The Cost of Disruptions

Introduction

Every operational disruption is unique and the ultimate cost to those organisations affected by it will depend on many factors. Nevertheless, in order to allocate appropriate budgets for business continuity management (BCM), it is important to have some idea of the scale of losses that other organisations have suffered.

Research in this area is quite scarce but this short article summarises the findings of four important studies conducted in the US. Each is based on the "Event Study" method, a rigorous technique that has been applied in many areas of finance and economics. In this method the performance of a company's shares over a period around the event of interest becoming publicly known is compared to the performance of a suitable benchmark to measure the impact on the overall value of the firm. The performance of the company's shares relative to the benchmark is known as the *Cumulative Abnormal Return* (CAR) and a negative CAR indicates that the company has decreased in value.

Security Breaches

Bianchi and Tosun (2019) analysed the market reaction to 41 deliberate (ie criminal) security breaches that occurred in large US firms between 2004 and 2016. The authors found that firms experiencing such a security breach experienced a loss in value of between 1 and 1.5% over a period of 2-3 days around the first public announcement of the breach. Given that the firms involved were amongst some of the largest corporations in the US, this equates to losses of billions of dollars to shareholders for each incident. Interestingly, the study also found that security breaches had long-term effects on the companies affected, specifically they observed:

- Reduced spending on Research and Development activity; and
- Reduced dividends to shareholders.

Over a five-year period after the breach. Finally, and perhaps surprisingly, the authors also found that:

- The pay of CEOs in affected firms increased after a breach relative to unaffected firms; and
- Security breaches had no effect on the rate of CEO turnover.

This would seem to contradict anecdotal evidence, such as the high-profile examples of TalkTalk and Equifax where CEOs left the firm shortly after breaches.

IT Outages

Baradwaj, Keil and Mähring (2009) studied a sample of 213 IT failures over the period 1990 – 2000. This included both operating failures in existing systems and failures to implement new systems. Overall they found an average CAR of -2% over 2 days when the failure became public. Crucially, their analysis also established that the CAR was much greater when the company had experienced previous IT failures. They also found that the reaction to implementation failures was generally more severe than the reaction to operating failures.

Supply Chain Glitches

Hendricks and Singhal (2005) studied a sample of 827 "Supply chain glitches that resulted in production or shipment delays" over the period 1989 – 2000. In common with other studies they looked at the impact over a 2-day window around the first media reports of the problem and found an average CAR of -7.2%. They also looked at the impact over longer periods, finding average CARS of:

- -13.7 % in the year before the 2-day window;
- -10.5% in the year after the 2-day window; and
- A total of -40.1% in the period from 1 year before to 2 years after the first media report.

Product Recalls

Chen, Ganesan and Liu (2009) studied 153 recalls of consumer products over the period 1996 – 2007. Focusing purely on the day of the recall announcement, they found a CAR of -0.6% for 'Pro-active recalls' (ie recalls that were initiated before any safety incidents had been reported). Interestingly, no significant CAR was found for 'Passive recalls' (ie recalls that were initiated after safety incidents had been reported).