Five key actions to build business resilience in 2016

First there was disaster recovery, then came business continuity and now companies are looking for ways to build business resilience.

©Dmitriy Shironosov via 123RF

"This changing vocabulary reflects the nature of the business context and how companies are looking to mitigate risk," says Michael Davies, CEO of ContinuitySA, a provider of business continuity solutions. "There's a growing realisation that the whole process of creating a business continuity plan does more than address the identified risks - it helps the company to understand itself better and improves its ability to overcome the challenges that are now part of everyday business life."

Davies and his executive team meet towards the end of the year to identify some of the hottest risk areas. Based on this information, the team has identified five key actions to build business resilience in 2016:

• **Address leadership issues, particularly with regard to the CIO**

Deloitte's 2015 Human Capital Trends Report shows that 86% of companies globally see developing leaders as a critical challenge. "We think African CIOs are under considerable pressure at the moment as they move from their traditional IT support role into one that demands innovation leadership. Technology's role as a business disruptor means that IT is expected to deliver business value, and help the company compete with upstarts from outside the industry sector. Amazon is just about everybody's competitor these days."

The difficulty with which many CIOs are rising to this challenge worsens the risk posed by the need for constant innovation, Davies explains. For example, the big data trend is not just about the ability to capture and analyse huge data volumes, companies need to be able to respond to the challenges or opportunities that data analysis reveals. Davies adds that the greater frequency of crises in today's interconnected and unstable economy is placing the whole C-suite under pressure.

• **Understand your supply chain risk, including utilities**

Today's business environment is characterised by long supply chains and greater collaboration with business partners - something that introduces more risk into the equation.

"Risk can no longer be compartmentalised, so to build true business resilience you need to understand your key dependencies and how resilient your partners are," says Davies. "One trend that worries me is that as companies use cloud providers to supply more of their IT requirements, they take those cloud providers' ability to recover from a disaster for granted. My advice: don't assume your cloud provider has a good business continuity plan."

Another key risk relates to the ever-present danger of local utilities running into delivery challenges - a question mark now hangs over power and water supplies, and this threat could affect the whole supply chain. Even more serious for business, Davies notes, is the threat that erratic power supply poses for telecommunications providers.

• **Ensure you have viable manual processes in place where practical**

"Business is highly dependent on information and communication technologies, which creates vulnerability. It's just as well to identify which key processes could be run manually if the systems go down," Davies says. "Modern companies are basically dependent on IT, but if some parts of the business can continue manually, that's a big step towards resilience."

• **Be prepared for cyberattack**

Cyber threats, from terrorism to industrial espionage to holding data for ransom, are growing in frequency and companies simply are not keeping up with the threats. RSA's Cyber-security Poverty Index shows that nearly 73% of global companies reported they had insufficiently mature levels of security. The survey further adds that the greatest security risk was the ability to measure, assess and mitigate cybersecurity risks, with 45% of the companies surveyed describing their capabilities in this area as 'non-existent' or 'ad hoc'.

By contrast, only 21% reported that they are mature in this area. "Cybersecurity is not only a technology problem, it is a function of the entire enterprise. This lack of maturity in prioritising cybersecurity investments and activities thus indicates an overall lack of business resilience that is worrying," Davies observes.

• **Understand the geopolitical risks for your company and its supply chain**

There is not much a company can do about terrorism, war or the like, but it must understand the risks it faces and have contingency plans in place. This is particularly relevant for companies with supply chains that stray into troubled regions.

Davies says that customers must be at the centre of the whole business continuity process. "Know who is relying on your company - and thus who depends on your ability to recover from disaster. A company that takes business continuity seriously is by nature resilient to change or threat, and it can use that resilience to build its reputation in the market, especially as we are all increasingly sensitive to risk as the world becomes a more complex and volatile place," he concludes.