In the area of risk management the survey produced the following highlights:

- **Allocation of risk responsibilities.** 37% of survey respondents said their boards have no clear allocation of specific responsibilities for overseeing major risks among the board and its committees, while 57% were not comfortable with their understanding of the company's social media response plan in the event of a crisis.
- **Responding to the new US whistle-blower rules.** Most directors acknowledged that their companies took action to address the new whistle-blower rules: two-thirds placed more emphasis on employee awareness around ethics and compliance policies; 42% enhanced their follow-up policy on compliance-related complaints; and 42% increased reporting of such issues to the board.
- **Boards satisfy their risk appetite.** 97% reported they are at least "moderately comfortable" with the board's understanding of the company's risk appetite, and 91% of directors were at least "moderately comfortable" with their understanding of emerging risks (e.g., the European debt crisis, natural disasters).

The rather depressing conclusion we can draw from this is that, at C-level, there remains a lack of recognition of the need for a comprehensive and holistic approach to risk and a lack of coordination between the internal functions responsible for different aspects of risk management. For the BC manager, the response needs to be persistence and cooperation with other risk management areas within the organization – constant efforts to create a holistic approach to risk management.

0.6 Technology Challenges

This section selectively synthesizes various forecasts[34] for technology challenges impacting BC and disaster recovery over the next few years, supplemented by a few of my own. The 2013 BCI Horizon Scan report[35] identified that unplanned IT and telecom outages are the leading cause of concern, with 70% of respondents concerned or extremely concerned about these areas, followed by data breach (66%), and cyber attack (65%). Here are the top technology challenges that BC professionals need to consider.

0.6.1 Proliferation of Internet-Connected Devices

Bring Your Own Device (BYOD), driven by employee expectations, is seen by SunGard as having implications for security and availability. Ian Kilpatrick[36] identifies the Achilles' heel of BYOD: while BYOD has changed both the data transfer and performance expectations of users, these expectations have not been met, with many networks still inadequate in their coverage and performance. Legacy networks will creak under the strain until high-density wireless is able to provide companies with high coverage and high performance, supporting business critical applications and delivering complete site coverage.

The **Internet of Things (IoT)** is a concept identified by Gartner to describe how the Internet will expand as physical items such as consumer devices and physical assets are connected to the Internet. Key elements of the IoT which are being embedded in a variety of mobile devices include embedded sensors, image recognition technologies, and Near Field Communication (NFC) payment. As a result, "mobile" no longer refers only to use of cellular handsets or tablets. Cellular technology is being embedded in many new types of devices including pharmaceutical containers and automobiles. Smartphones and other intelligent devices don't just use the cellular network; they communicate via NFC, Bluetooth, Local Exchange (LE), and Wi-Fi to a wide range of devices and peripherals, such as wristwatch displays, healthcare sensors, smart posters, and home entertainment systems. There were 93 million connected devices in 2000, rising to 5 billion in 2010 and 31 billion expected in 2020

(http://i-hls.com/2013/05/embedded-cyber-security-and-the-internet-of-things/). The IoT will enable a wide range of new applications and services while raising many new challenges, not least of which is security.

0.6.2 Mobile Working

There is general consensus that mobile working is now expected by employees and employers alike. Gartner[37] predicted that mobile phones would overtake PCs as the most common Web access device worldwide and that by 2015 over 80% of the handsets sold in mature markets will be smartphones: these predictions seem on track. However, only 20% of those handsets are likely to be Windows phones. By 2015 media tablet shipments will reach around 50% of laptop shipments and Windows 8 will likely be in third place behind Google's Android and Apple iOS operating systems. Enterprises will need to support a greater variety of form factors reducing the ability to standardize PC and tablet hardware. The implication for IT is that the era of PC dominance with Windows as the single platform will be replaced with a post-PC era where Windows is just one of a variety of environments IT will need to support.

> **Users will see [the personal cloud] as a portable, always-available place where they go for all their digital needs. In this world, no one platform, form factor, technology, or vendor will dominate...**

Ian Kilpatrick[38] sees these expectations as generating the need for mobile device management (MDM) solutions that offer features such as ensuring mobile device usage complies with company security policies, allocating access rights, managing configuration, updating policies, dealing with data leakage issues, and dealing with lost or stolen devices. Additionally, MDM solutions need to address the problem of managing both employer-owned and employee-owned devices, and differentiating between business use and personal use. End-point security solutions are proliferating, too. The risks implied by these developments include the possibility of losing small, powerful devices that are packed with or able to access confidential data, leaving the systems and data of individuals and organizations open to unauthorized access.

Users are familiar with anywhere/anytime access to corporate IT capability, and Gartner envisages this spreading into their personal lives, as a personal cloud that will gradually replace the PC as the location where individuals keep their personal content and access their services and personal preferences for their digital lives. It will be the glue that connects the web of devices they choose to use during different aspects of their daily lives. The personal cloud will entail the unique collection of services, web destinations, and connectivity that will become the home of their computing and communication activities. Users will see it as a portable, always-available place where they go for all their digital needs. In this world, no one platform, form factor, technology, or vendor will dominate, and managed diversity and mobile device management will be an imperative. The personal cloud shifts the focus from the client device to cloud-based services delivered across devices.

0.6.3 Protocol/Version Changes

0.6.3.1 Internet Protocol – IPv6

Internet Protocol (IP) provides a system for identification and location for computers on networks and routes traffic across the Internet. A session at the International Telecommunication Union Regulators Conference in Tokyo in 2013 recommended that all Regulators should mandate IPv6, the latest internet protocol version, in their nations. While IPv6 has been around for some 5 years, the majority of users still use IPv4. IPv6 has security, mobility and roaming benefits but the

migration period from IPv4 to IPv6 is likely to be long and, during this, security may be prejudiced and compatability issues may arise.

0.6.3.2 Voice Over Internet Protocol H.323 (VoIP H.323)

H.323 is a standard protocol for multimedia communications. It was designed to support real-time transfer of audio and video data over packet networks like IP. Its adoption is being driven primarily by quality of service and lower cost. Most VoIP applications use H.323. At the same time Session Initiation Protocol (SIP) is also widely used because it easily combines voice and Internet-based services. SIP needs to be interoperable with and coexist with H.323. There are different security needs for VOIP H.323 standard versus SIP. Other vulnerabilities include availability (power, denial of access); confidentiality (intercept and saving as audio files; undocumented ports and services); and integrity (identity theft; registration hijacking; proxy impersonation; call redirection).

These are just two examples. In terms of operating systems, we could add the termination of support for Windows XP and version changes from numerous software suppliers. Protocol and version changes may seem an issue for ICT security and change management. But, like cyber attacks, the result could be denial of service or impaired service which results in business disruption.

0.6.4 Espionage

The US has reportedly monitored computers used by French delegates at the UN, and the mobile phone of German Chancellor Angela Merkel. And Le Monde claims that the US National Security Agency (NSA) has monitored millions of French telephone calls.

Spy agencies in the UK, Australia, New Zealand, India, and the US have reportedly banned Lenovo PCs since the mid-2000s because of backdoor vulnerabilities. Lenovo PCs are manufactured in China. Ex-CIA and NSA head Gen. Michael Hayden claimed that Huawei has engaged in espionage on behalf of China (but note that, at the time, Hayden was a Director of Motorola Solutions, a competitor to Huawei). In May 2013, a backdoor was discovered in the ZTE Score M, a Chinese budget smartphone used by some US prepaid mobile carriers.

Again, espionage may seem more the domain of security. However, the ability to eavesdrop could also be a precursor for malicious cyberattacks causing loss or corruption of data and potential denial of service.

0.6.5 Utilization of "Big Data"

Gartner (http://www.gartner.com/it-glossary/big-data/) defines "big data" as high-volume, high-velocity, and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision-making. A combination of data from public data sources (e.g., the Internet, government, and other sources of usually unstructured data) and data accumulated by organizations from their own activities can be analyzed to tailor, personalize, place, and time services to attract and retain customers, to upsell, and to cross-sell. Gartner expands on this and says that "big data" is moving from a focus on individual projects to an influence on enterprises' strategic information architecture. Dealing with data volume, variety, velocity, and complexity is forcing changes to many traditional approaches. This realization is leading organizations to abandon the concept of a single enterprise data warehouse containing all information needed for decisions. Instead, they are moving towards multiple systems, including content management, data warehouses, data marts, and specialized file systems tied together with data services and metadata, which will become the "logical" enterprise data warehouse.

Gartner further identifies actionable analytics as of strategic importance: the resultant analytics delivered to users at the point of action and in context. With the improvement of performance and

costs, IT leaders can afford to perform analytics and simulation for every action taken in the business. The mobile client linked to cloud-based analytic engines and big data repositories enables potential use of optimization and simulation everywhere and every time. This new step provides simulation, prediction, optimization, and other analytics, to empower even more decision flexibility at the time and place of every business process action.

0.6.6 Hybrid IT and Cloud Computing

Gartner says that the internal cloud services brokerage (CSB) role is emerging as IT organizations realize that they have a responsibility to help improve the provisioning and consumption of inherently distributed, heterogeneous, and often complex cloud services for their internal users and external business partners. The internal CSB role represents a means for the IT organization to retain and build influence inside its organization and to become a value center in the face of challenging new requirements relative to increasing adoption of cloud computing as an approach to IT consumption. This shift brings with it issues of data integrity, recovery, and security.

0.6.7 In-Memory Computing

Gartner sees in-memory computing (IMC) providing transformational opportunities. The execution of certain types of hours-long batch processes can be squeezed into minutes or even seconds allowing these processes to be provided in the form of real-time or near real-time services that can be delivered to internal or external users in the form of cloud services. Millions of events can be scanned in a matter of a few tenths of a millisecond to detect correlations and patterns pointing at emerging opportunities and threats "as things happen." The possibility of concurrently running transactional and analytical applications against the same dataset opens unexplored possibilities for business innovation. Numerous vendors will deliver in-memory-based solutions over the next two years driving this approach into mainstream use. And quantum computing could transform IT.

0.6.8 Integrated Ecosystems

The market is undergoing a shift to more integrated systems and ecosystems and away from loosely coupled heterogeneous approaches, according to Gartner. Driving this trend is the user desire for lower cost, simplicity, and more assured security. Driving the trend for vendors is the ability to have more control of the solution stack and to obtain greater margin in the sale as well as offer a complete solution stack in a controlled environment, but without the need to provide any actual hardware. The trend is manifested in three levels. Appliances combine hardware and software, and software and services are packaged to address an infrastructure or application workload. Cloud-based marketplaces and brokerages facilitate purchase, consumption, and/or use of capabilities from multiple vendors and may provide a foundation for Independent Software Vendor (ISV) development and application runtime. In the mobile world, vendors including Apple, Google, and Microsoft drive varying degrees of control across an end-to-end ecosystem extending the client through the apps.

Users should benefit from significantly reduced downtime – typically in minutes – with instant recovery from disk backup, instead of hours, and instant recovery of virtual machines.

0.6.9 Data Backup and Recovery

Data volumes will get ever larger. Kilpatrick envisages backup requirements may be met by new data replication technologies for larger data centers, while smaller organizations will shift from tape to disk (and, in particular, removable hard disk drive (RDX(r)) technologies which combine the best of tape and disk will accelerate). Hybrid backup to RDX and then the cloud will increase. In volume terms, the lowest move (but in market-hype the biggest) will be significant growth in direct backup to the cloud.

ExaGrid Systems[39] predicts that data protection software products will continue to bring innovative features to market that allow customers to leverage their disk-based backups in production instantly in the event of failure, versus going through prolonged restore procedures. The use of synthetic techniques to create full recovery points will continue, driving increased adoption of de-duplication and other techniques that reduce the need to move full copies of data during backups, providing some relief to the backup window problem. Wide-area network (WAN) optimization will also ease backup timeframes and improve WAN productivity. However, offset against this is the need to backup ever bigger volumes of data. Users should benefit from significantly reduced downtime – typically in minutes – with instant recovery from disk backup, instead of hours, as well as instant recovery of virtual machines.

0.6.10 Social Media

In SunGard's phrase, "Crises now have 'wings'." Bad news travels fast, and availability becomes even more important. Social media will also become increasingly important as a source of actionable data. However, as Riskskills points out:[40]

"The huge rise in different types of mobile device platforms along with the corresponding growth of social media sites now poses a huge reputational challenge for corporations. Within minutes, organizations can be the victim of blistering customer backlashes which might or might not be justified. Many corporations are making a start by attempting to formally control how their own employees release company or workplace information through social media. The number of reported dismissals and legal cases for acting irresponsibly through social media is soaring. However, beyond this there are increasingly huge risks posed by being seen to 'get it wrong' at the 'social-communications' front line."

0.6.11 Data Leakage Protection

Kilpatrick identifies data leakage protection (DLP), potentially causing compliance breaches, as a major cause for concern. DLP will be coupled increasingly with security information and event management (SIEM) solutions. DLP concerns will also continue the growth curve for authentication (much of it hosted in the cloud) and encryption, to protect data, both in motion and at rest. Some companies will look to hosted security services and the cloud to cope with an increasingly complex security situation. Booze Allen[41] says such technology is not enough: firms must also invest in people and in fine-tuning processes to ensure not only the proper use of technology, but also that the processes that require interfaces between organizations are managed well and executed flawlessly. No matter how good a technology is, if not used correctly by skilled employees who follow well-defined processes, vulnerabilities will surface that can be leveraged by both internal and external threat actors.

0.6.12 Cyber Attacks

The BCI Horizon Scan 2013[42] identified that the use of the Internet for malicious attacks is the number one emerging concern and is fuelled by the prevalence and high adoption of Internet services, such as cloud computing.

A recent report[43] told of denial-of-service attacks (DoS attacks) and distributed denial-of-service attack (DDoS attacks) increasing in Q4 2012 compared to Q3 2012 in terms of attack sizes (20%), attack volume (up 27.5%), and duration (up 67%). "The take away for businesses from this Q4 [2012] report is to make sure that their DDoS mitigation provider can handle attacks in excess of 50 Gbps in a single location."