time-consuming, but is found at the top of the risk agenda for good reason.

Indeed, the seventh edition of the BCI Horizon Scan 2018, released by the Business Continuity Institute (BCI) in association with standards organisation, BSI, assessed the business preparedness of 657 organisations worldwide and shows that 53 per cent of business continuity and resilience professionals are 'extremely concerned' about the possibility of a cyber attack.

When you consider what's at stake, it is easy to see why. Countless stories are testament to the damage that can be wrought. Delegates at the inaugural event of Continuity Logic's Resilience for the 2020s series heard about the details of one such incident – the aftermath of a major cyber attack, which took less than 60 minutes to take down operations in sixty countries, kicking off a major incident. "This is part of a trend," explained associate partner, Business Resiliency Services at IBM, Robin Gaddum. "There are a number of newsworthy attacks but the main focus is these new, very sophisticated attacks, like WannaCry and NotPetya, that seem to have little or no financial gain for the perpetrators.."

Having been in the resilience business for many decades, IBM has extensive experience of dealing with both man-made and natural disasters that have impacted organisations all around the world; it is their business to keep clients up and running and help them recover but NotPetya was concerning in new ways. "All the firms that were attacked at scale had cyber security but the impact was still severe, as we saw with several high profile cases at the time," Gaddum recalls.

And that's just the damage you can see.

Additional, ongoing risks may not be apparent for some time later. With NotPetya, for instance, the malware was able to hide in the system – even replicating to backup sites. It is also worthy of note that this particular piece of malware got in through a supplier – a clear warning to carry out cyber security through the supply chain.

Detect, respond and recover

Creating resilience to cyber attacks, and plans that work towards a realistic recovery relies on communication, board-level buy-in, extensive testing, a joined up risk appetite, and the skill to make sure all these elements work together in symphony.

"The disaster recovery element of this has been seriously overlooked in recent times," Gaddum warns. "Risk professionals and IT teams must work together to challenge how breaches will be dealt with, working carefully through any assumptions in the plans and really examining how they will prepare to recover from such attacks."

Do business continuity managers need to spend more on addressing this risk? Gaddum points to an "underinvestment in recovery". "We need to start assuming an attack will get through and work out how we can respond and contain the effects of that attack."

Can geographical segmentation help stem the spread of an attack should the worst happen? Gaddum considers network containment to be useful. "You can also contain by segmenting operating systems. And think very hard about users and credentials. Threat actors are looking to get in laterally. If your help desk has access admin rights, they are a target, so they really need to be briefed about phishing attacks. There is more that can be done about segregating access and stopping the spread across departments."

Creating an air gap between back-up sites can also afford a greater degree of control. "Of course, there should be some way for data to travel back and forth and that needs to be copied to immutable storage, so that you have multiple versions of it," Gaddum advises.

Ultimately, cyber resiliency has got to be a 'team sport', which does require effort when it comes to breaking down silos – a notoriously difficult task. To help achieve this, Gaddum suggests trying to create a structure that's different.

"Resilience can be thought of as a 'finishing school' for top level stakeholders – as if you were conducting an 'operational tour in

resilience' to convey what to do when things goes wrong. I think that could develop a more sustainable model for resilience going forward."

A journey to resilience

In a society with minimal appetite for disruption, creating organisational resilience is synonymous with success, and having the ability to sustain that model is key.

This was part of the thinking behind the recent roll-out of Barclays' new Resilience Programme. Karen Azzopardi, head of Resilience Governance and Engineering at Barclays, shared insights into the new, more customer-aligned approach which considers the perspective of the customer first and foremost.

The Group Resilience team undertook the responsibility to drive a more holistic approach to resilience across the organisation, "We had to ensure that key areas across Barclays considered resilience in a completely different way to how we had done it before," she explained. "Starting by considering what the customer has to go through, each business unit was asked to think about what their front-to-back processes were. The business then proceeded to complete a detailed analysis to truly understand their resilience risk."

Echoing IBM's Gaddum's earlier point on the importance of cross-functional collaboration, Barclays advocates working with SMEs within technology, premises, suppliers and cyber to gain a full picture of resilience risk.

"Risk professionals need to go to the IT team and challenge them – find out if they're prepared to recover from these sorts of attacks. And then question hard the assumptions in those plans."

The success of the programme is already apparent and most notably due to buy-in from the top. A project of this kind and size wouldn't have got off the ground if not for board-level support, to which Azzopardi attributes much of its progress thus far.

"Without the support of senior members of the Executive board we would not have got as far as we have. This programme has additional appeal because it is set up from the perspective of the customer. If you can clarify the gains in terms of keeping the customer happy it makes resilience an easier sell" she explained. "With a naturally customer-centric culture, Barclays recognises that resilience is a key factor to success in its delivery to customers."

From planning to resilience

Evolving priorities and organisational change are driving the need for a different approach to business continuity. Paul Gant explains the role enterprise software can play in powering the complex shift from traditional planning to resilience

Business continuity management is evolving in its priorities. Where once responding to events was its primary focus the emphasis is now shifting to incorporate the identification of vulnerabilities and the required actions to strengthen them. The concept of analysis and prevention is far from new, but the attention and the level of detail around the execution is. As a consequence organisations truly are becoming more resilient. Risk leaders refer to this shift as a move from business continuity to resilience.

Enterprise software has two crucial roles to play in supporting this shift: the first, freeing the time of business continuity professionals to incorporate resilience alongside planning; the second, helping to find and fix the vulnerabilities where resilience measures are most required. Here we explore them both.

Free professionals' time through 'industrialisation'

The shift towards resilience offers a potential step up in value for those professionals involved in the process. But there is a challenge here, because while resilience may now be considered high value it does not eliminate the need for an effective response – rather it sits alongside it; and the people who are best placed to build resilience are those who have learned their trade through response – typically through designing business continuity strategies.

This brings about two requirements when it comes to traditional business continuity planning. First, simplify it. Like any profession, business continuity has generated much debate and disagreement around methodology and best practice. Now is the time to cut through that and seek simplification where possible. The second need is to provide structured support through software in order to automate, or industrialise, the process. Software offers huge scope for eliminating administrative and repetitive tasks, securing effective contributions from non-specialists and third-parties (eg. suppliers), and placing the resultant plans into the hands of those individuals who might need to use them. The time saving that this generates can then be diverted towards building resilience, and the hard analytical work that this demands.

Seek out the vulnerabilities

Identifying weaknesses in order to fix them is not new – neither is risk management as a formal discipline, but in 2018 the aim of building organisational resilience goes well beyond the original risk matrix approach.

The first imperative is to build links between the elements of the organisation which lead to the delivery of an output. And those links need to be mapped, not just noted. It is not sufficient to list the software applications required to deliver an output. It must also be possible to turn that around and look at all the outputs that depend on each application. And that's just the beginning because each application in turn depends on its own services – whether that be a cloud provider or a datacentre, and so on. This is tracing 'upstream', and is a key strength of effective business impact analysis software.

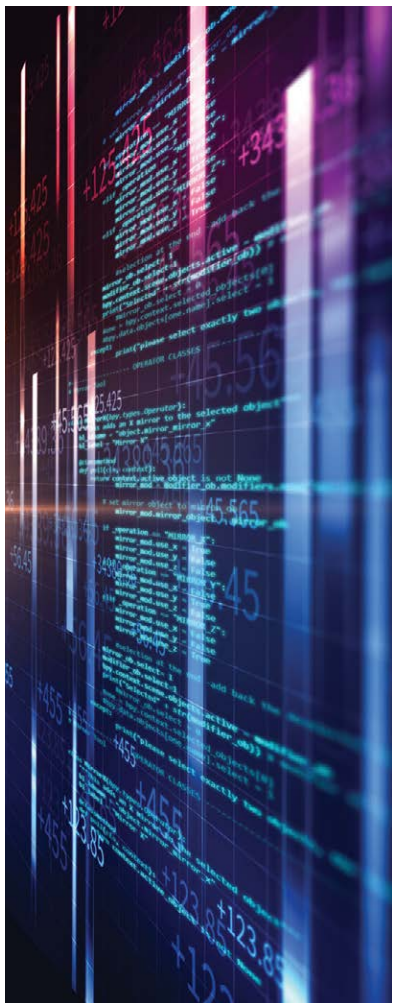
Then it is necessary to link services together in order to take the view of the customer who is engaging with the organisation. So while you may care that, say, the finance department is down, the customer cares if any of the services in your organisation on which their experience depends is down.

Simply put, resilience involves tracing the route along which the customer journeys and strengthening that route from beginning to end. And vulnerabilities are sought not by looking down a list of departments but by using analytics and visualisations to identify weaknesses in rigorous manner and then using the same capabilities to strengthen them.

Continuity Logic's role in delivering this resilience

Any effective business continuity software product will have a contribution to make in the delivery of resilience. But from our deep experience in the market we know that there are certain areas in which our application is particularly strong. These are worth covering briefly here.

The first key strength relates to the



identification of vulnerabilities. In a conventional business continuity programme – even one of substantial sophistication – vulnerabilities are typically assessed department by department, or at best by process. So, for example, the finance department delivers the invoicing process. I therefore need to know which applications and third party vendors that depends on, and maybe even which other departments and/or processes. That would represent a sophisticated dependency map for almost all business continuity programmes.

For a resilience programme, this information would be just

the beginning, because from the perspective of an organisational resilience programme, invoicing is just one of many steps on a journey that is taken by the customer. The first step may have been contracting with the legal department, the second may have been customer setup from customer services, and the third may have been product delivery from fulfilment. From the customer's perspective, any failure in this chain would represent a failure in his/her overall experience. Therefore, to make the organisation resilient requires all of these elements to be linked and then strategies developed to reinforce that entire journey. And this would need to be repeated for multiple transactions. The second key strength of the Continuity Logic application relates to industrialisation. The core skill of the business continuity leader lies in interpreting data in

"The core skill of the business continuity leader lies in interpreting data in order to build powerful recovery and resilience strategies"

order to build powerful recovery and resilience strategies – strategies that would not occur to the layman. The administrative role of the business continuity leader, however, is a skill that is shared by many. It is also a skill that can to a large extent be automated, or industrialised, if it is approached properly. This is where over-simplified out of the box solutions can fail in their objectives. Most organisations that we encounter have peculiarities and/or nuances which may be absent if they were to start with a clean sheet. But clean sheets are a luxury that very few can afford and so software needs to be entirely adaptable to the circumstances in which the industrialisation is to be applied.

A persuasive case

We believe that the case for pursuing resilience is persuasive. Some will rightly argue that it's nothing new but that's beside the point. What is new, and highly significant, is the corporate emphasis that is being placed upon it. Planning for an effective response has often been viewed by cynics as a necessary evil. This may be because corporate leaders have a tendency towards a risk taker's mindset with the associated hope that nothing untoward will happen – so why worry about planning? But even the biggest risk taker wants to be part of something that is strong. And resilience is strength.

ContinuityLogic

Resilience for Thought Leaders

Leading edge business continuity management software

Continuity Logic has been at the forefront of business continuity management software since 2006. Our software is deployed with some of the world's largest corporations and leading brands as well as with a wide range of mid-sized organisations seeking an out-of-the-box solution for their needs. Large or small, these organisations see Continuity Logic as a way to future-proof their investment of both time and money by delivering capability for both today's requirements and tomorrow's possibilities.

4 x LEADER Gartner Magic Quadrant

ContinuityLogic

www.continuitylogic.com

info@continuitylogic.com

European Operations
24/25 The Shard
London Bridge Street
London SE1 9SG
United Kingdom
Tel: +44 (0)20 7770 6446

Corporate Headquarters
400 N Tampa Street Suite 1750
Tampa FL 33602
United States of America
Tel: +1 866-321-5079