Resilience: the key to business continuity

October 5, 2015 | By David Bogoslaw

Strong governance program seen as starting point when assessing a company's ability to rebound quickly from cyber attacks and other business disruptions

Last Wedneday, Setember 30, was National Preparedness Day, the culmination of National Preparedness Month, the purpose of which is to get local communities to focus on ways to be ready for unforeseen physical threats such as wildfires and flash floods. But it's just as critical that companies focus on potentially disruptive events that can inflict harm on their customers, shut down their business operations – and put a big dent in profits and their stock price.

These days, companies are much more likely to be threatened by data breaches and other kinds of cyber-attacks than natural disasters. And the focal point of business continuity has become due diligence in your supply chain, says Al Berman, president of Disaster Recovery Institute International (DRI), a nonprofit that provides education and accreditation to organizations worldwide to help them prepare for and recover from disasters.

Regulatory bodies such as the Office of the Comptroller of the Currency, which is responsible for national banks, and regulations such as HIPAA, which provides oversight for hospitals and other healthcare organizations, are creating vetting programs to help companies better understand the security of their suppliers. And regulators are urging companies to look at prevention of cyber-attacks as 'an all-inclusive process' that takes into account not only their own vulnerabilities but also those throughout their supply chain, Berman says.

One indication of how intricate business continuity risks have become, and how attentive organizations need to be in order to prepare for them, is the seven relatively new kinds of cyber-risk insurance now being sold. Cyber-extortion coverage, for example, is widely familiar now that more companies have experienced or heard of a hacker taking control of a business network, encrypting the data and demanding ransom to unencrypt it for the victim. Then there is media liability insurance, which protects copyrights and intellectual property defense costs, as well as remediation policies that cover the costs of notification and credit monitoring that companies typically incur after they've been hacked.

'All of them come with a warning that essentially requires you to talk to your attorneys because they're difficult to understand,' Berman says. 'They have redefined what's known as insured peril, which used to mean some physical damage; now we're seeing the damage doesn't have to be physical.'

c

The cover story in *Corporate Secretary*'s fall issue provides tips on buying cyber-risk insurance, and one source

notes that higher-quality companies are able to show they are more resilient to cyber-attacks in terms of how they manage a crisis and minimize its impact. DRI evidently agrees: earlier this month, it unveiled new awards for Hub of Resilience and Resilient Enterprise that it will give out later this fall.

‘[Insurance companies] want to see you have an understanding of what the impact [of an attack] would be,’ Berman says. ‘Their objective is to minimize their payments, so the less vulnerable you are, the less they’ll have to pay for and therefore your premiums would be reduced.’

For DRI, measuring an organization’s resilience starts with looking at its corporate governance and the extent to which what the organization says it wants to do aligns with what it is in fact doing.

‘Much of it also includes things like compliance with regulations and protection of individuals to be able to minimize the financial loss,’ Berman says. ‘Lack of governance, from my perspective, just obliterates whatever targets you’re trying to hit. You have no idea what you’re looking to accomplish.'