Chapter 7
Comments on Standards in Information Security, Disaster Recovery, Business Continuity, and Business Resilience

This Chapter looks at some aspects of the private sector approach to resilience. There are a number of ways this can be approached by both business and as a subject. However, over the last twenty years or so, there has been continuous development of an approach related to firstly disaster recovery, then business recovery, then business continuity, and, most recently, a move toward business resilience; which will potentially obsolete all the former. This progression has seen the development of some standards. These have been focused on the regulated businesses. This Chapter charts this journey and ends by comparing a significant number of the different standards now in use. As this book goes to press the new Business Continuity Standard in the UK, BS25999, has been published, which is really the next step in the business continuity industry's development. As with all Critical Infrastructures, the mission critical elements of a business are almost always related to Information Infrastructures these days. Hence the concentration on standards related to Information Infrastructure. This Chapter reproduces text from articles by the author originally published in Continuity Planning's online newsletter.[165]

There have been, are, three developing themes in the business risk management industry – business recovery, business continuity, and business resilience – and all have a common driver: regulation. In the latter's case, however, there is also the business strategy driver to consider.

Regulation during the 1980s in the banking industry, especially in Europe and the City of London, drove players to evolve procedures that could recover financial data, in particular, from disrupted media in such a way that information could be retrieved and businesses could continue to operate. At the same time, companies, such as Kroll[166] and Control Risks,[167] were starting to look, again in regulated businesses and/or high-profile businesses, at the risks to business and began drawing up procedures to handle them. The personnel involved at the time were often ex-forces or maverick IT-types.

---

[165] All articles available at http://www.contingencyplanning.com (Accessed: 7 January 2007).
[166] More information available at http://www.kroll.com (Accessed: 7 January 2007).
[167] More information available at http://www.controlrisks.com (Accessed: 7 January 2007).

In the mid 1980s a number of London banks and their subsidiary "network" management companies[168] started to develop bespoke approaches for their clients. Many of these approaches have stood the test of time in a number of ways, or, at the very least, have provided a foundation for future developments. The sort of advice they gave at the time, however, is almost unrecognizable just 20 years later.

The following is the checklist given to Managing Directors, in the 1980s, to control sensitive information of a company that excelled in electronic innovations:

- Is there a classification for company information?
- Does the procedure require certain controls?
- Are copies of the procedure issued to all employees?
- Is each employee provided with somewhere safe to lock things away?
- Is there a shredder beside each photocopier?
- Is all sensitive waste shredded?
- Are microfiche readers controlled and negatives disposed of securely?
- Are microfilms prepared by outside contractors securely handled?
- Is telephone equipment checked form time to time for eavesdroppers?
- Is data transfer, whether by computer or telefax, secured against intervention from outsiders from a physical as opposed to a virtual sense?
- Are board and conference rooms checked on a frequent, random basis to detect bugging?
- Is access closely controlled to rooms and stores where confidential documents are kept?

Electronic data transfer at that time was limited to a few major international centers. e-Mail existed via the company's own satellite system, but only on a limited basis. Even so, the controls in place then for managing data were more relevant to the recovery of the business than to the preservation of the data. In fact, the preservation of data and information was not a particularly big issue. This was a private company and the owner pretty much decided what it was or what it was not appropriate to keep. Today, even as a private company, this organization could not be quite so independently minded as to the sort of information it chose to keep – especially in Europe and the United States, and even in a relatively lightly regulated industry. In the international field, the company operated freely and carried little in the way of data or presentations, except that which employees kept in their heads or on traveling overheads. (In 1989, one Managing Director had an early Amstrad laptop confiscated at six airports during a two-week trip through Africa.) Decisions were made on the spot and contracts were rarely more than two pages long.

In the banking industry, then as now the most regulated of services, things were being looked at a little differently. Again, a number of London (and New York) banks were involved. Their checklist for computer security still has some resonance today.

---

[168] E.g. Hambros Bank's Network Security Management Limited.