Beyond the Protection of Assets: The Broader Benefits of Security

Professor Martin Gill
Charlotte Howell
Amy Randall

September 2015

CONFIDENTIAL

INVESTOR IN PEOPLE

Copyright

Acknowledgements

SRI Members

Adidas

CAT

emprise

e·on

G4S

interr

KPMG

M&S

mitie

nedap

OCS

Royal Mail

SECURITAS

sia
Security Industry Authority

sodexo
QUALITY OF LIFE SERVICES

VSG

Preface

This report highlights the ways in which security contributes to organisations. For too long, as a field of activity and as a discipline, it has undersold itself, focusing on the ways in which it protects assets rather than the ways in which it crucially supports business activities. It has been too narrowly and negatively defined. At its best good security certainly protects assets but it does more than that: it facilitates and enables good business and protects against bad business; it contributes to good governance and staff wellbeing; it protects and enhances reputations; it protects profits but also makes profits. The worst part of it is that the security sector has kept many of the benefits it generates a secret and permitted a focus on bad security with all its power to disrupt and undermine good business.

The findings of this report suggest that security can be an enormous influence and facilitator of good. The findings need to be heeded and built upon; the message needs to be that security when done well can be a powerful influence for good. The security sector needs to let the secret out of the bag, and the sooner the better.

Table of Contents

Executive Summary

Introduction

Discussing the true value of security has been thwarted by it being viewed as an intangible. This expenditure on security is therefore characterised as being without joy, a grudge. But there is a different way of looking at security, that far from being marginal, it is crucial to organisational effectiveness. Not least because security is essential beyond reducing the chances of threats impacting, it is crucial to maintaining order, and generates many other non-security benefits for different parts of the organisation and different areas of activity. The problem is that these benefits are rarely acknowledged.

The benefits are not recognised

- it is viewed as an intangible which complicates attempts to calculate a persuasive return on investment; success in security is often defined as 'nothing is going wrong'.
- it is poorly understood by senior managers and other corporate departments, often appreciation of the broader benefits of security exists in pockets;
- security staff have not been good at promoting security and the impacts it has; security typically adopts a rather self defeating stance.

What are the benefits?

1. **Security prevents loss**

A good security culture prevents the losses associated with crime (that is familiar territory), but it can also reduce the likelihood of other threats occurring:

- it can reduce insurance pay outs, fines and penalties for non-compliance with requirements and can reduce the losses caused by emergency situations.
- Crucially it can ensure a good reputation and protect against damage to reputation – something vital for success. But this role is rarely acknowledged.

2. **Security enhances success**

Good security has often been shown by independent research to be a significant and sometimes a main differentiator providing a competitive advantage:

- where people live, work, study and shop, the websites they choose to access are all affected by security;
- some companies will not trade with a company deemed to be insecure;
- building security into products and service can enhance their attractiveness to customers, and therefore help generate additional revenue.

Further, security can facilitate business expansion, enable operations not least in (risky) areas that others may not be able to achieve; and permit better

business decisions via a better determination of risks and how they can be managed.

Security can also help to retain business by (for example):
- aiding quicker recovery after an incident (and quicker than competitors);
- providing a source of advice to clients and partners enhancing business relationship;
- creating efficiencies for clients.

3. Security enables operations

Security enables staff to be productive by preventing barriers/disruptions, facilitating flexible working hours, relieving employee concerns about safety when travelling; providing an effective first response when problems occur; ensuring compliance with policies and procedures. It also enhances wellbeing more generally (again something rarely acknowledged) by creating a positive working environment, protecting staff and helping them when incidents do occur, but also by equipping staff with skills in the workplace that enables them to better protect themselves outside work.

Security can play a crucial role in generating trust – something which is good for business – and when poor can serve to undermine it. Furthermore, security keeps the organisation honest, following rules and preventing rule breaking and dishonesty. It is also a trusted advisor to staff, partners and collaborates with others (including competitors) to reduce threats.

Corporate Social Responsibility is a legal requirement. Security often plays a (largely unacknowledged) key role in ensuring that this is undertaken successfully. It is also enhanced by effective security which creates a diffusion of benefits effect on the community:
- by providing information and intelligence to other organisations to help them tackle local crime and improve security;
- by organisations using their own security services to support local initiatives;
- and offering environmentally friendly security services, and supporting local areas by providing job opportunities.

Communicating the benefits

It was abundantly clear that a key challenge for security is to better communicate the benefits and in doing so, to better 'sell' itself. If this is not done, security will continue to be associated with negatives rather than positives.
Good security is based on engaging people and there is a need for security to take the lead and set examples about how best to engage staff (especially marginalised staff). Integration with other departments is vital – a key focus is to build awareness and practices in to the roles of others (rather than security only being undertaken by 'security'). Security is not just a business enabler, it is an important one at that.

Section 1.   Introduction

1.1   This project was initiated to better understand what benefits security brings to an organisation. By and large the discussion about the value of security focuses on three rather unhelpful points. The first is to advance the case that security is an intangible; it cannot be measured and so, as a consequence, one cannot 'prove' value has been added in any meaningful way. This has caused the second point, namely the evaluation of a range of quite complicated mechanisms for measuring say return on investment which are easy to dispute or disprove. Thirdly, the real success of security is that if successful nothing happens – no offences or incidents take place - and measuring the value of something that doesn't happen is a forlorn task. Often investment in security is driven by regulatory requirement or in response to a major problem or crisis, and so without a defined financial return model that enjoys widespread confidence it is perhaps not surprising that security is sometimes viewed as a grudge purchase.

1.2   Further, in both corporate security departments and amongst security suppliers, there has been a very narrow focus on the benefits from services provided; in fact most often that focus has been on specific security-related benefits. But there is evidence that a host of other non-security benefits are derived from having good security. Just one example is the use of CCTV typically justified in terms of reducing crime and making people feel safe can also be used – remaining sensitive to people's freedoms - for example, to validate accident claims, count footfall and assess customer buying behaviour.

1.3   In this project the aim was to get beyond this narrow base and begin to address the broader ways in which security benefits an organisation. Key questions included:

- What are the benefits of having good security that are more than just good security?
- What benefits do other corporate functions/departments derive from having good security?
- To what extent does security contribute to the fulfilment of company aims? And in what ways could it do so?
- What commercial benefits evolve from having good security? Does it enhance reputation and brand? Does it help make a profit?
- If security was a person selling its benefits what would he/she say?
- To what extent are some of the fundamental elements of business, such as trusting relationships, staff wellbeing, corporate governance, dependent on good security to be successful?
- When organisations buy security, what do they expect to get in return?

- What are the security and non-security benefits of specific crime prevention measures (such as CCTV, Alarms, Access Control)?
- How can crime prevention 'concepts' such as deterrence inform our understanding of the benefits of security?

1.4 In fact there is a wide range of benefits that you get from a good corporate security function compared to a bad, and from a good security supplier compared to a poor one. In this project we will catalogue the broader security benefits. We want to encourage a different way of thinking about the true value of security from a different evidence base.

Section 2.   Learning from prior research

2.1   This section provides a brief review of previous work on the benefits of security. First, we consider how security can be viewed as a positive despite the negative connotations it sometimes invokes; and what organisations hope to gain by 'consuming' security. We then consider the additional (often unintended) benefits of specific crime prevention measures. We move on to assess the ways in which security can positively influence success in an organisation; and finally consider how security can provide a competitive advantage.

Security really is a good thing

2.2   What is 'security' is a hotly contested topic[1]. Many textbooks introducing the topic start by defining security, and tend to allude to the fact that it is about the protection of assets, or protecting people and entities from intended threats. Sometimes there are more negative associations with the word 'security':

> *The problems associated with negative security in part stem from the dark and repressive practices associated with its exercise: the deadly symbiosis between prison and ghetto; the growth and extension of dark side surveillance technologies; and repression, more generally, in the developing security state.[2]*

2.3   As the authors go on to note:

> *Security has developed as a concept but in ways that have led to its separation (indeed divorce) from the concept of cura (or care) to which it was once connected.[3]*

2.4   In a text that was designed to focus on the positive aspects of security, the editors suggest that there are more positives than negatives in the definition:

> *If we begin by looking at the etymology of the word 'security', for example, we find that a negative interpretation of the concept is limited at least. The Dutch*

---

[1] See, for example: Brooks, D. (2009) 'What is Security: Definition through knowledge categorisation'. *Security Journal*, 23(3), 229-239.
Manunta, G. (1999) 'What is Security?' *Security Journal*, 12(3), pp. 57-66.
[2] Hallsworth, S. & James, D. (2014) 'Growing Sanguine About the Weeds. Gardening and Security Revisited'. In, Schuilenburg, M., van Steden, R. and Oude Breuil, B. (eds) *Positive Criminology: Reflections on Care, Belonging and Security*. The Hague: Eleven International Publishing, p. 57.
[3] Hallsworth, S. & James, D. (2014) *op cit, p. 69.*

word for security [veiligheid] is etymologically closely linked to the word velich in Old German and felig in Old Frisian, words that have connotations with what is now called 'trust', 'being beloved' and 'friendliness' (Van Zuijlen 2008). In addition, we may think of a range of concepts that can further colour connotations as love, friendship and liberty. This is all the more clear when we look at cultural-anthropological notions like 'home', 'belonging', and (transnational) 'community-building' as a way to resist hegemonic and negative meanings of security.[4]

2.5   Indeed, there is a whole range of ways in which the negative aspects of security are being reconsidered. For example, many students of security and policing will be aware that there has been considerable discussion of the negative effects of privately controlled public space on social life 'including encouraging racial and class stratification, reducing the variety of public activities and generating a decline in street vitality'[5], but it has also been highlighted that the presence of security guards can in fact increase feelings of security and therefore enable people to enter and use spaces and participate in group activities[6].

2.6   A number of writers[7] have pointed to the priority given to safety and security (which typically includes physical security) in Maslow's[8] Hierarchy of Needs model. In short, next to physiological needs (breathing, food, water etc), safety and security are the next most essential human needs.

2.7   The prominent social theorist Anthony Giddens[9] has discussed the importance of ontological security which describes the importance of a sense of continuity in people's lives that enables them to be stable characterised by the absence of chaos, anxiety and harm. Dupuis and Thorns[10] described ontological security as "*a sense of confidence and*

---

[4] Schuilenburg, M., van Steden, R. & Oude Breuil, B. (2014) 'A Critique of security: Towards a positive turn in Criminology'. In, Schuilenburg, M., van Steden, R. & Oude Breuil, B. (eds) *Positive Criminology: Reflections on Care, Belonging and Security*. The Hague: Eleven International Publishing, p.14.

[5] Huang, T. (2014) 'Not 'Fortress Los Angeles'. Design, and Management of Privately Owned Public Spaces in New York City'. In, Schuilenburg, M., van Steden, R. and Oude Breuil, B. (eds) *Positive Criminology: Reflections on Care, Belonging and Security*. The Hague: Eleven International Publishing, p. 117.

[6] See: Huang, T. (2014) *op cit.*

Franck, K. (2014) 'Security in Support of Safety and Community. Thoughts From New York'. In, Schuilenburg, M., van Steden, R. and Oude Breuil, B. (eds) *Positive Criminology: Reflections on Care, Belonging and Security*. The Hague: Eleven International Publishing.

[7] For example see: Smith, C. & Brooks, D. (2013) *Security Science: The Theory and Practice of Security.*

[8] Maslow, A. H. (1943) 'A theory on human motivation', *Psychological Review*, 50(4), pp. 370-396.

[9] Giddens, Anthony. (1984). *The Constitution of Society: Outline of the Theory of Structuration*. University of California Press.

Giddens, Anthony (1991). *Modernity and Self-identity: Self and Society in the Late Modern Age*. Stanford University Press.

[10] Dupuis, A. & Thorns, D. (1998) 'Home, home ownership and the search for ontological security', *Sociological Review*, 46, 1, 24–47.

trust in the world as it appears to be. It is security of being." And of course social order is an essential element of personal freedom in society but also in families and workplaces[11].

2.8 Linking security to positives is relatively rare. In reality supporters of (private) security tend to understate the dangers that bad security can create, while critics of security tend to pass over the crucial role that good security plays in protecting freedoms and lifestyle choices and perhaps especially for the most disadvantaged.

2.9 In this study we have set out to show the ways in which good security is important, indeed essential. This is not just in protecting people from harms and facilitating personal freedoms, but in many other ways too. We seek to show the ways in which good security is more than just good security, it is fundamental way beyond that.

Security consumption

2.10 Before assessing the benefits of security, it is worth briefly considering why organisations buy it in the first place. In a very literal sense it is of course purchased to protect the organisation, yet Goold et al[12] describe organisations as reluctant purchasers viewing security as a low priority. They describe this as '*price-sensitive, quality-insensitive*' purchasing. In other words security consumption is motivated by paying the least possible for the services needed to achieve an environment that is appropriately secure for their staff and customers. So the argument goes security is rarely purchased for pleasure.[13]

2.11 Such a position disguises the view that staff can provide benefits beyond the immediate security objectives that they are purchased to achieve. This begs the question, whether organisations are missing an opportunity to 'make the best' of these resented purchases by maximising their potential for further outcomes beyond meeting the security needs of the organisation.

Benefits of Crime Prevention Measures

2.12 Drawing on crime prevention literature, it is evident that crime prevention measures (when implemented effectively) can have a number of intended benefits; they reduce crime; they can produce savings and prevent losses (both personal and financial); and they can reduce fear of crime. Less established however is the range of benefits

---

[11] Cooley, C. (1902) *Human Nature and Social Order*, C. Scribner's sons: New York.
[12] Goold, B., Loader, I. & Thumala, A. (2010) 'Consuming security? Tools for a sociology of security consumption', *Theoretical Criminology,* 14(1), pp. 3-30, p 12.
[13] But see, Hopkins, M. and Fox, G. (2013). The Choice-Structuring Properties of Security Consumption: An Exploratory Study of Security Consumption Culture Within Small Shops, *Security Journal* 10.1057/sj.2013.28.

that are derived from having good security, that are not intended when a measure is introduced. These exist in two key contexts. First, crime prevention measures have been observed to create a diffusion of benefits, by reaching further than originally intended. Second, specific measures (such as CCTV) have evolved to be used for a multitude of purposes beyond crime prevention, due to their capacity for gathering useful information. These 'collateral' benefits of crime prevention measures are important to consider.

Diffusion of benefits

2.13   A concept known as 'diffusion of benefit' is used to describe a situation, "*whereby the positive effects of an intervention extend beyond the operational range of the intervention.*"[14] In other words, that measures may reduce crime not only where interventions are situated but also in the surrounding areas[15]. This has been argued to be, '*at least as likely as crime displacement*'[16]. There are two main explanations for the diffusion of benefits:

- The **deterrent** value of the intervention - offenders are likely to perceive a higher level of risk of detection, because they are unaware of the functioning limits of an intervention[17]. For example, CCTV installed in three university campus car parks reduced vehicle crime in not only those three car parks with the cameras but also a fourth that did not have any. The publicity of the cameras influenced the offenders' view of the risks of committing crime in nearby areas[18].

- **Discouragement** - protecting one target may increase the perceived level of risk and difficulty of seeking a new target, reducing the attraction of committing crime elsewhere[19]. Research found that where coin fed gas and electricity meters were removed from council houses, which had been the target of burglaries, the whole estate experienced a reduction in burglary; that was sufficient

---

[14] Johnson, S., Guerette, R., and Bowers, K., (2012) 'Crime Displacement and Diffusion of Benefits'. In. Farrington, D. and Welsh, B. (Eds) (2012). *The Oxford Handbook of Crime Prevention*. Oxford, p. 338.
[15] See: Kim, Y. S. (2008) 'The measurement of prevention effect of open-street CCTV in South Korea: displacement of crime or diffusion of crime control benefits?' *Journal of Korean Private Security Studies*, 11 (2008), pp. 209–245.
Park, H., Oh, G., Paek, S., (2012) 'Measuring the crime displacement and diffusion of benefit effects of open-street CCTV in South Korea.' *International Journal of Law, Crime and Justice*, Vol 40(3), September 2012, pp. 179–191.
[16] Displacement theory suggests that placing crime prevention measures in one place, results in shifting crime to another, less protected area, Johnson et al (2012) op cit, p. 339.
[17] Clarke, R., & Weisburd, D. (1994) "Diffusion of Crime Control Benefits: Observations on the Reverse of Displacement." In *Crime Prevention Studies*, vol. 2, edited by Ronald V. Clarke. Monsey, NY: Criminal Justice Press.
[18] Poyner, B. (1992) 'Situational Crime Prevention in Two Parking Facilities'. In Clarke, R. (ed) *Situational Crime Prevention*: *Successful Case Studies*, New York: Harrow and Heston.
[19] See Clarke & Weisburd (1994) *op cit.*
Johnson et al (2012) *op cit.*

to discourage potential burglars as they could not be sure of finding a cash meter when they did go to the trouble of breaking in[20].

2.14 This concept illustrates a pertinent point – that the introduction of security measures to respond to risk, may have unexpected additional crime prevention benefits, but further raises the question whether they may hold additional non-crime related benefits; an issue we will return to.

'Alternative' uses of security measures

2.15 Some relevant examples of the use of security measures beyond just security include the following, the points here are highlighted to illustrate the point rather than to provide a definitive list:

- Where there are inaccessible settings[21], CCTV can be used to assess conditions remotely, for example progress on building or construction sites.

- In the retail arena, CCTV has been used to give insights in to the behaviour of shoppers[22] with video analytics software showing how to target shoppers and staffing to improve customer satisfaction, and generate sales. It has also been used to verify accident claims, avoiding the costs and wasted time associated with wrongful claims.

- CCTV has been used for traffic flow analysis[23], enabling observation of behaviour to be conducted more effectively and at a lower cost than when collected manually.

- In a similar way, the observational capabilities of CCTV and access control can be used to assess compliance with rules and procedures (such as sanitation techniques, packing methods etc)[24].

- CCTV has also been used to, determine what action and resources are needed to respond to incidents such as lost children, public meetings or demonstrations, and alarms.[25] CCTV has to be used

---

[20] See: Pease, K. (1991) 'The Kirkholt Project: Preventing Burglary on a British Public Housing Estate', *Security Journal,* 2, pp. 73-77.
Hill, N. (1986) *Prepayment Coin Meters: A Target for Burglary. Crime Prevention Unit Paper 6*, London: Home Office.
[21] Vintech website (2012) *Top 10 Non-Security Uses for Surveillance,* accessed on 20/11/14 - http://www.vintechnology.com/journal/cctv/top-10-non-security-uses-for-surveillance-cameras/
[22] Andy Clutton (October 2014) *The non-security uses of CCTV recommended for retailers*, PSI Magazine, accessed 20/11/14 - http://www.psimagazine.co.uk/the-non-security-uses-of-cctv-recommended-for-retailers/
[23] CCTV information website (date unknown) *Alternative Uses for CCTV*, accessed 20/11/14 - http://www.cctv-information.co.uk/i/Alternative_Uses_for_CCTV
[24] Vintech website (2012) *Top 10 Non-Security Uses for Surveillance,* accessed on 20/11/14 - http://www.vintechnology.com/journal/cctv/top-10-non-security-uses-for-surveillance-cameras/
[25] Ratcliffe, J. (2006) *Video Surveillance of Public Places*, Response Guide No.4: POP Centre. (http://www.popcenter.org/Responses/video_surveillance/)

ethically of course, that is crucial, but there are real benefits beyond crime prevention in so doing.

- Access Control systems can be used to track and locate individuals (including in an emergency); and to restrict staff from entering certain areas or using certain equipment (which may be hazardous); they can even limit the number of people in an area at any one time, to prevent a prescribed safety limit being exceeded[26].

- Access control technology has been observed to be useful in both an HR and Finance context - by recording employee attendance and working hours, comparing this data with shift patterns, and using it to inform the payroll system so that it is accurate[27].

2.16 Ultimately these alternative uses of security measures – and these are just examples - illustrate that a resource that many organisations pay for anyway, can be used in additional ways - creatively - to solve (and pre-empt) problems, create efficiencies, benefit customers and reduce the costs (or increase profitability) of other aspects of business.

Security & Business Success

2.17 There is also evidence to suggest that security can benefit different aspects of business activity, including those crucial to its success, namely staff wellbeing, company reputation and a culture of trust.

Staff wellbeing

2.18 An emphasis on wellbeing in the workplace is becoming increasingly politically important. The UK Government change agenda has defined this as "*creating an environment to promote a state of contentment which allows an employee to flourish and achieve their full potential for the benefit of themselves and their organisation*".[28] The point is not lost on the Institute of Directors which provides guidance on wellbeing at work[29].

---

[26] Nortech Website (date unknown) *What is Access Control? - Additional Applications*, accessed 25/11/14 - http://www.nortechcontrol.com/access-control/what-is-access-control/additional-applications.aspx
[27] Nortech Website (date unknown) *What is Access Control? - Additional Applications*, accessed 25/11/14 - http://www.nortechcontrol.com/access-control/what-is-access-control/additional-applications.aspx
[28] Tehrani, N., Humpage, S., Willmott B. and Haslam, I., (2007) *What's Happening with Well-being at Work?* Change Agenda, Chartered Institute of Personnel and Development, London.
[29] Institute of Directors (2006) *Wellbeing at work: how to manage workplace wellness to boost your staff and business performance*, London: Director Publications.

2.19   In terms of the factors affecting wellbeing, unsurprisingly research has
        linked wellbeing with security[30]; being secure, that is free from intended
        danger and harm, and protecting people from crime and chaos, is
        considered crucial for achieving well being[31].

2.20   Previous research has identified the following factors:

  • Poor neighbourhood security has a dramatic impact on an
    individual's wellbeing - living in a dangerous area significantly
    reduces an individual's life satisfaction[32].

  • Further, fear of crime and worries about personal and family safety
    also have a negative impact on wellbeing[33].

  • Poor physical security can have a direct detrimental effect on
    physical and subjective wellbeing; which in the workplace indicates
    a lack of employer attention to basic staff needs[34].

  • Poor physical working environments reduce job satisfaction while
    good quality environments reduce work stress[35].

  • However, if onerous, security policies and procedures may have the
    potential to reduce staff freedom, independence and job
    satisfaction[36]. This highlights the distinction between good security
    and bad security[37].

2.21   Wellbeing then, is clearly an important condition, and evidently it is
        important to adopt proportionate responses to security, that balance the
        needs of staff against the risks identified. This begs the question, why

---

[30] See for example: Wills-Herrera, E., Islam, G., & Hamilton, M. (2009) 'Subjective well-being in cities: A
multidimensional concept of individual, social and cultural variables', *Applied Research in Quality of Life*,
4(2), pp. 201-221.
Dupuis & Thorns (1998) *op cit.*
Thoilliez, B. (2011) 'How to grow up happy: an exploratory study on the meaning of happiness from
children's voices', *Child Indicators Research*, 4, 2, 323–51.
[31] See: Renata, F., Zvjezdana, P-L. & Ljiljana, K. (2012) 'Personal Security and Fear of Crime as
Predictors of Subjective Well-Being'. In: Webb, D & Wills-Herrera, E. (eds) *Subjective Well Being and
Security*, Social Indicators Research Series 46, Springer: London.
Gonzalez, M., Casas, F., Figuer, C., Malo, S & Vinas, F. (2012) 'Satisfaction with present safety and
Future Security as Components of Personal Wellbeing Among You People: Relationships with Other
Psychosocial Constructs', In: Webb, D and Wills-Herrera, E (eds). (2012) *Subjective Well Being and
Security*, *Social Indicators Research Series 46*, Springer: London.
[32] Lelkes, O. (2006) 'Knowing what is good for you: Empirical analysis of personal preferences and the
'objective good'', *The Journal of Socio-Economics*, 35(2), pp. 285-307.
[33] Møller, V. (2005) 'Resilient or resigned? Criminal victimisation and quality of life in South Africa'.
Social Indicators Research, 72, pp. 263-317.
[34] Bryson, A., Forth, J. & Stokes, L. (2014) *Does Worker Wellbeing Affect Workplace
Performance? NIESR. Department for* Bussiness Innovation and Skills. October 2014
[35] Huang, X. and van der Vliert, E (2004) 'Job level and national culture as joint roots of job satisfaction',
Applied Psychology: An International Review, 53, pp. 329-348.
[36] Grant, A., Christianson, M. and Price, R. (2007) 'Happiness, health or relationships? Managerial
practices and employee wellbeing tradeoffs', *Academy of Management Perspectives*, August 1, pp. 51-
63.
[37] Gill, M. (2014) 'Exploring Some Contradictions of Modern Day Security', In M. Gill (ed) *The Handbook
of Security*, Second Edition. London: Palgrave.

security does not systematically seek to highlight the quite crucial role it plays in bringing about a condition that is essential for both a happy life and good business?

Company reputation

2.22   Reputation is acknowledged to be valuable to companies because it is considered key to commercial decision-making[38]. An investor or consumer must trust a company and its ability to achieve results before he/she will commit finances. People therefore base their opinion on reputational information about an organisation from the media and other sources[39].

2.23   The exact value of reputation to an organisation can be very difficult to ascertain, precisely because it is a non-physical resource[40]. Yet, research has shown a company's reputation is correlated with economic success[41].   Indeed, a worldwide study of 950 business executives found that global business influencers estimate that 63% of a company's market value is attributable to its reputation[42]. Clearly then, a good reputation is worth protecting.

2.24   Once established, a good reputation can produce a number of benefits:

- indicate product quality to customers resulting in increased business and profits[43].

- improve a company's success by attracting top employees[44].

---

[38] Dowling, G. (1986) 'Managing your corporate images', *Industrial Marketing Management*, 15, pp. 109-115.

[39] Fombrun, C. & Shanley, K. (1990) 'What's in a name? Reputation Building and Corporate Strategy', *Academy of Management Journal*, 2(33), pp. 233-258.

[40] Coombs, W. (2008) 'Reputation management'. In Coombs, W (2008). *PSI Handbook of business Security*, Praeger Security International.

[41] See for example: Dube, S. (2009) 'Good management, sound finances, and social responsibility: Two decades of US corporate insider perspectives on reputation and the bottom line', *Public Relations Review*, 35, pp. 77–8.

Fombrun, C. (2001) 'Corporate reputations as economic assets'. In Hitt, M., Freeman, R. & Harrison, J. (eds.) *Handbook of strategic management*, Oxford: Blackwell.

Roberts, P. & Dowling, G. (2002) 'Corporate reputation and sustained superior financial performance', *Strategic Management Journal*, 23, pp. 1077-1093.

Schuler, D. & Cording, M. (2006) 'A Corporate Social Performance – Corporate Financial Performance Behavioral Model for Consumers', *Academy of Management Review*, 31(3), pp. 540-558.

[42] Weber Shandwick (2006) *Safeguard Reputation™* Survey, http://www.corporatereputation12steps.com/Downloads/PDFs/2_WS_Safeguarding_Reputation_exec_s ummary.pdf

[43] Klein, B., & Leffler, K. (1981) 'The role of market forces in assuring contractual performance'. *Journal of Political Economy*, 89, pp. 615-641.

Milgrom, P. & Roberts, J. (1986) 'Price and advertising signals of product quality', *Journal of Political Economy*, 94, pp. 796-821.

[44] See for example: Backhaus, K. B., Stone, B. A. and Heiner, K. (2002) 'Exploring the relationship between corporate social performance and employer attractiveness', *Business and Society*, 41:3, pp.292-318.

Turban, D. & Greening, D. (1997) 'Corporate social performance and organizational attractiveness to prospective employees', *Academy of Management Journal*, 40, pp. 658–72.

- motivate employees to work harder[45].

- reduce staff turnover[46].

- Create a tactical advantage over competition[47] by differentiation from competitors[48].

2.25 Meanwhile a bad reputation can produce the opposite effect[49]. Crucially, a threat to reputation has the potential to disrupt operations and destroy an organisation[50]. Security can be seen to play an important role in preventing incidents, which could damage reputation and ultimately destroy an organisation:

- in the context of data breaches, security failures have had a significant affect on reputation – research in the US found that where the breach was of customer data, 81 per cent of respondents felt it would affect the economic value of their reputation and brand image, on average diminishing it by 21 per cent[51].

- In another study[52], data breaches were rated third among those most likely to pose a major risk to reputation. And notably the two rating highest - non-compliance with regulation/legal obligations and exposure of unethical practices - were also security related issues.

- Negative publicity for a city, region or country is often due to a reputation for criminality or the mismanagement of crime[53]. Indeed, Porter[54] identified fear of crime as the key reason companies avoid or move away from city locations. Citing Belfast as an example,

---

[45] See for example: Greening, D. and Turban, D. (2000) 'Corporate social performance as a competitive advantage in attracting a quality workforce', *Business and Society*, 39, pp. 254–89.
Lievens, F. & Highhouse, S. (2003) 'The relationship of instrumental and symbolic attributes to a company's attractiveness as an employer', *Personnel Psychology*, 56, pp. 75-102.
[46] Caves, R. & Porter, M. (1977) 'From entry barriers to mobility barriers', *Quarterly Journal of Economics*, 91, pp. 421-434.
Wilson, R. (1985) 'Reputations in games and markets'. In Roth, A. (Ed.) *Game-theoretic models of bargaining*, New York: Cambridge University Press.
[47] Smythe, J., Doward, C, & Reback, J. (1992) *Corporate Reputation: Managing the New Strategic Asset*, Century Business Ltd: London.
Rayner, J. (2003) *Risk Management – 10 principles*, Elsevier plc Group, Great Britain.
[48] Coombs (2008) *op cit*.
[49] Coombs (2008) *op cit*.
[50] Barton, L. (2001) *Crisis in Organizations II*, South-Western College Publishing – Thomson Learning: Cincinnati, OH.
Coombs, W. (1999) 'Information and Compassion in Crisis Responses: A Test of Their Effects', *Journal of Public Relations Research.* 11:2, pp. 125-142.
[51] Ponemon Institute LLC (2011) *Reputation Impact of a Data Breach: US Study of Executives & Managers*, Ponemon Institute
[52] Economist Intelligence Unit (2005) *Reputation: Risk of Risks*, An Economist Intelligence Unit white paper sponsored by Ace, Cisco Systems, Deutsche Bank, IBM and KPMG.
[53] Gertner, D. and Kotler, P. (2004) 'Country as brand, product and beyond: a place marketing and brand management perspective'. In Morgan, N., Pritchard, A. & Pride, R. (eds.) *Destination branding: creating the unique destination proposition*, Oxford: Butterworth Heinemann.
[54] Porter, M. (1995) 'The Competitive Advantage of the Inner City', *Harvard Business Review*, May-June.

Bradley[55] argued that a city's long-term image is damaged overwhelmingly by a reputation for civil unrest and violence.

2.26 An emerging issue, impacting on reputation is the contribution businesses make to address corporate social responsibility (CSR). To an investor, companies with low CSR may appear to be a riskier investment, because this may be interpreted as an indicator of low management skill and an inability to obtain capital consistently[56]. Further, investors will expect increased costs from fines and legal fees for companies not acting responsibly[57]. Meanwhile organisations that operate a higher degree of CSR may experience a lower level of financial risk due to the links with government and financial bodies making them more resilient to external events and governmental changes[58]. Research is needed to consider if and how security can contribute here.

2.27 Given the potential benefits to a company of having a good reputation and the role that security plays in safeguarding reputation, this would suggest that the role of security is crucial to the success of a business. Yet again, the question remains, why this status is not recognised and promoted.

A culture of trust

2.28 Some criminal offences that affect organisations such as types of insider frauds are often directly linked to a lack of or breach of trust within the organisation[59]. Thus good security is in part about ensuring that there is a trusting environment whereby staff and clients share common values and uphold ethical and legal principles in the ways they conduct business.

2.29 Trust has been found to contribute to higher levels of staff satisfaction and where it exists it helps improve both internal staff relationships and

---

[55] Bradley, A., Hall, T. and Harrison, M. (2002) 'Selling cities: Promoting new images for meeting tourism', *Cities*, 19:1, pp. 61–70.

[56] Alexander, G., & Bucholtz, R. (1978) 'Corporate social responsibility and stock market performance', *Academy of Management Journal*, 21, pp. 479-486.

McGuire, J., Sundgren, A. & Schneeweiss, T. (1988) 'Corporate social responsibility and firm financial performance', *Academy of Management Journal*, 31, pp. 854–72.

[57] McGuire et al (1988) *op cit.*

[58] McGuire et al (1988) *op cit.*

[59] Levi, M. (2008) *The Phantom Capitalists: The Organisation and Control of Long-Firm Fraud*, 2nd edn. Aldershot: Ashgate.

Shapiro, S. (1984) *Wayward Capitalists*, New Haven, CT: Yale University Press.

Shapiro, S. (1990) 'Collaring the crime, not the criminal: Re-considering the concept of white-collar crime', *American Sociological Review,* 55, pp. 346-65.

those formed with clients[60]. This can lead to improved competency at work[61], facilitating a competitive advantage[62] for the business.

2.30 In short the absence of trust is a facilitator and even a trigger for crime while the presence of trust can be seen as essential for good business[63]. This is another way in which good security has broader organisational benefits[64].

2.31 However, there is another dimension to this. A good security culture can help prevent major threats from emerging, creating knock on benefits for a good safety culture, thereby preventing or reducing the likelihood of other hazardous events[65].

2.32 Some benefits from a good security culture in fact extend beyond good security as the second and last three items in this list indicate:

　I. Vibrant security regime applicable to entire workforce responsive to new threats (particularly insider threat);
　II. Improved chemical safety arrangements and lower insurance rates;
　III. Reduced across-the-board theft and diversion;
　IV. Better IT security and protection of trade secrets;
　V. Reduced risks of vandalism and sabotage by employees and outsiders;
　VI. Improved mechanism for personnel control and accounting under emergency conditions;
　VII. Better relationship with local authorities and the surrounding community; and
　VIII. Better reputation with host government[66].

2.33 There are other benefits to the creation of a trusting culture, as noted, for staff in terms of their enjoyment and productivity and perhaps inevitability their self worth.

---

[60] Driscoll, J. (1978) 'Trust and Participation in Organizational Decision Making as Predictors of Satisfaction', *The Academy of Management Journal*, 21(1), 44-56.
Tomkins, C. (2001) 'Interdependencies, Trust and Information in Relationships, Alliances and Networks', *Accounting, Organisations and Society*, 26:2, March, pp 161–191.
[61] Tzafrir, S. (2005) 'The relationship between trust, HRM practices and firm performance', *International Journal of Human Resource Management,* 19:9 September, pp. 1600-1622.
[62] Newman, J. (1998) 'The Dynamics of Trust'. In: Coulson, A. (ed) *Trust and Contracts.* Bristol: Policy Press.
Young, L. (2006) 'Trust: looking forward and back', *Journal of Business and Industrial Marketing,* 21, 7, 439−445.
[63] Gill, M. & Crane, S. (2015) 'The role and importance of trust: a study of the conditions that generate and undermine sensitive information sharing'. *Security Journal.* Secur J advance online publication, May 18, 2015; doi:10.1057/sj.2015.13.
[64] Burrill, D. and Green, K. (2011) *Value from Security*. Milton Keynes: Author House, refer to security as a 'trust enabler'. This is a helpful text in advancing the case for security as a business benefit rather than a cost.
[65] Khripunov, I. (2005) 'Nuclear Security: Attitude Check'*, Bulletin of the Atomic Sciences*, January/February, pp 58-64.
Khripunov, I. (2007) *The Human Factor and Security Culture*, Presentation to the International Council of Chemical Associations. The Hague, 1 and 2 November.
[66] Khripunov (2007) *op cit.*

Competitive Advantage

2.34 In many industries, gaining a competitive advantage to set themselves apart from others is crucial to the success of a business. Organisations therefore constantly seek to offer better value for money. As will be shown, the literature suggests that one way of doing this is through the use of security. Indeed security can have both a direct and an indirect influence on competitive advantage – both of which are considered in turn.

Direct influence

2.35 Security itself can be a factor, which influences customer decision making:

- In some industries (such as banking and hotels for example) companies must act to reduce risk to meet their own needs but also to match the level of security provided by competitors, because security can play a very important role in customer choice[67].

- Security accreditation schemes have shown that the benefits offered (improved security for customers offering reassurance of safety) helps to attract custom[68].

- Among the factors that make an area 'a good place to live' the most important are safety and security - well over twice as important as housing, green space, policing and education[69].

- Online shopping is another case in point, where security is a high priority for customers when deciding which company to buy services from. Here, security, privacy and trust were seen as the most common barriers to shoppers[70].

- Previous studies into online brand trust have indicated that security plays a vital role in the success of commercial websites[71], which in turn play a key role in generating and enabling sales.

[67] Rosmaini, T., Aliyu, A., Gafar, M., Abubakar, M., Lame, S. & Takala, J. (2013) 'An empirical investigation of factors influencing customer service delivery of ATM users in Malaysia: Kano's model approach', *Advances in Natural and Applied Sciences*, 7(3), 269+.

[68] See for example the Park Mark scheme - www.parkmark.co.uk/key-issues-for-drivers (accessed 2nd October 2014) and the discussion of Secured By Design in Armitage, R. (2013) *Crime Prevention through Housing Design*. Basingstoke: Palgrave.

[69] Beck, H. (2012) 'Understanding the Impact of Urban Green Space on Health and Wellbeing'. In Atkinson, S., Fuller, S. & Painter, J. (eds) (2012) *Wellbeing and Place*, Ashgate: Surrey.

[70] Alam, S. & Yasin, N. (2010) 'What factors influence online brand trust: evidence from online tickets buyers in Malaysia', *Journal of theoretical and applied electronic commerce research*, 5:3, pp. 78-89.

[71] See for example: Lee, M. & Turban, E. (2001) 'A Trust Model for Consumer Internet Shopping', *International Journal of Electronic Commerce*, 6:1, pp. 75-91.
Sultan, F., Urban, G., Shankar, V. & Bart, I. (2002) *Determinants and role of trust in e-business: A large scale empirical study*, MIT Sloan Working Paper, pp. 4282-02.
Ha, H. Y, (2004) 'Factors influencing consumer perceptions of brand trust online', *Journal of Product & Brand Management*, 13:5, pp. 329-342.

Indirect influence

2.36 Security can also contribute to other aspects of business in a way that can make them more competitive, by improving the service offered.

2.37 Crime prevention measures have been identified as resulting in 'collateral' benefits to business. In the context of supply chain management, Peleg-Gillai et al[72] found that the introduction of security measures to secure the supply chain improved aspects such as product safety, inventory management, supply chain visibility, product handling and customer service. They concluded that the changes improved operation, improved relationship with customers and ultimately increased profitability. As a result they felt that a different perspective of investment in security was warranted:

> *'We therefore recommend that companies not consider such investments solely as expenses that are required to meet government regulations and mitigate risk, but rather as investments that can have business justification, result in operational improvements, and ultimately may promote cost reduction, higher revenues and growth leading to positive ROI.'*
>
> *(Peleg-Gillai et al, 2006:29)*

2.38 This raises the question whether in other contexts (beyond supply chain management), crime prevention measures can positively impact on factors affecting the success of an organisation by creating a competitive edge.

2.39 In 2005 Sheffi[73] argued that organisations should not leave risk management and business resilience to specialists such as security professionals and instead adopt flexibility, agility and corporate resilience throughout the organisation to develop competitive advantages. Sheffi highlights the importance that security is embedded within organisations to protect it from harm. This includes "*security: layering, balancing, profiling, collaboration, culture and drilling*". In order to "*use security measures for process tightening*" to enhance competitive advantage.

Generating a profit

2.40 Taking the concept of competitive advantage a step further to direct profit generation, in the retail sector research has been conducted to consider how an organisation can profit by avoiding loss, specifically in terms of tackling shrinkage (loss of intended sales income due to theft,

---

[72] Peleg-Gillai, B., Bhat, G. & Sept, L. (July 2006) *Innovators in Supply Chain Security: Better Security Drives Business Value*, The Manufacturing Institute: Stanford University
[73] Sheffi, Y. (2005) *The Resilient Enterprise, Overcoming Vulnerability for Competitive Advantage*, MIT Center for Transportation & Logistics. See also, Burrill and Green (2011) op cit.

error and damage of inventory). Beck[74] reflects on previous findings[75] that loss prevention strategies add value to the business - if shrinkage is eliminated, profits could grow by as much as 62 percent. He notes this is:

> '*A remarkable statistic and one that any other part of the business would find utterly impossible to deliver.*'

2.41   Further, he notes that this 'powerfully persuasive message'[76] has been underplayed, but could be used to motivate the organisation to take the action necessary to prioritise reduction of shrinkage.

2.42   Looking beyond shrinkage, given that security is associated with preventing loss (due to crime) in an organisation, further consideration is warranted of the impact that the work of security in preventing losses has on profit generation, and whether the importance of that work is similarly underplayed.

Summary

2.43   Although it has not been very prominent, a search through current literature has provided references to ways in which security can be considered important to business beyond just preventing a crisis. The aim of the next section is to report on research designed to add depth and insight into the ways security adds value and to test out whether security can argue its case that it is a fundamental part of doing business as opposed to a marginal activity working on the periphery of organsiations.

---

[74] Beck, A. (2009) *New Loss Prevention: Redefining Shrinkage Management*, Palgrave Macmillan, p.133.
[75] Beck, A., Bilby, C. & Chapman, P. (2003) 'Tackling Shrinkage in the Fast Moving Consumer Goods Supply Chain: Developing a Methodology'. In M. Gill, *Managing Security: Crime at Work Series Volume 3* (pp. 195–212). Leicester: Perpetuity Press.
[76] Beck (2009) op cit, p 167.

Section 3.   Thinking about what security can do for organisations

3.1   This section reports the findings from one to one interviews and focus group discussions held with:

- Security professionals (n=46) - 30 clients (typically security managers for corporate organisation that lead an in-house security team and/or purchase goods and services) and 15 suppliers (leaders from organisations that supply security goods and services) and 1 academic.
- Non-security corporate departments (n=9) – Two were freelance consultants; of the remaining seven, six worked within an organisation that offered security services and one for an organisation that purchased security services[77].

3.2   This section is focused on understanding the benefits that security generates in the workplace, incorporating differing perspectives. The aim here is to get behind the headline grabbing references to 'value' and look in more detail at the nuances of what security can and does do. The aim is to highlight some examples, from the many we have been given, of the ways in which security can have an impact.

What are the barriers to recognising the benefits of security

3.3   Speaking to clients and suppliers revealed that the perception of security among senior management very much varies from organisation to organisation, and is often subjective depending on the individual:

> *I think this varies really wildly. Some managers really respond to it and say it is really crucial. Other senior managers see it as an encumbrance and a cost.*
> *(CEO, Security Supplier)*

3.4   That said, a number of interviewees noted that senior management (in particular) were increasingly aware of the significance of security in achieving organisational success:

> *I think the higher you go up the more they understand it. If you have a big bank or hedge fund then customers do care and security is critical to them to what they offer their customers.*
> *(Director, Security Supplier)*

---

[77] Roles included HR (3), Sales and Marketing (2), Quality (1), Finance (1), Facilities (1), and Operations (1).

> *I think we have come a long way in the last five years; there is such a high number of people that we are able to touch within the business now. The senior managers trust us to tell them how we are getting on and tell them how they can help.*
>
> *(Security Director, Construction & Energy)*

3.5 Despite this, it was clear that there remain a number of barriers to the full benefits of security being recognised.

3.6 It was noted that there was a temptation for senior management to use a somewhat simplistic evaluation of current levels of incidents to inform security need, signifying a lack of awareness of the broader and potential risks faced by the organisation:

> *If you haven't had an incident in six months then they will say why do we need it at all?*
>
> *(CEO, Security Supplier)*

3.7 It was precisely this view, that security was there merely to manage risks, rather than as an integral part of the organisation enabling it to operate legally and securely at all times that has driven the view that to be truly effective security should strive to integrate within the business, aligning itself with the main business objectives, and providing support and guidance on security issues to other departments. A number of interviewees commented that this does not always happen, and that a lack of integration leads to inadequate security protection and conflicts with other departments:

> *We are business people first. The business end comes first, the more you can integrate it into what you do, the better.*
>
> *(Resilience Director, Insurance & Investment Property)*

> *Security should be seen as integral as it would be to HR or Finance and I don't think it has quite the same level of involvement from the starting point as the other functions.*
>
> *(Global Security Director, Security Supplier)*

> *We have a corporate statement, and it does not include security but we protect the product for the patients and we are kind of under the covers, not really sexy, but important. No, in health care security is not taken seriously, with multiple activities it is not in the DNA of health care.*
>
> *(Chief Information Security Officer, Pharmaceuticals)*

3.8 One issue that cropped up time and time again, was that even when senior managers were on board, this may not filter down through the organisation. As a result staff may only truly value security when things go wrong and they need help:

> *Most often it is when things go wrong that they realise they have a professional service.*

There is often a block between management and staff. The managers will be security aware and talk amongst themselves but it does not often get passed down to the people on the shop floor.

(CEO, Security Supplier)

If they are doing ok they will not worry. The security is not that high on the agenda unless something happens.

(Head of Security, Banking)

Bad security is more of a disadvantage than good security is an advantage.

(Security Standards Manager, FM Supplier)

3.9   Certainly this point was validated by those in a non-security role. They thought that security was important in the workplace, but that it largely sits in the background protecting the organisation and ensuring compliance. While some thought it supported or enabled their work, others thought it would go largely unnoticed among staff in their day to day roles unless an incident occurred:

'Most of our security is access control – it does not really have much influence on my role or the business.'

(Facilities Director: Security Supplier)

3.10 Perhaps the most significant barrier identified to fully recognising the benefits of security[78], was that the value of those benefits cannot be accurately measured in terms of understanding the financial return on investment. It is hard for security departments to demonstrate the impact of the benefits their work has brought – particularly since it is impossible to measure the incidents that didn't happen. It can be hard to convincingly justify the spending on security and consequently, it may be seen as an unnecessary expense to be targeted for cuts:

It is always hard to show a return on investment. People may say why you are putting up these fences, why are there these cameras? How are they based on risk? And it is important for the managers to understand that risk.

(Security Director, Construction & Energy)

Then you come to the age-old questions always, which is deterrent you can't put a value on that. But it is a hard sell when all clients are worried about the bottom line.

(CEO, Security Supplier)

If it goes bad - it is obvious to see the impact on the share price. But when it is going well it is difficult to quantify.

(Global Security Director, Security Supplier)

We have been labelled silent achievers no one says well done as nothing has happened … if you were to ask what

---

[78] Also acknowledged by those in non-security roles.

was important about nothing happening, they would not say security.

3.11 In short, there has been a challenge for security in being recognised, this is in part because it can be difficult to present the case for security in pure financial terms, not least where the organisation itself does not define security as important, or where senior managers do but don't filter it throughout and down the organisation, where other business units don't see the benefits, or where a lack of incidents and/or an under appreciation of the risks means security is seen as more of a cost than a benefit. This is the context in which the range of benefits needs to be considered.

Preventing loss

3.12 It is perhaps an 'obvious' rather than 'additional' benefit of security, that it can prevent loss. After all, security is there to stop offences, regulatory breaches, or other unwelcome incidents that impact negatively on the organisation. But the feedback from the interviewees suggested that the losses prevented by effective security fall in to two main categories, each considered in turn, reputational and financial.

Reputation

3.13 While the concept of reputation is by no means regarded as synonymous with security (which supporters of security need to address), both clients and suppliers felt that protection of organisational reputation was a key benefit brought by security departments. Clients in particular viewed security departments as having a critical role to play in preventing damage to reputation (and the loss that ensues):

> *It is vital to reputation, the iconic brands are expected to have security, it was nice in the past but now it is essential.*
>
> *(Chief Information Security Officer, Pharmaceuticals)*

> *Reputation is critical, organisations live and die by their reputation. Security is critical to everything we do anything that risks it; monitoring threats being aware of the risk.*
>
> *(Resilience Director, Insurance & Investment Property)*

3.14 It was noted that expectation on security to prevent incidents is very high and there is a particular onus on eschewing a perception of incompetence:

> *If someone steals your data you are seen not as a victim but as incompetent, it has changed.*
>
> *(Chief Information Security Officer, Pharmaceuticals)*

People might not think as much as we would like them to [about security] but when something does hit the media it will get their attention. Then the security team are left to answer for it.

(Operations Director, Security Supplier)

3.15 One of the reasons security was considered so significant to reputation, was that damage to reputation is not necessarily proportionate to the scale of the issue or incident. Even a minor incident can have dramatic consequences and cause significant damage to reputation (and especially so, if the public are affected):

It does not have to be a large incident at all but if the media get hold of a very trivial matter. I would say any incident could have an impact.
(Global Security Director, Security Supplier)

It would not have to be a major incident to be serious. We had a petty theft of a device in a customer data centre and that theft was leveraged against us in negotiations with the customer; it happened just at the time the contract was coming up for renewal.
(Security Director, Data Storage & Management)

You never know how big it will need to be. It can seem minor but it can make a big splash in the newspaper. Especially now the financial services are seen as bad apples responsible for the financial crisis of 2008. A minor incident can be blown out of proportion.
(Head of Security, Banking)

3.16 Similarly it was highlighted that in certain sectors (the nuclear industry is a case in point) perceived as high risk, the public response is likely to be disproportionate to the scale of the incident:

Its reputation is critical. The word nuclear has an impact. The word nuclear and security incident is not a headline you want. It is disproportionate. The classic example would be if you had a breach of a fence of a gas power station you would get a significant reaction to that.
(Head of Security, Nuclear)

3.17 Now, more than ever, with the presence of not just physical threats, but also computerised and online threats, the potential for damage to reputation was thought to be significant and complex:

Historically security was about protecting the perimeter and certain internal aspects. Now everything is more integrated, that is threats and systems to protect. The impact of a mobile phone now is major.
(Senior Manager, Security Supplier)

> *'You may have confidential information online about clients. I think clients are certainly worried about data it is something people think about much more now.*
>
> *(Marketing Consultant)*

3.18 The modern day presence of social media was also cited as an aggravating factor that can quickly highlight weaknesses in an organisation:

> *If there is damage it will then go, these days, all over the internet. It will go viral and your competitors will want to see that this environment has been taken out. Particularly when you talk about high-end retail and jewellers and things like that. It is always in the news if you have one of your shops ram-raided or attacked which is bad for business. While before people would go away and chat about it, now it can go global in minutes if you have a major incident, so for sure, it is crucial.*
>
> *(CEO, Security Supplier)*

> *Visiting dignitary who is visiting at 5 o clock. Social media releases the information at half past 3. People turn up to protest. Not necessarily a serious incident but in real terms that can be quite impactive on the media image of the university. It can impact the reputation of the university.*
>
> *(Head of Security, Higher Education)*

3.19 Consequently, it was noted that security also plays a crucial role in responding both speedily and effectively when incidents do occur to demonstrate control over the situation and to enable business to return to normal:

> *If there is an earthquake or tsunami it is how well do our responses work and how well our business continuity plans are being constructed to be able to continue business as soon as possible. It is big things like that that would really affect our reputation.*
>
> *(Director of Security, Engineering & Construction)*

> *Reputation of security is based more on how you deal with it. You cannot always avoid something happening but you can control how you deal with it.*
>
> *(Security Standards Manager, FM Supplier)*

> *'If things are tackled immediately [customers] are reassured that they are safe. Public perception – it is in the interest of everyone to have good security.'*
>
> *(HR Consultant)*

3.20 To take this point a step further two clients highlighted that a good response to incidents by security, could even give a competitive edge, one by recovering quicker than competitors:

> *We had a hurricane impact on our business, and we were back to work earlier than other companies and we were helping agents and others as well. Indeed, one of our groups is so ready to react to crisis they see it as a potential competitive advantage; to be ready to react.*
>
> *(Vice President of Security, Insurance Services)*

3.21   The other (data storage and management), used their security operations centre to monitor global events, and were able to identify any issues likely to affect their suppliers and secure alternatives to ensure their supply chain, thus creating a commercial advantage over others who did not have this foresight.

3.22   The process by which security can best minimise negative impacts on reputation is interesting not least because it highlights once again the varied ways in which security relates to the business. Examples were given of processes developed by the organisation that merited a security mind being applied to them. One example, and a key area was in defining procedures to protect confidential information (such as personal data, financial data, intellectual property):

> *A large part of a security team's role is to play the guardians of reputation and the guardians of acting with integrity whether that is protecting or drafting policy.*
>
> *(Global Security Director, Security Supplier)*

3.23   Another pertinent example is that provided by a security manager describing how his department was able to create a better solution for recording data, that reduced the likelihood of damage should a loss of data occur:

> *In one area doctors were using their social security number as a business ID, it is the doctor's individual number and that connects to loss of personal information and this could be abused if it got into the wrong hands. We were worried that as this was on our database, should that be compromised we would be accused of having put doctors at risk. Now encrypting that database was going to cost millions, so I said let's just buy them a licence. I mean it is much cheaper. If you have data you have to protect it, so think instead what if I don't have the problem in the first place.*
>
> *(Chief Information Security Officer, Pharmaceuticals)*

3.24   The input of security was considered important in other ways, in managing the broader conduct of staff (including security staff):

> *A major high profile issue, the appearance that people that work for us do not follow our values and code of conduct could really damage our reputation. That could affect share price. We need to make sure that from a security perspective companies that we use to support us*

are working within the values, code of conduct and protocols. We need to make sure they understand that and that they are trained with that so that they can represent [us].

(Security Director, Construction & Energy)

3.25   Another aspect of reputation, which security was considered important to maintaining, was that of confidence in the organisation. It was highlighted that you could have an excellent product, but if customers do not believe they or their information or belongings are safe, this can make or break whether customers and investors are attracted and retained, ultimately impacting on commercial success:

Our staff, the people we are helping, our donors; they can all lose confidence. If security is done in the wrong way it can have an immediate effect on the reputation.

(Regional Security Advisor, International Aid)

It impacts on your reputation and it will impact on the client expectation if you do not have that capability and credibility.'

(Financial Director: Security Supplier)

The students and the staff need protecting. That is the most important reputational point for the university as a whole. I think if it is articulated no one would argue with that.   If someone was getting hurt here and it was happening on a routine basis would you send your kids here?

(Head of Security, Higher Education)

3.26   The issue translates to less commercial settings too (e.g. healthcare), and, for example, to the importance of having a reputation for good duty of care and tight controls on patient confidentiality. Security has responsibility for the protection of often vulnerable, high-risk patients and their confidential information. Incidents such as leaking of information about a high profile patient, and child sexual assault on a ward were cited as examples that would seriously affect the reputation of a hospital:

We would have lots of investigations and it would be in the press. This would affect the services and the commissioner. It could affect the money flow- staff– recruitment and retention. If we have an incident of patients absconding and committing suicide by jumping under trains there are serious case reviews. The most important thing will be a around care and abuse of patients.

(Security Specialist, Healthcare)

3.27   One security manager (food manufacturing) argued that not only can security provision prevent internal losses, but it can have a knock on benefit for clients, by protecting the reputation of client's brands:

> *We contribute to the band protection. Some of our clients come to us and they like AEO and CTPAT, where we can demonstrate that not only are we saying we have sound programmes but we can show it through Government certification of our assets. This shows that their brands, these big brand names we supply to, will feel protected.*
> *(Director of Security, Food Manufacture)*

3.28   Looking beyond the issue of reputation, we now turn to consider in more detail, how financial loss in an organisation may be prevented by good security.

Financial

3.29   It was evident that a key benefit of security is to prevent the losses associated with incidents of crime by managing risk. Interviewees pointed out that ultimately this has a close link to the financial 'wealth' of an organisation:

> *If [security] was not there, it would cost us a lot of money.*
> *(Head of Security, Nuclear)*

> *It definitely protects what we have got.*
> *(Financial Director: Security Supplier)*

> *Our whole core is to support their business and make them money. If we do a good job or if we allow security to lapse it will affect the bottom line.*
> *(Director, Security Supplier)*

3.30   But it also involves physically protecting the payment process so that it is robust:

> *If there are cash payments to be made to vulnerable people in vulnerable areas we will be involved in ensuring that they get the money.*
> *(Regional Security Advisor, International Aid)*

> *Ad hoc requirements, say a bank cheque is questioned, we would help investigate that or figure out what to do. Also if we send a company a payment and they say they have not got it we may find out where payment is mislaid.*
> *(Director of Security, Energy)*

> *We [assist] in vetting certain clients and in certain acquisitions and in managing some vendor issues or managed service partners, those groups operate around the world and we investigate whether they operate well and in line with our principles.*
> *(Vice President of Security, Insurance Services)*

> *Making sure [the organisation] bid on work smartly.*
> *(Chief Security Officer, Security Supplier)*

3.31 But other ways of preventing financial loss were also reported. Security could provide information from its systems that corroborated or negated insurance pay-outs. Similarly, examples were provided that illustrated the savings that could be made by reducing the likelihood of incurring fines and penalties for non-compliance with a range of requirements:

> *Security lessens the liability that comes with fines for regulatory breaches, which then can create a loss of confidence. There are potential fines for compliance failure so a poor security posture could put the company at risk either of fines or extra oversight, which would make producing power more expensive. In a competitive market that can be damaging.*
>
> *(Director of Security, Energy)*

> *[The regulator] may look and see a data loss. The fine will be 5-6million. The regulator will come in and the fine will be significantly higher without having robust security.*
>
> *(Resilience Director, Insurance & Investment Property)*

3.32 Another security manager detailed how security expertise in responding to incidents/scares has potential to reduce losses and impact:

> *If you have a 2 minute investigation period you want the security team to get to the point quickly and schedule the evacuation before then. With the right training the right individuals in place you can. Somebody not so well trained would think "we need to evacuate" and cost you millions or serious danger to staff.*
>
> *(Head of Security, Professional Services)*

Enhancing success

3.33 The views of both clients and suppliers suggested that while security is not traditionally viewed as enhancing success or generating something positive, it is in fact capable of doing just that. Attracting, expanding, and retaining business were all key areas for company success noted to be generated by security, and it is to these aspects that we now turn our attention.

Attracting business/ sales

3.34 Conventionally security has been seen as something that an organisation may not wish to draw attention to when marketing a product or service. Indeed, some of those who noted security has a key role to play alluded to the fact that important as it was it 'just can't be

advertised'. This is because the need for security, could be interpreted negatively[79]:

> *If you are going into a jewellers, for example, high end retail and it is all bars and shutters and you have four big guards on the door a lot of people would be very nervous about going in there but because, crikey, you know, "why do you need all this?" So a lot of time we need to have it as a sort of soft cell merging into the background … it is not a case of big sort of sales tool for sure. It is much more of a necessity than a glamour item.*
>
> *(CEO, Security Supplier)*

3.35 Yet interviewees provided a number of examples where they considered the standard of security at an organisation to be a very effective sales and marketing tool, capable of attracting business. It was evident that there are a number of ways in which it can affect customers in their decision making process.

3.36 When choosing between an organisation and its competitors, it was clear that the reassurance offered by security in providing for a safe environment can be a deal maker. The following examples illustrate the point:

> *Profit is not the main aim of a university but the safety of an environment and the friendliness of an environment is clearly an important factor for potential students and parents. A nice safe environment will help attract lots of students.*
>
> *(Head of Security, Higher Education)*

> *The security posture at HQ is that we sublease most of the building but part of the sales pitch that real estate use is the security … is better than others in town and indeed the tenants took the space because they had confidence in security.*
>
> *(Director of Security, Energy)*

> *In the tender documents they would have sections on security and we would need to provide evidence of the security service we can provide. It is an insurance measure for the client. Those kind of issues can determine if you are picked for the project or not.*
>
> *(Director of Security, Engineering & Construction)*

> *[Marketing] can use our information and the marketing people are always looking for new angles to convince people that our bank is best, so security is a very important element … We may do a radio interview or organise a public discussion on security issues such as fraud.*

---

[79] This point was also raised by those in a non-security role.

3.37 One security manager noted that this could go beyond simply beating the competition to the business, but could even enable the organisation to demand higher fees than their competitors:

> *Savvy companies will use security as a leverage. In some cases if you don't have security they wont do business so security becomes a part of the requirements to do business. In essence they are asking us to state and show we have the basics in security in place. So basic security overall and a basic supply chain security programme and employees safety and requiring us to attest to these as part of the deal. They use this as a negotiating position. So they say if you don't have this or that we should pay less. I have done this myself in the past. Our aim was to find some flaws in security and use that as an argument to pay less.*
>
> *(Security Director, Data Storage & Management)*

3.38 Some noted that security accreditations showed how security was being taken seriously. In another way, security provided reassurance and enhanced the customer experience:

> *Museum visitor numbers reduced when there was a threat. We took away bag searches and some visitors complained. If they don't feel safe then they will vote with their feet … Bag searching does not have to be a bad experience. We did it with sniffer dogs and initially people thought it would put people off and in fact it worked and people got through quickly. You can change the profile of security so that people are pleased that you have it.*
>
> *(Security Director, Museum)*

3.39 One organisation shared customer survey results which measured how important a range of factors were in their choice of service provider. Security (78%) scored notably higher than cost (63%) in eliciting a strong rating ('very' important) although overall both were valued[80]. Almost all respondents valued security, with a very large majority indicating that security was 'very important'.

3.40 The importance of design to security has long been recognised and these points were reinforced here. In a similar way it was highlighted that building security in to an operation/service (thus making it quicker or more effective) can also be beneficial:

> *There are commercial benefits including expedited processing for imports and also enhanced commercial*

---

[80] In total, 92% scored security as important (either 'very' or 'fairly') and 93% scored cost as important (either 'very' or 'fairly').

relationships with customers. It sets out our company as a leader in that space in supply chain security.
(Director of Security, Food Manufacture)

We win a lot of business over many international organisations we need to demonstrate that we can offer the right level of duty of care. We need to demonstrate that security gives us an advantage.
(Head of Security, Professional Services)

3.41 In a similar vein, examples were given of how the security department supported the marketing department with events to promote their new products, maintaining the security of the product both before and during the event, which was critical for attracting customers.

3.42 A security manager highlighted how the resilience and recovery afforded by good security could be a distinct advantage in retaining clients, and could be used as a selling point:

If we look at data hosting. This is one area where having a strong security footprint of limiting the number of incidents and making the right mediation [is important]. That helps us win business. A couple of years back there was extreme flooding, we were able to get up and running and get products back in the market much quicker than the competition.
(Vice President of Security, Technology)

Expanding business

3.43 Clients in particular highlighted that a security function could be critical to enabling an organisation to expand. Their role was particularly pertinent to enabling growth into potentially hazardous environments. Security departments could assess whether there was merit in pursuing the idea (based on assessment of risk), and determine the level of security required to ensure safety:

Part of it would be we are putting a toehold in Africa we have to analyse if it is reasonable to do so. It is not in the forefront of everybody's mind but without security we cannot expand the business.
(Resilience Director, Insurance & Investment Property)

We work in Iraq and Afghanistan because the company can accept that the level of risk is extreme and the rewards of being there are very good in terms of the cost and earnings. Therefore we have the right balance between the minimum possible security we need to apply to ensure safety versus what it costs to supply that.
(Director of Security, Engineering & Construction)

> *We provided a very strong intelligence around world events and emerging markets and we let them see that. So we are 'go to' people for areas they are looking to do business. Without security they would be operating blind. We offer the floodlights. Sometimes we protect them from themselves. We want to ensure they are safe and the company wants to know that too.*
>
> *(Director of Security, Food Manufacture)*

3.44   It was also apparent that enabling operations in dangerous environments could further increase the profitability of the company, where this meant they were a step ahead of the competition, who did not apply security in the same way:

> *They are closed on Saturdays but our bank was the only one working in that environment. We look at it on the upside, if we can put something in place we can capture all those customers, it costs extra to operate on a Saturday but the return will be double without exposing our staff and customers in harms way. Soon competitors will start to open their branches on a Saturday when they find out how to make that work. But we have had the advantage until then.*
>
> *(Head of Security, Banking)*

Retaining business

3.45   Of course, businesses are concerned not only with attracting custom, but with retaining it. Security can play a part in satisfying customers and strengthening client relationships.

3.46   Some clients highlighted how security provision enabled their customers to save money (good security enabled more effective use of staff for example), thereby providing the type of added value likely to increase the chances of retaining their business:

> *Some customers did away with staff at helpdesks because of the faith in our security processes; they had confidence in not having to have people mulling over claims.*
>
> *(Security Manager, Communications)*

> *There were 30 customers who were significant enough, big enough, coming up for tender, and a proportion don't see any value in security. But of those who open the door we have an opportunity to sell security. One in particular, we talked about our security so we could show what security does and how it adds value to the customer. We could show how security with us did help them save money.*
>
> *(Security Manager, Communications)*

3.47 Other security managers reflected how sharing their security expertise and intelligence with client companies gave added value that strengthened their relationship:

> *There are things we can do. But it is not a benefit we would expect. You have a client based in India and he wants to invest in Bangladesh we can help them. We can give them intelligence, a geo breakdown of Bangladesh where we believe there will be secure investment. It works for the vast majority of small to medium clients. For private clients of high net worth may really value our advice. It does not work for every client. It is all about relationship making.*
>
> *(Director of Security, Banking)*

> *Continuity and trust is really important, security provides for that level of trust. I may travel to a supplier and meet with the owner and manager and help them with security and help them improve their processes. This helps us and the security of our supply chain, and the supplier benefits in the way it does business and this is all free of charge.*
>
> *(Director of Security, Food Manufacture)*

3.48 Making all staff security aware was another way in which interviewees felt they added value for the customers:

> *The whole security awareness for our own and the training we have provided. All of our receptionists are bundled with security so first impression to clients. The security and reception is a crossover and that add values.*
>
> *(Head of Security, Professional Services)*

3.49 Looking at customer satisfaction, interviewees observed that a competent and experienced security provision will have an impact on the customer perception of efficiency of the organisation as a whole. Good security will make all aspect of the organisation run smoothly and clients will value and retain contracts with a non-security supplier that is perceived as competent on security matters:

> *Good security will reflect in customer image of efficiency. It is about the bigger picture rather than just security.*
>
> *(Security Standards Manager, FM Supplier)*

> *Security presence can improve the overall service customers receive, which will improve the likelihood they will visit your hotel or shopping centre again over the competition.*
>
> *(Security Standards Manager, FM Supplier)*

> *'In retail, security is as much about customer service as it is about security itself – so that can add to the customer experience.'*
>
> *(National Sales Manager: Security Supplier)*

Operational success

3.50   In addition to the overt ways that security can impact on the avoidance of (or reductions in the amount of) loss as well as generating gain, interviewees reported a myriad of other ways in which security supported and enabled the smooth running of a business. We now consider how security is a 'general' enabler to business by engendering 'trust'; how it helps to provide for and show support for staff; and how it contributes to corporate social responsibility.

Enabling Trust

3.51   Overwhelmingly, the role of security was described by clients and suppliers, as one of enabling the efficient operations and running of a workplace by preventing and/or resolving disruptions. Indeed, this was also the main facet recognised by those in a non-security role. Examples included:

- supporting/advising employees and/or customers accessing and navigating the building/site
- facilitating flexible working hours (security presence means staff can safely stay on to work when they might otherwise be vulnerable such as at night)
- relieving employee concerns about safety issues when travelling
- responding to customer concerns about being able to supply goods and services in an emergency
- providing an effective first response when problems occur - at the lower level this might be a security officer dealing with broken equipment, at the upper level it may mean a security director providing advice to the board about how to respond to a major disruption to the business
- tackling issues to prevent escalation (which would otherwise disrupt operations)
- ensuring compliance with policies and procedures (which if ignored could lead to compliance breaches, or otherwise be dangerous and/or disrupt operations.

3.52   Clients highlighted benefits in security solving problems, and these could be quite varied. At its core was the need for security itself to be trusted:

> *One thing we tell folks, if they are having problems with boyfriends, they can tell us and we hold those trusts very closely. People will tell us because we have a culture of looking forward to prevent problems not just security.*
>
> *(Director of Security, Healthcare)*

Whereas I am trying to build the reputation of security where we are seen as more a partner, tell me your problem and I will sort it out, bringing people into the fight against threats.

(Director of Security, Energy)

We have business relationships going back over a century and with generations of families and employees and we have managed these closely. Continuity and trust is really important, security provides for that level of trust.

(Director of Security, Food Manufacture)

3.53 Trust it was argued was generated in another way; in keeping the organisation honest. At the lower level this involved ensuring basic rules were followed (be they security related or otherwise), and at the upper level by contributing to the generation of a trusting and co-operative environment which made rule breaking and dishonesty less likely and anyway easier to identify. This though necessitated security be seen as a supporter and friend rather than 'a policeman':

The level of trust within the organisation will suffer if security has to be overly aggressive with some departments over security issues.

(Security Standards Manager, FM Supplier)

3.54 There were at least three (overlapping) principal components in setting a context of trust that were re-iterated time and again in interviews. First, security had to be effective at securing the organisation but doing so in a way that put people at the forefront of any strategy; presenting a professional and courteous image – with staff but not least with clients and customers – was crucial:

That is one of the most important things. If people don't trust the bank they are closing their account and moving their money somewhere else. We will go down the drain. In the financial sector this is so important. Would you bank with a financial institution you don't trust?

(Head of Security, Banking)

I think the customers perceive this in a number of ways even when it comes to something like a fire procedure if it is done professionally. If you are a customer in the middle of your meal and everyone knows exactly what to do and they take you through to the correct place and you are in and out very quickly it is all dealt with very well and people actually think "yes that was handled really well throughout".

(CEO, Security Supplier)

'The knowledge that everything is safe and secure. It has an effect on the approach employees have with customers. Our approach gives clients a high standard of service … It is very specific client to client but without that

basic promise our relationships with clients will not have that trust.

<div align="right">

(Financial Director: Security Supplier)
</div>

3.55   Second, security needs to generate competitive advantage (in making profits of course but also in enabling operations to be conducted safely as noted above), with that comes respect from colleagues. This was frequently seen as the quintessential criteria for generating trust internally and externally:

> *I may travel to a supplier and meet with the owner and manager and help them with security and help them improve their processes. This helps us and the security of our supply chain, and the supplier benefits in the way it does business and this is all free of charge.*
>
> <div align="right">

(Director of Security, Food Manufacture)
</div>

> *They put measures in place to respond to Ebola … So they send people out into the field. But in one area they did not prepare for their arrival, they just showed up and the locals killed some of them. The staff there did not understand that you have to get the elders on board and that only then can you deploy. In security we emphasise that you need to do the advance work. People get killed because of a lack of preparation.*
>
> <div align="right">

(Regional Security Advisor, International Aid)
</div>

3.56   Indeed, one point that came across strongly among non-security interviewees was the importance of security as a trusted advisor for issues affecting staff safety.

3.57   In security generating trust frequently entailed working with others. In some cases security departments work together when colleagues in other departments are prevented from doing so such is the level of competition:

> *One of the reasons we collaborate on security where other disciplines are worried about competitor advantage is because if something happens to my consumers' brands and we are say both selling pepper, they don't stop buying my brand or their brand they stop buying pepper. We need to protect the product, I want it to be tastier etc but that is not my job.*
>
> <div align="right">

(Director of Security, Food Manufacture)
</div>

> *Because our competitors have just as big a security department, I am not in competition with other companies about security. We have forums and we are constantly looking at how to share information. Criminals will try and get all of you. They would then think let's see if we can do that to another bank.*
>
> <div align="right">

(Director of Security, Banking)
</div>

Staff wellbeing

3.58   The interviews confirmed the point noted in section two that security made an important contribution to the wellbeing of staff, and further in supporting Human Resources in their duty of care for staff. It did so in at least three ways. First, it was noted that by providing a secure environment for staff, it attracted new staff to want to work with them and retain the good staff they had. One key factor raised here was ensuring that security protected people which was deemed especially important when they were vulnerable. Sometimes this might require security action against a specific threat such a spate of robberies or assaults on staff. Sometimes the vulnerability evolves from factors such as lone working, remote working, working out of hours or working away from base and sometimes in difficult or unfamiliar territories:

> *Out of hours working where security is very important for people. Security will deal with any problems.*
> *(Head of Security, Professional Services)*

> *When employees are travelling we track events and if there is a major taxi strike in France we will tell them. If on vacation we will help them with information if they ask and need us.*
> *(Security Director, Data Storage & Management)*

> *Security is about preventing loss but it is also about creating an environment in which people want to stay, and any help that company can get in reducing turnover is a big contributor to cost savings.*
> *(Security Manager, Retail)*

> *We are good at getting in and managing the threat and getting life back to normal so it does not spread. Manage incidents and contain them so they do not spread, that is key.*
> *(Security Director, Data Storage & Management)*

3.59   Second, security was deemed important in acting quickly to remove or nullify negative workplace events[81]. In one case where staff dealt with sick and dying children security had a role to play in minimising the impact on staff by removing bodies speedily after death and this had to be done sensitively. There were more, less extreme, examples:

> *We had a situation in one of the US factories were there was negative graffiti – racist. We investigated it and found who was responsible and restored a positive environment.*
> *(Vice President of Security, Technology)*

> *If someone has property stolen it lowers moral if we can minimise the risk then it increases staff moral and their perception of safety.*

---

[81] This was an issue also raised by non-security staff, particularly those in an HR role.

We keep toxic issues out, so we can hire and retain better people.

3.60 Third, by providing workplace support there can be additional advantages for staff at home[82], and vice versa. Interviewees gave examples where security training at work had helped people at home from such varied topics as First Aid, internet awareness and security, self defence to how to deal with conflict situations. But there were other ways security helped too:

> *We have protected employees when the threat was nothing to do with work, but clearly they were worried, it sends out a message that we protect our staff … we will provide counselling, sometimes financial assistance, we may engage others like clergy, psychologists so that the employee is helped. There is no set budget, the aim is do the right thing.*
>
> *(Director of Security, Food Manufacture)*
>
> *Domestic violence was discussed because it is a cause of workplace violence, it can spill over from home to work, and we discovered some people who had suffered and needed help, and we offered them advice and sometimes counselling so it has other benefits.*
>
> *(Vice President of Security, Insurance Services)*
>
> *We will support them wherever they are in the world and security is part of doing that. We provide Apps to help them assess security in their country and so we are part of the package, this is about attracting staff. We also do the families so they are supported.*
>
> *(Security Group Head, Insurance Services)*

3.61 Running through the responses on this issue were a range of comments that alluded to the point that security work of this kind directly contributed to the bottom line and in a variety of ways, and many not obviously tangible. One interviewee recounted a situation where nursing staff were encouraged to leave as soon as their shift was finished because they had expressed concern about leaving the premises when it was dark. The problem was that it led to working inefficiencies not least the poor briefing of the following shift. Security staff assessed the situation and by providing reassurance and support, and some additional lighting they facilitated a more effective handover and staff were happier and care for patients was improved.[83] Some other examples include:

> *My theory is a safe and working environment allows for a full focus on work,*

---

[82] This issue was also highlighted by those in a non-security role.
[83] We would like to thank Dr Mark Siegel for his insights here.

If they don't feel safe they will be in a negative state of mind that may mean they wont be able to do their job.

(Regional Security Advisor, International Aid)

Reduce incidents and injuries to staff, which will also reduce staff absence from being off with stress, or injury. This is how to reduce the cost of staffing.

(Security Specialist, Healthcare)

We can save lives. Being clear about important issues of security and personal safety means everyone can understand what needs to be done and that makes a happier and more productive work force.

(Chief Security Officer, Security Supplier)

By us removing a lot of the impediments you might see, we let people focus on work, and they don't have to be concerned about peripheral things, and let's get them focussed on their jobs. It seems mundane but it is not hard to have a toxic environment, one arsehole or bully can become a major distraction and we work with HR on this.

(Vice President of Security, Insurance Services)

3.62   The last section discussed the importance of effective workplace cultures generally and security cultures specifically in generating business benefits. Many interviewees highlighted the importance of security in supporting staff wellbeing in generating these, as one interviewee summed up, 'it shows that the company cares'.

Corporate Social Responsibility (CSR)

3.63   Encouragingly the interviews were again replete with examples of ways in which the role of security enhanced an organisation's commitment to effective CSR. There were five ways in which security contributes. The first drew a focus on the ways in which good security is synonymous with CSR by ensuring that the workplace does not become a magnet for vandals and thieves avoiding the 'broken windows' syndrome; where a broken window breeds another and another generating an impression of an environment which is uncared for commencing a spiral into a decline where crime is commonplace:

If you have a collection of buildings that has good security it will lower crime and that brings people in which helps the business. It also makes for a safer environment.

(Director of Security, Energy)

I belong to numerous crime prevention associations. I would say it is beneficial for the local area. Enhancing security in your own office it has a knock on effect for the local area.

(Head of Security, Professional Services)

3.64   Overlapping this, the second set of answers highlighted the role of security in building up information and intelligence about security which could be passed to the community to help it better protect itself, or to other agencies such as the police to help them protect community members. It was noted that liaising with other organisations generated both opportunities to practice CSR by offering help of some kind, but was also good for business in building up contacts. A security manager at a university gave the example of how the university is pooling its security expertise with the police and government to address a serious national issue that also affects their students.

> *In [place] there has been a marked rise in rape and serious sexual offending on people aged 18 to 24. As a result of that we are working with students and external agencies to get a fresh approach in dealing with that and heighten awareness to keep people safe. We are devising something that should be usable by other universities if they chose to use it. This is in association with the police, the rape crisis, the student representative bodies, [and the] violence reduction unit in [the] government are (sic) involved.*
> *(Head of Security, Higher Education)*

3.65   There were other examples too:

> *We open up some of our expertise to the local community with things like personal security, we open that up to maybe the pupils or parents of the school and get them involved.*
> *(Global Security Director, Security Supplier)*

> *We take part in that in the area of preventing financial crime. We provide statistics about telephone fraud and we will discuss it openly. Via Internet media, radio, tv we would never refuse the opportunity to talk about it. And the telephone fraud incidents are on the decline. We also talk to neighbours and competitors to keep the fraud under control. Being open and transparent and talking about this problem is a big part of social responsibility.*
> *(Head of Security, Banking)*

> *If people are say setting fires in Brazil, we can provide information if you know about fires, and you can make links, private security may see more data points that can be linked much more than Government. Hacking is another one, we noticed what the Chinese were doing. We noticed and the Govt were not acknowledging what was going on and we found out the details for ourselves.*
> *(Chief Information Security Officer, Pharmaceuticals)*

> *We have done work with charitable organisations that need security advice we offer that pro bono.*
> *(Head of Security, Professional Services)*

3.66 The third focus, moved from providing information and intelligence to providing specific security-related services. It was noted that there were benefits in living near an organisation that was low crime where there was a diffusion of benefits from the work place to the local community as discussed in the last section. More specifically, corporate security guards can provide a point of contact for local residents and businesses. Security officers at manned operations can be available 24 hours 7 days a week to offer support and assistance in the local area in the case of an emergency.

> *We are involved with … law enforcement who can use our cameras if something is going on.*
>
> *(Director of Security, Food Manufacture)*

> *We will respond to incidents in locality – officers have training in first aid – assisting people - that has nothing to do with the business.*
>
> *(Security Director, Museum)*

3.67 Fourth, security can play its part as a corporate function in supporting communities in the ways other parts of the corporation may do. One interviewee noted that it has pursued a policy of the use of environmentally friendly security equipment following a strong corporate line on such practices. In a different way this may include the security department itself and/or its partners and contractors recruiting from the local community and also targeting disadvantaged groups to offer a form of support. Both clients and suppliers noted that security can be a labour intensive task requiring a high volume of casual workers:

> *I am thinking about solar powered CCTV cameras; wireless video signal transmission rather than wires in the ground; solar and crank powered FM radio because if all comms go down we can still listen to national news which you can also use to charge mobile phones; it is mostly about solar. This is an area where there is a need. Green security solutions also makes donors happier and may even make them more willing to give funds.*
>
> *(Regional Security Advisor, International Aid)*

> *We do a lot of recruitment from the local community we try and target and work with the local community to train up people that have been out of security for a long period of time. In giving jobless people the training and the licencing required.*
>
> *(Global Security Director, Security Supplier)*

3.68 A security manager for a South African bank took this a stage further and encouraged a member of staff to start a security company:

> *We had one person not fitting in – the company proposed, we will set you up to start your own company – help set it up, apply for loan – walk with you all along –*

> *today that company is still existing – they have gone from guarding and armed response, created jobs for others, and now in installation and technical.*
>
> *(Head of Security, Banking)*

3.69   Finally, there were some extreme examples - in developing countries - where the role of security included supporting communities to protect themselves in the immediate term but in making this sustainable. In a different way, where companies outsource to countries the security department may visit not just to risk assess operations but also to build up expertise there so that there is sufficient faith in the ability of the organisation to continue. For example:

> *Human rights are an issue if we were in a location were the military or police have the right to secure the site. They are usually very poor so they will abuse local communities. We make sure we ensure the training is there for the local authority so they are not a risk. The military wanted to build a barracks there as it was part of their infrastructure. We engaged with, negotiated with the government and persuaded them not to do that. There would be all sorts of problem for the local people if they had.*
>
> *(Director of Security, Engineering & Construction)*

> *We use outsourced manufacturing of laptops to places like China and Malaysia in those areas looking at corporate social responsibility. So certainly one the things we do is get involved in supplier audits. We go out with our security department and we will help them do supplier audits. That it will help with the standards for workers.*
>
> *(Vice President of Security, Technology)*

Moving forward: communicating the benefits

3.70   A key theme running through the answers – across samples – was that the benefits of security need to be couched in terms which recognises that there are both different roles for security in organisations, and that whatever role security adopts it needs to be effective in order for benefits to be generated and recognised.

3.71   In one focus group discussion it was noted that security personnel can be and should be ambassadors for their employers and the security contractors they deploy. Only some believe that current security leaders are generally equipped to fulfil that role effectively. So what other factors are deemed important in presenting security as a benefit?

3.72   Where security leaders are seen as ambassadors for good security practice then security is more likely to be appreciated. Where there are metrics that support that, this makes the broader aim of showing impact

all the easier. At least it does if the metrics are meaningful[84]. Some of those taking part in the research felt they were ahead of the game:

> *One of the things we want is a security scorecard for all operations which our senior management can look at. So we can see how we are doing on security. That is happening in safety and environment in terms of performance and we thought security could do the same thing. That was sponsored and suggested by senior management.*
>
> *(Director of Security, Food Manufacture)*

> *I think through the communication and the information that we can now show these guys when we meet with senior managers and go to business shows they can really appreciate what we do.*
>
> *(Security Director, Construction & Energy)*

3.73 While this is not the place to dwell on the sorts of security metrics that can be helpful, in one focus group discussion those present pointed to the number of taxi bookings made (for staff at night), and the number of medical emergencies they attended and the role security played; easy to relate to statistics such as this can be impactful at high levels in the organisation. A security manager for a delivery company argued that in the past negative publicity was measured and valued in terms of its effect on the reputation of the brand:

> *We used to measure negative media space and the communication teams put a value on it, its eroded but it is being asked about again. If we had a major loss of customer information then you can imagine that would impact on share price or brand. We are not good at talking about, let alone measuring, positive impact on reputation.*
>
> *(Security Manager, Communications)*

3.74 Generating a good feel about security is in part about communication. Clients and suppliers highlighted the value of newsletters, training staff in security awareness, and having meaningful and helpful engagements with staff during routine activities. Where organisations build security awareness and practices into staff roles across the organisation it heightens interest in and appreciation for security. The importance of 'integration', not as a technical term but as a process of making security a part of business operations was re-iterated in interviews. If the traditional role of security has been to be a secret department on the edge of activities there was more evidence here that over the years it has metamorphosed into one that is at the heart of every process and activity. For example:

---

[84] See ASIS (2014) *Persuading Senior Management with Effective, Evaluated Security Metrics,* https://foundation.asisonline.org/FoundationResearch/Research/Current-Research-Projects/Pages/Metrics-Research-.aspx

The idea of making sure each business leader or individual is responsible for security in their area. Security staff can't look after everyone all the time. Each and everyone is responsible for the risks in his or her environment.

(Head of Security, Banking)

Getting staff engagement in security was always key, and the best ways of doing this are to have simple messages that people can understand and follow. It is better done by a store manager than a security person who can communicate in the terms staff will relate to. So security can add value by being able to engage non security people.

(Security Manager, Retail)

3.75 What is not in doubt is that security is seen to have a lot to offer. While it is unsurprising security interviewees said that good security will be met with support and enthusiasm from other able professionals, this view was supported by inputs from professionals in other roles. The key things that emerged from the interviews were that: often little is known about security and what it can and does offer and more needs to be promulgated; often there is a view that security is a given rather than a positive – 'unremarkable', 'discreet', 'normal' - and that maybe in part because positives are not articulated; sometimes there is too greater association with negatives rather than positives:

'I don't think there are any [negatives] – if its done in the right way. The issue HR could have would be surveillance – they are already seen as big brother, so anything that contributes to that would hinder – if surveillance was used against staff.'

(HR Consultant)

3.76 Participants in this study noted that one of the main limits of security was its inability to sell itself – and this of course was one of the main points of the research and somewhat confirms the point. It was noted that technology and social media affords security the opportunity to engage with the organisation and its stakeholders more directly and meaningfully but this was only just beginning to be exploited. One interviewee noted that security is the 'classic insurance policy', it costs but there is a purpose to it. Comments made here included:

Too much selling the 'sausage' and not enough selling the 'sizzle'. Security helps the business make a profit. Is everyone clear how it helps organisations make a profit? It can, but the majority of people can't understand it.

(Managing Director, Security Membership Organisation)

By being present and open and by understanding what other departments and what the organisation wants to achieve, [be a] business enabler not a business disabler.
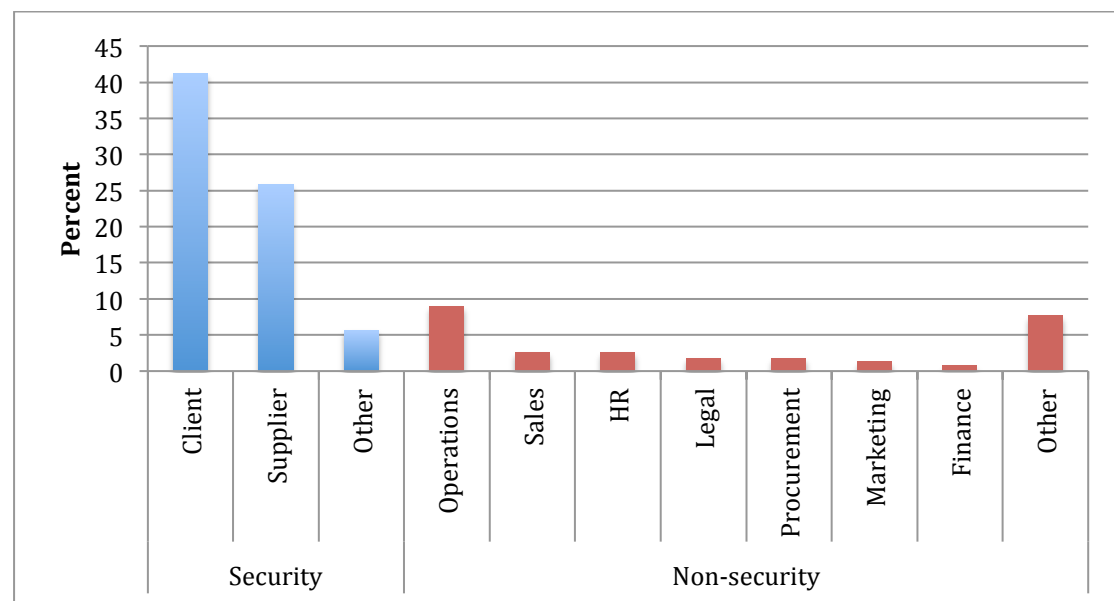
(Head of Security, Banking)

Section 4.   Gauging the impact of security: A Survey

4.1   To support the findings from the one to one interviews, a survey of both 'security' professionals and professionals from 'other' (non-security) corporate roles was conducted, in order to get a sense of how important security is seen as in the workplace, and how it helps other areas of the business.

Background

4.2   The findings discussed are based on 445 eligible responses[85]. Of these 70.7% (n=315) were security professionals and 29.2% (n=130) from 'other' corporate departments. The breakdown by role is described in Figure 1.

Figure 1: Breakdown of respondents by role (%)

4.3   Almost half of the sample described themselves as senior managers (48%, n=217), a quarter as junior management (24%, n=109), 14.4% (n=64) as non-management and only 12.4% (n=55) were board executives. Further demographic information can be found in Appendix 1: Methodology and Sample.

How important is security?

4.4   Respondents were asked to indicate how important a range of factors were to organisational success. Unsurprisingly most factors scored highly, but the key was to establish how important security was

---

[85] In total 502 were collected, but some were removed due to being significantly incomplete.

considered among these factors. 'Being good at security' was rated 'important' or 'very important' by 91% (n=406) of respondents – and it was notable that 'security' professionals only rated it a little higher than those from 'other' corporate departments[86] suggesting security is widely valued.

4.5   However, this figure equates to a ranking of eighth out of the twelve factors offered. 'Staff feeling free from threats of crime of danger' ranked one place higher with 93% (n=411) viewing this as 'important' or 'very important'. Table 1 describes the factors most highly regarded by respondents. For the full breakdown of factors see Appendix 2: Additional Data tables[87].

Table 1: Respondents' views on the importance of a range of factors to the success of an organisation, on a scale of 1 (not at all important) to 5 (very important) (n=438-444)

Highest Scoring Success Factor	Important or very important (4-5)	n
Good customer/client relationships	97.3%	432
Staff believing they are cared about by the company	97.1%	431
A good reputation	96.1%	424
Meeting legal/regulatory requirements	95.4%	423
A trusting working environment	94.7%	416
A strong brand image	93.5%	414

4.6   Given the findings from the interviews that security (whether good or bad) can impact on many of these factors (considered most important to success), this adds further weight to the argument that security can be very significant for the wider business.

How is security perceived?

4.7   Following on from this, respondents were asked to indicate their level of agreement with a number of statements designed to understand in more detail how security is viewed within the workplace. Overall, those surveyed had a very positive view – a large majority 'agreed' or 'strongly agreed' that 'security is a fundamental part of all of an organisation's operations' (82.6%, n=342). This view was more commonly held by those at higher level management (board executives, 84%; and senior managers, 88.9%) than lower level staff (junior managers, 76.7%; and non-management, 71.2%)[88], in keeping

---

[86] 95.4% and 89.6% respectively. The difference was statistically significant, chi square test, $p<0.05$.
[87] Table 3
[88] The difference was statistically significant, chi square test, $p<0.05$.

with the interview findings that an emphasis on security may not always be apparent to staff.

4.8   Table 2 displays the full breakdown of views.

Table 2: Respondents' views on how security is viewed at work, on a scale of 1 (strongly disagree) to 5 (strongly agree) (n=414-417)

Statement	Agree or strongly agree (4-5)	n
Security is a fundamental part of all of an organisation's operations	82.6%	342
Security knowledge gained in the workplace raises staff awareness for when at home and out and about	79.6%	331
Security in the workplace is a way in which an organisation cares for the staff	74.5%	311
The benefits produced by security outweigh the costs	74.3%	309
Security is primarily about protecting an organisation from threats like crimes	53.8%	224
Security is primarily about the protection of organisational assets	50.6%	210
Staff are generally not aware of security requirements at work	44%	183
Security in the workplace is viewed as something of a negative	37.2%	154

4.9   The findings show promising trends; nearly three quarters felt that 'the benefits produced by security outweigh the costs' (74.3%, n=309); and scoring much lower were statements that represented a very limited view of the benefits of security: that security is primarily about protection from crime (53.8%, n= 224)[89] or protection of assets (50.6%, n= 210). This suggests that overall security is becoming less limited to these traditional definitions.

4.10   There was though an interesting difference in how sub-groups rated this issue. Security professionals were more likely to agree that security is primarily about 'protection of organizational assets' than those from 'other' corporate departments[90]. On one level it is surprising that they see security from a more limited view, but perhaps reflects that security professionals are more familiar with this terminology (and have been

---

[89] Suppliers (64%) were more likely than clients (49.1%) to agree that security is primarily about protecting an organization from threats like crime. The difference was statistically significant, chi square test, $p < 0.05$.
[90] 56.4% and 38.7% respectively. The difference was statistically significant, chi square test, $p < 0.05$.

told for so long that that is what they do) and perhaps further illustrating how security tends to undersell itself.

4.11   There remains a notable level of concern that staff are not aware of security requirements (a view more commonly held among suppliers than clients[91]) with over two fifths (44%, n=183) 'agreeing' or 'strongly agreeing'. This adds weight to the interview findings that there is a need for better communication with staff about the value of security, how it can help them in their role and how it can support the business.

4.12   In-keeping with the importance placed on security in the interviews for promoting staff wellbeing, nearly four fifths of the survey respondents agreed or strongly agreed that 'security knowledge gained in the workplace raises staff awareness for when at home and out and about' (79.6% n=331). Similarly three quarters felt that 'security in the workplace is a way in which an organisation cares for the staff' (74.5%, n=311)[92]. Yet lower level staff were less likely to make this connection than higher level managers[93], again raising the argument for better informing staff of the value of security.

What is the impact of security?

4.13   Respondents were next presented with a range of statements designed to test the link between security and those factors noted to be important in business, specifically whether security had an impact on success. While the full breakdown is provided in Table 4 in Appendix 2: Additional Data tables, the key findings are summarised below.

4.14   Overall, there was agreement, that security does have a knock on impact on a range of issues (not least that poor security in an organisation potentially offers rivals a competitive advantage[94]). This shows that when presented with these ideas, professionals are able to see how security can help – indeed there was little difference between 'security' and 'other' professionals in how the majority of the issues were rated. These ideas then are not controversial, they just need attention drawing to them. Further, it confirms that the standard of security in the workplace has far reaching implications for business.

4.15   A key issue covered in the interviews, was the importance of security for protecting reputation. In the survey reputation was ranked (in Table 1 above) as the third most important success factor for business. The vast majority of those surveyed 'agree' or 'strongly agree' that 'poor

---

[91] 54% and 36.9% respectively. The difference was statistically significant, chi square test, p<0.05.
[92] Viewed more so by clients (84.4%) than suppliers (65%). The difference was statistically significant, chi square test, p<0.05.
[93] Board executives (84%) and senior managers (82.2%), compared with junior managers (61.9%) and non-management (63.5%). The difference was statistically significant, chi square test, p<0.05.

[94] 87%, n=341. Also, clients (86.2%) were more likely than suppliers (73.5%) to agree. The difference was statistically significant, chi square test, p<0.05.

security could damage the reputation of an organisation' (96.4% n=390). While over three quarters of respondents 'agree' or 'strongly agree' that 'you cannot have a strong brand image if an organisation is vulnerable to security threats' (77.8% n=392).

4.16 A further issue raised in the interviews (and ranked in Table 1 above as the most important success factor for business) was maintaining good customer relationships; earlier we saw how customer's belief in security helped to retain business, create trust and how this was affected by the reputation and credibility of an organisation. This was confirmed by the survey respondents, with over four fifths of those surveyed 'agreeing' or 'strongly agreeing' that 'customers/clients are less likely to trust organisations with poor security' (81.9% n=321)[95]; and over three quarters (77.6%, n=302) that 'customers/clients value good quality security in an organisation'[96].

4.17 Returning to the issue of staff wellbeing (ranked in Table 1 above as the second most important factor for a successful business), it was clear that security was important to enable staff to do their work and promote a sense of wellbeing - 88.1% (n=345) 'agreed' or 'strongly agreed' that 'if staff do not feel safe they cannot work to maximum effect'; and 87% (n=341) that 'good security enables a sense of wellbeing amongst staff'.

4.18 Somewhat more surprisingly, despite the view among interviewees that security's return on investment is hard to define, survey respondents indicated that security plays a notable role in profitability. The majority (93.4% n=393) of those surveyed said they 'agree' or 'strongly agree' that 'poor security results in losses that affect the profitability/value of an organisation'[97].

Does security contribute to other departments?

4.19 Turning to the view of security professionals, the majority felt that security makes 'some contribution' or 'a significant contribution' to a number of other corporate departments (that were listed) to achieve their organisational objectives[98], displayed in Figure 2.

---

[95] Clients (87%) were more likely than suppliers (73.7%) to agree. The difference was statistically significant, chi square test, p<0.05.
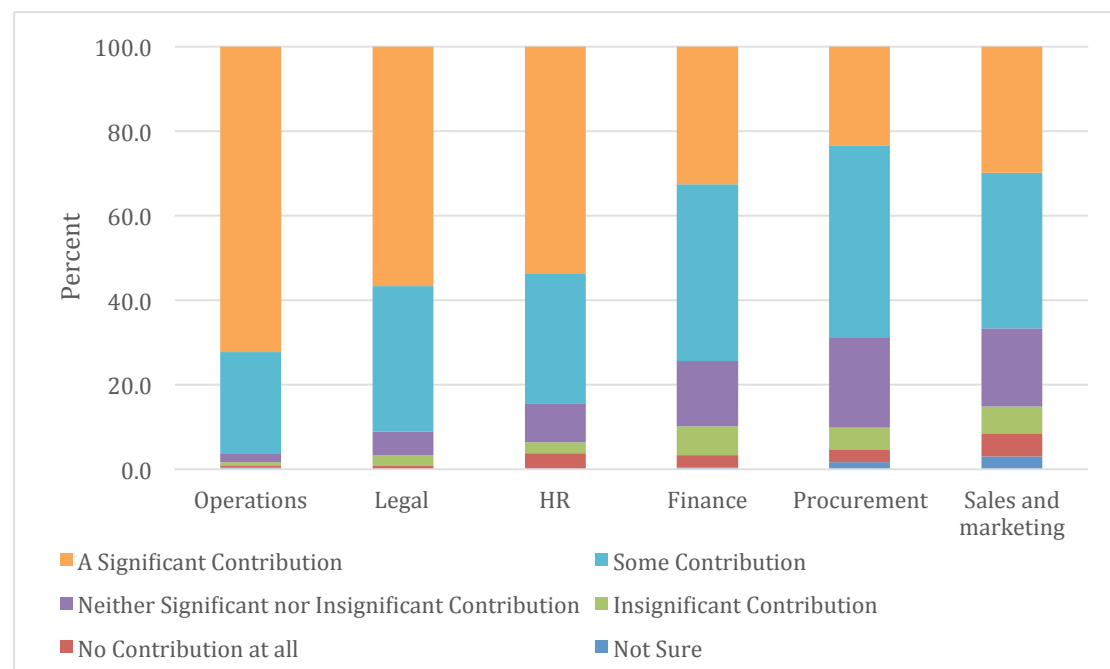[96] Clients (84.3%) were more likely than suppliers (68.8%) to agree. The difference was statistically significant, chi square test, p<0.05
[97] Clients (96.3%) were a little more likely than suppliers (89.5%) to agree. The difference was statistically significant, chi square test, p<0.05.
[98] Corroborating this, agree-ers with the earlier finding that 'security is a fundamental part of an organisations operations' were more likely to believe security contributed in this way to each department than the disagreers (with the exception of 'Legal' which was seen by both agree-ers and disagree-ers as being contributed to by security). The difference was statistically significant, chi square test, p<0.05
Operations. The figures can be found in Table 5 in Appendix 2: Additional Data tables.

Figure 2: Security professionals' views on the extent to which the role of security helps the following departments to achieve their organisational objectives (n=234-245)
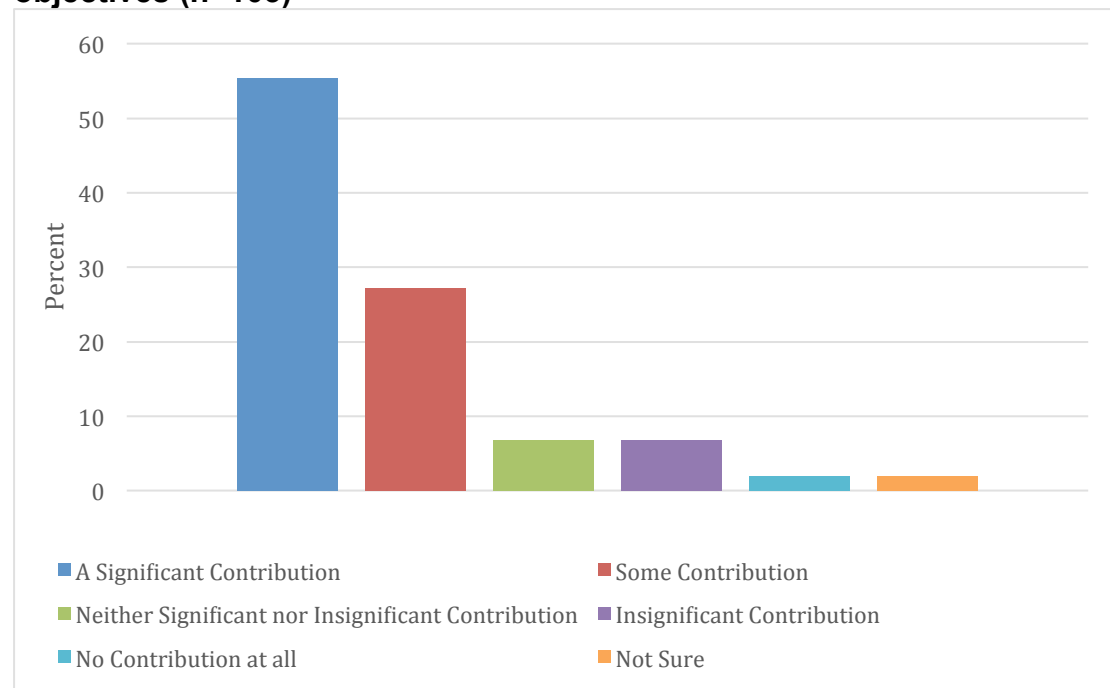

4.20   Further, clients saw a stronger contribution than suppliers did to both 'Sales and Marketing' and 'HR'[99], an interesting finding when we reflect how interviewees suggested security presented a selling point and contributed to staff wellbeing (factors which respectively affect those departments).

4.21   Addressing the views of professionals from 'other' corporate departments, the majority (82.5% n=103) agreed that the security provision at their business offers 'some contribution' or 'a significant contribution' to help their department to achieve their organisational objectives.

---

[99] Sales and Marketing - clients (74.8%) were more likely than suppliers (59.8%) to agree; HR - clients (89.1%) were more likely than suppliers (77.6%) to agree. The difference was statistically significant, chi square test, $p<0.05$

Figure 3: Non security professionals' views on the extent to which the role of security helps their department to achieve their organisational objectives (n=103)

- A Significant Contribution
- Some Contribution
- Neither Significant nor Insignificant Contribution
- Insignificant Contribution
- No Contribution at all
- Not Sure

4.22 Respondents who agreed that 'being good at security' is important (90%) for organisational success were vastly more likely than those who rated being good at security as unimportant (40%) to also agree that security helps contribute to their department[100].

4.23 (Security) respondents were given the opportunity to give examples of how security has helped another corporate department to achieve their own objectives. The responses (n=146) very much reflected the ideas presented earlier by interviewees:

- For HR, this was providing services such as employment screening, disciplinary action and compliance investigations as well as protecting staff and making them feel safe at work, and in supporting them to fulfil their duty of care of staff (generally and when in dangerous situations/locations).
- For Sales and Marketing this was by providing good customer service and improving customer experience and safety, including creating efficiencies for clients, generating trust in the brand and providing a good reputation for integrity. Further that security could provide a selling point and act as a differentiator, particular around key issues such as data security. Security was also seen as important for protecting new products before launch and distribution.

---

[100] The difference was statistically significant, chi square test, $p < 0.05$

- For Finance this was investigating losses, detecting fraud, theft and implementing policy and training for staff on how to handle cash and financial transactions to reduce loss.
- For Legal this was by ensuring legal, ethical and safety standards are met, the right decisions are made and complied to protect the reputation of the organisation. Security can also assist with legal policy reviews and conduct confidential investigations for the legal department.
- For Operations this was by implementing procedures to reduce loss and to increase standards (thereby reducing customer complaints), by assessing site security and improving compliance to company policy.
- For Procurement this included supporting bid processes and giving advice/ assessing prospective partners, evaluating the efficiency of suppliers and also managing contracted services. Security also gave support in checking deliveries and protecting the supply chain.

4.24 Many of the security professionals surveyed argued that corporate security support other business departments and enable organisations to function safely. Respondents noted that security can provide an independent overview, advise and audit business processes to maintain high organisational standards and manage risk. Security was also seen as having a role maintaining business continuity and improving communication between departments.

4.25 Professionals from 'other' corporate departments were asked 'what more, if anything, do you think security could do, to help you achieve your objectives in your role?' Key suggestions included (n=47):

- Increased security training and advice to increase awareness, including legal requirements and the risks of cyber crime. Using 'mystery shoppers' to test staff was an example of an alternative way that security awareness could be maintained.
- Increased customer service training for security staff to add value by becoming more involved in the business.
- Increased focus on security outside of the workplace (but particularly in a work context when on business travel).

Summary

4.26 The picture emerging from the survey is a positive one. One might expect security people to be positive about the role security can take but that other professionals were in general agreement is encouraging. It suggests again, and re-iterating points raised in the interviews, that positive security is welcome. However, there was also recognition that many of the benefits of good security are not obvious, this is true of those who work in security to some extent, in other corporate roles too, and certainly amongst more junior members of the organisation.

4.27 Crucially, security was seen as important in contributing to factors that are essential to the effective running of the organisation such as customer relationships, staff wellbeing and reputation. The challenge remains in spreading this knowledge. This is a subject we return to in the final section of this report.

Section 5.   Conclusion

The true value of security: agreeing not to keep it secret

5.1   Recent developments in the practice of security management, including such buzz phases as 'enterprise security risk management', 'convergence', 'bundling', has brought security into the working environment of other business functions. Missing from this development has been limited acknowledgement of the different benefits that accrue to these departments – as well as the organisation more generally - in having security. It is another way in which security has undersold itself. Indeed, the primary conclusion from this study is that security generally has undersold itself.

5.2   There are barriers to recognising security, beyond the difficulty of measuring it, and this includes the fact that some organisations don't value what security does. At least part of the difficulty here is the interpretation of what is meant by 'security'. We have gone back to basics in this report and suggested that the word has a more benign etymology than is commonly supposed and more in fitting with the direction modern security management is taking.

5.3   Moreover, and as has been noted in previous SRI reports[101], there is a growing realisation that to define security as 'the protection of assets' is to do it an injustice. Not only can other departments claim that they too are protecting assets (e.g. Human Resources, people; Finance, finance), but also because, as this research has confirmed, it underplays what is really involved. Modern security management recognises that risks exist in all organisational activities, and all people (employed, contracted and various other stakeholders including customers) can, through their daily activities, create risks for the organisation, means that security has to be a part of every process, every job role and every activity. This is why a definition and approach to security, as an organisation's friend rather than its police officer is fitting; any organisation approach that is embedded so broadly in its range of activities needs to be a supporter of good practices and mindful of the need to protect freedoms and rights and not infringe them, that is what good security always does (and bad security does not).

5.4   The focus of security on the protection of assets has been somewhat damaging in another way; it has typically taken a rather narrow view of 'assets'. The somewhat typical definition, often found in textbooks and essays on the subject has in its simplest form referred to people, property and information. But what it has not done has highlighted that security is a key component of some of the key strategies for achieving success. It is important to pause and underline these points here.

---

[101] And discussed in Gill (2014) *Handbook of Security*, op cit.

5.5   When security is seen as playing a part in protecting the organisation's reputation then it was more highly valued; that good security will always help with this represents a major opportunity for security to sell itself better. The reason why security needs to be at the heart of every process is that even a minor incident can sometimes have a major impact (and you can't always tell which minor ones can cause a lot of damage). Moreover, the power of channels such as social media affords the opportunity for even small incidents to be widely circulated. An alert security process then becomes all the more vital.

5.6   A speedy and effective response can minimise reputational damage. Incidents cannot always be prevented but they can always be dealt with well or badly, and where it is done well it can generate a competitive advantage over competitors. The costs of getting it wrong need to be couched in the currency of reputational damage. The costs can be financial loss, contract failure, inability to retain customers or recruit and retain good staff. More on generating revenue later.

5.7   This report has highlighted the ways in which security contributes to staff wellbeing, and it is not a marginal role. Protecting people from danger, forecasting dangers and mitigating them before they evolve, minimising the impacts when they occur so suffering and harm are contained and minimised, equipping organisations to protect their staff well are core security tasks, are not 'nice to haves', they are essential if staff are valued, and a key ingredient of corporate success.

5.8   Another role of security, somewhat overlapping the point about protecting the organisation against reputational damage, is that it helps to keep the organisation honest. Responsibility for ensuring organisational rules governing staff behaviour are fair, are often developed outside the security portfolio, and often applied within operational units, but security has a key role in monitoring infractions of these, and much more laws of the land, and ensuring a fair, judicious and prompt response. It contributes to a sense of fairness and justice which are characteristics of good business practice. We have seen that good security involves helping the organisation to take its corporate social responsibilities seriously. And this is not just an internal role: providing support to community groups that have *bona fide* aims with information and security expertise can be important for those on the receiving end. What is often not noticed is that the security function, just like other corporate functions can play a key role in the delivery of the corporate aim and we have cited examples such as buying and using environmentally friendly security services and helping people to get jobs.

5.9   It seems likely that security has too readily accepted a label of being a grudge purchase, as an unwelcome cost on the bottom line. While the intangible nature of much (but not all) of what security does

complicates neat financial calculations that show a Return on Investment, this process has somewhat got in the way of real revenue generating practices that are possibly omnipresent. Certainly the skills and knowledge about security that employees learn at work can be important for their lives outside work.

5.10   Interviewees outlined a range of ways in which security is able to generate income:

- sometimes by providing better security than competitors and deflecting crime there - although more often there is a shared approach across security functions to preventing mutual threats;
- by having excellent security which was highly valued by clients and customers in their choice of who to work with;
- by reducing insurance costs and other expenditures that come with being victimised;
- by creating safe and secure environments to enable the organisation to operate at all;
- in enabling the organisation to trade or exist in areas and types of activity that would not otherwise be possible;
- in providing or helping to provide the sort of environment that will attract customers and staff and keep them and reduce the cost of churn;
- in enabling staff to work flexibly;
- by contributing to a trusting culture and a supportive environment to work;
- in reducing the risks of breaches that can attract fines, unwelcome publicity and loss of reputation.

5.11   Some companies (non security ones) sell their security expertise to others, some give it freely to clients, collaborators and community groups contributing to goodwill, some used the offer of security advice to help build and maintain important corporate relationships. These are merely examples of course. Security can play a part in winning business, maintaining business, and in expanding it, in fact when done well it usually does and directly contributes to the bottom line, it is just that its exponents have neglected to tell anyone.

5.12   In this research we approached a range of other professional groups to discuss the impact of security on them. There were two rather general conclusions from those we spoke to. The first was that they tended to be supportive of security as a general principle, although tending to see it as an important if marginal activity. It was most visible when things went wrong. The second, was that they also felt that staff would benefit from greater interaction with and understanding of security and how it impacted on the organisation. It is another example of security keeping what it does secret and somewhat highlighting the need to increase awareness about the ways in which good security impacts positively on the organisation.

Setting an agenda for change

5.13   There are real barriers to change including the following: some of what is described as security in this report is not the responsibility of the security department; according to this sample of both corporate security departments and contractors some of the current holders of security are not well placed to extol its virtues; the message has never been fully articulated and so presenting it will be outside the comfort zone of many; the groups that need to be influenced - perhaps those who use security and other corporate business leaders are priorities - are not currently listening to what is happening in the security world and so effort needs to be devoted to attracting their attention; and there are no easy routes or channels to influence and new ones may have to be created.

5.14   Therein rests the challenge for good security, in all its guises. The security sector needs to educate itself and then influence others. In so doing it will contribute to the professionalisation of security, at least if that is taken to mean a move to up skilling its exponents, engaging with its stakeholders, and raising awareness that there is a lot you get from good security, a lot, that you don't get from bad.

Appendix 1: Methodology and Sample

The approach

The study involved a review of existing literature on the benefits of security to identify any issues and themes arising that could direct our research questions.

This was followed by two main approaches: interviews with professionals about the topic, including a number of focus groups (UK and abroad); and a survey of the benefits of security in the workplace. Both approaches sought the views of security professionals but also those from other (non-security) corporate departments to understand their perspective and how they felt security contributed to success in the workplace.

One to One Interviews and Focus Group Discussions

The approach in this work was to identify a wide range of individuals to help understand what additional benefits security may generate in the workplace beyond crime prevention. A snowball sampling strategy was used. This involves using contacts and word of mouth to identify relevant people to take part. In fact, primarily two distinct routes were used; personal contacts and contacts of personal contacts; and individuals who volunteered to offer more details after taking part in the survey.

An advantage of this method is that it allows access to members of the population who may be difficult to identify and engage by other means. Obtaining the sample in this way allows for potentially more valuable responses as those taking part are more likely to be knowledgeable about the research. Indeed, one of the early findings was that the topic was not one that was often discussed despite a general agreement among the profession that security has a lot to offer in business. The interviews typically lasted thirty to sixty minutes (focus groups a little longer) and detailed semi-structured interview schedules were used. The schedules were based on the information taken from the literature review as well as previous research. An advantage of a semi-structured schedule is that it gives the flexibility for interviewers to probe the issues raised.

In total, 55 individuals were interviewed via one to one or focus group discussions. Of these, 30 were with 'clients', '15' with 'suppliers', 1 was a security academic, and 9 were with individuals from 'non-security' roles including HR, Sales, Marketing, Finance, Quality, Facilities.

Survey

The aim of the survey was to target a wide group of clients, suppliers, and additionally those from other corporate departments that are not security providers. The survey addressed three key areas – factors contributing to success in business, perception of security in the workplace, impact of security in terms of contributing to success. In addition those in a security role were asked what contribution security makes to other corporate departments.

Those in a non-security role were asked what contribution security makes to their department.

For those in the security professional role there is no sampling frame, that is there is no defined population listed or recorded anywhere. The sample was therefore self recruited. This means that it is not representative. Actually the aim was to help us identify whether or not security was perceived as being important in business and capable of generating additional benefits beyond preventing crime. An attempt was made to publicise the survey widely, this included via participants from previous research who had elected to be contacted for future research; a link in the Perpetuity newsletter and via Perpetuity social media; announcements made at conferences and other security events; and a range of organisations were contacted and informed of the survey and invited to publicise it and pass on the details to their members, these included:

- ASIS (UK Chapter)
- ASIS International
- Security Institute (SyI)
- British Security Industry Association (BSIA)
- International Professional Security Association (IPSA)
- Infologue
- Professional Security Magazine
- Risk UK

We cannot be sure that all groups disseminated relevant information to all audiences, but most helped for sure.

For those in a non-security role, it proved difficult to make contact via membership organisations for the profession which did not typically see the relevance of a survey about security. The sample therefore was again self selecting – with the main sources for publicity via social networking channels and non-security professionals working within the security industry. Certainly we expected a low response from those from other departments in non-security roles who may struggle to see the relevance of answering a survey about security. We were therefore pleased with the level of response albeit a basis on which others need to build.

The findings helped identify the importance of various issues from a broad range of people. The data though have mainly been used to provide a context to, and help frame the major part of the work, the interviews; this is reflected in the emphasis placed on the survey findings discussed in the report.

The survey ran from 21st January to 13th March 2015.

In total 502 survey responses were completed. Some were removed due to being significantly incomplete, leaving 445 eligible responses. Of these 315 (71%) were security professionals and 130 (29%) were from other corporate departments. The data was analysed producing frequencies, and where

appropriate crosstabs[102] were run to compare sub-groups and establish any significant differences in how they answered the questions.

Other demographic information:

- By far the majority were male (82.4%, n=376) and white (84.3%, n=376). Two thirds were over 45 years of age (67.8%).

- Most worked for UK based organisations (46.1%, n=445). Indeed the majority of respondents indicated that they had mostly worked in Europe within the last 5 years (69.4%, n=445) with 26.1% working in the US, 13.9% in Africa, 12.8% in Asia, 8.7% in Australia and New Zealand and 8.3% in South America.

- Respondents represented a wide range of sectors (and they could select more than one and describe an 'other' sector), with the highest representation from 'Public Admin & other Government Services' (16.2%), followed by 'Manufacturing' (15.1%), 'Post & Telecommunications' (13.6%), 'Health' (12.4%) and 'Finance' (12.1%). The full breakdown by sector is presented in Appendix 2: Additional Data tables.

---

[102] Using Chi square. Information was only included where the findings were statistically significant, that is p<.5.

Appendix 2: Additional Data tables

The following tables provide a more detailed breakdown of the survey findings.

Table 3: Respondents' views on the importance of a range of factors to the success of an organisation, on a scale of 1 (not at all important) to 5 (very important) (n=438-444)

Success Factor	Important or very important (4-5)	n
Good customer/client relationships	97.3%	432
Staff believing they are cared about by the company	97.1%	431
A good reputation	96.1%	424
Meeting legal/regulatory requirements	95.4%	423
A trusting working environment	94.7%	416
A strong brand image	93.5%	414
Staff feeling free from threats of crime or danger	93%	411
Being good at security	91.4%	406
Being competitive	91%	403
Making a profit (if a non-profit organisation: providing value for money)	90.6%	397
Conducting business in a way which is socially responsible	88%	389
Being seen as responsive to the needs of the local community	72.7%	320

Table 4: Respondents' views on the impact security has on factors that affect the success of an organisation, on a scale of 1 (strongly disagree) to 5 (strongly agree) (n=389-393)

Statement	Agree or strongly agree (4-5)	n
Poor security could damage the reputation of an organisation	96.4%	376
Poor security results in losses that affect the profitability/value of an organisation	93.4%	376
Good security helps an organisation to meet their legal/regulatory requirements	92%	361
Any organisation that introduces a new	88.5%	345

product or service would benefit from ensuring that it does not pose a security threat		
If staff do not feel safe they cannot work to maximum effect	88.1%	345
Poor security in an organisation potentially offers rivals a competitive advantage	87%	341
Good security enables a sense of wellbeing amongst staff	87%	341
Customers/clients are less likely to trust organisations with poor security	81.9%	321
If an organisation has poor security it will have difficulty operating effectively	81.3%	317
Poor security in an organisation makes it a less attractive place to work	79.2%	308
Good security can help an organisation to produce better products/services	79.1%	310
You cannot have a strong brand image if an organisation is vulnerable to security threats	77.8%	305
Customers/clients value good quality security in an organisation	77.6%	302
Organisations with good security are more likely to be good corporate citizens	71.4%	279
Good security in an organisation will have knock on benefits for the community in making it safer	69.8%	273

Table 5: The difference between agree-ers and disagree-ers with the sentiment that security is a fundamental part of all an organisations operations in also believing security contributes to other corporate departments.

Department	Agree-ers	Disagree-ers
Operations	97.9%	90.5%
HR	89.2%	69.80%
Finance	81.60%	48.80%
Procurement	73.9%	53.50%
Sales and marketing	73.9%	48.8%

Table 6: Sector respondents were operating in (n=445)

Sector	Percent (%)
Public Admin & Other Government Services	16.2
Manufacturing	15.1
Post & Telecommunications	13.7
Health	12.4
Finance	12.1
Energy	11.5
Education	11.5
Retail	11.0
Property	11.0
Construction	9.4
Transport	8.8
Production	6.7
Leisure & the Night Time Economy	6.7
ICT	6.5
Mining, Quarrying & Utilities	5.8
Hotel & Catering	5.8
Wholesale	2.7
Motor Trades	1.8
Other	29.0

All respondents that selected 'other' had also selected one of the main categories listed. 'Other' sectors stated by respondents included for example: Defence, Health & Fitness, and Media.

Appendix 3: The multiple benefits of security

During the research we encountered a multitude of ways in which security contributes to organisational success. We list below some of the different ways that good security (that was ethical, proportionate and effective) was seen to contribute. This is not a definitive list; we suspect that would be a very long list indeed, an interesting finding in itself. What it is though is illustrative of the ways, the very diverse ways in which security makes a contribution. It is perhaps a list on which others might usefully build.

Security measures can be used for alternative purposes
- to solve problems, create efficiencies, benefits customers and reduce costs of other aspects of business – CCTV and access control for example can enable remote monitoring of operations, analysing customer behaviour, measuring compliance, responding to non-security incidents, tracking individuals in emergency situations, using data for other purposes (such as a shift patterns/payroll).

Security helps to protect reputation (something critical to success)
- Without security incidents would occur that would damage reputation.
- Without a good response by security when incidents do arise, issues would escalate and damage to reputation would occur.
- This type of emergency preparedness can even give a competitive edge because of an ability to recover quicker than competitors or foresee and mitigate disruptions including to the supply chain.
- Security can provide a framework (through procedure) for ensuring confidential information is protected, preventing damage occurring.
- Security can instil codes of conduct for staff, so their conduct does not erode reputation.
- Security creates confidence in an organisation. By being effective security staff give credibility to an organisation and a reputation for good security can contribute to commercial success.

Security helps to protect financial loses
- It protects the payment process.
- Provides information to corroborate or negate insurance pay-outs.
- Reduce likelihood of incurring fines and penalties for non-compliance with legal (and other) requirements.
- Responding well to incidents reduces the losses that would be associated with unnecessary disruptions to work/production.

Security attracts business/sales
- Safety/security can be a deciding factor for potential customer when choosing to spend.
- Better security than competitors can command better fees.
- Security (including accreditations) reassures and enhances the customer experience.

- Building security in to products and services can create a commercial advantage over competitors.
- Security can protect new products and services (before and during marketing events), attracting customers.

Security helps businesses expand
- Without the experience and knowledge of security organisations may be unable to expand in to potentially hazardous environments or to fully weigh up the business case for doing so.
- Enabling operations in dangerous environments could create a competitive advantage where others were not ready to apply security in the same way.
- Security can support bidding processes and give advice/ assess prospective partners, evaluate the efficiency of suppliers and also manage contracted services.

Security helps retain customers
- Security can enable clients to save money (through being effective or by innovating) which added value and increased the chances of retaining that client's business.
- Sharing security expertise and intelligence with clients strengthens the relationship.
- A competent and experienced security provision will influence customer perception of efficiency. Good security enables smooth running of the organisation and customers will return if they have a good experience.

Security enables
- Operationally security enables staff to work – it prevents and/or resolves disruptions caused by incidents, attends to safety concerns, enables effective use of a site and flexible working hours. It prevents issues escalating and ensure compliance with policies and procedures that would otherwise present danger and/or disrupt operations.
- Security engenders trust which is also an enabler for good working practices between colleagues, management, clients, customers, partners.
- Security keeps the organisation honest by creating a trusting environment in which rule breaking and honesty are easy to identify.
- Security creates trust by presenting a professional and courteous image.
- Acting as a trusted advisor and creating competitive advantage creates respect.
- Security works with others – putting competitive advantage aside, security generates trust and enables business by working with others to tackle threats to business.
- Security procedures may create other benefits such as improved inventory or better project management.

Security helps to care for staff
- Security can positively impact on staff wellbeing. By protecting staff, making them feel safe, and tackling potential vulnerabilities (such as lone working or working in unfamiliar locales) staff may feel more valued by their employer, helping to retain staff and attract new staff.
- Security can contribute to a positive working environment, not only through creating a general sense of safety but also by nullifying negative workplace events (thefts from staff, seeing discriminatory graffiti etc which can lower staff morale).
- Training staff and making them security aware can benefit them in other aspects of their lives.
- Safety concerns can create inefficiencies in working practices (staff may not liaise with colleagues if they are rushing to leave because of concerns). Security can mitigate these issues and thus improve working practices.

Security contributes to Corporate Social Responsibility
- Security in the workplace prevents a decline in the local area that could arise from businesses attracting crime.
- Security knowledge and intelligence can be shared with a community to help it better protect itself. Working with other agencies including the police helps the whole community to protect itself.
- Corporate security provides an additional resources for the local community – they may be able to assist in emergency situations (reporting incidents, using their CCTV, liaising with emergency services, providing refuge, providing first aid etc).
- Security can contribute to an environmentally friendly agenda in terms of the equipment and practices used.
- Security staff are often recruited from the local community, potentially tackling disadvantages by up-skilling and employing members of local communities.

About Perpetuity Research

Perpetuity Research is a leading research company with wide expertise in both quantitative and qualitative approaches. We have been extensively involved in evaluating 'what works' (and what does not). Our work has involved helping our clients to understand people's behaviours, perceptions and levels of awareness and in identifying important trends. Our mission statement is 'committed to making a difference', and much of our work has a practical application in terms of informing decision making and policy formulation.

We work closely with our clients. This includes businesses, national and local governments, associations and international organisations as well as charities and foundations. Our aim is to exceed their expectations and it speaks volumes that so many have chosen to work with us repeatedly over many years. We are passionate about our work and we would welcome the opportunity to work with you.

About the SRI

The Security Research Initiative (SRI) started nearly a decade ago. It involves a rolling program of research; each year a separate study is conducted on the security sector to generate new insights, help develop the response and role of security and act as a guide to improving practice. The SRI is supported by the British Security Industry Association, The Security Institute, and ASIS International (UK Chapter), and includes membership from leading security suppliers and corporate security departments who share the commitment to the development of new knowledge.

Previous studies have focussed on the relative benefits and drawbacks of buying security as a single service or as part of a bundle; an industry wide survey; a study of the value of security. We have developed two toolkits, including one on developing a security strategy. The findings from the research are made available free of charge to all to benefit. More information on the SRI is available at: www.perpetuityresearch.com/security-research-initiative/

About the Authors

Professor Martin Gill

Martin Gill is the Director of Perpetuity Research and Consultancy International. He started the company in 2002 and it was formally launched by HRH Prince Michael of Kent. Martin is also a Professor of Criminology – he has Honarary/Visiting Chairs at the University of Leicester and University College London - and for over two decades has been actively involved in a range of studies relating to different aspects of crime and its prevention.

Martin started and leads the Security Research Initiative. Martin has published widely (14 books and over 100 articles including 'Managing Security' and 'CCTV' published in 2003, and the 'Handbook of Security', the first edition was published in 2006 and the second edition in 2014) and is editor of Security Journal. In 2002 the ASIS Security Foundation made a 'citation for distinguished service' in 'recognition of his significant contribution to the security profession'. In 2010 he was recognised by the BSIA with a special award for 'outstanding service to the security sector'. IFSEC has twice placed him in the top 15 most influential fire and security experts in the world.

Charlotte Howell

Charlotte Howell joined Perpetuity in January 2009 and currently works as Research Manager, managing and delivering research contracts. Charlotte has experience in a variety of research skills. Her quantitative skills include analysis of datasets such as survey responses, client data and performance data. Her qualitative research skills include undertaking literature reviews and undertaking consultation through interviews, focus groups and street surveys. Charlotte has consulted with a range of individuals, including stakeholders (such as individuals from the police, local authorities, teachers and service commissioners and staff), offenders (both in prison and in the community), and clients accessing services (including children and their families) such as weight management services, drug and alcohol treatment services, domestic abuse services and support services for sex workers.

Prior to working for Perpetuity, Charlotte graduated from the University of the West of England with a first class LLB (Hons) in Law in 2003. Following this she received an MSc in Criminology from the University of Leicester in 2004. After graduating, Charlotte worked for the Leicester Criminal Justice Drugs Team, analysing and reporting on Class A drug misuse and treatment information, to maintain and improve performance.

Amy Randall

Amy Randall joined Perpetuity Research as Research Assistant in October 2013. Since joining Perpetuity she has been involved in a range of research tasks and is currently working on a project interviewing insurance fraudsters. Amy has a good knowledge of a range of

methodological approaches, both qualitative and quantitative. She has experience conducting interviews and focus groups and has strong research design skills. As well as this she has a working knowledge of data analysis techniques and a good proficiency in relevant software packages and experience working with large data sets.

Prior to working for Perpetuity, Amy graduated from The University of Kent with a First class BA (Hons) in Sociology. She has an MSc in Social Research Methods at London School of Economics and Political Science.