StrategicRISK

BI risks in the intangible economy

As the intangible business economy grows, so too do the risks, potentially causing costly business interruption

FROM DATA BREACHES AFFECTING CUSTOMER TRANSACTIONS to reputational blunders following a risk incident, risks to data, intellectual property and brand – or intangible assets – are significant threats in today's complex business landscape.

Add to this, another layer of risk complexity in the advent of advanced technologies. The internet of things, artificial intelligence, and automation, for example, are digitalising and automating production methods; and connecting businesses from one region to another at an unprecedented rate. Indeed, this has been beneficial for many, increased efficiency, reduced costs, and international expansion. But these technologies are also creating new vulnerabilities: the risk of a business interruption (BI) arising from threats to intangible assets. And as businesses become more global, so too do the risks.

Competitors may seek to disrupt your vendors, delivery routes and deteriorate your ability to deliver the products in time

Hans Laessoe, AKTUS

Intangible BI

Hans Laessoe, principal consultant at AKTUS and former senior director of risk at the LEGO Group, draws examples from the manufacturing sector to illustrate the BI and global impact arising from risks to intangible assets.

He explains that large companies are joining the race to digitise manufacturing processes as it becomes increasingly clear that automation holds the key to the future. But as this shift occurs, the risk register will undergo substantial change, with both new and traditional risks rising to the fore.

Among these is the risk of disruptive innovation and being outcompeted as key manufacturing capabilities become obsolete, and the potential for cybercrime and IT vulnerabilities, grow as systems become increasingly connected.

"By digitising your manufacturing, you acquire tonnes of data and options to control machinery, product flow, planning, etc. While this is all good, any piece of data that hits the internet or the cloud can be hacked and looked at by competitors and criminals seeking profit."

He cites the example of disruption caused by the ransomware attack NotPetya to a global shipping giant. The company revealed that it had to shut down its global information technology network; and that the total cost of the attack was $300m in business interruption as it was forced to reinstall 4,000 servers as part of a complete infrastructure overhaul. This was one of many examples of how the Petya cyber attack caused widespread disruption to many businesses.

Supply chain risks reimagined

Intellectual property theft is likely to be one motivation behind manufacturing cyber attacks in the future – and third-party suppliers and vendors along the supply chain are not immune. An attack to suppliers will likely cause a costly BI.

"There is a risk that competitors may hack in to your systems, potentially using third-party 'vendors', and steal your product ideas," says Laessoe. "This is a major issue for several companies, and of one where a copy-cat manufacturer actually launched a product before the company that designed it."

"Competitors may also hack in to your systems with the intention of disrupting your manufacturing processes. Likewise, they may seek to disrupt your vendors, delivery routes and deteriorate your ability to deliver the products in time," he continues.

Alistair Jupp, head of global technical services for Crawford UK, agrees. He says as systems and supply chains become more connected, new BI exposures are introduced. Drawing examples from the construction industry and erection of smart buildings and factories, he says "Buildings are becoming a lot more complex and the more complicated a building, the higher the risks are. Now, if you have a breakdown in a building management system, it can shut everything down."

People risks

However, for one risk expert, the less known risk to intangible assets is people. Karla Gahan, deputy head of risk and advisory at VinciWorks and former risk and business continuity manager at DLA Piper, says while people are a company's most critical asset, they can inadvertently exacerbate or contribute to risks to intangible assets.

The people element is perhaps one of the most challenging risk to identify. "Organisations may neglect the impact to people during a disruption, or the fact that people behaviour can be a risk in itself. We live in a time where constant change can impact our health and wellbeing and our behaviour may be negatively impacted – from stress-related illnesses causing absence of key individuals, to insider threats and fraud, as well as the possibility that a negative organisational culture can cause people to leave. And these behaviours are simmering even before a significant incident affects an organisation.

"Each of these outcomes has the potential to cause disruption [to intangible assets], for example a cyber incident, major fraud, and may not have been considered during the risk identification process or business continuity planning."

For 21st century businesses, the intangible economy presents a real challenge but getting to grips with the risk will deliver tangible results. SR