Organisational perspectives on the value of security

Security Research Initiative (SRI) report

Professor Martin Gill
Emmeline Taylor
Tom Bourne
Gemma Keats

2008

INVESTOR IN PEOPLE

Perpetuity Research & Consultancy International (PRCI) Ltd
148 Upper New Walk · Leicester · LE1 7QA · United Kingdom
www.perpetuitygroup.com/prci
prci@perpetuitygroup.com
Tel: +44 (0)116 222 5555
Fax: +44 (0)116 222 5557

Copyright

Table of Contents

Tables

Acknowledgements

We are grateful to a variety of people for the help we received in conducting this study. In particular, Jim Norton of the Institute of Directors for permitting us to include questions about security in a survey of members; Tony Bird of the Confederation of British Industry for his support in facilitating contact with member organisations; and Pottengal Mukundan of the Commercial Crime Services (CCS) division of the International Chamber of Commerce (ICC). We are especially grateful to all those individuals who gave up their time to answer questions, formally or informally, or completed a questionnaire. They must by necessity remain nameless but we truly appreciate their input.

We would like to thank Chris Richardson and Walter Palmer for comments on a draft of this report.

This study is a product of the Security Research Initiative, supported by ASIS International, the British Security Industry Association and the Security Institute. The study has been possible because of the support of the following companies:

- Advance
- Case Security
- CMP
- HSBC
- Johnson Controls
- KPMG
- MITIE Security
- Norbain
- OCS-Resolution
- Spinnaker International
- The Corps
- Wilson James
- Wyeth Pharmaceuticals

Additional support was provided by Argos and Homebase. We are grateful to them all. It is important to note that all comments in this report and the interpretation of the findings are the exclusive responsibility of the authors.

Section 1. Executive summary

1.1 The main aim of this study was to gain a better understanding of the view of the security function from those in senior management positions within organisations but not those specialising in security. In particular to explore the following issues:

- What is the role of security and how important is it compared to other functions?
- How can security add value to an organisation and how can this value be demonstrated?
- What makes security effective?
- Are security personnel able?

1.2 The research was based predominately on the following three sources of data but has also been supplemented with a review of relevant literature and discussions with academic and professional colleagues.

- A survey of members of the Institute of Directors (IoD)
- A targeted business survey of organisations sourced from the Confederation of British Industry (CBI), UK FTSE 100 companies and the Commercial Crime Services (CCS) division of the International Chamber of Commerce (ICC).
- Nine interviews with Director level employees with responsibility for security in UK and international organisations.

1.3 Findings from the IoD and targeted business survey suggest that security was commonly considered to be an important function within an organisation.

1.4 The security function was considered on average to make an exceptional contribution to the success of an organisation by almost two thirds of the respondents.

1.5 Security was ranked on average only marginally lower than human resources, finance and marketing in terms of its importance to the success of an organisation.

1.6 Moreover, the targeted business survey supports these findings. Over three quarters disagreed with a statement that security was one of the least important functions. Over half agreed that security was at least as important as human resources and finance whilst well over a third reported that it was as important as sales.

1.7 Findings from the targeted business survey revealed that over ninety percent of respondents agreed that security impacts on all aspects of an organisation. Over half disagreed with a statement that security was marginal to core organisational activities.

1.8 Against this, a quarter of the IoD survey respondents, perceived the security function to make a minimal contribution to the success of an organisation.

1.9 Interviewees viewed security as important in a wide range of roles particularly in terms of its ability to help manage risks.

1.10 Interviewees felt that the role of security within an organisation needs to be a combination of assessing and monitoring risks with good intelligence and the ability to react speedily if incidents occur.

1.11 Interviewees' responses suggest that whether security is considered a core or peripheral function depends on the nature of an organisation and the risk environment in which it operates.

1.12 A reoccurring theme amongst the interviewees was the need for security to be co-ordinated with other departments within an organisation and aligned with the overall aims of the company.

1.13 The IoD survey explored the extent to which three aspects of security (internet and computer security, physical security and personnel security) could add value to an organisation in respect to a) meeting the objectives of an organisation and b) cost effectiveness.

1.14 Internet and computer security were on average perceived to add more value to meeting the objectives of an organisation than personnel and physical security. However, these latter two aspects of security were also considered to be value-adding, albeit to a lesser extent.

1.15 Organisations classified as financial services or distribution and hotels were more positive about the value that all three aspects of security could add to meeting the objectives of a business compared to other industry sectors.

1.16 Echoing the previous trend, internet and computer security were on average perceived to deliver greater value for money than personnel and physical security. Although to a lesser extent, physical and personnel security were also considered to deliver value for money.

1.17 The IoD survey found that electronic security precautions (e.g. firewalls and virtual private networks) were considered on average to generate a greater competitive advantage than six other aspects of security.

1.18 Onsite security guards, CCTV monitoring, alarm contractors and physical security (fences, ages and locks) were considered more of a cost without sufficient benefit than a competitive advantage.

1.19 The targeted business survey found two thirds of the respondents agreed that security was a value adding function whilst almost three quarters disagreed with a statement that it was an unwelcome burden on the bottom line.

1.20 The majority of the targeted business survey respondents did not associate security with adding value through generating a profit; a quarter of respondents agreed that security was a profit making function.

1.21 Over half of the targeted business survey respondents felt that security shows measurable financial benefits. Over a half also felt that it is important for organisations to collect data in order to identify how security adds value to a company.

1.22 Only four in ten respondents reported that their organisation collected metrics or data that could be used to calculate the value of security. Moreover the majority were of the opinion that it was difficult to calculate the value that security could add to a business.

1.23 Similarly a number of interviewees reported that it was difficult to measure the success that security could add to an organisation whilst data collection was highlighted as problematic.

1.24 Most of the interviewees adopted a mixture of qualitative and quantitative measures to monitor and evaluate security functions.

1.25 The vast majority of the targeted business survey respondents considered it important to communicate the benefits of security within an organisation.

1.26 The interviewees noted a number of issues that would need to change in order for security to be accorded a higher status within an organisation. These were:

- The recruitment of high quality people to improve the perception of security

- Obtaining senior level support for the security function and what it is trying to achieve

- Security departments to raise awareness of the tasks they perform and how these impact positively on core business.

1.27 The majority of security reviews undertaken by the IoD survey respondents during the last two years had been conducted by either internal security personnel or external security contractors. Reviews by the police were less common.

1.28 On average the security reviews undertaken by internal security personnel, external security contractors and the police were all perceived to have been effective however internal security personnel were rated slightly higher.

1.29 Internal security reviews were perceived to be particularly effective by financial services.

1.30 The attitude of the head of a company and the culture within a company were considered by IoD respondents on average to have the most positive impact on the security of a business.

1.31 In comparison more tangible factors such as security technology, rules and regulations, incident monitoring and security guards were perceived on average to have less of a positive impact.

1.32 Security guards were rated by IoD respondents to have on average the most negative impact on the security of an organisation particularly by government, education, health and personnel services.

1.33 Security guards were viewed most favourably by financial services however they were still perceived negatively.

1.34 Three of the Board interviewees felt that they managed security well despite not having a security strategy in place whilst those organisations which did have strategies stressed they were important.

1.35 The interviews indicated that the effectiveness of security was not generally assessed through the objectives of Board members.

1.36 The targeted business survey revealed that senior security personnel were respected and considered experts in their fields.

1.37 Only a small minority of respondents felt that senior security personnel were viewed as business leaders however over one third did not think that they lack business acumen.

1.38 The majority of respondents agreed that the closer the Head of Security is to the Board, the higher the status of the security function within an organisation.

1.39 There were mixed views amongst the targeted business survey respondents in respect of the preferred skills and backgrounds of senior security personnel. Over a third felt that it was important for security staff to have good military or law enforcement backgrounds whilst almost one half did not think that it was more important to have business skills as opposed to security skills.

1.40 Similarly there were mixed opinions amongst the interviewees with regard to the most important skill set for senior security personnel: business or security skills.

1.41 Furthermore the general consensus amongst the interviewees was that security specialists were unlikely to be on the Board of a company or appointed as a Chief Executive Office (CEO) principally because they lacked the skill sets.

1.42 There were mixed views of security contractors in terms of the quality of services they provided. They were viewed positively by some respondents because only a small minority felt that they were unreliable and rarely meet their key performance indicators. However only a small proportion of respondents agreed that security contractors generally exceed their expectations.

1.43 Half of the respondents reported that their organisation paid security contractors enough to deliver a good service whilst only five percent said they did not. Just under half said that they were good at managing security contractors.

Section 2. Introduction

2.1 This study builds on the first two years of the Security Research Initiative (SRI). In the first year the SRI examined what buyers looked for when choosing security products and suppliers; such as manned guarding, cash transit, confidential waste management and consultancy. The study identified that there was a need to develop a body of knowledge about the value of 'security' because many buyers did not perceive it as a value adding function.[1]

2.2 Subsequently the aim of the second study was to fill this gap in knowledge and begin to understand what value security generates for an organisation.[2] This involved interviewing security professionals to elicit their views on the role of security within organisations and the value it contributed. The study found that some security professionals did not feel that security added value to an organisation; and was viewed more as a cost on the bottom line. Furthermore the ways in which security could add value had often not been considered. For example, some interviewees did not perceive 'reducing loss' as a way of contributing to profit.

2.3 However other security professionals were of the opinion that security should be perceived as an important part of the business process rather than a separate function on the edge of an organisation. These professionals recognised that security affects all aspects of a business, its staff and contractors, and as such should be integral to its processes. As a result they were keen to promote the case for security to be seen as a business enhancing service rather than merely protecting assets.

2.4 The study found some examples which demonstrate the value security can add to an organisation; for example 'good security' can be used as a pre-requisite for getting insurance and negotiating a lower premium, or in the finance sector can result in regulators granting more freedom to use capital.

2.5 Furthermore many security professionals said that the organisations they worked for did not systematically collect data in order to calculate the value of security. Indeed collecting relevant metrics was often a problem because many organisations undervalue security and do not place a premium on it.

2.6 Meanwhile some professionals, who had collected good data and were able to demonstrate the value of security, admitted that they had not

[1] Gill, M. & Hemming, M. (2007), 'A Study into the Procuring of Security: SRI Report,' Perpetuity Research and Consultancy International Ltd.

[2] Gill, M., Burns-Howells, T., Keats, G. & Taylor, E. (2007), 'Demonstrating the Value of Security: SRI Report,' Perpetuity Research and Consultancy International, Ltd.

always communicated this well. Moreover the name used to describe the 'security function' was highlighted by some security professionals as an important factor in communicating its value. For instance some preferred 'security' because most people would understand what it meant however others were of the opinion that this term was 'old fashioned.' Instead 'Profit Protection,' 'Loss Prevention' and other similar such terms were favoured by those who wanted to create a more 'up to date' image for security.

2.7 The second study also revealed that there was some criticism of the dominance of military and law enforcement backgrounds of senior security personnel. It was argued that whilst they brought good contacts they lacked business acumen and knowledge of business processes. Indeed some of the security professionals interviewed believed that a modern security function should be lead by a person with business rather than security skills.

2.8 It was argued that the lack of business acumen amongst some senior security personnel meant that the security function was likely to be marginalised within some organisations. This was because senior security personnel were not fully respected by senior colleagues in other functions due to their lack of business experience and were therefore unable to influence all the relevant business processes. . Furthermore marginalised internal security functions make it difficult for security contractors to fully contribute to the process of adding value.

2.9 If the position and perception of the security function is to change for the better, then the security sector must be encouraged to see itself as adding value. This is the aim of the 'Best Value for Business' campaign which emerged from the work undertaken in the first two years of the SRI. The campaign was launched by Perpetuity in conjunction with *Security Management Today*, the British Security Industry Association, ASIS International and the Security Institute. It is equally important to change organisations' views of security; to demonstrate to the leaders that security has the capacity to be business enhancing rather than just a cost on the bottom line. As a stepping stone, it is important to understand the views of organisations and their leaders; specifically, how they view the current state and potential of the security function. This has been the aim of the third year of the SRI.

Aims and objectives

2.10 The main aim of this study is to gain a better understanding of the view of the security function from those in senior management positions.

2.11 This study will specifically examine whether employees in senior management positions perceive security as a business enhancing

function or an inevitable cost on the bottom line. It will also explore the following issues:

- What is the role of security and how important is it compared to other functions?
- How can security add value to an organisation and how can this value be demonstrated?
- What makes security effective?
- Are security personnel able?

Section 3. Views of the Security Sector

3.1 There is very little research on what organisations think about their own security function or how important they think it is compared to other functions, how able they perceive security personnel and their perceptions on whether and/or the extent to which security adds value. Indeed, consultation with security scholars in different parts of the world has confirmed that while this is an important area of enquiry it remains a much neglected one.[3]

3.2 What evidence there is suggests that organisations, perhaps inevitably, have a mixed view of security. A few years ago a high profile security expert reported, 'I have found a significant absence of security practitioners who can operate strategically in general, and particularly within today's corporate setting.'[4] Certainly some security professionals that were interviewed in a recent study reported elsewhere[5] feel that they have not always attracted positive attention at least in part because they have not been seen as sufficiently businesslike. For example:

> *I have seen loads of pitches by security people and they cannot convince boards, they just don't speak the language, they turn them off. They have egos, they don't admit they don't understand. Boards think of ROIs and SWOT analyses, security don't.*
>
> *Security Director, Multinational*

3.3 The finding that there are different perceptions of security has emerged from other research. One study,[6] conducted in the aftermath of 9/11 found that bigger companies or at least those where there was likely to be a security manager in place 'were 5-6 times more likely to report frequent security-related interactions with facilities, risk management/auditing, legal, and financial units, and 3-4 times more likely to report such interactions with human resources and operations, compared to' a sample that included small and large companies that did not necessarily have a security head.

3.4 Analysing the findings a stage further it was striking that more than 7 in 10 of the larger companies reported more than six interactions with

---

[3] And there is nothing new in stating a topic related to security is under researched. As a variety of authors have noted, while security as an activity has a very long history, academic interest is relatively recent. For a discussion of this and related issues, see, McCrie, R. (2002) (ed) *Readings in Security Management.* Alexandria: ASIS Foundation,.

[4] Williams, T. *Security Issues are Business Issues First*. In McCrie, Ibid.

[5] Gill, M. Burns-Howell, T., Taylor, E., Keats, G. (2007), Op Cite www.perpetuitygroup.com/prci/publications.html. This study is an output of the Security Research Initiative (SRI).

[6] ASIS Foundation, p 43, op cite.

human resources, operations and facilities. And over half the same with risk management/auditing, legal and financial.

3.5 Similarly, a study in retailing found that loss prevention directors had extensive contact with managers across the company including, store managers, store operations, inventory control managers, human resource managers,[7] internal audit, information technology, as well as finance.[8]

3.6 There are various views as to what is an appropriate role for security. Some security professionals and security departments view their role as 'Traditionalists' whereby security is viewed as a service function that inevitably involves a cost on the bottom line, similar to other service functions and where success is measured in terms of arrests made, or number of investigations conducted.

3.7 Conversely, 'Modern Entrepreneurs', see security not as a discrete function but as a factor that impacts upon every facet of the organisation. As such, good security knowledge needs to be accompanied by business skills and an understanding of business processes.[9] After all, how can anyone influence the business with security advice if that person does not understand both business and its processes and security principles?

3.8 The different approaches will inevitably impact upon the perception of security. Indeed some books on security warn of the danger of security being seen as the organisation's enforcement officer and thus inhibiting the potential of the security function to generate a security culture which promotes the need to protect the organisation's assets as everyone's business.[10]

3.9 Some have argued that the relationship between security and other functions should be harmonious as the 'interface serves to solve potentially disruptive problems shared by both functions'.[11] However, the reality is that 'this harmony is not always found'[12] not least when the authority of the security function is not clearly defined. Or when the advice provided by security professionals is seen as getting in the way

[7] For a good discussion o the importance of human resources skills sets to security, see, Lane, K. (2001) Human Resources: Is It a Weak Link in the Security Chain of your Company. *Security Journal*, 14,4, pp7-16.
[8] Hayes, R. (2003) Loss Prevention: Senior Management Views on Current Trends and Issues. *Security Journal*, 16, 2, pp7-20.
[9] The two classifications reported here are presented as 'ideal types' to portray different ways security professionals themselves view security. See ibid.
[10] For a good discussion on security culture, see contributions to, Khripunov, I., Ischenko, N. And Holmes, J. (2007) (eds). *Nuclear Security Culture: From National Best Practices to International Standards*. Amsterdam: IOS Press.
[11] Fischer, R, and Green, G. (1998) *Introduction to Security*. Boston: Butterworth-Heinemann, p112
[12] Ibid, p113.

of business rather than enhancing it (at least without what is interpreted as good reason). This will invariably be viewed as 'bad' security.

3.10 Similarly, another writer has made the point that because security is an integrated function (or at least where it is seen as such), if the security director's remit and aims are 'contrary to or foreign to that of other business units heads, support will be difficult to obtain, if not outright impossible'.[13]

3.11 The key point here is employees. On the one hand they present a threat to security by being careless or reckless, or by being dishonest and even acting in collusion with other offenders, but on the other they are also the key means of ensuring that security is promoted.[14] These staff will mostly be under the management of other personnel and functions and so influencing them will require an understanding of the role they play in different parts of the organisation.

3.12 Recognising that security is integrated with other functions provides a key way of measuring its success. As Dalton has noted, the value placed by internal customers that is other parts of the organisation becomes a key measurement of the overall contribution of security to the aims of the business.[15] Yet, it is far from clear that such measures are common.

3.13 One British Security Manager, Wyllie, has argued that the security manager's first role is that of sales person, to management as well as staff across the organisation. That it is essential for the security director to relate to all business functions.[16]

3.14 This point is also reiterated by Briggs and Edwards who argue that, 'It is imperative to foster close communication and understanding between specialist managers ... which is likely to involve extensive networking between senior management'.[17] Their publication includes a focus on the need for security to be closely aligned to the organisational goals.

---

[13] Dalton, D. (1995) *Security Management: Business Strategies for Success*. Boston: Butterworth-Heinemann, p190.

[14] See, for example, Purpura, P. (1998) *Security and Loss Prevention: an Introduction*, Boston: Butterworth-Heinemann, p81.

[15] Dalton, D. (1998) *The Art of Successful Security Management*. Boston: Butterworth-Heinemann. For a discussion of the different roles of security, including that of internal customer, see, Gill, M. (2006) Introduction. In Gill, M. (ed) *The Handbook of Security*. London: Plagrave.

[16] Wyllie, B. (1998) *The Millennium Security Manager*. Private publication, Woodhouse Eaves, Leicester.

[17] Briggs, R. and Edwards, C. (2006) *The Business of Resilience*. London: DEMOS, p57.

Meeting the Challenge

3.15 Realising the potential of security to impact on the organisation is likely to be testing. Research has shown that corporate security executives face challenges persuading senior management that their area is an important one.

3.16 A study in the US found that executives tend to prioritise security in terms of operational risk, such as compliance and regulation. Less focus is placed on strategic issues, such as competitive advantage and brand management.[18] More recent research has highlighted the general difficulty CEOs face in having their policies executed effectively and again highlights the importance of brand protection as an important issue, and the need for security operatives to be skilled in a wide variety of areas.[19]

3.17 There is evidence from a study of retailing that there are major differences in perspectives on loss between retail executives on the one hand and loss prevention directors on the other. Indeed there were major differences on priorities. The report, by Protiviti, argues that the reason is that retail executives on the one hand and loss prevention manages on the other come from different professional and educational backgrounds, and note that the latter do not have broad experience of business. The report argues that there is a need for loss prevention to align itself with the business if it is to be successful.[20]

3.18 Another study in the US has found that companies that invest in security tend to be those that have the most to lose.[21] Indeed, concerns at some type of significant loss, and worries about meeting regulation concerns drive interest in security. Where these are not priorities then security faces a challenge to be heard.

3.19 The same is true in the UK, where one study has found that, 'the majority of senior management interviewed stated that, in their experience, concern about crimes, other than those committed directly against the business was negligible ... it is difficult to argue that they will do anything that is not required by law unless the actuality or risk of crime unequivocally reduced shareholder value'.[22]

---

[18] Thomas E. Cavanagh (2006) *Making the Business Case for Security*. The Conference Board. Report Number: A-0200-06-EA

[19] See, Security Magazine, may 2008, for report on a survey of 100 CEOs, and see also, The Conference Board report, CEO Challenge 2007: Top 10 Challenges.

[20] Protiviti (2007/8) Loss Prevention: Bringing Executive and Loss Prevention Perspectives into Alignment. Provtiviti report, US.

[21] Thomas E. Cavanagh (2006) *Navigating Risk: The Business Case for Security*. The Conference Board. Report Number: R-1395-06-RR

[22] Levi, M., Morgan, J., and Burrows, J. (2003) Enhancing Business Crime Reduction: UK Directors' Responsibilities to Review the Impact of Crime on Business. *Security Journal*, 16, 4, p19.

3.20 To date there has been very little consideration of how the role and status of internal security impacts upon contract security, but it is significant. Procurers often take advice from internal security professionals when buying security, and this presupposes those who lead security departments have the necessary expertise to offer good insights. The choice of contractor will be guided by what is required by the security strategy (or should be), but this often does not exist. If the status of the internal security function is low, or marginalised, or lacks expertise or is not guided by a strategy, then what hope is there for security contractors no matter how good they are? The fact of the matter is, the role of the internal security function and the perception of it to internal peers has a major impact on what contractors can do.[23]

3.21 This is further complicated because in some cases, for example manned guarding, the security officers typically work at the client site. Unless officers are properly supported, and this may involve the need for a 'partner care strategy' or something akin, then the ability for the security provider to maximise its influence is inevitably compromised.

3.22 It is helpful to examine this issue a little further. Certainly private security has had a somewhat tarnished image. The Private Security Industry Act 2001 was justified, in part, on the need to raise standards in an industry where performance was variable but sometimes unacceptably low. The response was to introduce compulsory licensing for persons conducting some security functions, and a voluntary 'Approved Contractor Scheme'.[24] But this was never going to deal with the broader problem that faces security; getting proper recognition of the role of security within organisations, and thereby enhancing recognition as to how the whole security function (internal and contractors) can enhance the business aims.[25]

3.23 And it is important not to lose sight of the fact that security measures are typically valued by the public, this is true of a range of measures from security guards and CCTV.[26] And security measures have often been perceived favourably by those who work in different environments.[27]

---

[23] See, Gill et al, op cite.

[24] For further information see, http://www.the-sia.org.uk/home

[25] This is not a criticism of the Security Industry Authority, merely a recognition that it tackles only a small (but important) part of what it will take to professionalise the service.

[26] For example, see Gill, M and Spriggs, A. (2005): *Assessing the Impact of CCTV*, Home Office Research Study 292. London: Home Office. www.homeoffice.gov.uk/rds/pdfs05/hors292.pdf; Department for Transport - Fact sheet 4 - Perceptions of security on train and underground rail travel. See also, Button (2007) *Security Officers and Policing*. Aldershot: Ashgate.

[27] See, Wakefield, A. (2003) Selling Security. Collumpton: Willan; Wakefield, A. and Gill, M. (forthcoming) When Security Fails: The Impact of Human Factors on the Deployment of Retail Security Personnel. *Policing and Society;* and going in back in time, Beck, A. and Willis, A. (1995) Managing the Risk to Safe Shopping. Leicester: Perpetuity Press.

3.24 The police often work quite closely with security, and they too have expressed some diverse views. Some of those who have worked with security operators (at least pre-regulation) sometimes did not trust their judgement or consider them reliable.[28] And there has often been a tendency for the police to worry about the accountability of private security. But again there is plenty of evidence of good working relationships. In the US one study found that police and security had very positive views of each other.[29]

3.25 In the UK, one initiative that gains the most attention these days is Operation Griffin[30]. This started in London and has now generated off shoots wider a field including the US. Although even here there has not been any independent evaluation. There are other examples. For example business schemes flourish around the UK, and Action Against Business Crime[31], which by its very nature encourages liaison between the police and the private sector. Although in these cases too there is a lack of independent evaluation determining whether they work or not or why they do or do not.[32]

Summary

3.26 The important point to make, at least for the purposes of this study, is that the security sector has had what might best be described as a 'variable' relationship with partners, be that law enforcement or organisations. The very strong trend that emerges across the literature is that security needs to influence all parts of the organisation, in the big companies at least it seems security professionals are interacting with other functions, what is less clear is how successful those interactions are, or what the perceptions of security are amongst other departments.

3.27 There has been concern, and this comes from security professionals themselves, that security people are not very business-like and therefore they have not been able to influence the organisation and talk the language of business. What is needed is a better understanding of the views of organisations. The aim of this research therefore is to help fill a knowledge gap, about how security is perceived.

---

[28] Gill and Spriggs, op cite.

[29] Nalla, M. And Hummer, D. (1999) Relations Between Police Officers and Security Professionals: A Study of Perceptions. *Security Journal*, 12, 3, pp 31-40. For a good summary of some of the research on this issue, see Wakefield (2003) op cite.

[30] Project Griffin aims to encourage members of the community to work in partnership with the police to deter and detect terrorist activity and crime. For more information see: http://www.cityoflondon.police.uk/CityPolice/CT/ProjectGriffin/

[31] Action Against Business Crime (AABC) is the national organisation for Business Crime Reduction Partnerships (BCRPs) whose aim it is to reduce crime and anti-social behaviour which affects businesses. For more information see: http://www.brc.org.uk/aabc/default.asp?content_id=1

[32] For a good critique of Business Watch, see, Charlton, K. and Taylor, N. (2005) The Trouble with Business Watch: Why Business Watch Programs Fail. Security Journal, 18, 2, pp7-18.

Section 4. Organisations' perspectives of the security function

4.1 This section reports on the findings of two sources:

- The IOD survey - A telephone survey with 500 members of the Institute of Directors (IoD).
- The targeted business survey – 112 questionnaire responses completed by members of the following associations: Confederation of Business Industry (CBI), UK FTSE 100 companies and the Commercial Crime Services (CCS) division of the International Chamber of Commerce (ICC).

4.2 Each of the themes explored in the IoD survey have been examined by region, industry, number of employees, turnover and the job title of the respondent. Only where this breakdown illuminated interesting trends have these been reported throughout this section.

4.3 Similarly where appropriate the targeted business survey respondents have been broken down, and any differences in the responses made by CBI/FTSE 100 members and CCS members highlighted. (Please refer to the Methodology section in the appendix for further details)

4.4 Whilst the IoD survey is representative of its membership, caution should be taken when interpreting the targeted business survey findings due to the small and unrepresentative nature of the sample.

4.5 This section begins by exploring the role of security, exploring in particular the importance attributed to security when compared to other organisational functions. The section then moves on to consider:

- Security as a value adding function
- Whether or not security is viewed as generating a competitive advantage.
- The information which organisations do or do not collect in regard to security.
- The factors which are believed to make security effective or not
- Organisational views of both internal and external security staff.

The role of and importance of security

4.6 The first topic explored by the IoD survey was the importance attributed to the security function by organisations. As noted earlier in this report, this is an area considerably lacking in research evidence. To measure the value attributed to departments, respondents were asked to rate various functions in terms of their importance to the overall success of the organisation. Scores were sought on a scale of one to seven, where seven inferred an exceptional contribution and one inferred a minimal contribution. The results are displayed in Table 1 below.

Table 1: Importance of security to the success of an organisation compared to other functions

Function	Mean[33]	Standard Deviation[34]	Number[35]
Sales	5.7	1.9	491
Finance	5.0	1.6	496
Human Resources	5.0	1.7	493
Marketing	4.9	1.7	494
Security	**4.7**	**1.8**	**490**
Facilities	4.0	1.6	486
Operations Manufacturing	3.7	2.3	448

4.7 Although security was ranked fifth out of the seven functions, the scores of those functions ranked second to fifth were close. Security was rated higher than facilities, and that it should be viewed as close to human resources and finance is striking. Clearly, in many organisations, security is not viewed as the poor relation.

4.8 Whilst sales was (perhaps expectedly given its business development role) attributed the highest level of importance in regard to influence upon the success of an organisation security was awarded substantial emphasis. Security's average score of 4.7 is approaching the upper echelons of the seven point scale. As such, it can be inferred that security is viewed by this sample as important to the success of the organisation.

[33] Results have been rounded up/down to the nearest decimal place for purposes of presentation.

[34] Standard deviation measures how widely spread individual responses typically were from the average (measured in the same units as the data). Standard deviation therefore provides a good measure of how widely dispersed the scores are from the average and thus highlights consistency/inconsistency.

[35] Whilst the term "number" refers to the actual number of responses achieved, the mean score awarded to each function was adjusted so that all functions had a "weighted" response of 500 individuals. Having the means based on an identical number of responses allows a greater degree of comparability.

4.9 A detailed breakdown of individual responses (see Table 2 below) again shows the importance attributed to security in regard to the overall success of an organisation with almost two thirds of respondents awarding security a score of 5, 6 or 7. It can be inferred therefore that, in their view, security is important to the success of their organisation. The similarity between the response breakdown of security and human resources, again demonstrates security as a significant function. Still though, it is important to note that over a quarter claimed security was not important, a minority, but not a tiny one.

Table 2: Importance of security to the success of an organisation compared to other functions

Function	Scores of 5, 6 or 7 (important)	Scores of 1, 2 or 3 (not important)
Sales	80%	15%
Finance	70%	19%
Human Resources	65%	20%
Marketing	68%	20%
Security	**60%**	**26%**
Facilities	43%	34%
Operations Manufacturing	40%	43%

4.10 Whilst organisations taken as a *whole* awarded the security function an average score of 4.7 (from a maximum of seven), it is interesting to consider the mean score awarded to the security function by industry sector presented in Table 3 below.

Table 3: Industry sector: the importance of the security function to the success of an organisation (mean score)

Industry Sector	Mean	Number (N)	Weighted Total
Financial Services	4.9	80	80
Distribution and Hotels	4.9	25	25
Business and Professional services	4.8	200	205
Govt., Education, Health and Personnel Services	4.5	62	65
Other incl. Construction, Mining and Transport	4.5	72	75
Manufacturing	4.4	50	50

4.11 The crucial point to draw from Table 3 is that when analysed individually, each industry sector considered security to provide an above average contribution to the success of an organisation. This is reflected by average scores of 4.0 or above for each sector (note that a score of four is considered to be a neutral response[36]).

4.12 A second issue of note is that the security function was considered slightly more important by financial services, distribution and hotels and business and professional services compared to government, education, health and personnel services, manufacturing, and sectors included in the 'other' category such as construction, mining and transport. Further, comments about perspectives on security by the different sectors are reported below.

Targeted business survey findings

4.13 Several of the statements in the targeted business survey were also designed to elicit respondents' views on the importance of the security function in comparison to other functions.

4.14 Findings from the targeted business survey suggest that security was regarded with some degree of significance by respondents, supporting the IoD results. A number of individual results support this claim. First, the vast majority of respondents (80 per cent/n=88) either 'disagreed' or 'strongly disagreed' that security is one of the least important functions within an organisation. Secondly, and perhaps more tellingly, targeted business survey respondents rated security on a par with many other organisational functions. Table 4 (below) indicates that at least half of the respondents 'agreed' or 'strongly agreed' that security

[36] The **only** neutral response available for respondents was to award a score of "4". For this reason, overall mean scores greater than 4.0 have been considered above a neutral response throughout this report.

was at least as important as human resources and finance. Well over a third reported that security was as important as sales; a finding all the more striking given the emphasis placed upon sales in the IoD findings above.

Table 4: The importance of the 'security' function compared to other functions within an organisation

Statement	Strongly Agree and Agree	Strongly Disagree and Disagree	Neither Agree or Disagree	Don't Know
Security is at least as important as Human Resources	62% (n=68)	19% (n=21)	18% (n=20)	1% (n=1)
Security is at least as important as Finance	51% (n=55)	29% (n=32)	18% (n=20)	2% (n=2)
Security is at least as important as Sales	42% (n=46)	29% (n=32)	28% (n=30)	1% (n=1)

4.15 Table 5 (below) is a breakdown of those respondents who 'agreed' or 'strongly agreed' that security was at least as important as Human Resources, Finance and Sales by sample: CBI/FTSE 100 sample compared to the CCS sample. The table shows that the CCS respondents were more likely to think that security is at least as important as other company functions, compared to the CBI/FTSE 100 sample. Importantly, this infers that CCS respondents attach a greater degree of value to the security function in comparison to CBI/FTSE 100 respondents. This is not necessarily surprising when one consider that CCS respondents have proactively chosen to affiliate with an organisation which provides information, advice and consultancy on issues such as fraud, money laundering and counterfeiting detection and prevention.[37]

[37] The statistical significance of these results was tested however due to the small sample size this was not possible to determine because the assumptions of the chi-square test were not met.

Table 5: CBI/FTSE 100 and CCS respondents whom considered security at least as important as Finance, Human Resources and Sales within an organisation

Statement	CBI/FTSE 100 respondents (sample 1): Strongly Agree and Agree	CCS respondents (sample 2): Strongly Agree and Agree	Percentage points increase (from sample 1 to sample 2)
Security is as important as Finance	33% (n=18)	69% (n=37)	+ 36%
Security is as important as Human Resources	52% (n=29)	72% (n=39)	+ 20%
Security is as important as Sales	26% (n=15)	59% (n=31)	+ 33%

Security as an organisational function

4.16 Questions were also included in the targeted business survey to explore the remit of a security department within organisations. To measure remit, two statements were included.

1. Security is primarily about the protection of assets

2. Security is about ensuring compliance with regulations

4.17 Nearly two thirds of respondents (sixty three percent/n=70) felt that the role of security is primarily about the protection of assets compared to only 23 per cent (n=25) who disagreed. There was no clear distinction amongst the respondents as to whether the security function is about ensuring compliance with regulations, with 44 per cent (n=49) of the respondents agreeing with this statement, almost a third (31 per cent/ n=34) disagreeing and a quarter (n=27) undecided/neutral.

4.18 Whilst these statements explore, and arguably confirm, 'traditional' views of a security department as providing protection and enforcing compliance with regulations, later the role of security as a value adding and profit making function is explored.

The scope of a security function

4.19 Findings from the targeted business survey again confirmed that security is perceived as an important function within an organisation. Furthermore, the findings suggest that security is not a marginal function, and influences core organisational activities. Crucially, at least 90 per cent of respondents 'agreed' or 'strongly agreed' that the security function impacts on all aspects of business and should be integrated into all aspects of an organisation. These findings are further supported by the high proportion of respondents (57 per cent/n=63) who disagreed or strongly disagreed that security is marginal or insignificant when compared to core organisational activities. Only 22 per cent (n=24) agreed with this statement.

Summary

4.20 Whilst the sales function was ranked as most important to the success of a business, out of seven organisational functions, security was rated only slightly below human resources, finance and marketing. On the whole security was not viewed as a poor relation.

4.21 The general consensus amongst the targeted business survey respondents was that the role of the security function was primarily in terms of the protection of assets. Latter sections investigate the role of security as a value adding function.

4.22 Targeted business survey respondents felt that security should be integrated into all aspects of a business, and that security is significant to all core organisational activities. It is clear therefore that security is commonly perceived to be important to the success of a business.

The value security can add to an organisation and how this value can be demonstrated

Security and meeting the objectives of an organisation

4.23 The IoD survey included questions to ascertain the extent to which security was perceived to add value to organisations (if at all). Three key aspects (physical, personnel and internet/computer security) were explored.

4.24 To measure perceptions, respondents were asked to rate the importance of these three aspects of security on a scale of one to seven. A score of seven denotes that the security aspect being referred to adds substantial value to the organisation helping it to achieve its objectives. Conversely, a score of one means that the security aspect

adds little value to meeting company objectives. The results are displayed in Table 6 below.

Table 6: Important of internet and computer security, personnel security and physical security to an organisation

Aspect of security	Mean	Standard Deviation	Number[38]
Internet and computer security[39]	6.2	1.1	499
Personnel security[40]	4.6	2.0	496
Physical security[41]	4.5	1.0	495

4.25 Table 6 clearly demonstrates one striking result; that, internet and computer security adds value to organisations and helps them to meet their objectives. With a mean score of 6.2, this security aspect was viewed as extremely important.

4.26 When judged in direct relation to internet and computer security, personnel and physical security were perceived as adding less value to meeting the objectives of the organisation. However, the mean scores do suggest that, overall, they are perceived as important too.

4.27 Perhaps one explanation for this is the extent to which personal computers and the internet pervade the everyday working life of most workers. Moreover, there has been a lot of publicity about protecting data, and there are legal requirements governing confidential customer information. By contrast, personnel and physical security may appear more distant.

4.28 The importance attributed to internet and computer security is further emphasised by examining the 91 per cent of respondents (see Table 7 below) who awarded this aspect of security a score of 5, 6 or 7. In contrast, only three per cent of respondents awarded a score of 1, 2 or 3. Again though, it is clear that the majority of respondents feel that personnel and physical security are also important.

Table 7: Importance of internet and computer security, personnel security and physical security to an organisation

Aspect of security	Scores of 5, 6 or 7 (important)	Scores of 1, 2 or 3 (not important)

[38] Each aspect of security had a weighted response of 500 individuals.
[39] I.e. firewalls, anti-virus software, intruder detection systems, encrypted virtual place networks, etc.
[40] I.e. following up references, police checks, etc.
[41] I.e. guarding, intruder alarms, CCTV, safes, etc

Internet and computer security	91%	3%
Personnel security	56%	29%
Physical security	56%	32%

4.29 Tables 8, 9 and 10 (below) outline the value added to meeting the objectives of an organisation by the three security aspects for different industry sectors.

Table 8: Industry sector: The value added to meeting the objectives of an organisation by *internet and computer security* (mean score)

Industry sector	Mean
Financial Services	6.4 (n=80)
Business and Professional Services	6.3 (n=205)
Distribution and Hotels	6.1 (n=25)
Government, Education, Health and Personnel Services	6.1 (n=64)
Manufacturing	5.9 (n=50)
Other incl. Construction, Mining and Transport.	5.8 (n=75)

4.30 From Table 8 it is clear that financial services and business and professional services perceived internet and computer security as adding more value to meeting the objectives of an organisation in comparison to other sectors, particularly those included in the 'other' category such as construction, mining and transport and in the manufacturing category. The mean score awarded by the financial services was also slightly higher than the overall mean ranked by the whole of the sample for internet and computer security. This is perhaps predicable give the services provided by financial services such as on-line banking and the financial and sensitive data stored on their information systems.

Table 9: Industry sector: The value added to meeting the objectives of an organisation by *personnel security* (mean score)

Industry sector	Mean
Financial Services	5.1 (n=81)
Distribution and Hotels	5.1 (n=25)
Government, Education, Health and Personnel Services	4.9 (n=66)
Business and Professional Services	4.4 (n=205)
Other incl. Construction, Mining and Transport.	4.4 (n=72)
Manufacturing	4.2 (n=49)

4.31 Table 9 summarises the mean scores for personnel security. The results suggest that this aspect was considered by all industry sectors to add an above average amount of value to meeting the objectives of an organisation; it is noted however that financial services, and

distribution and hotels attributed a higher value to personnel security than other sectors.

Table 10: Industry sector: The value added to meeting the objectives of an organisation by physical security (mean score)

Industry sector	Mean
Distribution and Hotels	5.1 (n=24)
Other incl. Construction, Mining and Transport.	5.1 (n=73)
Financial Services	4.9 (n=79)
Government, Education, Health and Personnel Services	4.4 (n=63)
Manufacturing	4.3 (n=51)
Business and Professional Services	4.1 (n=204)

4.32 Table 10 summarises differences between industry sectors in relation to physical security. The results demonstrate that all industry sectors perceive physical security as adding an above average amount of value to meeting the objectives of an organisation. Physical security was given the most emphasis by distribution and hotels, the 'other' category and financial services. This is important as it highlights that physical security is valued alongside other security aspects in some organisations.

4.33 Although only cautious comparisons can be made between industry sectors due to sample size, it is interesting to note that financial services and distribution and hotels are more positive about the value that security in general adds to an organisation compared to the other sectors.

4.34 Further analysis of the IoD sample revealed one additional finding of note. Figures 1 and 2 below show that with one exception (in both cases the echelon – "101 to 200 employees") the degree of value attributed to a) personnel security and b) physical security in terms of meeting the objectives of an organisation gradually increased according to employee size.[42]

[42] Due to the fact Perpetuity did not have sight of the raw data set it was not possible to crosstab industry sector by employee size. This makes it impossible to assess any correlation between these two variables and the effect any correlations will have on the results. Clearly, this limitation needs to be borne in mind.

Figure 1: Employee size: the value added by 'personnel security' to meeting the objectives of an organisation (mean score)

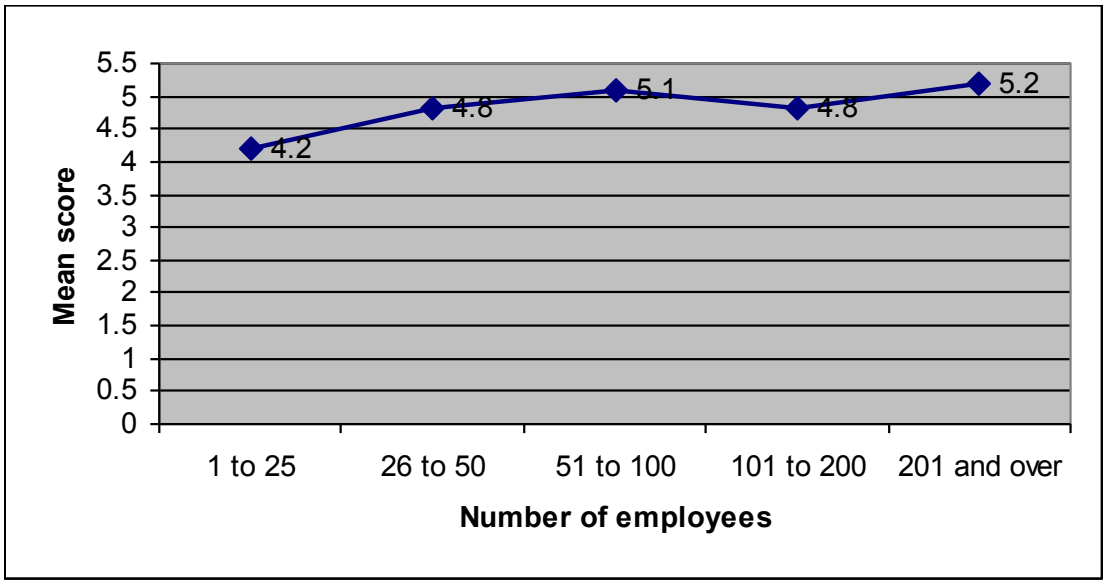
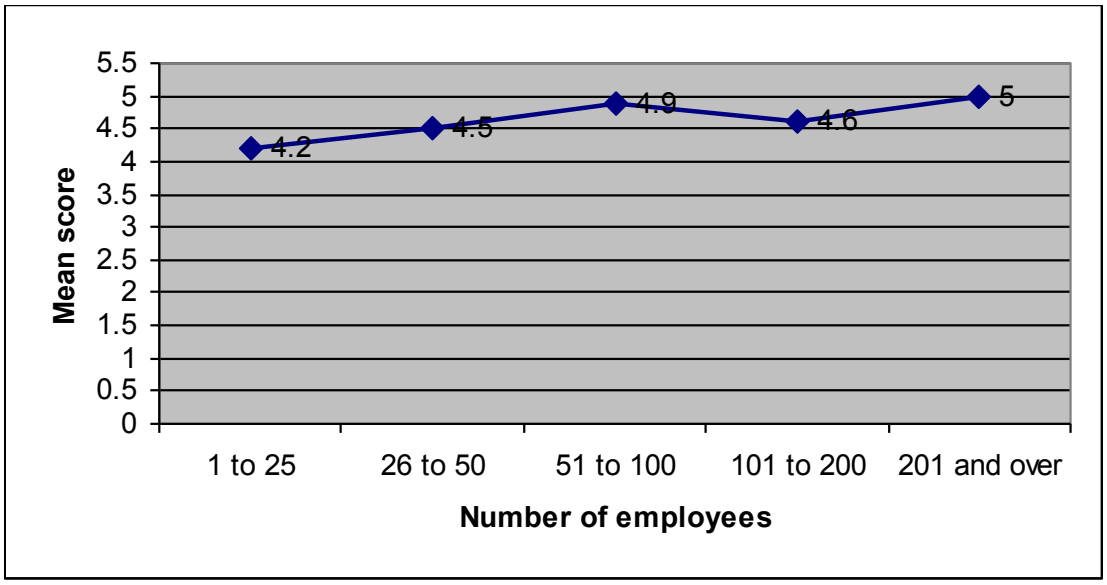


Figure 2: Employee size: the value added by 'physical security' to meeting the objectives of an organisation (mean score)



4.35 The trend[43] described above is most apparent in the increase of mean scores given by respondents in the following categories: '1 to 25,' '26 to 50' and '51 to 100;' after which the mean scores become more stable. This suggests that the larger companies tend to consider personnel and physical security as adding more value to an organisation than smaller firms.

[43] Caution should be taken however in light of the inconsistent samples upon which the mean scores for each employee category are calculated (between 40 and 257 responses for 'personnel security' and 40 and 256' for 'physical security'); in addition to the small increases between the mean scores (between 0.60 and 1 for 'personnel security' and 0.30 and 0.80 for 'physical security'

Value for money

4.36 In order to measure value for money, respondents were asked to consider the money they have spent on physical, personnel and internet and computer security and then rate its effectiveness on a scale of one to seven. In this instance a score of seven represented an overall sense of excellent value for money. Conversely, a score of one represented a sense that no value for money had been achieved. The results from this line of questioning are demonstrated in Table 11 below.

Table 11: Organisations' perceptions of the value for money delivered by internet and computer security, personnel security and physical security

Aspect of security	Mean	Standard Deviation	Number[44]
Internet and computer security	5.7	1.3	493
Physical security	4.6	1.8	480
Personnel security	4.5	1.8	477

4.37 The results displayed in Table 11 demonstrate that internet and computer security is perceived as delivering the greatest value for money (represented by an average score of 5.7 out of a maximum of seven). In comparison, physical and personnel security were perceived as delivering less value for money yet still offering a degree of cost effectiveness (4.6 and 4.5 out of seven respectively). These trends are again reflected in Table 12 where individual scores are considered. It is striking that eighty-three per cent of respondents awarded internet and computer security a score of 5, 6 or 7.

Table 12: Organisations' perceptions of the value for money delivered by internet and computer security, personnel security and physical security

Aspect of security	Scores of 5, 6 or 7 (Excellent value)	Scores of 1, 2 or 3 (No value)
Internet and computer security	83%	7%
Physical security	59%	25%
Personnel security	54%	26%

4.38 Interestingly there is synergy between responses to the previous two IoD survey questions concerning the value which security can provide organisations. Internet and computer security is unequivocally perceived as adding value to the organisations sampled in two respects. Firstly it adds value to meeting the objectives of the organisation and secondly it is perceived to be cost effective. Whilst the

[44] All aspects of security had a weighted response of 500 individuals.

same trend is also apparent in terms of personnel and physical security, these aspects were not rated to the same degree.

4.39 To extract a further level of detail, the following three tables depict a breakdown by industry sector of the mean scores awarded to internet and computer security, personnel security and physical security in terms of their value for money.

Table 13: The cost-effectiveness of *internet and computer security* broken down by industry sector

Industry sector	Mean
Financial Services	6.0 (n=80)
Business and Professional Services	5.8 (n=200)
Other incl. Construction, Mining and Transport.	5.6 (n=73)
Distribution and Hotels	5.5 (n=25)
Government, Education, Health and Personnel Services	5.5 (n=63)
Manufacturing	5.5 (n=51)

4.40 It is clear from Table 13 that all industry sectors considered internet and computer security to deliver a high degree of value for money (mean scores were 5.5. or above). Financial Services and business and professional services awarded it the highest mean score compared to other sectors.

Table 14: The cost-effectiveness of *personnel security* broken down by industry sector

Industry sector	Mean
Distribution and Hotels	4.9 (n=23)
Government, Education, Health and Personnel Services	4.9 (n=61)
Financial Services	4.7 (n=77)
Business and Professional Services	4.5 (n=195)
Manufacturing	4.3 (n=47)
Other incl. Construction, Mining and Transport.	4.2 (n=71)

4.41 The mean scores awarded by each industry sector to personnel security (as shown in Table 14) infer that this specific security function is perceived as providing reasonable cost effectiveness. It was attributed the highest mean scores by distribution and hotels,

government, education, health and personnel services, and financial services compared to other sectors.

4.42 Similarly the mean scores awarded by each sector to physical security (as shown in Table 15) infer that this aspect of security is also considered to provide reasonable cost effectiveness. Distribution and hotels and manufacturing ranked the cost effectiveness of physical security the highest out of all of the industry sectors.

Table 15: The cost-effectiveness of *physical security* broken down by industry sector

Industry sector	Mean
Distribution and Hotels	5.1 (n=23)
Manufacturing	4.9 (n=48)
Financial Services	4.7 (n=75)
Government, Education, Health and Personnel Services	4.6 (n=60)
Other incl. Construction, Mining and Transport.	4.5 (n=74)
Business and Professional Services	4.4 (n=196)

Targeted business survey findings

4.43 Whilst the IoD survey investigated the cost effectiveness of physical security as a general category, the targeted business survey explored one aspect of physical security in particular, specifically the role of security contractors. Findings revealed that respondents had mixed views with regards to the value for money they delivered. One third of the respondents (n=34) felt that they did tend to deliver good value whilst 13 per cent (n=13) did not think they did, and 39 per cent (n=38) gave a neutral response.

Security as generating a competitive advantage

4.44 Security managers' views on security were assessed in the second year of the SRI. Views varied markedly. Some security professionals did not think that security added value to organisations. Some reported that their organisations did not collect any metrics to assess whether they added value. Others were keen however to promote security as a business enhancing service rather than mere asset protection.

4.45 In light of these findings, the IoD survey included a question aimed at assessing whether various elements of security are viewed as being a cost on the bottom line or as generating a competitive advantage. Respondents were asked to rate seven aspects of security on a scale of one to seven, where a score of seven infers a strong competitive

advantage and one a cost without sufficient benefits. Findings from this question are presented in Table 16 below.

Table 16: Organisations' perceptions of whether aspects of security are a cost without sufficient benefits or generate a competitive advantage

Aspect of security	Mean	Standard Deviation	Number
Electronic security precautions (firewalls, virtual private networks)	5.1	1.8	478
Defined security policy communicated to all staff	4.4	2.1	477
Personnel checks (following up references, etc)	4.1	1.8	477
Physical security (fences, gates, locks, etc)	3.5	2.0	472
Alarm contractors	3.5	2.0	468
CCTV monitoring	3.1	2.0	445
On site security guards	2.5	1.8	422

4.46 In terms of generating a competitive advantage, electronic security precautions (including firewalls and virtual private networks) were awarded the highest average score. Again, synergy emerges between this finding and that of earlier findings which suggest that internet and computer security is both cost effective and adding value to organisations.

4.47 Four security measures were awarded an average score placing them towards the lower echelon of the seven point scale; physical security (3.5), alarm contractors (3.5), CCTV monitoring (3.1) and on site security guards (2.5). In response to these findings, there is a real need for the security industry to explain and disseminate the value that these physical security measures can provide organisations.

4.48 Having a 'defined security policy communicated to all staff' (viewed as critical by security experts) was rated only fractionally above a neutral response. Moreover, (as seen in Table 17) 30 per cent of respondents awarded scores of 1, 2 or 3 to a 'defined security policy communicated to all staff' suggesting that this measure was more of a cost without sufficient benefit than a source of competitive advantage.

Table 17: Organisations' perceptions of whether aspects of security are a cost or generate a competitive advantage[45]

Aspect of security	Scores of 5, 6 or 7 (competitive advantage)	Scores of 1, 2 or 3 (cost without sufficient benefit)
Electronic security precautions (firewalls, virtual private networks)	64%	18%
Defined security policy communicated to all staff	53%	30%
Personnel checks (following up references, etc)	45%	36%
Physical security (fences, gates, locks, etc)	34%	47%
Alarm contractors	31%	48%
CCTV monitoring	25%	51%
On site security guards	15%	62%

4.49 A more detailed exploration of the IoD sample revealed that those companies with a low number of employees (under 100) and a low annual turnover (under ten million) tended to rate on site security guards and CCTV as more of a cost than a benefit. This supports the finding in paragraph 4.36 that smaller companies are less likely to report that security adds value to their organisation.

Targeted business survey findings

4.50 Whilst the IoD survey analysed the competitive advantage provided by particular aspects of security, the targeted business survey sought to elicit organisations' perceptions of the value of security as an overall function. These perceptions were measured in response to three statements: (responses are shown in Table 18 below)

1. Security is an unwelcome burden on the bottom line
2. Security is a value added function
3. Security is a profit making function

4.51 Encouragingly the findings from the targeted business survey show that the majority of respondents felt that the security function could add value to an organisation in some way.

[45] Whilst it was possible to analyse previous questions by industry, a detailed exploration in this case generated no findings of interest.

4.52 Table 18 shows that almost three quarters of respondents 'disagreed' or 'strongly disagreed' that security was an unwelcome burden on the bottom line. Furthermore two thirds also agreed or strongly agreed that security is a value adding function. There is clearly already a reasonable degree of understanding amongst organisations with respect to the value security can add to an organisation.

4.53 Crucially however, whilst the majority of targeted business survey respondents viewed security as a value adding function, Table 18 indicates that they stopped short of claiming it to be a profit making function. In fact, only a quarter of the respondents felt that security could generate a profit for an organisation compared to almost a half that 'disagreed' or 'strongly disagreed'.

Table 18: Respondents' perceptions of the value of the security function

Statement	Strongly Agree and Agree	Strongly Disagree and Disagree	Neither Agree or Disagree	Don't Know
Security is an unwelcome burden on the bottom line	10% (n=11)	72% (n=80)	17% (n=19)	1% (n=1)
Security is a value adding function	67% (n=75)	20% (n=22)	12% (n=13)	1% (n=1)
Security is a profit making function	25% (n=28)	49% (n=54)	24% (n=27)	2% (n=2)

4.54 A closer examination of the targeted business survey respondents by sample (CBI/FTSE 100 against CCS) indicates that more of the CCS respondents felt that security could add value to an organisation than CBI/FTSE 100 companies. For example, while 84 per cent (n=46) of the CCS respondents did not believe that security was an unwelcome burden on the bottom line, only 61 per cent (n=34) of the CBI/FTSE 100 sample thought the same. Similarly a greater proportion of the CCS respondents (79 per cent/n=43) reported that security was a value adding function compared to CBI/FTSE 100 respondents (57 per cent/ n=32). Finally, almost twice as many of the CCS respondents (33 per cent/n=18) agreed that security was a profit making function compared to CBI/FTSE 100 respondents (17 per cent/n=10).[46]

4.55 Once again these results show that the CCS respondents had a more positive perception of the value security could add to an organisation. These results are also somewhat predicable given the security emphasis of the CCS.

[46] It was not possible to determine the statistical significance of these results because the assumptions of the chi-square test were not met due to the small sample size.

Measuring and communicating the value of security

4.56 The second year of the SRI discovered that many organisations did not collect metrics or data which could be used to assess the value of their security. However many security professionals were keen to promote a case for security to be seen as a business enhancing service rather than merely asset protection. Thus statements were included in the targeted business survey focused on the collection, calculation and communication of the value of security.

4.57 Findings from the targeted business survey reveal that over a half of respondents (55 per cent/n=59) agreed that security shows measurable financial benefits and that it is important for organisations to collect data in order to identify how security adds value to a company (56 per cent/n=58).

4.58 However in reality, only 4 in 10 reported that their organisation collected metrics or data which could be used to achieve this.

4.59 Furthermore only 17 per cent (n=17) of respondents felt that it was easy to calculate or measure the value of security whilst over 6 in 10 felt it was difficult. Interestingly, of the 40 per cent (n=41) of respondents who reported that their organisation did not collect data to measure the value of security, over three quarters (n=32) noted that it was difficult to calculate the value that security could generate.

4.60 The vast majority (87 per cent/n=91) of the targeted business survey considered it important to communicate the benefits and advantages of security within an organisation.

Summary

4.61 The general consensus amongst the IoD respondents was that electronic/internet security contributed more value to a business than other aspects of security. For instance internet and computer security was perceived as adding greater value to meeting the objectives of an organisation and delivering greater value for money than personnel and physical security. Similarly electronic security precautions (including firewalls and virtual/private networks) were considered to generate the greatest competitive advantage in relation to five other aspects of security.

4.62 In comparison, aspects of security which fall under the umbrella term physical security (alarm contractors, CCTV monitoring, security guards, fences, gates and locks) were perceived as more of a cost without sufficient benefit than a source of competitive advantage. This highlights the need for the security industry to raise awareness of the value that physical security can contribute to organisations.

4.63 Furthermore it is of concern that organisations did not view 'having a defined security policy communicated to all staff' as generating more of a competitive advantage and instead rated it only fractionally above a neutral response. This is clearly another area which the security industry should address.

4.64 The majority of targeted business survey respondents clearly considered the security function to add value to an organisation in some manner. Almost three quarters did not think security was an unwelcome burden on the bottom line whilst two thirds agreed that security was a value adding function. Nevertheless most did not perceive security as adding value through generating a profit.

4.65 At least half of the targeted business survey respondents agreed that security shows measurable financial benefits and that it is important for organisations to collect data in order to identify how security adds value to a company. Overall however, only 4 in 10 of the respondents stated that their organisation collected such data. Furthermore the majority of respondents were of the opinion that it was not easy to calculate or measure the value of security.

4.66 It is clear that there is much that the security industry could do to assist organisations in the future collection of this extremely valuable information. Strategies to address this will undoubtedly cover data collection, storage and analysis methods.

The effectiveness of security

4.67 Questions were included in the IoD survey to examine organisational views of the effectiveness of security. Organisations were first asked whether they review or evaluative their security.

4.68 All 500 IoD respondents were asked whether they had conducted any type of security review for their organisation in the last two years. Multiple responses were possible as some organisations had conducted more than one review. A break down of the responses is presented in Table 19 below.

Table 19: Security reviews conducted within the last two years

Agency	Total[47]
Internal security personnel	174
External security consultants/ contractors	164
Police	100
Total	**438**

4.69 Where they had taken place, security reviews were almost as likely to have been conducted in-house as by external security consultants/contractors. Reviews by the police were less common.

4.70 Respondents were asked to rate the effectiveness of the security reviews they had received on a scale of one to seven. A score of seven inferred 'most effective' and one 'non-effective.' The mean scores for these responses are presented in Table 20 below.

[47] In total, 480 responses were received. For ease of analysis and interpretation, only those agencies with a substantial response rate have been included.

Table 20: The effectiveness of security reviews

Agency	Mean	Standard Deviation	Number
Internal security personnel	5.6	1.0	165
External security consultants/ contractors	5.3	1.3	158
The Police	5.0	1.7	96

4.71 Although each of the agencies was rated as providing an above average security review (as can be seen in Table 20), it is of note that internal security personnel received a highly consistent average score of 5.6. Moreover 85 per cent of respondents awarded internal security personnel a score of five, six or seven. One school of thought is that it is inevitable organisations would rank their own security the highest, and some reviewers of this fining have suggested in personal communication it is surprising it is not higher and that by contrast; the external security reviews have fared well.

4.72 A more detailed analysis of the IoD respondents by industry sector revealed that the reviews completed by internal security personnel were held in particularly high regard by the financial services industry who awarded the in-house reviews an average of 6.1 (n=33).

4.73 In comparison to internal security personnel, external security consultants/contractors and the police received a slightly lower average score, although the respective means (5.3 and 5.0) suggest that on a seven point scale the reviews they have completed were viewed as above adequate, without being outstanding. It is of particular note that the industry sector classified as 'other' which includes construction, mining and transport rate the security reviews of both external security consultants and the police considerably (one whole point) lower than all industry sectors taken as a whole.

4.74 Respondents were also asked to rate a list of factors, again on a scale of one to seven, to establish which factors contribute towards security being viewed as effective. A rating of seven denoted that the factor had a positive impact on security effectiveness whereas a score of one denoted a negative view of the factor contributing towards security being viewed as effective. Tables 21 and 22 summarise the findings.

Table 21: The impact of factors on whether security was viewed as effective

Security factors	Mean	Standard Deviation	Number
Attitude of the head of the company	6.1	1.3	487
Culture within the company	5.5	1.6	477
Security technology	4.8	1.7	479
Rules and regulations	4.5	1.6	482
Measuring the number and type of security incidents	4.2	1.8	465
Security guards	2.6	1.8	409

Table 22: The impact of factors on whether security was viewed as effective

Security factors	Scores of 5, 6 or 7 (positive influence)	Scores of 1, 2 or 3 (negative influence)
Attitude of the head of the company	87%	4%
Culture within the company	75%	10%
Security technology	58%	22%
Rules and regulations	54%	25%
Measuring the number and type of security incidents	42%	34%
Security guards	15%	57%

4.75 Results from Tables 21 and 22 illustrate that attitudes and culture were viewed as critical to the success of security within the organisations sampled. The attitude of the head of the company was rated as the most influential factor receiving an average score of 6.1. Eighty-seven per cent of respondents awarded this factor a score of five, six or seven. The influence of the head of the company was even more marked in the distribution and hotelier industries, with an average score of 6.4 (n=25) being awarded by each.

4.76 Culture within the company received the second highest score (5.5) with 75 per cent of respondents awarding this factor a score of five, six or seven. Culture within the company was scored highest within the industry sector classified as ‘other’ which includes construction, mining and transport industries (5.9/n=70).

4.77 Interestingly, more tangible factors such as security technology (4.8), rules and regulations (4.5), incident monitoring (4.2) and security guards (2.6) received lower than average scores in relation to the less tangible contributing factors, namely attitude and culture. Again, and mirroring earlier comments, it is critical that the security industry as a whole address this issue and demonstrate the benefits that may accrue from deploying these more tangible measures.

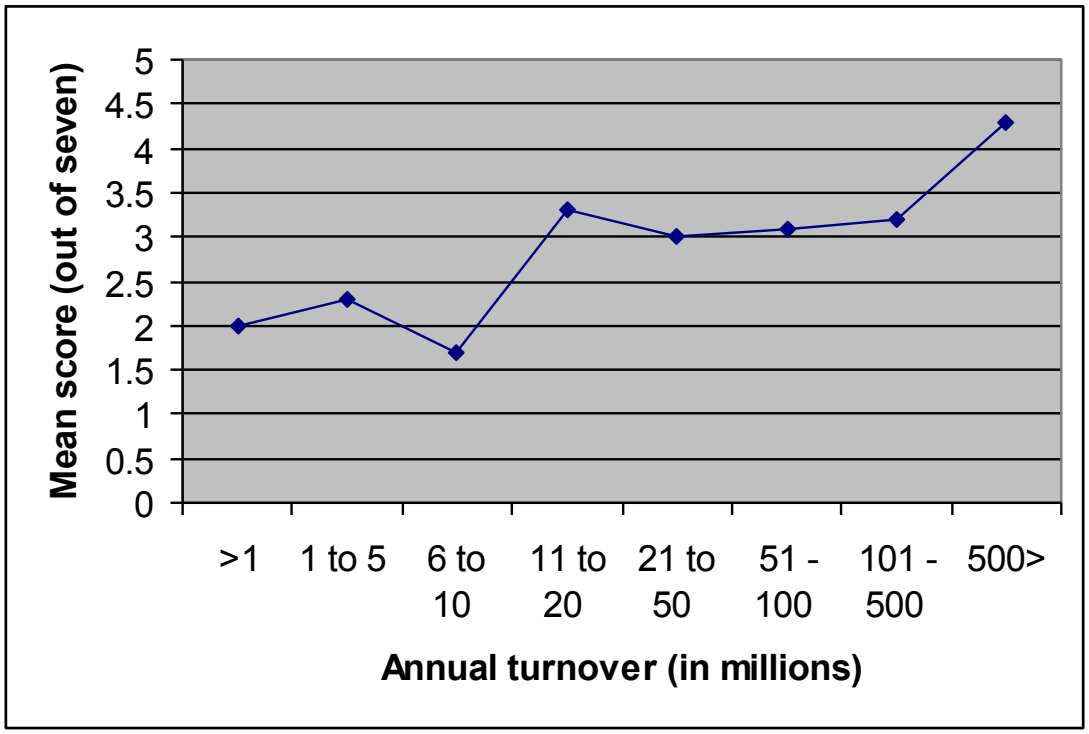
4.78 It is particularly striking that security guards received an average score of 2.6 and are not perceived to contribute to the perception of security being effective in anything other than a negative way. This may be inevitable given the role that many see guarding companies fulfil. Further analysis revealed that industry sectors such as government, education, health and personnel services rate security guards more negatively with an average score of just 2.1 (n=56). This finding seems all the more remarkable given the high number of incidents teaching and health professionals face on a day to day basis[48]. Conversely, financial services (as an industry) rated security guards a whole point higher averaging 3.1. Financial services higher regard for security guarding in comparison to other industry sectors seemingly reflects their higher regard for security as a whole, and is consistent with earlier findings.

4.79 A second interesting finding in relation to security guards is that companies with a higher annual turnover assessed the impact of security guards in a more positive light than those with a lower annual turnover[49]. This trend raised incrementally as can be seen in figure 3 below.

[48] Upson, A. (2004) *Violence at work: Findings from the 2002/2003 British Crime Survey*, Home Office: London

[49] Unfortunately, the format of the data received by Perpetuity did not permit cross-tabulations. Here it would have been useful to cross-tab industry sector by annual turnover in order to assess whether the financial services sector might make up the bulk of the companies with large turnovers – meaning that it is not necessarily the annual turnover that is linked to the perception of security guards, but instead the type of industry. However, the data that was received suggests that companies with proportionately larger annual turnover were not over-represented by the financial sector.

Figure 3: The impact of security guards on the security of an organisation



4.80 This finding again supports an emerging trend across the data, which suggests that larger companies rate security more positively than smaller ones. Given that the questions were focussed on perceptions of security, quite independent of whether an organisation was using security, this may be viewed as encouraging. if, as seems the case (at least with regards to security officers)

Summary

4.81 Where security reviews have been completed (whether by internal security personnel, external security consultants or the police) they were generally viewed as effective.

4.82 The attitudes of the head of the company and the type of organisational culture are viewed as critical to the success of security. Meanwhile, more tangible factors such as security technology, rules and regulations, incident monitoring and security guards were perceived as less important. This finding is consistent with the view that 'good security' is principally about having strong leadership and a healthy culture which views security as important and a shared responsibility. Security measures are a way of assisting and supporting other organisational/management processes.

Organisational perspectives on security staff

4.83 The IoD survey generally focused upon security at a strategic level, whereas the targeted business survey also explored organisations' perceptions of the skills sets required by internal security personnel and the performance and management of external security contractors. The following section examines organisations' views of internal security staff.

Internal security personnel

4.84 Statements were included in the targeted business survey focusing on respondents' perceptions of internal security personnel. These statements and the respondents' answers are shown in Table 23 below. The table indicates that the majority of respondents 'agreed' or 'strongly 'agreed' that security staff are experts in their field. Furthermore over one third reported that senior security staff are widely respected within their organisation. This is clearly a positive viewpoint.

4.85 The survey findings indicate that senior security personnel are respected and considered experts in their own field by some respondents, however only a small minority felt that they were considered as business leaders. Yet, just over a third of the respondents did not think that senior security personnel lacked business acumen.

4.86 Unsurprisingly, the majority of respondents agreed that the closer the Head of Security is to the Board, the higher the status of the security function within an organisation.

Table 23: Respondents' perceptions of internal security staff

Statement	Strongly Agree and Agree	Strongly Disagree and Disagree	Neither Agree or Disagree	Don't Know
Senior security staff are viewed as business leaders	9% (n=9)	50% (n=53)	32% (n=34)	9% (n=10)
Security staff are experts in their field	65% (n=69)	3% (n=3)	26% (n=27)	6% (n=6)
Senior security staff lack business acumen	15% (n=16)	38% (n=40)	37% (n=39)	10% (n=11)
Senior security staff are widely respected in the organisation	38% (n=40)	13% (n=14)	36% (n=38)	13% (n=13)
The closer the Head of Security is to the board, the higher the status of the security function is within an organisation	69% (n=73)	4% (n=4)	21% (n=22)	6% (n=7)

4.87 A further three of the statements in the targeted business survey focused on the desired background and skills of senior security staff. These statements and the respondents' answers are shown in Table 24 below. As expected, views were extremely varied.

4.88 Table 24 shows that 41 per cent of respondents 'agreed' or 'strongly agreed' that it was important for senior security personnel to have good military or law enforcement backgrounds. More than a quarter felt that security staff were best recruited from these environments.

4.89 Almost half of the respondents disagreed that it was more important for senior security staff to have business skills rather than security skills whilst 17 per cent considered it was. This finding is likely to have been influenced by the fact that only a small number of respondents viewed senior security personnel as business leaders.

Table 24: The background and skills of senior security personnel

Statement	Strongly Agree and Agree	Strongly Disagree and Disagree	Neither Agree or Disagree	Don't Know
It is important that senior security staff have good military/ law enforcement backgrounds	41% (n=44)	12% (n=13)	39% (n=41)	8% (n=8)
Senior security staff are best recruited from military/law enforcement backgrounds	29% (n=30)	13% (n=14)	47% (n=50)	11% (n=12)
It is more important that senior security staff have business skills than security skills	17% (n=18)	49% (n=52)	28% (n=30)	6% (n=6)

External security contractors/providers

4.90 In addition to exploring perceptions of internal security staff the targeted business survey also included a number of statements designed to elicit respondents' views on security contractors, guarding companies and technology providers, particularly on the quality of services they provide. The responses are shown in Tables 25 and 26 below.

4.91 Table 25 shows that there were mixed views of security contractors, and from a third to a half 'neither agreed or disagreed' with the statements.

4.92 The most salient points emerging from Table 25 are as follows:

- Only a minority of respondents thought that security contractors generally exceed expectations. Just over a quarter disagreed with this statement

- A small number of respondents agreed that security contractors are unreliable and rarely meet their key performance indicators.

- The largest proportion of respondents did not have a firm opinion as to whether 'of all the contractors our organisation has, 'security' is the best.'

With regards to the management of security contractors:

- Only forty-four per cent of respondents considered their organisation to be good at managing security contractors.

- Half of the respondents reported that their organisation paid security contractors enough to deliver a good service. A small minority disagreed.

Table 25: Respondents' perceptions of security contractors

Statement	Strongly Agree and Agree	Strongly Disagree and Disagree	Neither Agree or Disagree	Don't Know
Security contractors generally exceed our expectations	9% (n=9)	26% (n=26)	47% (n=46)	18% (n=18)
Security contractors are generally unreliable	9% (n=9)	43% (n=43)	31% (n=31)	17% (n=17)
Security contractors rarely meet their key performance indicators	12% (n=12)	30% (n=30)	38% (n=37)	20% (n=20)
Of all the contractors our organisation has, 'security' are the best	18% (n=18)	16% (n=16)	45% (n=44)	21% (n=20)
Our organisation pays security contractors enough to deliver a good service	50% (n=49)	5% (n=5)	30% (n=29)	15% (n=15)
Our organisation is good at managing security contractors	44% (n=43)	7% (n=7)	36% (n=35)	13% (n=13)

4.93 Table 26 suggests that almost half of the respondents have a positive perception of security guard companies. Forty-four per cent (n=44) did not agree that they generally perform badly in comparison to a minority who thought they did (9 per cent). Furthermore, 36% of respondents disagreed that security guard companies are generally poorly managed compared to 16% of respondents who thought they were. .

Table 26: Respondents' perceptions of security guard companies and technology providers

Statement	Strongly Agree and Agree	Strongly Disagree and Disagree	Neither Agree or Disagree	Don't Know
Security guard companies generally perform badly	9% (n=9)	44% (n=44)	30% (n=30)	17% (n=17)
Security guard companies are generally poorly managed	16% (n=16)	36% (n=36)	27% (n=26)	21% (n=21)
Security technology providers generally perform badly	5% (n=5)	44% (n=44)	33% (n=33)	18% (n=18)

Summary

4.94 On the whole, internal security personnel were respected and considered experts in their field. Senior security personnel were not viewed as business leaders, however (and this is an important point), most considered them to have business acumen.

4.95 The status of the security function within an organisation is in part dependent upon the relationship between the Head of Security and the Board. The majority of respondents reported that the closer the Head of Security is to the Board, the higher the status of the security function.

4.96 There were varied views on the preferred background of senior personnel. Sometimes military/law enforcement backgrounds were preferred. Almost half of the respondents did not agree that it was more important for senior security staff to have business skills rather than security skills.

4.97 External security contractors were certainly not viewed as unreliable, and on the whole organisations were fairly positive about contractors. However, only a small minority of respondents thought that security contractors generally exceed expectations.

4.98 Half of the respondents reported that they believed they pay external security contractors enough to deliver a good service whilst just short of that number reported that they were good at managing security contractors.

Section Summary

4.99 Results from this section highlight a cluster of overarching findings which overall, suggest that the security industry has created significant platforms to build upon but could improve.

Positives:

4.100 Positively, the majority of respondents perceived security as important to the success of their organisation, rather than as a poor relation in comparison to other functions. Respondents also deemed security as significant to all core organisational activities, reporting that it should be integrated into all aspects of a business. In particular, financial services seem to recognise the benefit of security more than any other industry sector, a point which is worthy of future research. The targeted business survey revealed that senior security personnel were respected and considered experts in their fields.

4.101 In regard to adding value, (specifically through facilitating the meeting of objectives and by demonstrating cost effectiveness) internet and computer related securities were given strong emphasis. Similarly, electronic security precautions (including firewalls and virtual/private networks) were awarded the highest score by IoD respondents with reference to generating a competitive advantage. The majority of targeted business survey respondents disagreed that security was a cost on the bottom line

Negatives:

4.102 Physical security did not perform as positively. Onsite security guards, CCTV monitoring, alarm contractors and physical security (fences, ages and locks) were considered more of a cost without sufficient benefit than a competitive advantage. Clearly, there is a real need for the security industry to respond, explaining and disseminating the value that physical security measures can provide organisations, or, perhaps focussing on how these measures can be important, as part of a strategy in security adding value to an organisation.

4.103 A crucial issue going forward is demonstrating the value that security can add to organisations. Over half of the targeted business survey respondents agreed that security demonstrates measurable financial benefits and that it is important for organisations to collect data in order to identify how security adds value to a company. However, only a quarter of the respondents stated that their organisation collected such data with the majority of the opinion that it was not easy to calculate or measure the value of security. Whilst respondents appreciate the value that security could provide, they stopped short of claiming that it was a profit making function.

Critical success factors:

4.104 The attitudes of the head of the company and organisational culture were viewed as critical to the success of security. Moreover, it was reported that the status of the security function within an organisation is in part dependent upon the relationship of the Head of the Security to the Board.

Section 5. Directors' Views of Security

Other functions in the company are integral to the business, security is at some level a choice. It is always cast in the light we would all love not to have it.

Board Director

It underplays itself as a function ... in only some cases is it well done because it has become a hindrance to people doing their jobs rather than a support. It definitely needn't be like that. A lot of senior executives think they can solve security needs with technologies and this has a role to play, but this can become heavily administrative and only as good as the people who can operate it. Often the technology does not fully work, and you have to be prepared to have intrusive things, like spot checks, signing registers. And this needs organising and implementing. Technology is OK, but it is only a part of the answer, you always need people and you always need to manage them.

Board Director

The art of good security is that it is always on at some level. I look at it like a light switch, now that is always on or off, never in between. Well security is more of a dimmer switch, one that is always on and so we need to engage with the board all the time because it is on all the time, but sometimes it is turned higher and sometimes lower.

Board Director

5.1 This section is based on information gathered from nine in-depth interviews with Directors of companies. None were security specialists, but all had responsibility for the security function (or a major part of it) at Board level and the Head of Security reported directly to them. The interviews provided an opportunity to tease out important issues regarding the way security is managed and senior attitudes towards it. Clearly, the data here should not be interpreted as being representative of all organisations but it does provide a foundation for further explorations of senior staff perceptions of security.

5.2 The key issues that are discussed are as follows:

- The role of the security function in organisations
- Perceptions of security personnel
- What makes security effective?

- Demonstrating the value of security

The role of the security function

5.3 There has been some debate about the appropriateness of the word 'security' to describe the range of activities it incorporates. Directors were asked their opinions, and there were some bold views:

> *I think they should be called what they are, not bullshit titles like profit protection, call the thing what it is, security.*
>
> *My personal view, avoid bullocks. Personnel is personnel, law is law, security is security and make sure it does what it says on the tin.*
>
> *It is what they do that counts not what they are called.*
>
> *It does matter, and call it security. I am pragmatic and it is all about protection of assets, and that is security.*

Some argued that it did not make a difference, while it was also argued that there were better words to describe the broad range of activities that involved securing an organisation's assets. The retail director, argued the case for 'profit protection', while one interviewee, who favoured using 'security' admitted the following:

> *Some people have a mindset about security, such as checking your pass as you come into the building, but there is also a strategic element, and our business warrants that. We had an anti illicit trade problem, we needed to manage this in different ways, public affairs and engagers explaining to politicians what the problem is, and people to make sure nothing is taken. We also need a group of professionals who can deal with problem. We have a team targeting the crooks, very focused but specialist and critically important for us, but to be honest I am still not sure where it should report. Recognising a business problem cannot always be done by security professional, they don't always have the skill-sets.*

5.4 The issue here was that security impacts on all aspects of the organisation. During the interview Directors were specifically asked about their expectations of the security function and their responses revealed that they viewed security as important in a wide-range of roles. Typically they saw security in terms of its ability to help manage risks, with the nature of risks varying with the function of the organisation. It was widely accepted that security threats cannot be eliminated and so the role of security needs to be a combination of

assessing and monitoring risks with good intelligence, and the ability to react speedily if incidents occur. Some typical comments included:

> *We operate in risky parts of the world, e.g. ... in Africa and Asia and Russia and Columbia and Venezuela, and so our approach is to accept we cannot eliminate risk but we can manage it.*
>
> *To proactively identify security weaknesses, and actions to address these. To reactively provide support to management in the event of a breech.*
>
> *In my view it is to provide a secure environment in which our business can be conducted efficiently and responsibly.*
>
> *In strategic terms, I am expecting the security function to protect the interests of individual, information and estate. So people, information and physical security are the key areas.*
>
> *Expectations are really around not having any surprises, and recognising that no approach can give 100% guarantees that you won't get a security event but we need to avoid it as best we can, we need a structured approach to security.*

5.5 More extended answers revealed a variety of ways of achieving this. One Director, who had spent a considerable amount of time thinking about the role of security, underlined the importance of bringing all security related functions under one umbrella:

> *We have co-mingled physical security, cyber security, emergency response and Business Continuity Planning. Most threats come from physical and cyber channels and so we believe that we should keep these functionalities together, they come from different tribal groupings, but terrorists think as one.*
>
> *This came from a review I did on five-year plans. I got the idea from the US secret service. It took three years to understand what this may look like. We had to do a lot a lot of work, but the teams now would not have it any other way and they learn from each other. So we work on intelligence led security. We are evolving rapidly and learning insights we did not get before.*
>
> *The function is not a big one, so it has to operate with few high grade people. This is more about an intelligence level and risk management... the Head of Businesses*

around the world now have only one conversation to have with one person about security, just one interface and they can plan accordingly.

5.6 Another Director underlined the role of security in getting the business to think through how they promote good security practice. The role is varied; on the one hand getting people to think about working safely, and on the other ensuring that all products (in this case, finance related ones), are security tested:

In group risk we have (an) oversight function, the job is to make sure the business is doing what it should be. In each of the businesses there is an embedded security function with people hopefully doing the right things, our job is to make sure they are. The key expectation is to enable our people to work safely. When people travel and for CEOs when at home; we must ensure that that they are safe. Also when we launch business around the world security is at the forefront of our minds.

5.7 A representative of one organisation that supplies systems to Governments and large public sector organisations noted that the problem of security, and the effectiveness of it, was largely dependent on whether it was regulated or not:

There is cross over between security and compliance ... So where we have to obey requirements we are quite good, but on areas where security is not a requirement then it will be more marginal.

5.8 This latter point will be discussed again later. What is clear is that while security remits are largely similar, the way they operate varies.

5.9 In another question, respondents were asked whether security was a core or a peripheral function. The overwhelming observation made by respondents was that it depended on the organisation in question and the risk environment in which it operated. It also depended on the type of security response that was in operation. One Director (of a multi-national which operated a range of businesses) argued the following:

Varies. For a mine in (South America) we have 6,000 staff, we have 1,000 security staff, so a sixth, and so security is fundamental to doing business, absolutely crucial. But take our (other) business in the UK, well I think it would be more peripheral. In diamonds and metals then security is huge, very core. Also where we operate, in (Asia) not a big deal, one of the safest places, but there the problem is corruption. So it depends on the type of business and the location.

It varies enormously. If you are dealing with MOD contracts its core, and others peripheral. And what is obvious is that IT security is visible, and often that is really the only security person there is, but it is not the only security role. Of course that means security can be seen as peripheral, it does matter. Where peripheral, either people have made an assessment that security risks are low, therefore they don't need to pay too much attention to it, or they have just ended up with unsatisfactory solutions. This can happen, it is an example of security not having a recognised contribution ... Security has got to be presented as making a contribution, we need a process of capturing the benefits, and the downside of not having security and this is an opportunity, definitely. But it is typically not done or not done very well.

5.10 Most argued that security was core, for example:

Core. Because we are licensed retail, and when you get drink and lots of people, security is of paramount importance. Our security team is incredibly highly valued. Because of the support and guidance they provide in sometimes nasty situations. I think most people would agree that security is core.

Core, you can see from our annual report that we are losing millions from retail theft; the opportunities for improving by a relatively small percentage can provide quite big savings.

Core ... in terms of policy security is seen as central to our business success. The Board understand that security is core because of the nature of the materials we deal with and the consequences of sabotage, and they include radio active materials and radio active waste. Also, we own and hold information relating to nuclear technology. And we have commercial assets and interests which need protecting.

5.11 It is suggested that security departments will find it easier to demonstrate that their role is core to business success where security threats are obvious. To explore this matter further, respondents were asked whether security was less or more important than other organisational functions. Some were clear that it is less important than other major organisational functions:

On balance I believe it is less important, I think if you compare security to HR or Finance the number of issues we deal with in these areas have a bigger impact. I think

having the best quality people and getting the books right are much likely to have a bigger impact.

It is difficult to argue security is more important, but it could be central. In every organisation the line manager is expected to be first line personnel manager and also the first line security officer because these central functions have been denuded, but they are too busy and few have the stamina and charisma. It undoubtedly could be more important; it is about the intellectual coherence of the argument. If you have a threat analysis and it is clear what are we concerned about and why, and we are looking at threats and how physical and IT and personnel all respond, then we have something we can relate to.

5.12 Some Directors noted that the role of security in their organisations was as important as major other functions because of the nature of their business, but they tended to add qualifications to this view:

Equally important and lower profile. For example, we give chief executives a quarterly report on credit risk, on security risk we would not report at all if performance is within appetite. There are hotspots, vetting for new staff, getting passes off of people who leave. We have a new product process that is vital, but more so in some countries and less so in the UK. We have a fraud team who manage security and they will look at those types of risks.

In our organisation, core because of the business. Security is boring and not match happens, maybe low level and crime and fraud, and for it to be strategic you must have strategic assets that need protecting.

5.13 A recurrent theme that emerged amongst Directors was the need for security to be coordinated with other departments and be aligned with the overall purpose of the organisation. For example:

Security should be treated as any other part of the organisation, but clearly as any other group of operators, they have different focus, so a marketer and finance does things in different ways from security, but they must all face the same direction as the Group.

5.14 Ensuring the alignment of approaches is perhaps best guided by an overarching security strategy. Yet, some security professionals have made the point that without a security strategy, the security function is rudderless.

5.15 It is perhaps surprising then that Directors of some leading organisations felt that they generally managed security well whilst at the same time admitting that they operated without a security strategy. They were asked whether they had a security strategy in place, the responses are outlined below:

> *No, but we should, we are discussing this. Historically we have been decentralised, and big business parts have managed these things by themselves and so we have been thinking about a more intrusive role for security within the separate business functions.*
>
> *No, we don't to be honest. We are too busy on a day to day business to be honest. Security are action oriented and they tend to go for the action end rather than think about things like, theory, concepts are an overarching strategy.*
>
> *No. It is just too difficult, but you are probably right we should have one. We have some paragraph on security but there is a gap between this and processes in practice. If you have a UK base company with only marginal assets outside, then it is much easier to have a one culture and one standard approach. But we are a big company and we don't work like that so a security culture and process that is standardised is difficult. Acquisitions also make it difficult. This is the complexity of the business, this is the difficulty we face in practice, lots of practices, lots of cultures.*

5.16 It is a striking finding that companies felt that they could operate without a strategy, a framework and reference point for action. Another respondent, a Director of multi-national company, conceded what they had was only partial: 'We do but only on the physical security side.' It is important to stress that while three of the nine admitted to not having a strategy, and one only a partial one, this cannot be generalised to companies generally.

5.17 Conversely, some Directors stated that their companies did have security strategies in place and furthermore that they were important. For example:

> *It is essential. We had changed our Head of security, and one of the first things I set him, I asked him to work up a position around security which ensured there was security alignment with group strategy. This is something I have been doing in other functions. The idea is that we have set of strategic objectives of the function identifying where we can add most to strategic benefit to corporate*

objectives. The people must been seen as professional at the heart of business.

We have a comprehensive one, it was one of the earliest ones we developed. We have a strategy around security which looks at physical security, information and people security, and these three strands look organisation wide.

Yes. If you were to look at our Group Security Strategy, and our security programme you would see that it dovetails into our broader security objectives. It is important to us in terms or our reputation, relations with Governments. We see security in the same set of areas as safety and environmental performance.

Perceptions of Security Personnel

5.18 As noted earlier in this report, there is a debate about whether the security function was best led by someone with security skills (typically related to a former police or military career) or business skills. Some security managers argued that without business skills one could not understand the organisation and as such would struggle to offer the type of security advice that could be most beneficial to the business. Conversely some argued that without security skills one could not optimise the best security advice for the organisation, with others arguing that they were both important to some extent. The views expressed by Directors were similar, with comparable reasons for these views being offered.

5.19 Those who argued that business skills were the most important argued that security was an aspect of risk and this guided their choice of response:

I think to be honest you do need to have someone who is business savvy. What we found is that we need people who help us understand and manage risk. One of the things that security has to deal with is doing business in difficult parts of the world, we have to operate there and we need someone who is business savvy, this must be a competence. There is no point in them saying you cannot go here because it is risky, we have to go there and they have to help us. The consultants we use help us understand risk. Who we appoint varies, in South America we have someone who can establish relationships with the military, that is vital, we actually need the army to help us. I am not trying to be smart here but we have tended to pick someone with the right attitude for the right job. Usually we have someone to

whom they report who does the business interpretation if we feel they cannot do that themselves.

Business skills, because security is no more than another type of risk and too many typical security people can't contribute to a team because they lack the knowledge. I would never recruit a military person, or a policeman. We need broader commercial expertise and experience. Traditional security backgrounds are driven by compliance and regulation, not by risk assessment, risk management and performance and that is what we are about.

5.20 Conversely, some argued that security skills were the more essential principally because subject knowledge was essential for the task (although frequently the point was made that business skills have their place too):

My people are mainly domain specialists with a business brain. You cannot be in that space as a general purpose business manager without subject or domain knowledge. They have to come from that tribe otherwise they are not in that club. So security is more important.

If I could have one, I would probably go with security skills first and then teach business skills. I would want the professional understanding of security as a priority, that needs to be sorted first, building the business around knowing security has been dealt with is essential. I would then teach them business skills, that is the right way around.

Well I think you must have security skills or you will not be able to offer your security colleagues a set of options. But a security manager must understand the business. They must have a security background, they must understand the latest security solutions, but I would expect him to be capable of learning business drivers and business needs and our business culture.

5.21 The majority argued that both were essential, and that a good Head of Security could not operate without both sets of knowledge:

Both. One of my objectives for the current head, is changing direction of security to tackle this very point. We do have a clear strategy for the whole business, I am strongly of the view that everyone must align functional strategy with group strategy and this includes security. We are all trying to hit the target of each group. So you need people at all levels and especially senior people

who have both. Our recruitment of security professionals follows a traditional line, military or security professional from the police, or intelligence corps, because they retire young. But we have been moving towards those who are younger. I probably should not speak about age but it is important, and anyway grow them as managers so they are more business focused.

They need to have both, they must have expertise and be aware of the business, on this question I want to cheat and say 'both'. We do tend to go for police or especially military, they are uncompromising they will tell it as it is. They have no fear of being transparent. I think this is an advantage, in some ways business people know how to work the business, but those with a military background just get to the point and expose the risk and their favoured solution. It is important that they are good at supporting the business, and they have to acquire business skills. But they come from the background that we will be dealing with in a crisis and that is very beneficial for all parties, including the police. Indeed, they have told me this.

Both important, relating to business and security are both important. As you get more senior the balance changes so that business skills become more important, but you need the right technical background. To be able to explain security issues to senior people so they get it is crucial. I was quite surprised how often I had to have several conversations to get senior security people to explain things to me as a non security specialist. I chose someone who was also good at communicating.

Both are essential. It is interesting, our head joined 30 months ago, we never had a person doing the same thing before, the guy came from the police and there is no doubt that he has added more value as his knowledge of the business has increased, and as his knowledge of the security in sector has improved. Our operational heads, same again. We generally look for people who have sector experience so there is less relevance if they come from airport security, he needs to understand retail. We need security and retail knowledge. If you asked me about lawyers, I would say the same. There are those who know about law and there are those who have worked commercially and those who have worked in retail and they are the best for us.

5.22 One respondent admitted that his company had the wrong person in charge of security. The individual does not have a security background;

unfortunately this person also lacks business skills. He described the problem as such:

> *We have someone in security, we get pissed off with her because she is former manager, perfectly competent and good at process, and grand for keeping up records but not the person to be interface with business units. The problem is because of her approach security is seen as an impediment to business and so people distance themselves from it. Modern security needs to be about risk management, what is threat, what are risks? She is someone who is comfortable in her role, but security is not seen as the glamorous end of corporate life, it can be similar to training and human resources, you sometimes get loyal but not overly dynamic people in there and this does not help the perception of it within the organisation. In IT everyone wants the latest gadget, but monitoring these is a tedious process, access controls and all that. And senior management have to set examples, and they often have not brought in to the security needs and security strategy and so when they don't follow it all falls apart then.*

5.23 The value of skill sets of security personnel were tackled in another way. Interviewees were asked whether they felt that a security specialist could ever be on the Board or appointed as a Chief Executive Officer.

5.24 The common view was that a security expert's background generally precluded them from being a credible candidate for CEO:

> *No, I have never seen one that could reach that level. There is not the ability there. Also there is not that route.*
>
> *No, they come from too narrow a perspective. As I said earlier they are uncompromising and that comes from a different background, a police or military one, that is fit for purpose, fit for being in a security role, but not an overall business role.*
>
> *I don't know of any cases like that. And why do they want that? But unlikely, they have not got the breadth of business knowledge and having credibility of the business would be important. Most are on second careers and they like their work. In the main there are more members of a function than of a firm.*
>
> *Unlikely, because it is too narrow a function. They may have advisors to the Board but not more than that.*

In this massive organisation the skill set required is so broad I just don't think security gives broad enough access to the way the business is run.

5.25 It was also noted that the way organisation's work made it unlikely that a security expert would ever be in contention, as one interviewee noted:

It depends on the individual, but in most organisations that would require a change of mind sets amongst, for example, nomination committees. They have a tendency to go to finance and marketers, they could, but without the right profile and right business values it is difficult for them to be have the profile and show they can deliver at the high level.

5.26 Another respondent stated that it would only be possible for security personnel to reach Board level in a security company. Indeed, the representative from the public security organisation did feel it was possible.

5.27 Generally, a career in security is not seen as providing the necessary skill sets for Board membership. The role of the security function is also seen as lacking the necessary corporate weighting to get the department, or its head, noticed. As one respondent summed up:

Security is up there with corporate social responsibility, at least potentially it is, but the security world has not presented itself like that.

What makes security effective?

5.28 It is clear that the role of security varies across organisations. Consequently any discussion surrounding effectiveness needs to take this into account. Establishing the extent to which security is built into the objectives of the Board is one method of assessing how security is perceived.

5.29 Of the nine interviewees, only three said that security was explicitly built into the objectives of some Directors. Others argued that it was not necessary to build security into Board members objectives. Typical comments included:

No. Probably not, I think in our business you need to be cognisant of it, but probably not more. There are a whole lot of things that are threshold things that enable the organisation to function, finance for example. Security is one of those things that Directors assume we have processes in place for, and they are assured by audits,

and so that is why it does not get on the radar. We only have four or five key objectives so there are usually more important things.

Not explicitly, but implicitly, if you don't have a secure premises then you cannot grow your customer base, so it is an input rather than an output. It is not really necessary, unless there were lots of incidents or things were going wrong, then it would be different.

Not explicitly. We have four Directors and a Director General and security is not a specific objective, it is explicit. We have regular briefings. Our Chair gets involved personally.

5.30 The three respondents who stated that security is explicitly built into Board objectives revealed that it was specifically written into their own objectives. For example:

Yes it is, the head of security reports to me, I have a broad objective relating to security ensuring that we have (an) integrated security function engaged with business, and contributes value, and carves out a value adding role, so it is there as a broad objective. The retail store director has a focus on retail security.

5.31 The means by which security was governed varied, and setting security objectives was not viewed as necessary for the Board. Furthermore, there was a general sense amongst the interviewees that their own arrangements were satisfactory in this regard. These findings merit further analysis in future studies.

5.32 The interviews demonstrate that the effectiveness of security is not generally assessed through Board objectives. So, how was effectiveness judged? Looking at the comments made it is clear that not everyone had a system for judging the effectiveness of their security function:

I don't know that we do, it is a good question. This is top of the head, to be honest, because nothing happens. A good security function is one you don't have cause to talk to or worry about.

5.33 Another noted:

I guess the key way is no surprises.

5.34 Others however, had fairly well developed systems, and fairly straight forward measures:

The profit protection people are measured by reference to shrink in stores. We think this is a significant issue and this is focused.

One way of measuring security in the supply chain is measuring seizures and we have mechanisms for doing that.

5.35 A number of the respondents reported that it is difficult to effectively measure the success of security:

... the absence of incidents is no indicator that security is successful. If we don't get an anti nuclear incursion it does not mean security is successful, there just may not have been one, they are not that frequent after all.

5.36 Data collection is also problematic for a variety of reasons. One respondent noted that:

…around information we make assumptions. We may find we have to play the percentage game

5.37 because of a lack of good data. Another said that his company had arranged for all its businesses around the world to deal with one centrally located security team providing a focal point for information and advice. I It was felt that this would increase the flow of information about threats and potential threats boosting recording and opportunities for assessment.

5.38 One Director noted that when an organisation is focused on sales it can sometimes be difficult to persuade colleagues of the need to be security aware. This includes appreciating the need to collect data and then actually doing so:

I knew nothing about security 9 months ago, but I have learnt security is a different risk. Take say credit risk people, now they can play down credit risk because they are targeted on profitability. So they manage it well, but they may do it by being deliberately slow in reporting. But in the case of security is in no one's interest to cheat the system, so once you explain why you are concerned about security you get support. The problem is senior people, they cannot see immediate benefits in pounds and pence to investing in security now but they can see a cost, so that can be more difficult. At least in security they can see it is in their own interest to change.

5.39 Interviewees were asked whether they collected metrics, the question was linked to whether they used them to show they add value to their organisation. Interestingly, two out of the nine interviewees admitted

that they did not collect metrics, and one did report this to be a weakness:

> *No, not that I have ever seen. I suspect they are missing a trick, they could do something here to change perceptions but I am not aware this is on their radar.*

5.40 Most respondents reported that their organisation did use metrics to some extent. However, the value of this assessment was limited by the type of data collected and a lack of comprehensive storage systems. . Qualitative feedback was often seen as equal to quantitative work in the assessment of security functions; in fact in some cases it was considered to be more useful. Some examples of answers provided in response to data/metrics questioning are included below:

> *I can see the argument, but it is old fashioned ... Let me give you an example, in a given city in the Far East a bomb goes off, luckily security were advised and they evacuated and everyone was OK. Now how can you put a value on that? I think you can be overly clinical and I am not sure where it gets you to. I do benchmark against others in conversation with others in a closed shop.*

> *Information security has some metrics, we do report on security incidents ... but it is difficult to come up with specific metrics. We have details of seizures we have made but we are not judged on it ... what I mean is failing to hit target is not the security guy's failing.*

5.41 Two respondents reported that their companies collected metrics, but questioned whether they added value. In both cases it was felt that metrics help reduce risk but do not add value. For example:

> *We have metrics to show where we are against the risk profile and not to add value.*

5.42 Others did use metrics, sometimes driven by compliance requirements:

> *Yes. In every area of security. Most security is based on compliance, if you have a programme of security which is risk management and performance based then metrics are a part of that. We need to ask, what do we need to achieve and what is the gap? We have killer questions around metrics so that if you had to go to a major enquiry or a court you would want an answer available to the killer question. For example, you may need to know who has clearances to act and be in certain areas, are we aware of any anyone who has access to areas without clearance? Our answer can never be 'we don't know'. These questions forced us to think about the integration*

of data, for example on vetting and access to the different parts of the organisation ... we don't have to run metrics for the regulator, we just prefer to do that this way. People are not motivated by compliance rules, they are motivated by the risks and doing the right things about them.

5.43 Most of the interviewees' organisations appear to adopt a mixture of qualitative and quantitative measures to monitor and evaluation security functions. Examples of the former include the perceptions of people in the organisation towards security, or how the organisation is judged by outsiders including the police. For example:

I do assess the attitude to security in the business, I do this by speaking to managers and getting their feedback, I can questions them and you can tell a lot by their reaction. In a different way we can assess how well we respond to a security incident.

We also monitor serious business incidents ourselves ... We also learn from the police. We can tell a lot by whether we are invited to participate in events with the police. And we are. We had a spate of burglaries and we were commended by the police for our response.

The problem with measuring security is that it is difficult to measure until it goes wrong. For this reason a lot of measurement is qualitative. When we had a spate of burglaries it was our own data that spotted this, and we told the police and then they pursued their investigations. There are lots of ways of measuring security.

5.44 Setting measurable objectives to monitor performance is a key factor alongside the qualitative and quantitative measures already noted. Once again though, it was emphasised that it is key that staff understand that security should be integral to all processes and of all staff have a responsibility for it. For example:

In my view security is integral to everything. It is not a group on the edge of organisation, it is part of the way we do business. What I am encouraging is raising the level of awareness about security. We are a high security organisation, and everyone has a responsibility and there is a cultural issue about embedding security in a culture. The key is to ensure that the people in the organisation have a responsibility for security. Security in our business is vital. You have to introduce a culture where everyone understands that they are part of a secure organisation and have responsibilities.

5.45 Similarly it was noted that events that are not in themselves security events can have major security implications. One representative from a multi-national company noted that

> *Asian Flu was about not the medical impacts but the impact of a breakdown of law and order*

5.46 Consequently, they had focused on their response on the possibility an outbreak could occur.

5.47 Others pointed out that in addition to staff, clients and the security function itself playing a part in judging success, the Board needs to ensure that it has properly assessed risks and made informed judgements in relation to the allocation of resources:

> *It (security) must contribute to the objectives of the organisation. We need to be a reasonable and prudent operator: if things go wrong at board level because we have under provided resources then they would say in a well run company we should have dealt with it in a better way. So the board must say this was OK.*

5.48 The results demonstrate that there are a variety of methods for measuring whether security is effective. They also showed that no single organisation had considered all the various ways. This is perhaps unsurprising given that there are no easy reference points, or a widely adopted code of practice. This evidence indicates that security can present judgements on its contribution in many different ways, and that opportunities do exist. However these are not commonly exploited.

Demonstrating the value of security

5.49 Respondents were asked whether they considered security to be a profit making function – a business enabler - or a cost on the bottom line. It emerged is that security has not always been a strategic consideration; one respondent noted, for example that:

> *Security is just a cost of doing business. I suspect this, because we have never thought about it*

5.50 For the most part security is viewed as a business enabler. The Director of one non profit making agency, which focuses on delivering security, noted that it was a very important business enabler:

> *It is a fundamental enabler. For the business I am in, for us to be successful we need to be confident the information we have is protected, the people we employ do not allow information to be passed around, so we*

cannot effectively ensure the right outcomes without a highly effective security culture, without that our business would be less effective. I see security as a fundamental part of what we do, essential, not a cost on the bottom line.

5.51 Two respondents pointed out that security can be described as a business enabler, in one case evidencing this view with the observation that the company would make major investments and not consider the security implications:

Not a profit centre. It is a business enabler. It is, if anything, closer to cost than to profit.

We would take major investments without reviewing security.

5.52 The most common response was that security is an enabler, in that without it the organisation would not be able to go about its normal business. Some typical comments included:

A business enabler, we are a licensed business and if we don't have security we would lose customers and ultimately licence. At the end of the day security is only part of it, you need business skills, you need to be good at the business you are in, but security enables us to do this better.

Enabler. Because if we did not have a security function we would be in a mess.

5.53 Others saw security as essential to doing business, but had not interpreted this in a positive light in the same way as the other respondents. One respondent felt that his organisation had not been sophisticated in its thinking on this issue:

I have not seen it being expressed as a profit enabler, it is a cost on the bottom line generally speaking. It is not a dead weight cost, at least not in the Defence industry, it is not wholly a negative. We are not clever enough to see security as a profit enabler. We will not win repeat business if we are not security conscious, so it clearly does add value. Hiring the wrong people costs a fortune so it must be possible but it is not something I have seen. I think in this company it is seen in latter way, as a cost. It is essentially a cost but not resented and not the first to be hit in a crisis like training or going to conferences. I think the difficulty is capturing benefits and putting values on them is quite difficult. I have not seen any work which brings that out clearly.

5.54 Some respondents doubted that security should be considered as profit generating. One noted that:

…my reaction, or initial reaction is that it would just make life complicated.

5.55 Another respondent felt that it was difficult to measure value and that such an exercise would generally be unhelpful:

We know what the costs are, we don't do a cost benefit but we would be trying to calculate what costs we have avoided, what threats we have avoided, which is difficult to prove and it is also difficult to price. For me I would not bother with a business case around it. The problem is proving the case, it is difficult to put a value on it. I come from a very pragmatic school and in my experience organisations put numbers on things but really, they should not bother, they can be useful sometimes to compare, but in others and security is a case, I doubt whether there is a useful measure.

5.56 Another commented:

It is not as crass as a cost to business, it is a cost of business. It is not a grudge purchase here. But it is never a profit making function, they would make a fake thing, that is just about playing shops and there are internal costs to do that sort of thing.

5.57 One interviewee did see security as potentially profit making. He noted that although the cost of running the security function was about £30 million annually, the. company could offset some of the costs by selling their security expertise. The problem was that this was not their core business and there were implications that the company was currently considering:

We cover our costs by using our people externally to make money. The way it works is this. The Governments and others need advice and help with specific programmes so we provide those and we do that at healthy consultancy rates and we make a profit. The thing that stops making it a profit centre is a problem because it is not our core business, and the core responsibility is to manage the core programme and we need to make this a priority ... As the business restructures we may think though how the experience we have gained could then help others. We do security awareness we could sell that. We are very large and we have large demand for services and we will look at reselling.

5.58 The retailer did feel that reducing shrink (a loss) was tantamount to improving profit, but admitted that the company's own internal structure meant that it would not always be interpreted in that way:

I think it is a profit making opportunity to the extent that it is more than just a cost on the bottom line. Shrink is a cost on business and the cost flows through to reduced profits .... we know how much our shrink is on a store by store basis and we have regional security managers, and we now have people responsible for shrink in store. At a central level it is far more difficult, it is more nebulous, improving overall protection. That has to be a bit of a finger in the air because there is no direct profit line that this person can be measured against. There is no specific target centrally referenced to a numerical target, that there is in the operational area.

5.59 The interview included questions about the benefits of security departments. Interestingly, the need to add value featured. For example:

I think that security is not central most of the time. I think they could show how they add value and we might re-evaluate it.

Some organisations support security, but some don't. There is a tendency looking at security, or HR or Estates, or other support units and they tend to be pigeon holed, and they don't understand that security is always a driver, and if things go wrong it will damage us badly. That is not always case. But we need to educate people about the dangers.

5.60 The importance of a security strategy and the role of a security culture was once again emphasised:

... the key is to look at where the organisational strategy is taking you, where the risk profile identifies areas of improvement and making sure security can cover.

The main issue is how you implement a security culture across the company.

5.61 It is also interesting to note that there was an emphasis on recruiting the right people:

Then success of the function is very dependent on the quality of the people. We need to deal with police at a high level and so a relevant background in security really does help. They have tremendous confidence with people they deal with in our organisation. When we had the London bombings our security checklist was given out to other businesses. Now that is a good endorsement and a good sign as far as I am concerned, the police think we are getting it right.

5.62 It is encouraging for consistency that, when interviewees were asked what would need to change if security was to be accorded a higher status in organisations, similar issues emerged**.** There was a clear sense that high quality people are key to an improved perception of security:

I suspect on balance we probably have to have higher quality people, not retired policeman, and then they would have to show how they contribute, and by that I mean how they contribute at the higher levels. Companies see security in a narrow way, as getting to offices safely and preventing people nicking computers and when you think of it like this it is more police like. There is a tradition that if you need to stop nicking you need a policeman. The same is true of the security consultant, it is difficult to find one who has not worked in the secret service. Also, I suspect, security is not viewed as a proper profession and so you will not get graduates flooding to it, the security world has to change that to move forward.

But you also need people who can explain that threat and how worried we should be. So you need good and friendly security professionals at senior level who are able to communicate. I was horrified that senior people in security who I interviewed were not good at the business side of things.

Hire smart people, and have a seat at the table so that they are recognised as value adds. Hire the very best,

people who are recognized for their security knowledge. You need good people at different levels, not just leaders.

5.63 The need to obtain senior level support for the security function and what it is trying to achieve was highlighted by others:

> *Probably the buy in of the chief executive. For us we live and die by security, so there is no real problem.*
>
> *If the reporting line went to the chief executive it would raise (the) status.*

5.64 It was also noted that security departments need to raise awareness of the tasks they perform and how these positively impact on core business. These ideas must be expressed in terms that the broader business will understand. One respondent nicely summed up the range of issues viewed as significant here:

> *I think it is recognition by board of Directors that in applying Turnbull and the Combined Code that when they think of managing risk they don't just think about financial risk, but also about security risks. Security metrics and performance need to be considered. Security need sot see itself as a risk. They need to approach this from a risk management perspective, try and avoid the risk managers being ex military and 45 and white and looking like they have a clip board in their hands, you cannot enamor yourself to a board this way, it is not about breaking rules it is about managing risk and measuring performance and do we all, the staff that is, in the company understand the threat and what are we all doing. It is about setting out what the business thinks are the perceived risks. Once you have developed design based threats then you can say what are the measures that need to be in place. That is what you need to discuss in business.*

Section summary

5.65 Most importantly, in terms of consistency of findings, a great deal of synergy has emerged across both the survey findings reported in the previous section and the data generated from interviews with directors of companies.

5.66 Interviewees viewed security as important in a wide range of roles particularly in terms of its ability to assess, monitor and help manage risks. However, clearly different companies have different security risks and so the day-to-day approaches to security differ. For this group of interviewees the importance of security varied with the risk environment

and this influenced whether it was viewed as core or peripheral. It was noted that security impacts on all aspects of the organisation and needs to be coordinated with other departments.

5.67 Perhaps the most alarming finding emerging from this section was the lack of emphasis placed on the importance of security strategies. Some interviewees felt that they managed security well despite not having a security strategy in place. Those organisations which did have a strategy stressed its importance.

5.68 There were mixed opinions amongst the interviewees with regard to the most important skill set for senior security personnel: business or security skills. The majority argued that both were essential, and that a good Head of Security could not operate without both sets of knowledge.

5.69 In terms of demonstrating the value of security, most of the interviewees adopted a mixture of qualitative and quantitative measures to monitor and evaluate security functions. Mirroring the findings of the previous section a number of interviewees reported that it was difficult to measure the success that security could add to an organisation whilst data collection in particular was highlighted as problematic. What is more, whilst respondents a) generally agree that security adds value to a business, and b) viewed security as a business enabler in that without it their organisation would not be able to operate they stopped short of viewing it as profit making.

Section 6. Discussion

6.1 Perhaps one of the most important findings to emerge from this work is that security is not regarded as the poor relation of other business functions. Most respondents, across both the surveys, felt that security made an important contribution to organisational success, slightly less but in the same 'ball park' as other mainstream functions such as human resources, finance and marketing. Security has its doubters (amongst smaller organisations in particular), but so do other functions such as human resources,[50] and the evidence suggests that security has no need to consider itself as inferior.

6.2 It is widely recognised that security affects all parts of the organisation. Board interviewees sometimes noted the importance of security objectives being aligned with those of the organisation, indeed, security needs to be on good terms with all organisational functions if it is to have an effect. The role of security varies, influenced by the activities of the organisation, the risk environment in which the organisation operates, the level of regulation/compliance requirements, and the attitude of the board, itself influenced by these factors. Commonly however, security operatives marshal information to identify and manage risks and provide the ability to react, quickly if necessary, to events when they occur.

6.3 Of course, it is important to note that not all areas of security are valued to the same extent. Although the aspects considered were all perceived to add value (a not insignificant finding), internet and computer security were rated more highly than personnel and physical security. If viewing security as adding value appears unproblematic, there was scepticism that it can generate a competitive advantage. In particular, onsite security guards, CCTV monitoring, alarm contractors and physical security (fences, ages and locks) were perceived as failing to deliver in this respect. Indeed, security was certainly not viewed as profit making, perhaps best described as a business enabler.

6.4 Perceptions of the effectiveness of security varied. Many admitted that the security function did not collect information on which to base judgements on whether security was really effective, an issue all too likely caused by the fact that this task was generally perceived as being extremely difficult. Indeed, evaluations of security performance were not a mainstream activity. As such judgements were sometimes made on qualitative assessments.

[50] See, S. Meisinger (2007) New Study Challenges HR, Illustrates Opportunity. *HR Magazine*. November, p8. It reports the findings of a new study which shows that human resource departments are, 'struggling to meet the strategic and operational challenges faced by organisations'.

6.5 Internal and external security reviews were favourably received and appear as valued and effective as police reviews. Some aspects of security, and this includes technology and security guards were not perceived so favourably, especially the latter. It is relevant here that only a half of respondents felt that contractors were paid enough to deliver a good service (although the majority were unsure), and less said that they were good at managing security contractors.

6.6 In terms of enhancing effectiveness, the attitude of the head of the company and the culture of the organisation were perceived as important, once again reinforcing the point that security is pervasive and needs organisational support to flourish.

6.7 At Board level having a security strategy in place is not always seen as essential since some Board members felt that they managed security well despite not having a security strategy in place. Yet, those organisations which did have a strategy stressed that it was important. Similarly, not all Boards have objectives for security, but again those that did underlined that this was helpful to good security. Another critical success factor was the closeness of the Head of Security to the Board; the more distant the relationship the lower the perceived status of security. There are perhaps lessons in this observation.

6.8 Another important finding was that senior security personnel are respected and considered experts, although generally not as business leaders. Sometimes their law enforcement/military background underlined their credibility as security experts, sometimes it reinforced the image of them as 'unbusinesslike' people. Certainly, Board members thought it unlikely security specialists would join the Board as they lacked all round business experience and the requisite skills sets. If this was ever to change organisations would need to recruit more qualified people; obtain senior level support for the security function and what it is trying to achieve; and raise awareness of the tasks they perform and how these impact positively on core business.

6.9 Overall, there is much good news for the security function. The findings suggest some possible areas of action:

- We need to call upon trainers and those responsible for education of security personnel to include business studies and related disciplines as key components. This is essential if security is to relate to other areas of business.

- There is much to commend the development of Masterclasses, run by highly credible leaders, on the role of security in business. These could be designed to appeal to security personnel already employed in the sector at different levels.

- The security sector needs to raise its profile within the business community showing how it adds value. Developing case studies,

writing in magazines other professionals might read, presenting at their conferences, may all have an appeal and ultimately an impact.

- Adding value is very much a preoccupation of the information security world. There may be wisdom in developing some joined up thinking and learning from each other.[51]

- Security associations and groups might consider joint ventures with other associations. It is interesting that the desire to gain more recognition and standing for the contribution it can make to organisations is not the exclusive concern of security; human resources and procurement, to name but two, face similar challenges. There may be opportunities for collaboration here.

- More emphasis needs to be placed on providing the tools and examples of how security can and does add value and how the contribution can be measured. There are both qualitative and quantitative methodologies but they are not always recognised and are far from commonplace. Showing that you make a difference is not easy, but it is not impossible either.

- We need to better understand what a good security strategy looks like.[52] How does it deal with 'integration' and 'convergence'? How does it relate to the objectives of the organisation? How does it set priorities and targets? Ensuring that security has a remit which relates to an organisations core activities is key, but it is often lacking. We need to develop templates and reference points.

- There is a direct link between internal perceptions of security and the role of security contractors. But we need to better understand what the needs of security contractors are and how best organisations can manage these. Could we develop a Charter for the Effective Management of Security Contractors?

- The role of security as business enabler needs to be thought through. Where are the models of good practice? What does good look like? How does security best influence organisational practice? It may be possible to develop a set of case studies.

- There needs to be a special focus on SMEs. Smaller businesses appear less favourably disposed towards security. It is less likely they will have a dedicated and expert security resource and so communicating the advantages and potential value of security

[51] An example of thinking in this area is included in the following*: Security Economics and the Internal Environment*, www.enisa.europa.eu/pages/analys_barr_incent_for_nis_20080306.htm.

[52] This is the focus of the current Security Research Initiative project, see, http://www.perpetuityresearch.com/researchclubs/sri.html.

will require a different approach. But they must be reached and helped to understand how they understand their security risks and mitigate them most cost effectively.

- There needs to be more downloadable tools to help SMEs, non security specialists and aspiring security managers to identify problems and manage them to best effect.

- We need to develop ideas and frameworks for creating a security culture and bringing employees across organisational functions on board the security message. We need to understand the best ways of encouraging staff to follow good security practice, building it into their day to day routine, without unacceptable negative consequences for their operational duties and communicating them effectively.

- We need to develop a methodology that will enable security functions to benchmark their performance against best practice. Providing the opportunity for organisations to identify where they are operating below best practice is likely to provide a crucial incentive for change.

- The interest in security would be enhanced if companies were required to report their crime levels and plans for mitigation in annual reports. This happens with information security breaches in some US States.

Section 7. Appendix: Methodology

7.1 The research is predominantly based on three sources of data. Supplementary material includes a review of the relevant literature and discussions with fellow academic and professional colleagues. The three primary data sources are listed below:

- A national survey of members of the Institute of Directors (IoD)
- A targeted business survey of organisations
- Nine interviews with employees in Board positions (or representatives) who are non security specialists but have high level responsibility for security

7.2 The response rates for security surveys are notoriously low. This is inevitable. Security is seen as something of a secret activity within some circles and as such is an issue that some organisations refuse to discuss. Indeed, when the Confederation of British Industry (CBI) approached their members on our behalf they replied that security was a 'largely no-go area'. Indeed, even an approach by the CBI elicited a very poor response. We were advised not to request too much information about companies in surveys, but this did little to encourage a good response.

7.3 There is another difficulty in surveying organisations, in that it is particularly difficult, not to mention time consuming, to obtain a representative sample (by region, size, annual turnover and industry sector etc). For example, the Inter-Departmental Business Register (IDBR) – a list of UK businesses used by the Office of National Statistics (ONS) and other governmental departments– is known to be missing some small businesses operating without VAT[53] or PAYE[54] schemes.[55]

7.4 In light of these difficulties Perpetuity approached, and secured, the support of the following three associations in disseminating surveys to organisations: the IoD, the CBI and the Commercial Crime Services (CCS) division of the International Chamber of Commerce (ICC). The principal reason for choosing these associations is that it was hoped that members would be more likely to respond if the associations demonstrated their support and backing for the project. This is, as noted above, an area where getting a representative sample is notoriously difficult, and so the varied membership of these organisations (representing a cross section of small, medium-sized and

[53] VAT- Value Added Tax
[54] PAYE- Pay As You Earn
[55] Inter-Departmental Business Register (IDBR): www.statistics.gov.uk/idbr/idbr.asp

large organisations spanning a variety of industry sectors) maximised the potential to boost the response rate and obtain a more representative sample.

7.5 The findings in this report should not be generalised or considered to be representative of businesses as a whole. Firstly this is because they are based on a small sample of responses, specifically 612 surveys (500 from the IoD survey and 112 from the targeted business survey) and nine interviews. Secondly the two survey samples do not represent all businesses due to the problems already noted in obtaining a representative sample.

7.6 The methodological issues behind the IoD survey, the targeted business survey and the nine interviews are discussed in detail throughout the remainder of this section.

IoD survey

7.7 The IoD is an international association comprised of personnel from a variety of organisations ranging from large public companies to small private firms. The IoD survey a sample of their members with a set of core questions approximately every two months. Perpetuity was offered the opportunity to add a series of questions to this survey to elicit members' views of security. This was a rare, and valuable opportunity to obtain the views of a national sample of organisations.

7.8 Questions were included on issues such as the importance of the security function in comparison to other organisational functions, the value that different aspects of security add to meeting the objectives of an organisation and the effectiveness of security reviews. The IoD members were asked to answer each question using a scale of one to seven, where seven indicated a positive response and one a negative response.

7.9 The survey was conducted via the telephone by a firm (not Perpetuity) on behalf of the IoD. Five hundred members were surveyed in total in a sample which was representative of the IoD membership by region, company size and industry sector.

7.10 A breakdown of the sample revealed that the organisations were spread across England, Wales, Scotland and Northern Ireland. Four hundred and eighty were private sector firms and 20 were public sector companies. The organisations spanned a cross section of industry sectors. These sectors were as follows:[56]

- Business and Professional Services

[56] These are the industry classifications used by the IoD which are based on Standard Industry Codes.

- Distribution and Hotels
- Financial Services
- Government, Education, Health and Personnel Services
- Manufacturing
- Others including Mining, Construction, Transport etc.

7.11 The size of the organisations ranged from those with up to 10 employees to firms with 500 or more staff. Similarly the annual turnover of the private sector organisations also varied from companies earning less than £500,000 per year up to those with a turnover of more than £500 million.

7.12 The individuals who responded to the survey held a range of senior positions within the organisations in which they were employed. Examples included Chief Executive, Managing Director, Chairperson, Partner, Owner Proprietor and Directors (covering various departments including Finance, Marketing and Sales).

7.13 It is important to note that the findings cited throughout this report are based on secondary analysis of the IoD survey data. That is Perpetuity did not have sight of the raw data set listing individual organisations' responses to each of the questions in the survey. As such it was not possible to perform certain statistical tests on the data.

Targeted business survey of organisations

7.14 A survey was designed in order to elicit views on the value of security from employees in senior management positions within organisations. It was comprised of 38 statements relating to either: the role of security within an organisation, internal security personnel, the measurement and communication of security, or security contractors. Organisations were asked to rank each statement on a scale of 1 to 5 where 5 denoted 'Agree Strongly' and 1 'Disagree Strongly;' 3 is 'Neither Agree or Disagree.' The survey was hosted on-line, as well as being available in an electronic or paper format.

7.15 A link to the on-line survey was either posted or emailed to a sample of 1,399 contacts. In many cases a hard copy of the survey was also sent to the contact. The contacts were selected from three data sources. The three data sources were: the CBI National Directory, UK FTSE 100 Index, and the CCS division of the (ICC).

7.16 The following provides further detail about each of the three data sources: CBI, UK FTSE 100 and the CCS.

Confederation of British Industry (CBI):

7.17 The CBI is a lobbying organisation for UK business on national and international issues. It works with international legislators, policy makers and the UK Government to help UK businesses compete effectively. CBI membership is comprised of organisations from every sector of industrial and commercial activity including 200,000 small and medium size companies, 80 of the FTSE 100 companies, more than 20,000 manufacturers and over 150 sectoral associations.

7.18 The CBI hosts an online directory containing details of over 2,000 CBI members, trade associations and non-CBI members, and is divided into 32 industry sectors including accountancy, finance, law, insurance, utility companies, property, engineering and telecoms.[57] With permission and support from the CBI a random sample of the directory were selected for participation. Six hundred and ninety-nine organisations were selected in total spanning all of the industry sectors covered in the directory.

7.19 A letter with the link to the on-line survey and a hard copy (paper version) of the survey were initially posted to the named contact for each of the 699 organisations. They were asked to pass the survey onto the Board member responsible for security for completion, but only if that Board member was not a security professional. A link to the on-line survey was also emailed to those organisations where an email address was given.

7.20 Two members of the research team attended an event hosted by the CBI for its members in London on the 7th August 2007. Members of the CBI were informed of the SRI project and encouraged to complete the survey.

FTSE 100 Index:

7.21 The UK FTSE 100 Index is a share index of the 100 most capitalised companies listed on the London Stock Exchange. This is not a fixed list and changes according to the rise and fall in company values. The contact details for 98 Chief Executive Officers employed by companies listed on the FTSE 100 Index during 2006 were provided by one of Perpetuity's personal contacts at the University of Portsmouth.[58] The University had previously undertaken a survey of these companies.

7.22 A hard copy (paper version) of the survey and a letter with a link to the on-line survey was posted to the 98 Chief Executive Officers.

[57] Please refer to the Confederation of British Industry (CBI) website for a full list of the 32 industry sectors: http://www.cbidirectory.co.uk/search/category.php
[58] Our thanks to Dr Mark Button for his help.

ICC- CCS

7.23 The Commercial Crime Services (CCS) is the anti-crime division of the International Chamber of Commerce (ICC). The CCS is a membership organisation tasked with combating all forms of commercial crime. It is comprised of the following three bureaux and a Cybercrime Unit: International Maritime Bureau (IMB), Financial Investigation Bureau (FIB) and Counterfeiting Intelligence Bureau (CIB). These three bureaux offer their members a range of services to tackle a range of commercial crime including money laundering, shipping fraud, product counterfeiting, insurance fraud and document fraud in international trade.[59]

7.24 The types of organisations that are members of these bureaux include companies engaged in international business and law enforcement, banks, insurance companies, shipping companies, traders, manufacturers, law and accountancy firms. The companies range from medium sized companies to large multi-nationals. Membership is international including the UK, Western Europe, United States, Hong Kong, Singapore, Malaysia, Indonesia etc.

7.25 Unlike the CBI and FTSE samples discussed above all these members had a specific interest in security in terms of business orientation.

7.26 An electronic copy of the survey and a link to the on-line version was emailed by the CCS to all its members (approximately 550) who span all three of the bureaux: FIB, IMB and CIB.

Targeted business survey: response rate

7.27 From the initial 1,399 contacts, 112 surveys were completed in total reflecting a response rate of eight per cent.[60] A breakdown of the surveys revealed that 56 derived from the CCS and the remaining 56 from the CBI and FTSE 100 Index. The surveys received from the latter two sources have been combined together because there was too small a response rate in each sample individually.

7.28 As noted above Perpetuity was warned against requesting too much identifying information from the organisations surveyed due to the reluctance amongst some businesses to discuss the issue of security. Respondents were therefore invited to provide details of their job title and industry sector only; however this was not mandatory. A breakdown of the information that was provided by those respondents who chose to answer shows that these organisations were from a variety of industry sectors including finance, logistics, shipping, law,

[59] For more information on the CCS please see: http://www.icc-ccs.org/main/index.php

[60] Seven surveys were removed from the sample before it was analysed because they had been completed by professionals in security related roles such as Fraud Prevention Managers, Security Managers and Directors of Security.

trade associations, leisure and tourism, food and drink and utilities services. Most of the surveys were completed by employees in non-security related senior positions such as Managing Directors, Chief Executives, Finance Directors, Operations Managers and Compliance Managers.

Interviews

7.29 Interviews were undertaken with representatives from nine organisations; all of which were active in the UK whilst some also operated internationally. These included:

- A manufacturer and distributor of tobacco
- A manufacturer and supplier of aerospace, defence and security services
- A producer and supplier of mining and natural resources
- A provider of technology services and solutions for nuclear fuel
- A major high street retailer
- A major high street bank
- A operator of managed pubs and pub restaurants
- An auto dealership
- A security agency

7.30 These organisations are clearly not representative of all types of business, rather it was the intention to select a sample of organisations which differed in terms of the security threats they faced as this would alter the requirements of their security systems. The aim was to obtain insights into how security was viewed. The nine interviewees were all senior people within their organisation who were either the Board member responsible for security or reported directly to the Board about this issue. It is important to be clear that these interviewees were not specialists in security.

About Perpetuity

Perpetuity is an independent research and consultancy company specialising in the areas of security, risk and crime management. Perpetuity is a 'spin-out' from the University of Leicester and is part of the Perpetuity Group which includes Perpetuity Training and Perpetuity Conferences).

We are specialist in a range of Research and Community Safety areas, including drugs and alcohol, crime and disorder audits, evaluation, crime research, housing and regeneration and education.

We have a broad range of experience in security consultancy including risk surveys and security audits, CCTV specification, design and management, procurement advice, security policies and procedures, information security, crisis and contingency planning, executive protection and penetration testing.

Perpetuity also operates 'Secured Environments' a police accreditation process for organisations that manage their crime prevention and security well.

Perpetuity Research & Consultancy International Ltd
148 Upper New Walk
Leicester
LE1 7QA
United Kingdom
Tel: +44 (0)116 222 5555
Fax: +44 (0)116 222 5557
www.perpetuitygroup.com/prci
prci@perpetuitygroup.com