Tackling Cyber Crime: The Role of Private Security

A Security Research Initiative Report

Professor Martin Gill
Charlotte Howell

June 2016

Perpetuity Research & Consultancy International (PRCI) Ltd
11a High Street · Tunbridge Wells · TN1 1UL · United Kingdom
www.perpetuityresearch.com
prci@perpetuityresearch.com
Tel: +44 (0)1892 538690

INVESTORS IN PEOPLE

Copyright

Copyright © 2016 Perpetuity Research and Consultancy International (PRCI) Ltd

All Rights Reserved. No part of this publication may be reprinted or reproduced or utilised in any form or by any electronic, mechanical or other means, known now or hereafter invented, including photocopying and recording, or in any information storage or retrieval system, without permission in writing from Perpetuity Research and Consultancy International (PRCI) Ltd.

Warning: the doing of an unauthorised act in relation to copyright work may result in both civil claim for damages and criminal prosecution.

Acknowledgements

We would like to thank everyone who has assisted us with our research. First, the members of the Security Research Initiative who sponsor the research and their representatives who provide advice and share their experiences; they are: Stuart Hughes (Adidas), Hannah Watters and Tony Louden (Caterpillar), Sarah-Jill Lennard (Deloitte), Barrie Millett (E.on), Mark Beadle (Emprise), Stuart Walton (G4S), Mick Tabori and Joachim Ritter (Interr Security), Jerry Nelson (KPMG), Clint Reid (M&S), Jason Towse (Mitie), Daryn Flynn and Nienke Bomers (NEDAP), Steven Gardner (OCS), Martin Dunckley and Tony Marsh (Royal Mail), Sue Seaby and Brian Riis Nielsen (Securitas), David Humphries (SIA), Simon Pears and Jane Farrell (Sodexo), Keith Francis and Barry Dawson (VSG), and Geoff Zeidler for acting as our expert liaison.

We are especially fortunate in being able to draw upon the advice and support of other experts. James Willison was interested in the study from the start and his expertise in all matters relating to convergence and Enterprise Security Risk Management was invaluable. We are extremely grateful to him. So too all his colleagues on the ASIS European Convergence/ESRM committee for their interest and support especially the Chair Volker Wagner. Thanks are due to Professor Paul Dorey and Sarb Sembhi for their expert input. Dr Dan Prince of the University of Lancaster was a critical friend and helped us develop our thoughts on the findings. During the preparatory stages of the project we had very helpful and insightful conversations with a range of people, not least Dave Tyson (who has written a book on the subject) and Brian Allen (who is writing one), to these and all others we are grateful.

We needed help with promoting the survey and our key supporters were once again invaluable. ASIS (especially Dave Clarke, Mike Hurst and Graham Bassett), the BSIA (especially James Kelly and Trevor Elliott) and The Security Institute (especially Garry Evanson, David Thorp and Di Thomas) are valuable advocates of the Security Research Initiative. So too our longstanding enthusiasts from the security media: Bobby Logue, Mark Rowe and Brian Simms. A whole range of associations and groups helped promote the survey; those we know about we have listed and thanked in the Appendix. Their help is much appreciated we hope the findings will prove useful to them. We owe a special thanks to all those (anonymous) contributors who gave their time completing our survey and to the many who contributed insights and took part in interviews. They, by necessity and agreement must remain nameless but we acknowledge their important contribution here.

Finally, we would like to thank our colleagues. Rachel Horan, who conducted the analysis of the survey findings; Ashley Bennett who helped with the overall management of the project from arranging interviews to helping prepare the report; and Josephine Ramm who checked our calculations and provided a very helpful critique of a late draft.

Martin Gill and Charlotte Howell

© Perpetuity Research and Consultancy International Ltd

SRI Members

Adidas

Deloitte

M&S

Royal Mail

© Perpetuity Research and Consultancy International Ltd

Table of Contents

© Perpetuity Research and Consultancy International Ltd

© Perpetuity Research and Consultancy International Ltd

Executive Summary

Background

- In public debates about how best to respond to cyber crime, the role of private security has received scant coverage
- Given that much of the infrastructure that underpins cyberspace is owned and maintained by different elements of the private sector (which often uses private security suppliers), private business and, by extension private security, has a key role to play
- A lot of cyber-security expertise is in the private sector
- What constitutes cyber crime is much debated, what is no longer so contentious, is that the consequences of being a victim of a cyber attack can be very serious indeed
- There is untapped potential in cyber-crime prevention in that some companies are prepared to invest in cyber security to protect the national infrastructure because of a sense of 'civic-mindedness'
- People, and not least security staff, are crucial to protecting against cyber loss although this is often undervalued and under-stated.
- There is considerable (and often unrecognised) overlap between good cyber security and good overall security
- An adequate cyber response requires agencies to work together; the police are often relatively minor players
- The police sometimes lack trust in other partners and potential partners, including members of the public and the online community where there are concerns about issues such as vigilantism
- Police face problems when dealing with cyber crime, such as a lack of technical skills, a disjointed approach, insufficient resources, and a relatively poor understanding of cyber space
- Security itself can create opportunities for offenders; the increased prevalence of security technology in physical aspects of our world, the 'internet of things' provides endless new targets for cyber criminals

Survey findings

A survey of security professionals from around the world was carried out which generated 289 replies and this was supplemented by one to one interviews with both physical and cyber security specialists. The research addressed four key areas – the current approach to managing cyber security, the relevance of convergence between physical and cyber security, perspectives on law enforcement, and the potential role of private security in responding to cyber crime.

On managing cyber security

- Only 12% disagreed with a statement which stated that organisations were poor at preventing cyber crime

- 63% agreed that organisations were poor in knowing when there had been a breach of security. Those working mainly in cyber security were more likely than those mainly working in physical security to agree
- Of the respondents, 45% believed that cyber and physical security were equally important in the companies they were linked to, 25% reported that cyber was more important, and 25% that cyber was less important
- Over a half of the sample (55%) agreed that people issues were more important than technology in tackling cyber crime, and 81% agreed that an alert workforce was the best defence against cyber crime
- While it was recognised that there were similarities between cyber and physical threats, the sample also identified specific differences, for example, tracing offenders and the scale of consequences. Some felt physical security threats differed so much by location it made them more tricky to manage

On convergence

- Just 29% of the sample agreed that convergence (the bringing together of physical and cyber security specialists) was widely understood in relation to security
- When asked to identify the main barriers to physical security getting involved with tackling cyber threats, the most popular reasons were: the belief that cyber is outside the remit of physical security; the lack of cyber expertise amongst physical security experts; and the belief that cyber specialists generally operate in isolation
- Over a third (35%) felt that physical security experts did not want to get involved in cyber security and over a half (56%) that cyber security personnel did not want physical security experts involved in 'their' area
- There was considerable support for the idea of convergence. When asked for the preferred way of working 56% argued for some type of converged working, 38% for separate teams and 6% were not sure
- More research is needed to translate theory into practice and understand the different models/approaches of convergence and the associated pros and cons of each

On law enforcement

- Only 3% of respondents strongly agreed with the statement, 'the police are effective at tackling cyber crime', and only 4% thought they were experts in this area. Moreover, only 18% of respondents agreed or strongly agreed that police are very effective at tackling cyber crime, and 16% that they are experts at tackling it
- 69% of those who expressed an opinion either way agreed that it is impractical to report all cyber crime; this may undermine some collaborative attempts at intelligence building
- While some could point to examples of excellent practice in police work, the general view was that the scale of cyber offending and the

depletion of resources available to the police meant organisations will have to take primary responsibility for protecting themselves

On physical security and security patrols

- When asked whether any approach to cyber that did not include a physical response was a weak one, the majority of responders agreed (52%) and only a small percentage disagreed (17%)
- 79% thought that physical security was crucial to tackling cyber, but 38% of the sample agreed physical security suppliers often don't see opportunities for contributing to cyber security
- Over a half (52%) felt that manned guarding companies could make a contribution, rather less (38%) thought facilities management companies could, rather more thought security consultants could (91%)
- The role of security patrols was often seen as important in tackling cyber crime although not everyone thought so and there are potential opportunities for the physical security sector here

Final comments

- Physical security generally has underplayed the contribution it can make to tackling cyber crime; it has an extremely important role to play. Some felt that by not engaging in this area, it was missing a massive opportunity to influence and profit from this work
- There is a mistaken tendency to see the response to cyber crime in terms of technology. While technology is crucial, most agreed that people were more important and an alert workforce the best cyber security prevention measure
- Convergence is widely discussed – and has a lot of support - but there is a lack of clarity as to what it means. Supporters of convergence need to better articulate the pros and cons of different ways of working and the implications for security, mindful that some fear that a move to a converged approach will be driven by a desire to cut back on resources
- The police have an important role to play, not least in working with business, but there needs to be more awareness about what can be realistically expected on each side
- The cost of a technical cyber response can be high and this excludes many companies from being able to afford what they need; this is an important reason why the police need to be involved to protect those who are financially disadvantaged.
- Cyber threats are relatively new. The security and policing worlds are only now beginning to determine the merits of different approaches. There is a crucial need for more research on what works and why.

© Perpetuity Research and Consultancy International Ltd

Introduction

1.1 It seems strange that the role of private security and corporate security in addressing cyber crime has received such little coverage against a background where:

- the threat of cyber crime is growing;
- the consequences for organisations (and for that matter individuals) are serious;
- police resources are restricted and skills sets often less than adequate

1.2 What is clear is that there are a number of barriers which include:

- the lack of international legal frameworks and the lack of developed international police partnerships in all parts of the world focussed on cyber crime;
- the growing awareness that multi faceted approaches and multi agency co-operation will be essential yet structures and agreements are not widely in evidence;
- criminals see the opportunities expanding with limited chances of being caught or at least prosecuted;
- the lack of experts in cyber; demand exceeds supply.

1.3 The aim of this project is to explore in more detail what the role of private and corporate security is and what it could potentially be. There are four key areas that the research seeks to better understand. They are:

I. On what principles is cyber-crime prevention based? Is the priority a technology focussed approach or is it human centred? Why is this the case? Is the cyber threat different to the threats typically faced by physical security? What do current trends tell us about the direction of cyber security?
II. To what extent and in what ways do modern approaches, such as 'convergence' offer opportunities for corporate and physical security suppliers? How well understood is convergence? What are the barriers to collaborative working?
III. To what extent can the police be relied upon to respond to cyber offences? How effective are the police perceived to be? What are the experiences of working with the police and how might this be developed moving forward?
IV. What role is there for physical security (in corporate departments and amongst suppliers) in tackling cyber crime? How much is it core to current strategies and how much could it be going forward? How valuable are security patrols in preventing cyber crime? How much

recognition is there that security measures present a risk in themselves?

1.4 In practice these issues overlap. Moreover, there is a wealth of research which has touched upon the issues, despite them not being the specific focus. The next section explores them in a little more detail, examining some of the key aspects that have emerged from a variety of information sources including academic studies.

Section 2. The role of cyber crime and physical security

2.1 This project is focussed on assessing the role of the security sector, both private security suppliers and corporate security departments, in responding to cyber crime. Cyber crime can be a tricky concept to define as many commentators have attested to.[1] Definitions typically focus, to a lesser or greater extent, on whether offences are *cyber dependent*, *cyber enabled*, or *cyber assisted*.[2] Proposed definitions include, 'any proscribed conduct perpetrated through the use of, or against, digital technologies,[3] 'a crime that has some kind of computer or cyber aspect to it',[4] and, '*crime facilitated, enabled or amplified by the internet*'.[5] A more encompassing definition is perhaps helpful: 'illegal activities undertaken by criminals for financial gain which exploit vulnerabilities in the use of the internet and other electronic systems to illicitly access or attack information and services used by citizens, business and the Government'[6]. By extension, when we talk about 'cyber security' we are talking about the work of professionals to protect these systems from cyber crime and therefore encompass (electronic) information security.

2.2 In practice, cyber crime involves a wide variety of offences, some are routine and a nuisance and some are serious and can require a wide variety of skill sets to manage.[7] For example, cyber-trespass, which entails crossing boundaries into other people's property and/or causing damage, e.g. hacking, defacement, viruses; cyber-deceptions and thefts – stealing (money, property), e.g. credit card fraud, intellectual property violations (a.k.a. 'piracy'); cyber-pornography – breaching laws on obscenity and decency; cyber-violence – doing psychological harm to or inciting physical harm against others, thereby breaching laws relating to the protection of the person, e.g. hate speech, stalking and crimes against the state - activities that breach laws protecting the integrity of the nation and its infrastructure (e.g. terrorism, espionage and disclosure of official secrets).[8] Indeed, in the wake of the terrorist attack to the city of Paris on 13 November 2015, the UK Government

[1] See for example: Tavani, H. (2000) 'Defining the Boundaries of Computer Crime: Piracy, Break-Ins, and Sabotage in Cyberspace', *Computers and Society*, September 2000, pp 3-9.
[2] City of London Corporation (2015) The Implications of Economic Cyber Crime for Policing. City of London Police and City of London Corporation.
[3] http://assets.cambridge.org/97805218/40477/frontmatter/9780521840477_frontmatter.pdf
[4] http://uk.norton.com/cybercrime-definition
[5] Europol (2014) *The Internet Organised Crime Threat Assessment*
Available at https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta, p.11.
[6] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber crime-full-report.pdf
[7] Hargreaves, C. and Prince, D. (2013) *Understanding Cyber Criminals and measuring Their Future Activity: Developing Cyber Crime Research*. Lancaster University: Security Lancaster.
[8] For examples and a broader discussion, see, Lucas, E. (2015) *Cyberphobia*. London: Bloomsbury.

announced the creation of a National Cyber Centre and increased funding for the National Cyber Crime Unit recognising the threats posed by Islamic State militants in threatening cyber attacks against targets such as hospitals, and air traffic control.[9]

2.3 There is now a wealth of information on the scale of cyber crime,[10] including on the so called Dark Web,[11] and there are a host of authorities confirming that the costs are astronomical,[12] not least the cost of protection,[13] that the impact can be significant,[14] affect many,[15] and appear to be increasing.[16] In addition, there is evidence that the response is inadequate[17], and often under resourced,[18] leaving businesses searching for the right solutions.[19] Eric Hansleman, (451 Research) speaking at IFSEC 2015[20] highlighted the current problematic position, '*In the last year, businesses spent $70bn on cyber security. Meanwhile criminals will have made 10-20 times that amount*'. The threat is international and just by way of example, the Australian Cyber Security Centre 'Threat Report 2015' summarised the danger using these words: 'the cyber threat to Australian organisations is undeniable, unrelenting and continues to grow. If an organisation is connected to the internet, it is vulnerable. The incidents in the public eye are just the tip of iceberg'.[21]

2.4 Yet within the broader debate about how best to respond, the role of private security has received scant coverage. This is despite the fact that (or perhaps because of it) responses are evolving.[22] One source described the problem as such:

---

[9] http://www.bbc.co.uk/news/uk-34839800 (accessed 17th February 2016).
[10] This interviewed 5,128 respondents across 99 countries.
[11] For a good discussion, see Bartlett, J. (2015) I. London: Windmill Books.
[12] CPNI (2014) Cyber Attacks: Affects on UK Companies http://www.cpni.gov.uk/documents/publications/2014/oxford-economics-cyber-effects-uk-companies.pdf?epslanguage=en-gb (accessed on 24/09/15)
[13] Cabinet Office (2014) *The UK Cyber Security Strategy. Report on Progress and Forward plans 2014* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/386093/The_UK_Cyber_Security_Strategy_Report_on_Progress_and_Forward_Plans_-_De___.pdf (accessed on 24/09/15
[14] Not least the costs to business – estimated to be £4.1 million per year for large UK organisations; a year-on-year increase of 14% (Ponemon Institute (2015) *2015 Cost of Cyber Crime Study: United Kingdom*). Identifying the true costs of cyber crimes is a tricky task with a host of methodological issues to overcome (not least avoiding double counting any savings). That stated, this publication presents an interesting insight into relevant issues. It suggest that personnel with relevant expertise and appropriate security measures can be financially worthwhile investments.
[15] Maguire, M. and Dowling, S. (2013) Cyber Crime: A Review of the Evidence. Research Report 75. Home Office: London.
[16] Cabinet Office (2011) *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world*, London: Cabinet Office.
[17] Europol (2014) *The Internet Organised Crime Threat Assessment* Available at https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta,
[18] Deloitte & NASCIO (2014) *2014 Deloitte-NASCIO Cybersecurity Study*. See also: European Commission (2015) Cyber Security Report. Special Eurobarometer 423. Brussels: European Commission (http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf).
[19] This interviewed 1,860 businesses across 60 countries.
[20] Available at http://www.ifsecglobal.com/download-cyber-security-crashcourse-presentation-ifsec-2015/ (accessed on 24/09/15)
[21] Australian Cyber Security Centre Threat Report 2015. Canberra: Australian Government, p2.
[22] Levi, M. and Williams, M. (2012) *eCrime Reduction Partnership Mapping Study*. University of Wales, Cardiff.

'According to the ISBS 2013 survey, UK organisations now spend 10% of their IT budget on security on average (up from 8% in 2012). A key finding of the survey was that many businesses struggle to implement effective security defences due to ineffective leadership, weaknesses in risk assessment and skills shortages. Developing a cyber security strategy and identifying key areas of investment is therefore essential for effective targeting of cyber security expenditure and ROI.' (IT Governance Ltd, 2015:3)[23]

2.5 There are many reasons though to suppose that security suppliers and corporate security have a central role to play. After all, as the UK Cyber Security Strategy[24] notes, much of the infrastructure that underpins cyberspace is owned and maintained by different elements of the private sector; inevitably it is business that will need to take a leading role in offering protection. That stated, the evidence suggests that business has been and remains lacklustre in its response. One survey published by the IOD has revealed that while 91% of respondents considered cyber security important, only 57% had a cyber/information security strategy, less than half (49%) provided relevant training for staff and over two thirds were not aware of Action Fraud (to whom reports of fraud need to be made.[25]

Background; corporate security and tackling cyber crime

2.6 The private sector has a lot to lose from being a victim of cyber crime and the costs or consequences of victimisation manifest themselves in a variety of ways. For example:

- Financial loss from theft or fraud;
- Loss of invaluable customer information or intellectual property;
- Possible fines from legal and regulatory bodies (e.g. FSA, Information Commissioner) or expensive court actions resulting from breach of data protection or confidentiality regulations;
- Loss of reputation through 'word of mouth' and adverse press and social media coverage (and word can spread very rapidly indeed); and, under a range of scenarios,
- Survival of the organisation itself.[26]

2.7 Looking at losses that occur as a result of reputational damage – and cyber offences clearly represent a risk, as the Directors of high profile

[23] IT Governance Ltd (2015) *Cyber Security: A Critical Business Issue* (www.itgovernance.co.uk).
[24] Cabinet Office (2011) *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world*, London: Cabinet Office.
[25] Institute of Directors (2016) Cyber Security: Underpinning the Digital Economy. IOD Policy Report, March.
[26] IT Governance Ltd (2015:3) op cit.

victims like Talk Talk attest to[27] – can be instructive. A quick review of the literature[28] suggests the following:

- Loss of sales
- Fall in stocks and share prices
- Loss of profit
- Adverse media coverage
- Higher employee turnover
- Key staff/talent retention issues
- Employee disengagement and dissatisfaction
- A drop in consumer confidence
- The loss of suppliers or sales
- Reduction in influence of the organisation on policy-makers in their sector/industry
- The costs and complications of managing recovery and improving resilience after a cyber attack[29]

2.8 Further, some sectors face a greater risk than others. Finance and insurance are perceived to be at the highest risk, followed by information and communication, manufacturing, retail and wholesale and then energy and utilities.[30] That said, any organisation, in any sector, can be a victim of cyber crime of some description, and almost definitely all already have been (whether they know it or not).

2.9 While corporations have long focussed on the threat of cyber crime, there is increasing evidence that this is moving further and further up the corporate risks priority list, and not just to protect themselves. For example, there has been research which suggests that some companies at least would be prepared to invest in cyber security where it was necessary for protecting the national infrastructure because they placed a value on being good corporate citizens, or what one author calls 'civic-mindedness'.[31] Moreover, given that a significant part of the

[27] Talk Talk reported that profits more than halved as a direct results of being victimsed. See: http://www.bbc.co.uk/news/business-36273449. Accessed 12th May 2106.

[28] For example: Brady, A. K. (2003). How to generate sustainable brand value from responsibility. *Journal of Brand Management*, 10(4/5): 279-289; Dietz, G., & Gillespie, N. (2011). *Building and restoring organisational trust*. London: Institute of Business Ethics; Honey, G. (2009). *A short guide to reputation risk*. London: Gower Publishing; MacMillan, K., Money, K., Downing, S., & Hillenbrand, C. (2005). Reputation in relationships: measuring experiences, emotions and behaviors. Corporate Reputation Review, 8(3), 214-232.

[29] There are of course many other examples, see the experience of Carphone Warehouse for example: http://www.theguardian.com/technology/2015/aug/10/carphone-warehouse-uk-data-watchdog-investigating-customer-hack. Accessed 14-9-15.

[30] Accounting respectively for 25.33%, 19.08%, 17.79%, 9.37% and 5.08% of incidents.
IBM Security (2015) *IBM 2015 Cyber Security Intelligence Index*, IBM Corporation. (Figure 2, Appendix p3)

[31] Hare, F.B. (2009) Private Sector Contributions to National Cyber Security: A Preliminary Analysis. *Journal of Homeland Security and Emergency Management*, 6, 1, pp 1-20.

response to cyber crime is raising awareness, the private sector has a potentially important role to play.[32]

Information security, corporate security and security suppliers

2.10 Corporate security has taken on responsibility for some offence types, and fraud is one example, precisely because the police have been seen to be ineffective and sometimes unsupportive.[33] Of course, some organisations have large and dedicated ICT departments that are able to build up a profile of risks and develop appropriate responses.[34]

2.11 Traditionally information technology specialists held responsibility for tackling cyber threats, although commonly, responsibility has been allocated to groups with two distinct skill sets; those responsible for corporate security who are specialists in protecting the organisation against different types of threats, and those with knowledge of computers, systems and technologies from a typically information technology background. More recently, a new specialism has emerged in the form of 'information security officers', who incorporate technological knowhow as well as broader security knowledge. Indeed, there has been a shift from the information security lead being accountable to the Head of IT to other business functions.[35] Yet, while both information security and corporate security may be involved in heading a response to cyber crime;[36] practices vary markedly. It is perhaps worth pausing to consider the relative merits of each area.

2.12 Tyson (2007) who has written most extensively on the topic, notes the typically different skill sets and culture of those who emerge from information technology backgrounds on the one hand and physical security on the other. He underlines the point that each brings a different contribution to protecting against cyber crime. For example, Tyson notes, '*IT security requires technical expertise but not large numbers of staff, whereas physical security generally has the opposite*'.[37] And of course, while the response may involve technical

[32] The banking sector is one example, see: Bamara, A. and Bhatt, M. (2013) Cyber Attacks and Defense Strategies in India: An Empirical Assessment of Banking Sector. *International Journal of Cyber Criminology*, 7, 1, June, pp. 49-61.
[33] See for example, Doig, A & Levi, M (2013). A Case Of Arrested Development? Delivering The UK National Fraud Strategy Within Competing Policing Policy Priorities. *Public Money and Management*, 33, 2, 145–152.
[34] Corporation of London (2015) op cit, p51.
[35] Rossie, B. (2015) Top 6 Cyber Security Predictions for 2016. *Information Age*. http://www.information-age.com/technology/security/123460537/top-6-cyber-security-predictions-2016.
[36] An interesting study has been conducted by Frey and Osborne who evaluated the susceptibility of different jobs to computerisation. In all they found that approaching a half (47%) of US employment is at risk. It would be interesting to see how different parts of security fare under their analysis. See, Frey, C. and Osborne, M. (2013) The Future of Employment: How Susceptible are Jobs to Computerisation? University of Oxford. http://www.oxfordmartin.ox.ac.uk/downloads/academic/The_Future_of_Employment.pdf. (accessed 27-1-16)
[37] Tyson, D (2007) *Security Convergence: Managing Enterprise Security Risk*. Burlington, MA: Butterworth-Heinemann

issues, indeed it inevitably will, it may also draw upon the eyes and ears of both aware staff (across the organisation) and a focussed security function. Taking this final point further, Tyson notes that security officers understand the buildings, how they work and can feedback on things that look out of place (not least when they are prepared adequately in what to look for) adding:

> *With your in-house guard force you can then expand this role to look for more worrisome breaches, such as rogue wireless access points or passwords left on written notes around work surfaces.*[38]

2.13 The importance of a physical security role in protecting against cyber has been emphasised by other official sources. For example the UK Government's IT Governance Green Paper noted:

> *The physical avenue is through gaining direct, physical access to your organisation. An attacker may gain access to computers, hard copies of files, mobile devices such as laptops or tablets, and your employees. Mitigating this risk involves securing the physical perimeter, which is readily achieved and already standard practice in many organisations. Organisations should – at the very least – monitor all entrances and exits, train staff to report strangers within the perimeter, and place security measures on external doors and internal secure areas.*[39]

2.14 Yet, and this needs to be emphasised, when it comes to security suppliers, it is far from clear whether they are an unqualified good. For example one writer has lamented what he calls the, '*commoditisation of cyber security*' and argues:

> *'It's sad to say but many companies have been foolishly paying outrageously high fees for security experts that are little more than standards readers or script-kiddies armed with open-source software tools'.*[40]

2.15 There is one final point that merits attention here, in that one of the difficulties faced by companies looking to protect information is a lack of staff. One US study addressing the numbers of information security personnel found, *'surprisingly few full time employees per organization, and a disturbing number with none.'*[41] The number of applicants who lacked relevant skills was a major reason offered for this. Moreover,

---

[38] Tyson, *op cit*, p 115.
[39] Calder (2015:4) *Cyber Security: A Critical Business Issue*. IT Governance Green paper.
[40] Lacey (2015) David Lacey's IT Security Blog. Computer weekly.com. 25-1-15 (http://www.computerweekly.com/blogs/david_lacey/2015/01/predictions_for_2015.html). Not paginated.
[41] Whitman, M.E. and Mattord, H.J. (2015) *2015 SEC/CISE Threats to Information Protection Report*. Security Executive Council and Coles College of Business, Center for Information Security Education, Kennesaw State University, p. 12.

information security does not always report at the highest level, leading the authors to conclude that this might *'indicate a dilution of the strategic nature of information security in the organization'*.[42]

Engaging the workforce: the importance of Enterprise Security Risk Management and 'convergence'[43]

2.16 While the response to cyber crime involves a wide range of strategies[44], central to them, both as risk factors and important constituents of an effective response, is people. Malicious insiders have always been a major risk to organisations and the cyber revolution has merely increased the options for them to victimise a company. One research report has noted that the most common cause of the most frequent types of breaches, '*accounting for 90% of all incidents - is people*'[45] though this can commonly be inadvertent as well as malicious.[46] Often, good general security is also good cyber security, although the link is not always explicitly made.

2.17 Just as the general protection of the organisation has long been seen to involve all parts of the organisation (not just those dedicated to security), the pervasive nature of the cyber threat requires no less a commitment. After all, as Calder (2015) notes, staff retain company information on their own gadgets, '*which is increasingly beyond the employer's oversight*'.[47] Staff can both increase an organisation's vulnerability to cyber crime (through negligence as well as criminal activities) as well as act as a key ally in its protection.[48]

2.18 There is nothing new in highlighting the importance of a whole organisation approach to security.[49] Enterprise Security Risk Management has long made this case:

> *Security professionals are recognizing that whatever risks their organizations face, they need to reach across all business units to ensure that every department collaborates with the goals of enhancing security, increasing the bottom line, and assisting the organization in meeting its objectives. This is Enterprise Security Risk*

[42] Ibid, p16.
[43] The word 'convergence' is used with abandonment although it has many interpretations even when related to security. Here it concerns the convergence of corporate and information security, but for other interpretations, see: Booz Allen Hamilton (2005) *Convergence of Enterprise Security Organizations*. Alexandria, VA: The Alliance for Enterprise Security Risk Management. For an insight on ESRM specifically, see: https://cso.asisonline.org/esrm/Pages/default.aspx.
[44] That said, there are specific initiatives in evidence to provide holistic management of risk across different types of security activities. For example, see: https://gsrma.files.wordpress.com/2015/03/gsrma-announcement.pdf. Accessed 27-1-16.
[45] Verizon (2015) *2015 Data Breach Investigations Report*. Verizon, p32.
[46] For a discussion, see: Whitman, M.E. and Mattord, H.J. (2015) opp cite.
[47] Calder (2015) op cit p 4
[48] For a discussion on this issue, see, Gill, M. (2014) Exploring Some Contradictions of Modern Day Security. In M. Gill (ed) *The Handbook of Security*, Second Edition. London: Palgrave.
[49] For example, see, Beck, A. (2009) *New Loss Prevention*. Basingstoke: Palgrave.

> *Management (ESRM). It is a vital element of Enterprise Risk Management (ERM), which examines the universe of risks—financial, strategic, operational, legal, accidental, and so on—that an organization faces.*
>
> *But where ERM has typically been associated with the financial side of business—such as credit risk and commodities-pricing risk—ESRM highlights the protection of assets and activities such as physical security, investigations, crisis management, business continuity, and data protection. Any disruption in one of these areas could be as harmful to an organization's profit or reputation as a hedge-fund investment or currency-exchange practice. And, unlike a physical security lapse, a bad trade is not likely to put an employee in harm's way.*[50]

2.19 A word that is perhaps more common parlance than ESRM is 'convergence', (occasionally referred to as coherence), which also focuses on different security elements of the organisation coming together to tackle cyber crime, although as noted typically, but not always, refers specifically to corporate and information security partnering. Tyson (2007), defines it this way:

> *Security convergence is the integration, in a formal, collaborative, and strategic manner, of the cumulative security resources of an organisation in order to deliver enterprise-wide benefits through enhanced risk mitigation, increased operational effectiveness and efficiency, and cost savings.*[51]

2.20 The credibility of 'convergence' has been enhanced following its incorporation into a security standard that referred to it in the following terms:

> *In order to effectively protect its assets, an organization needs to recognize the interdependencies of various business functions and processes to develop a holistic approach to PAP*[52]*…the organization should consider: a) A common basis for risk ownership and accountability; b) An integrated risk assessment and harmonized treatment strategy; c) Common lines of communications and reporting for assessing and managing risk in a cross-disciplinary and cross-functional fashion; and d)*

[50] ASIS International, CSO roundtable (2010) *Enterprise Security Risk Management: How Great Risks Lead to Great Deeds: A Benchmarking Survey and White Paper*. Arlington: ASIS International. https://www.rims.org/resources/ERM/Documents/Enterprise%20Security%20Risk%20Management.pdf
[51] Tyson, 2007, op cit p 4.
[52] Physical Asset Protection

> *Establishing cross-disciplinary and cross-functional teams to achieve a co-ordinated pre-emptive and response structure.*[53]

2.21 However, that stated, convergence in security does not appear commonplace.[54] Nor is it clear how convergence can be implemented in different organisational settings most effectively.[55] Given the relatively high 'insider' risk noted above, whether through intentional, or inadvertent means, there is clear merit in the unification of different security elements, and most often the whole workforce to tackle the threat, albeit that this is commonly not the practice. Indeed, in one survey, amongst the main internal threats to information protection were; failure of staff to follow the set policy; and a lack of staff training.[56]

2.22 Moreover, organisations appear to lack faith that they will be able to prevent future attacks. One recent study reported that only just over a fifth of respondents were confident their organisation could withstand a cyber attack and:

> *(T)he results show that many organizations are apprehensive about their ability to deal with current and emerging threats and are either planning to increase spending on non perimeter security tools or have done so. A resounding 63% admitted to being only somewhat confident about stopping a cyber attack, while 16% confessed to being not very confident or almost certain of getting breached.*[57]

The response to cyber crime: incorporating the role of the police

2.23 There is a range of initiatives that have been developed by different authorities to help businesses respond more effectively to cyber threats. Bossler and Holt (2013)[58] and Taylor et al (2010)[59] are

---

[53] ANSI/ASIS PAP.1 - 2012 Standard, p. xiv. ASIS International is currently working with ISC(2) and ISACA International on a new security awarerness standard that will higjhlight again the benefits of a holistic response and the drawbacks of working in silos; this approach is very much in the convergence tradition.

[54] See for example finding to survey by Whitman and Mattord, op cit.

[55] A range of interesting papers have been produced on convergence from a variety of authorities but many are not published. ASIS International have been high profile in this area. See, Dorey, P. Willison, J. Sembhi, S. (2012) *Converged security Management Survey*. ASIS International and Information Security Awareness Forum; CSO Roundtable (2010) *Enterprise Security Risk Management: How Great Risks Lead to Great Deeds*. A benchmarking Survey and White Paper. Alexandria: ASIS International; Willison, J. (2009) *Security Convergence and ERM: A Case for the Convergence of Corporate, Physical and IT Security Management*. ASIS International and ISACA.

[56] Ibid.

[57] The Cyber Security Trend Report (2016). UBM. http://techbeacon.com/sites/default/files/2016-Cybersecurity-Trend-Report-UBM-Ponemon-HPE-study-report-survey.pdf, p.3.

[58] Bossler, A. and Holt, T. (2013) Assessing officer Perceptions and Support for On-line Community Policing. *Security Journal*, 26, 4, pp 349-366.

amongst those who have highlighted the need for and importance of private-public partnerships. One example is the *cyber essentials scheme*, which has been developed by the UK Government and industry to fulfil two functions. It provides guidance on the basic controls all organisations should implement to mitigate the risk from common internet based threats, within the context of the Government's *10 Steps to Cyber Security*. And through the Assurance Framework it offers a mechanism for organisations to demonstrate to customers, investors, insurers and others that they have taken the essential precautions.[60] Meanwhile the UK Home Office has published advice on how businesses and individuals can keep themselves safe online.[61] Moreover, there are some Government and industry led initiatives, for example, the Cyber-Security Information Sharing Partnership (CiSP)[62]: This is an online social networking tool that facilitates the exchange of information on threats and vulnerabilities as they occur in real-time.

2.24 In the UK, the National Crime Agency coordinates the national response to cyber crime and includes the National Cyber Crime Unit to lead this. The Unit has several aims in addition to providing an investigatory response to the most serious types of threats. These include supporting other police units as well as the private sector in developing capabilities to resist attacks. In the UK at least, reports of cyber crime are mostly be made via Action Fraud where the reports are then referred to a local police force for action. However, there is a wealth of evidence suggesting that the police have struggled to keep up with the fight against cyber crime. This is partly because their traditional skill sets are not those typically needed to tackle online offences.[63] Moreover, one of the main findings from research to-date suggests that the response to cyber crime will *inevitably* involve more skill and resources than the police have available. Wall (2007:197) has argued that the police is a, '*relatively minor player in the broader network of security that constitutes the policing of cyberspace*', and because policing the internet is complex, an effective response will depend upon the police forging links with other 'nodes' of security which are wide and varied, but will include corporate security departments. He argues:

> '*Corporate security organisations also exercise contractual governance over members of their organisation (employees and clients) as well as outsiders to protect their corporate interests through contractual terms and conditions (auspices) which threaten the removal of privileges, or private or criminal*

[59] For example, see, Taylor, R.W., Fritsch, E.J., Liederbach, J. and Holt, T.J. (2010) *Digital Crime and Digital Terrorism*, 2nd edition. Upper Saddle River, NJ: Pearson Prentice Hall.

[60] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317480/Cyber_Essentials_Summary.pdf (accessed 14/09/15)

[61] https://www.cyberstreetwise.com (accessed 15/09/15)

[62] https://www.cert.gov.uk/cisp/

[63] For a discussion around this topic where identity crimes are an example, see, Wall DS, '(2013) Policing Identity Crimes', *Policing and Society: An International Journal of Research and Policy*, 23.4, 437-46

prosecution in the case of more serious transgressions. In addition, corporate security organisations will employ a range of software solutions, not just to protect themselves, but also to identify and investigate abnormal patterns of behaviour in their systems and also, in some cases, amongst their clients.[64]

2.25 Wall (2007) notes that part of the difficulty is having trust in partners, and there is a lack of awareness of the capacity of other nodes to contribute to tackling cyber crime.

2.26 Yet other nodes do play a crucial role. To provide an example, one study has looked at the characteristics of an effective response to online auction fraud.[65] It concluded that a multi-faceted approach was required, including the need to educate the public in how to prevent themselves from becoming a victim, a greater focus on prevention in the private sector, better law enforcement investigation approaches, greater international police cooperation, and more public awareness when cyber criminals are identified and prosecuted.

2.27 In fact, raising awareness and engaging diverse audiences is a common theme in research concerning the response to cyber crime. Often this is focussed on involving experts, not least those with technical knowledge who can keep abreast with the advances in technology[66] many of whom are working in the private sector.[67] However, the general public also have a role to play here.[68] Some people have specific skill sets that enable them to track offenders and pass this information to the police, and note some successes in having some websites suppressed,[69] but also in being able to better protect themselves.

2.28 Yet evidence suggests that some police officers, at least, are sceptical, in part seeing outsider input as unnecessary, and perhaps understandably being concerned about motives, they also fear vigilantism.[70] Police officers participating in one study (Huey et al, 2012:94) saw '*public involvement in cyber-policing as something that*

[64] Wall D (2007) Policing cybercrimes: Situating the public police in networks of security within cyberspace. *Police Practice and Research* 8(2): 183–205. p, 188.
[65] Conradt, C. (2011) Online Auction Fraud and Criminological Theories: The Adrian Ghighina Case. *International Journal of Cyber Criminology*, January – June 2012, Vol 6 (1): 912–923
[66] It is worth noting, as one respondent has to this study, that various software solutions/technologies are being developed and sold as the 'solution' to preventing cyber crime because they identify and respond to the attacks on networks. It is big business as InfoSecurity Europe is evidence of. They have been around for quite a long time but undergo continuous development and refinement. They include Intrusion Detection systems, Identity Access Management, Firewalls, Anti-virus, Encryption, Network Defence Systems, Passwords, Security Incident Event Management Systems to name but a few. To be compliant with the various standards and Cyber Essentials you need evidence of good technical controls. The new European Data Protection Regulation will also expect to see evidence of how data has been protected and wants to see technology used as part of this.
[67] Cabinet Office (2011: 29) *op cit*.
[68] For example, see: http://www.dailymail.co.uk/femail/article-1269639/Amateur-sleuth-unmasks-male-nurse-encouraged-dozens-kill-online-watch.html. (accessed 14/09/5)
[69] Ibid
[70] Huey, L., Nhan, J. and Broll, R. (2012) 'Uppity civilians' and 'cyber-vigilantes': The role of the general public in policing cyber-crime , *Criminlogy and Criminal Justice*, 13:1, pp 81-97.

should be limited to providing basic tips', yet their study, *'suggests that the general public can be a significant partner to public law enforcement and the private sector in securing cyber-space*.'

2.29 Another study has looked at the potential of people in key strategic positions to be *'capable guardians'*,[71] in essence, to use their knowledge of the internet to disrupt activity.[72] One of the main barriers to doing this effectively has been a lack of awareness, but where this was tackled, via education awareness programs, it raised the possibility of adding to the cyber security prevention effort:

> *Our findings suggest that a more fundamental function of cyberspace managers (managers and developers of social media sites and Internet service providers, etc.) is to help facilitate capable guardianship by increasing guardians' contextual awareness of cyberspace. There are many ways in which this education of online users about their important role in crime control in cyberspace could be accomplished. For example, social media sites could display public ads describing cyber abuse, its consequences to the victims, and what ordinary bystanders could do to stop it. [73]*

2.30 In the UK, cybercrime investigative skills are increasingly (but slowly) being seen as a core part of any investigator's knowledge, rather than the preserve of a specialist.[74] However, much of the empirical research on the views of frontline police officers involved in tackling cyber crime has been undertaken in the USA. This shows that frontline officers often perceive at least some types of computer crime to be as serious as traditional crime types,[75] and being involved with tackling some types of cyber crime offered high levels of job satisfaction.[76] Additionally, at least some see merit in a collaborative approach. For example, those supportive of community policing generally were

[71] For an example of the application of this concept to a type of on-line offence see: Reyns, B. W., Henson, B., & Fisher, B. (2011). Being pursued online: applying cyberlifestyle-routine activities theory to cyber stalking victimisation. *Criminal Justice and Behaviour, 38,* 1149–1169; and Reyns, B. W., Henson, B., & Fisher, B.S. (2012). Stalking in the twilight zone: Extent of cyber stalking victimization and offending among college students.*Deviant Behavior, 33,* 1–25. Wall D (2007) Policing cybercrimes: Situating the public police in networks of security within cyberspace. *Police Practice and Research* 8(2): 183–205.

[72] One study has highlighted the role of internet communities in setting norms and expectations of behavior which contribute to a form of self policing, see: Wall D and Williams M (2007) Policing diversity in the digital age: Maintaining order in virtual communities. *Criminology and Criminal Justice* 7(4): 391–415.

[73] Vakhitova, Z. and Reynald, D. (2014) Australian Internet Users and Guardianship against Cyber Abuse: An Empirical Analysis. *International Journal of Cyber Criminology*, December, 8, 2, pp 156-171; 169.

[74] Baker, M. (2014) *College of Policing update on building police skills to tackle cyber crime*, available at: http://college.pressofficeadmin.com/component/content/article/45-press-releases/734 (accessed 01/10/15)

[75] Holt, T. and Bossler, A. (2012) Police Perceptions of Computer crimes in two Southeastern Cities: An Examination from the Viewpoint of Patrol Officers. *American Journal of Criminal Justice*, 37, pp 296-412.

[76] Holt, T. and Blevins, K. (2011) Examining Job Stress and satisfaction Among Forensic Examiners. *Journal of Contemporary Criminal Justice*. 27, 2, 230-250.

supportive of community policing online too[77] (which at the very least entails different police agencies engaging meaningfully with different online communities in a position to tackle online crime[78]). After all, and as alluded to above, the online community has been identified as the most significant group involved in policing the internet.[79]

2.31 A very good study has recently been published by the Corporation of London. This summarises some of the issues faced by police in tackling economic cyber crime, highlighting the law enforcement challenges. These include: the disjointed policing approach; the general reduction in police resources; the still emerging understanding of the profile of cyber offending diverse as it is; and the changing nature of cyber space making it both difficult to understand and access.[80] In any event, most businesses do not report most cyber incidents to the police[81] so there is not the opportunity to build up a comprehensive understanding of the problems.

Security and other technologies that afford opportunities for cyber criminals

2.1 Just as good people are a significant component of any security strategy,[82] so too is good technology. While it has long been obvious that technologies get hacked by the bad guys, what is emerging as a key consideration is the extent to which security technologies create opportunities for cyber offenders. The 'internet of things'[83] can be as good for the offender as for the homeowner or facilities manager, posing threats to the home, workplace and the national infrastructure.[84] The very complexity of systems for the 'average Joe' creates even more opportunities for the savvy offender.[85]

[77] Bossler, A. and Holt, T. (2013) op cit.
[78] For example, see, Brenner, S.W. (2009) Cyberthreats: The Emerging Fault Lines of the Nation State. New York: Oxford University Press; Jones, B.R. (2007) Comment: Virtual neighborhood watch: Open source software and community policing against
cybercrime. The Journal of Criminal Law & Criminology 97(2): 601–629.
[79] The work is a bit old now, but the arguments are in many cases still relevant: Wall, D.S. (ed.) (2001) Cybercrimes and the Internet. In: *Crime and the Internet*. New York: Routledge, pp. 1–17.
[80] Corporation of London (2015) opp cit, p29.
[81] Institute of Directors (2016) opp cit.
[82] Deloitte & NASCIO (2014) *2014 Deloitte-NASCIO Cybersecurity Study*.
[83] Just one of the many articles on this can be viewed here: Gershenfeld, N. and Vasseur, J. (2014) Foreign Affairs, March-April, 93 (2), not paginated (www.foreignaffairs.org).
[84] Watch and listen to a good discussion from a range of experts: www.youtube.com/watch?v=EIV6B_teQZ8. What emerges here – amongst other things -is the importance of 'trustworthiness'. Trust is a major issue within cyber security, for a discussion around some of the issues, see: Gill, M and Crane, S. (2015) The Role and Importance of Trust: a Study of the Conditions that Generate and Undermine Sensitive Information Sharing. *Security Journal*. doi:10.1057/sj.2015.13. Some of the more strategic and technical implications are drawn out in work by the National Institute of standards and Technology (NIST), see: https://pages.nist.gov/cpspwg/.
[85] For an interesting discussion on how DVR based CCTV as well as cloud systems create opportunities for offenders because providers are not closing gaps see: Is your CCTV Safe from Cyber Attack? Cloudview. http://www.cloudview.co/dls/white/cyber-attack-white-paper.pdf. Accessed 11 March 2016.

2.2 One classic case, following work by Flavio Garcia, a computer scientist at the University of Birmingham, with colleagues Baris Ege and Roel Verdult at the Radboud University Nijmegen in the Netherlands, found that weaknesses in the design of a car anti-theft device enabled it to be hacked.[86] Interestingly the car manufacturers attempted to prevent the finding from being published fearing it would lead to a spate of attacks (and no doubt undermine sales). In another example security flaws have been inadvertently built into (Dell) computers putting users' personal data at risk to hackers.[87]

2.3 An even more worrying finding emerged from research conducted by Kapersky labs which investigated the vulnerability of a range of internet connected devices around the home. In addition to the home security system, a range of other household products were found to have vulnerabilities that could be exploited by an offender. The research, '*discovered serious threats to the connected home. These include a coffeemaker that exposes the homemaker's Wi-Fi password, a baby video monitor that can be controlled by a malicious third party, and a smartphone-controlled home security system that can be fooled with a magnet'*.[88] Some solace was found in that credible vendors were considering and responding to such risks in the product development stages.[89] The scale of risk here is summed up in an article by Mark Johnson:

> *...there is no reason why a robot could not be maliciously programmed to hurt someone. Or someone could insert explosives into a robotic vehicle and program it to drive into a school. Or program a drone to fly into the engine of a jet liner as it comes into land. Or attach recording equipment to drones in order to collect news stories about senior employees of major corporations. Or use one drone to down another drone as it delivers valuable goods to a remote customer site. Or hack into a drone delivering medical products in order to learn who is taking what medication. Or…again, the list is almost endless.*[90]

---

[86] See, http://www.londonlovesbusiness.com/business-news/business/is-your-car-one-of-the-hundreds-of-models-at-risk-of-being-stolen-thanks-to-a-big-security-flaw/11162.article?utm_source=Sign-Up.to&utm_medium=email&utm_campaign=17719-308069-09%2F10%2F2015+London+newsletter

[87] Dell admits security flaw was built into computers. http://www.bbc.co.uk/news/technology-34910649. Accessed, 4th Feb 2016. See also, Lenovo: researchers find 'massive security risk'. http://www.bbc.co.uk/news/technology-32607618. Accessed, 4th Feb 2016. Attacks are not new of course, but the vulnerability of security systems has started to increase opportunities for offenders.

[88] The Risks of a Smart Home, Asia Specific Security Magazine, 9th November 2015. http://www.asiapacificsecuritymagazine.com/the-risks-of-a-smart-home/.

[89] For a discussion on the role of security suppliers in this regard, see, Tyson, D. (2015) The New World of Converged Security. *ASIS International, UK Chapter Newsletter*. Autumn, pp 1 and 14.

[90] Johnson, M. (2016) The Internet of (Hackable) Things. *Loss Prevention Magazine*. http://www.lpportal.eu/content/editorial/articles/web-and-mobile-fraud/internet-hackable-things/. Accessed 27-1-16.

2.4 Vendors though, as the following quote shows, can be exploited by cyber criminals in a different way, making the existence of 'harmful services' a disincentive for businesses to invest in protection:

> *There are also new forms of service delivery and types of services. These include services supplied by reputable online suppliers to legitimate users. There is also the delivery of harmful services via more sophisticated versions of crimeware-as-a-service, where criminals require no knowledge of computers or systems because online specialists supply them with the means. This might include malicious software, supporting infrastructure or stolen personal and financial data.*[91]

2.5 Tellingly, the authors also note:

> *As the internet continues to become entrenched in our daily lives and we share increasing amounts of data, cyber-enabled and cyber-dependent crime will increase if only because the permutations of incentive, opportunity, and low risk of investigation and prosecution traditionally invite criminal activity.*[92]

Cyber crime: a different threat or just like any other?

2.6 There are a number of overlaps between cyber crimes and conventional crimes. After all, some cyber enabled offences are equally possible to commit without the use of the internet:

> *'You don't invite criminals into your house from the street, don't let them into your house online.'*[93]

2.7 Moreover, the people aspect to defending against cyber offences, as has been noted, is a key – and often the most important one – in any response.

2.8 Yet, there are features of the 'cyber' threat that arguably make it unique[94] (to name but a few - speed, adaptability, innovation, scale, and that it is hard to detect)[95] and therefore requiring a distinct approach. The main arguments for categorising crime as cyber have

[91] Corporation of London (2015) op cit, p21.
[92] Ibid, p27.
[93] Blue Coat (2014) *Cybercrime vs. Non-Cyber Crime: What are the Comparative Effects?* Available at https://www.bluecoat.com/company-blog/2014-06-30/cybercrime-vs-non-cyber-crime-what-are-comparative-effects (accessed 22/10/15)
[94] Europol (2014) *The Internet Organised Crime Threat Assessment* Available at https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta, p.9.
[95] Europol (2014) *The Internet Organised Crime Threat Assessment* Available at https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta, p.9.

been summarised as legal, moral and informational/descriptive[96] but the question remains whether it is useful when determining the type of threat posed and the necessary response.

2.9 A key point here concerns the characteristics of cyber offenders, albeit that this is another area where insight is lacking.[97] Work on case files by the UK Home Office described offenders as, '*reasonably, but not excessively, technically skilled*.' Often, simple security measures would have helped tackle this type of offender, but they add that this is likely to represent just a fraction of the more capable offenders targeting businesses (who have not been identified or prosecuted). This, then, '*raises questions regarding how easy it is to find, or charge, an offender who is a stranger, overseas or is more highly skilled and careful*.'[98] In this way, the cyber threat can perhaps be seen as more distinct.[99]

2.10 There is another issue which makes it marks cyber crime out as different to other offence types and that is the pace with which it is developing. There are increasingly more ways of making purchases and not least from mobile devices, more information is being moved away from the direct control of business to the cloud, and technologies are continually emerging to make business and home life easier and quicker, but supply chains are no stronger than their weakest links (and these too are often outsourced). These new developments create new weak points that offenders are quick to exploit before vulnerabilities can be identified and fixed (zero day attacks). The cyber security learning curve is a very steep one.[100]

2.11 It seems cyber security threats are becoming a priority. The National Association of Board Directors in the US has outlined the principles governing how cyber crime should be managed underlining that it should be a key concern of the Board.[101]

---

[96] Tavani, H. (2000) 'Defining the Boundaries of Computer Crime: Piracy, Break-Ins, and Sabotage in Cyberspace', *Computers and Society*, September 2000, pp 3-9.

[97] Hargreaves, C. and Prince, D. (2013) opp cit, suggest ways in which a greater focus on offenders and victims can provide a more nuanced response to different types of cyber offences.

[98] Sutherland, C. & Dowling, S. (2015) *The nature of online offending*, Home Office Research Report 82, London: Home Office, p3.

[99] An interesting experiment was conducted, Project Cumulus, where a research team leaked a fictitious password to the Dark Web (owned by a banker) to see how fast the credentials would spread. Seemingly 'within days', 1400 hackers accessed the victim's Google Drive, bank account, and more. See: https://www.linkedin.com/groups/38412/38412-6111601826212098050. Accessed, 11th March 2016.

[100] There is one final point to emphasised here. Organisations employ a wide range of technologies some of which have been discussed above. There is every evidence that many have been very effective, not last in avoiding – so far at least – a cyber 9/11.

[101] See discussion, '5 Things Every Board Member Needs to Know about Security'. *Security*. http://www.securitymagazine.com/articles/86696-things-every-board-member-needs-to-know-about-security.

Conclusion

2.12 This section has sought to highlight both the opportunities for the private sector generally and private security specifically to fill gaps in the response to cyber security recognising the limitations of all the key crime prevention players which broadly encompass a lack of awareness, a lack of resources, a lack of prioritisation and skills set shortages, amongst others. It is clear that much of the national cyber security infrastructure is in private hands and that private business and private security have a key role to play in the development of the field. Moreover, many cyber security experts are in the private sector, the role of people in protecting against cyber crime is crucial, and private security personnel are in abundance.

2.13 The information in this section needs a context, it is almost a caveat. It has been argued by John Chambers that by 2020[102] three quarters of businesses will become fully digital, but much less than a third will be successful. That the vast majority of companies despite realising that digitalisation is crucial do not have a strategy for getting there. Where then is security in the great scheme of things?

2.14 We also know that, for a variety of reasons, including a lack of resources and expertise, the police are ill-equipped to tackle cyber crime alone; their success depends on forging close partnerships, yet all too often private and corporate security appear only as bit players in current partnership working arrangements. Security is not an unqualified good, security measures can create cyber crime opportunities, and that is why a crucial appraisal of the role of private security in tackling cyber crime is long overdue.

[102] John Chambers, keynote speech at the Internet of things World Forum. 15th December 2015. https://www.youtube.com/watch?v=k0EZRWNtN9I. Accessed 15 March 2016. One of the things he argues is essential is an effective 'security architecture'.

Section 3. The role of technology

The sample

3.1 While a fuller explanation of the methodology and the response rates are provided in the Appendix a summary is perhaps helpful here. An online survey of security professionals was conducted. A total of 289 responses were received, although not all of these included answers to every question. Of those who provided demographic information 92% of respondents were male, 13% were aged up to 34, 21% were aged between 35-44, 38% were aged were aged between 45 and 54, 23% were aged 55-64, and 5% were over 65. The respondents worked for companies operating in 19 different sectors. Approaching a half the sample said they worked for an organisation based in the UK (48%).

3.2 Of the 286 who gave details about their work, 161 (56%) could be described as 'mainly physical security', and 83 (29%) as 'mainly cyber security',[103] 42 (15%) described their work as 'other' (e.g. a researcher). Of those who were 'mainly physical security' all gave further details, and of these 67 (42%) were 'suppliers', 75 (47%) were 'clients' and 19 (12%) were 'other'. Of the 83 who were 'mainly cyber', 27 (33%) were 'suppliers', 42 (51%) were 'clients', and 14 (17%) were 'other'.

3.3 It should be noted, when reading the findings, that we cannot make any claim about the representativeness of the sample; we don't know enough about the populations, and this should be borne in mind.

3.4 The survey was supplemented by in-depth interviews. Additionally, throughout the development and implementation of the research the views of experts from around the world were sought and used to inform the progression of the project.

The findings

3.5 Of those who had an opinion either way, 84% agreed that corporate organisations were poor at preventing cyber threats, in fact only 12% disagreed in any way with this statement.[104]

3.6 Moreover, most of those who provided an answer agreed (69%) that generally speaking organisations were poor at e-testing cyber resilience and a low percentage (10%) disagreed in any way.

3.7 And most agreed (63%) that generally speaking organisations were poor at knowing when there has been a breach of security. Again a low percentage (12%) disagreed in any way. Those working mainly in cyber

[103] Here we have included those who noted that their main activity was exclusively in one area and mainly in that area.

[104] There were similar proportions agreeing from those who worked mainly in cyber security (65%) and those who worked mainly in physical security (62%). Clients though were proportionately twice as likely (17%) than suppliers to (8%) to disagree, but small numbers here (19 and 7 respectively) suggest caution with this finding.

security were much more likely to agree with this statement (73%) compared to those working in mainly physical security (55%). At least part of the problem was that offences are not always visible:

> *'Our clients, in most cases at least, don't see the threat of cyber, it is not visible, they would have to be shown something to notice'.* Head of Security, Construction

> *'It is not well understood, I work with start ups as well as multi-national companies, and on the whole, they think it will not happen to them. There is a lack lustre attitude, it baffles me…Security is not an easy sell. We have done workshops on security, and it is a tough sell, security people are associated with firewalls and they don't think of servers themselves … We say invest but they don't listen, it is silly because it could be prevented'.* Consultant, Website Development

3.8 Perhaps this underlines the reality that approaches to tackling cyber offending are still not developed. This is not to overlook the considerable progress that has been made over many years (it is worth noting that there was the *Computer Misuse Act* of 1990). It is perhaps more a reflection of the ubiquity of the internet in daily social and business lives, and the rather different security challenge this poses when security skills and legal frameworks have been developed for rather different types of threats.

Is cyber crime different?

3.9 Of the respondents, 45% believed that cyber and physical security were equally important in the companies they were linked to, 25% reported that cyber was more important, and 25% that cyber was less important (5% were unsure). Far fewer clients (14%) thought cyber was less important than suppliers (32%), in fact most clients thought they were of equal importance (56%) whereas this was true of just 38% of suppliers. There was little difference between those who worked mainly in cyber and those in mainly physical security.

3.10 When asked about the relevance of technology in tackling cyber offences nearly all of those who answered, predictably, highlighted its importance (92%), only 3% (6 people) argued that it was not fundamental. But when asked directly whether people issues were more important than technology ones over half of the sample (55%) agreed they were, although nearly a fifth (24%) disagreed. Interestingly, of those who shared an opinion either way, those who worked in mainly cyber security were less likely to disagree (23%) than those who worked in physical security (36%). More than 2 in 10 (21%) clients disagreed with the statement 'tackling cyber crime is more about people issues' and 3 in 10 (30%) suppliers disagreed.

3.11 When asked whether they agreed that the best defence against cyber crime was an alert workforce, far more agreed (81%) than disagreed (12%).[105] This is an important finding because it stresses the potential role of different parties in tackling cyber crime, a point that will be returned to later. Two comments made at the end of the online survey are worth quoting here:

> *'Education and awareness within a workforce is one key element to preventing cyber-security threats. You could have all the technical security solutions in the world and all it takes is the human factor to create risk and introduce a threat'.*

> *'We need cyber responsible employees and a much higher level of cyber crime awareness amongst cyber natives. But fundamentally we need boardrooms not to categorise cyber risks and harms as a matter for IT Security specialists, but a something that needs a whole company response. Directors and CEO's need to stop Dad dancing at the edges and using the excuse that they do not understand and have a techy that does this stuff. This is about every member of a company that uses the internet, not one or two techies who the board choose to ignore most of the time.*

3.12 Another interviewee stated:

> *'The humans, all of your staff are your most effective line of defence. Technology is a critical part'.* Head of Cyber Resilience, Security Supplier

3.13 As noted above, there has been a tendency to treat cyber crime as if it were a different type of offence. However, there is evidence from this study that such a position is misleading.

3.14 In the survey, respondents were asked to express their level of agreement with the statement, 'there is a clear distinction between cyber incidents/crime and physical incidents/crimes'. Of those who answered, the majority thought there was (55%), with a minority disagreeing (28%). This finding will be interesting to explore again in the future, as smart technology becomes more integrated in our everyday lives. During the interviews we were able to explore these differences a little more, since a range of arguments were offered in support of both views. There were those that argued the principles were exactly the same; both dealt with a threat that merited a response and that it was helpful to assess all security issues in this way:

[105] Those working in physical security were only slightly more likely to agree with this (81%) compared to those working mainly in cyber (78%). Those who believed cyber security was more important than physical security were less likely to agree (70%) than those who felt physical security was more important (85%).

'Cyber is just another risk. Badges and passwords are the same thing'. Head of Security, Telecommunications

'The physical security and the CISO are both in charge of access control, exactly the same thing with the same principles'. Director, Information Security, Manufacturer

3.15 Interviewees were asked whether the process of investment decisions for security were the same or different for physical and cyber, and again practices varied. There were those that argued they were different:

'Cyber is just a raw constant changing program as technology and breaches develop, there has been a dramatic increase (in spending on physical security) whereas cyber is a rolling budget'. Engineering Manager, Defence Organisation

'It is a fact that it is different. In the physical world the decision is in a sense limited to the presence of a threat in a specific area and you an respond in a pragmatic way because you can respond to the source of the attack, but in the cyber world the response is more complex and requires a multi agency approach which is different. Laws will apply differently too'. Security Integration Officer, International Association

3.16 Other comments pointed to the same practices:

'Physical access control is same as logical access control, so we can think in the same way'. Security Manager (Physical), Bank

'We adopt the same methodology and use the same language, threat, vulnerability and impact and then look at the cost benefit analysis and with those the same document process is done for both, so when it goes up the chain people understand it; in the IS world there is a lot of jargon'. Security Manager, Energy provider

3.17 While other interviewees attempted to bridge the gap:

'The processes should be the same, I don't think they are. The threat is of a vulnerability, that much is the same, and they should be measured in the same way…The cyber risk is often unknown and the number who can access it is limited and so they don't put same effort in'. Information Security Consultant

> *'They are probably different but each party needs to have an awareness. If you go back to what is security therefore, to me it is to know the risks of the client and why they are being targeted and by who. To do this I need to know their total threat'.* Global Security Director, Security Supplier

3.18 These different answers reflect both different views about how cyber should be treated, and as a consequence, different practices. Another interviewee noted how they felt there had been a change of thinking, and that it was more helpful to distinguish threats in other ways than cyber/physical:

> *'We used to distinguish between them and break down everything into cyber and physical. In the last year though we've reclassified simply into internal versus external threats and both cyber and physical map over those. We found that trying to break it down too much – it gets too confusing, so we introduced the new matrix. There is so much overlap anyway - with cyber for example, it can be an internal threat that manifests as external threat – that caused the risk or harm. An internal physical flaw can quickly become an external cyber flaw'.* Training Consultant

3.19 Others thought along similar lines in recognising that the overlap between physical and cyber was sufficient to approach risk assessments in a similar way. For example:

> *'I follow the same risk assessment and risk evaluation process. They may require different skill sets to get under the skin of threats and the availability and effectiveness of controls, but broad resilience risk management should follow the same thought process'.* Head of Resilience, Utilities

> *'In fact, more and more they are the same place, as in physical security we are moving towards the same assessments and policies and we are working in the same direction, in a couple of years we will merge'.* Security Manager (Physical), Bank

> *'There are commonalities in the cyber risk assessment…* [*they*] *have a common core understanding…Physical security is a fundamental component of a decent information security strategy'.* Cyber security consultant

3.20 Convergence advocates will note that all these responses offer support for a strategy that seeks to harness the links between the two. Some noted that the point was less about whether they are different or the

same, the key issues is to recognise that there is inevitably overlap, and a breach in one can cause a weakness in the other for example:

> *'The two are intrinsically linked. A breach of cyber can provide the adversary with information to allow a physical attack. If a cyber attack gathers data about what is going on in a certain location it can lead to a physical incident and the need for physical intervention'.* Engineering Manager, Defence Organisation

> *'If you have a cyber attack there is often a physical element to it, a demand or a ransom for example, so it will soon become a ransom management project; information is a valuable asset after all, and these offenders know that'.* Security Manager, Service Provider

> *'If you are running an energy company and there is a protest outside you will know how to deal with it, and you may or not call your IT department, to say, check the fire walls, because it is more than possible there will be a cyber attack too. They may not happen at the same time, but it has happened here in this city and you need to think of these risks in similar terms'.* Convergence Engineer

3.21 Then again, some interviewees pointed to the differences in impact. Here there were arguments that the two broad offence types being discussed were different because the impact was greater. Some argued that this was more the case for cyber, one in fact, noting that with cyber *'corporations are in an epidemic place'*. One interviewee, an owner of an information security consultancy noted that there were various types of risks, *'chemical, biological, radiological, nuclear, cyber, and cyber facilitates all of these'*. Another argued the case for physical:

> *'When looking at physical and cyber there is a difference. When something goes wrong what is harmful? In the case of physical security human beings can get hurt, if cyber goes wrong no one will get physically hurt, no one will die unless a cyber attacker hacks hospitals, so outcomes of risks are different, with physical you can die with cyber the harm is more financially'.* Global Security Director, Security Supplier.

3.22 Another argument was that the nature of the risks were different. Some argued that it was the nature of physical security that made it more complicated:

> *'The biggest difference that I experience – we have about 150 offices and they all look different – different types of buildings, different security – I have to achieve security in all those places. The cyber folks – when they go to*

address something on a network, they are doing the same thing everywhere – the network looks the same everywhere, the computers look the same'. Director of Physical Security, risk management company

3.23 Others felt that the speed of cyber attacks was what distinguished them:

'Cyber has different elements, you cannot say, 'I am prepared no one can get me with a DNS attack because I sorted it last time'. The same attacker can go back. The threat changes faster than any other risk'. CEO, Cyber Threat Consultancy

'These complicate responses, when risks move fast, and when responses on one day cannot be relied upon to work the next, when offenders can perpetuate attempts with little chance of detection and far less of apprehension, when it is easy to keep trying and success is frequent...'.. Global Security Director, Security Supplier.

3.24 A different focus came from those who argued that the problem with cyber risks is that they were newer, there was a less well developed body of knowledge about them and less established practice in responding, all of which complicated the development of an effective response. Suppliers noted that some clients were not thinking about cyber, or thought about it in technical terms, and some clients admitted that their companies were more adept at traditional security practices and had yet to adapt to the cyber threat:

'I am not certain we have measured the cyber risk, it is more of a reactive mode…we will work with the business to identify risks and identify policies and procedures to mitigate that risk and look at vulnerabilities and then do it again and again…we do assessments of our own facilities and third party entities, we are then in proactive mode….and then we focus on making recommendations. I don't sense, based on what I have seen, my information security team do anything in a similar fashion'. Associate Director, Global Security, Manufacturer

3.25 Related to this, some pointed to the fact that the cyber response was more complicated, not just because it was more technical (at least sometimes) but because many of those charged with responding were not as skilled in this area as they might be in others:

'In almost every single case the vulnerability that was exploited was known and there was a fix available for 18

months[106] *…To assess the risk properly you need the right tools for the risk your organisation faces. There are two types, commercial off-the-shelf, and those you make yourself, and the tools you need to detect weaknesses for each are different. What happens is that coders can implement some code that exploits the weaknesses. So, if you don't speak the language you are kind of screwed'.*
Director, Information Security, Manufacturer

Discussion

3.26 There are those who see cyber crimes as another type of risk to the organisation, meriting security risk management strategies that are similar to any other. This approach tends to emphasise the fact that the response to both cyber and traditional crimes share common elements heightened by the need for an alert workforce, trained and prepared to identify security weaknesses (of all types) and supplemented (in a big company) by a dedicated team overseeing all risks.

3.27 Then there are those who see cyber as a distinct threat, and the common thread running through concerns here appear to be focussed on the fact that it is a newer and evolving threat, and one that organisations typically are only just beginning to deal with. Threats appear to change, occur in different parts of the world and can generate major reputational damage. Thus Boards have become more concerned and this too has resulted in an impression that they are different. Couple this with the fact that organisations generally have expanded their trade online (a trend which seems destined to continue) and that a technological response requires specific technical expertise (sometimes at least), and it is easy to see why the threat can be perceived as different.

3.28 Some of these issues are re-examined in the context of an approach which has received much commentary but about which more analysis is needed, that of convergence.

[106] An observation that has general support form other sources: https://www.cert.gov.uk/resources/best-practices/patch-management-and-vulnerabilities/(accessed 16th February 2016).

Section 4. Convergence

4.1 Certainly, cyber security is a relatively new specialism (at least compared to physical security) and the practice of determining the best responses and the best structures for managing those responses are territories that need better charting. It is far from clear what the best forms of 'convergence' are, what the criteria for determining what works are, and as will be shown, some argue that it may not be in the best interests of organisations to converge at all. So while, as will be shown, convergence principles received considerable support from the findings of this study, it is not seen as an unqualified good, and some respondents presented potential difficulties that have still to be overcome. These will be discussed first, after a few words to set the context.

4.2 Less than three in ten (29%) of the sample agreed that convergence was widely understood in relation to security, more disagreed (47%), although a higher percentage of clients (33%) than suppliers (24%) felt convergence was widely understood, as did those working outside the UK (38%) compared with in the UK, (19%).

4.3 Clearly, the fact that many believe that 'convergence' is not fully understood undermines its potential to be considered as a central or common strategy. Indeed, the fact that convergence was not properly understood was expressed in interviews too:

> *'When you look on web, there is a mistake about convergence. People say it is between physical security and information security, but it is not, it is between physical security and the technology infrastructure. Physical security is increasingly making use of technology, blue tooth, big data, intelligence, so when you talk about physical and IT security as being separate it creates a bit of confusion'.* Security Integration Officer, International Association

4.4 In interviews, these points were discussed in more detail. Some felt that convergence was more than just physical and information security working together (and for that matter the technology infrastructure), and highlighted the importance of other functions as is typically discussed in the context of ESRM (discussed earlier in this report). Even where convergence was promoted as being between physical and information security the difficulty was the degree to which collaboration or joint working was deemed necessary to be considered 'convergence'. Moreover, there is a need to better articulate what the implications are – the advantages and disadvantages - for different models of working

and what different levels of 'convergence' or integration mean in practice.

Dependent, independent, interdependent

4.5 Whatever the supposed merits of convergence, the practice, it seems, on a strategic level at least, is for physical and cyber to be organised separately by organisations. 51% of suppliers and 53% of clients said that there were separate strategies for physical and cyber security in the organisations they were connected to. Suppliers (19%) were less likely than clients (34%) to state that there was an overall strategy including cyber and physical.

4.6 There is certainly logic to different types of arrangements. As noted above, when asked what was more important, physical or cyber, the most popular answer was that they were the same.

4.7 One interviewee discussed the role of the various security functions, *'...so what is the Mission of one with the other?'* and that if *'the Missions don't align you cannot converge'*. Another noted that convergence may be suitable at a point in time, dependent on a variety of factors, including the maturity of both the business and the security elements, the nature and scale of risks, and the risk appetite of the Board (to name but three).

4.8 One consultant who has worked with companies on convergence issues, spoke about the various potential approaches in terms of the departments being dependent, independent or interdependent. He felt there were potential problems in bringing departments together – same offices, same line manager etc - so that they were dependent on each other and were essentially, in practice, one department. The principal reason, noted, by a number of respondents was that they are often not staffed by compatible types:

> *'In physical they are pretty much driven to be physically dominant, alpha personalities, physical control over physical space and by and large info security services people don't have that cultural approach, they are geeky, introverted focused on their technologies and how they can be used, and they tend not to be very physical people'.* Cyber Security Partnership Manager

> *'There is an initiative but there is problem of language. The IT guys don't speak the same language as physical security does and they don't make an effort to make themselves be understandable'. Security Manager (physical), Bank*

> *'I don't favour one team. I do find the IS guys, whilst they talk about threats impacts and vulnerabilities, they are different individuals, not in intellect, their domain is IT centric and they don't like coming out of that sphere …*

> *The advantage of being separate is about skills sets, about being able to dedicate a focus to professionals in their dedicated sphere rather than being seen as a one-stop-shop'.* Security Manager, Energy provider

4.9 Some noted that bringing together different types of people, with different knowledge and skills sets, a different organisational language and a different view of how security should be practised was a skill all of its own and that only some organisations had recognised this and had good strategies for implementing it (and appropriately prepared people who in one case were referred to as 'cross-functional team builders'). One security consultant argued that such an approach forced people and skills together by way of organisationally structure but that if there are advantages in close collaboration (and it was recognised in this area there clearly are) then there ought to be other better ways of collaborating. The interviewee outlined the potential problems in 'dependent' convergence in this way:

> *'There is possibly a downside. I would be concerned how that business intends to refresh its knowledge base, how does one stop stagnation? This comes down to an organisational cultural aspect. Because you have two different functions in one unit,* [that's] *the tendency I have seen, anecdotal I must add, but they feed off each other and there is a lack of new ideas if there is not a refresh of staff.* Cyber Security Partnership Manager

4.10 There may be some logic, therefore, in keeping the two functions separate but increasing dialogue and opportunities for collaboration between them; the interdependent model. Sometimes the independent model may be best where, for example, they need to collaborate on a limited range of issues or where for other reasons they are benefits to working separately.

4.11 The point is not to suggest that working as one team is a bad idea, merely that it is not necessarily an unqualified good. Convergence, interpreted this way, brings with it the risk of stagnation and a forced way of working that may not be in the best interests of security (and this merits more research), not least if it is accompanied by downsizing for broader business reasons (good for the overall business perhaps but not necessarily the security element, a point that will be returned to later).

4.12 It was noted that there was a need to avoid 'divergence' which was presented as a form of independence that does not allow an aligned or joined up approach. It is important to note that these issues are not specific to security. For example, there are parallel arguments in other sectors, in education:

> *'Take it out of security and now put into an academic content, much has been made of multidisciplinary and interdisciplinary paths in universities. Should you take all*

disciplines out and put them in a single department or have multi departments and then foster relations between them'? Cyber Security Partnership Manager

4.13 In education, the case for the equivalent of security convergence in the form of one team is less accepted. Better collaboration and communication between departments can be achieved in a variety of ways. One other point may be relevant here, and relates to the maturity of the organisation. As any organisation grows or downsizes the most appropriate models of collaboration may change.[107] And how is new thinking and new ideas best brought about? There may be an initial boost as they feed off each other, however after this they may progress to a state akin to 'groupthink' where they draw on each other too much rather than look outside to a sufficient extent for new thinking?

4.14 One interviewee noted that in her company the cyber team had been part of the physical security team but it struggled to make its voice heard so it was separated out as a separate department, with what the interviewee perceived as a very beneficial result.[108] One security manager for a bank, with responsibility for physical security noted that although his team worked with the cyber team it, was on an *ad hoc* basis with meetings, *'from time to time'*. This interviewee was based in a European city and said that the culture was very much that departments worked separately:

> *'It could be better, more effective, it works now but it is not efficient. That is because although we work on the same topics we don't speak often enough…there is little or no exchange until we have an incident'.* Security Manager (physical), Bank

4.15 Some interviewees pointed out that there was often a form of protectionism taking place, with a strong head of physical or cyber arguing against more formal forms of collaboration to protect 'empires' or because of egos. While this was generally presented in pejorative terms, there was, in fact, another logic, in that convergence can be used by businesses to reduce the size of teams. Whether that is a good or bad thing will inevitably depend on circumstance, but it is a danger that some security professionals were worried about. Some typical comments here included:

> *'One of the problems is that if they agree to merging they may lose some of their power…the CSO does not agree with merging because he does not want to lose the physical security department, it is an issue of power I would say'.* Security Manager (physical), Bank

[107] For a discussion on this very point, and more data see: Whitman and Mattford (2015) op cit.
[108] Clearly this is an example of one company but it highlights some of the potential difficulties still to be overcome in some structures in bringing all security under one umbrella.

> *'...for example, you have two heads, and then you can reduce the two structures, so you don't have two heads, so convergence brings with it an opportunity to downsize and sometimes the purpose of convergence is cost reduction'.* Security Integration Officer, International Association[109]

4.16 One services-based corporate security manager reflected on how she was appointed to bring different security groups within the organisation together and benefited from having *'no empires to deconstruct'*. The interviewee felt that working in one department was much less important than being able to work together when appropriate.

Information security and corporate security

4.17 Respondents were asked whether, with the outsourcing of IT to the cloud, the IT department was no longer suitable for leading on cyber crime. Here the majority disagreed (55%) – and clients were more likely to do so (60%) than suppliers (49%) - although nearly a fifth (19%) of the total respondents agreed.

4.18 Perhaps this serves as further evidence that the skills sets of what have traditionally been considered 'corporate' security on the one hand and 'information security' (or something similar) on the other both have a value. Indeed, a number of comments alluded to this very point, for example:

> *'It doesn't matter which title you use, CISO or CSO, you need both'.* CEO, Cyber Threat Consultancy

4.19 In fact, a range of issues were alluded to in discussions about the role of each; the importance of the size of the organisation (with smaller companies more often not being able to afford specialist cyber people and therefore, 'tagging' the role onto other duties); its culture (and the level of joint working); the level of regulation it faced or scale of threats; and of course its experience of cyber crime. Points that will be returned to later.

4.20 Roles were explored in interviews and there a number of issues emerged where information security was under the governorship of the IT department and/or the CIO. These included a potential conflict of interest for security when it required changes in the IT department for security benefits; there was the danger that a CIO may choose not to prioritise security considerations because a higher emphasis was placed on other factors which only sometimes would be justifiable. Others noted that CIOs are not always experts or best placed to assess security because it is not their background, and examples were given

[109] It was also noted by another interveiwee that the reverse can be true too, that it can create the need for more staff with a greater appreciation of the scale and nature including complexity of the threat.

of different ways in which their job was impeded. Some typical comments here included:

> *'The core CISOs of this world were and are very much protective of their environment and do a very good job of security systems technically, but are not good at ensuring what they are doing affects the operational business'.* Head of Resilience, Utilities

4.21 A variation on this, was the level of the information security role within the information security department, and indeed the level of the department compared with others:

> *'IT team reports go up through the information management director who reports to the CIO, so part of the issue is that it is buried two layers down from the CIO, which is astonishing given that cyber is one of the top challenges. Also, quite honestly I am not sure the CIO has a full grasp of cyber issues, he has never spoken about it'.* Associate Director, Corporate Security, Manufacturer

4.22 A striking finding was that the sample felt the information security specialists generally operated in silos (71%) thought so. But as noted above, this is not necessarily negative:

> *'What is the right solution for business? It is not always overlap. Silos are generally bad unless there is some special reason for them…security needs to talk to the business, they both do, they need formal and informal processes to make this happen'.* Cyber security consultant

Examining the barriers to partnership working

4.23 In the survey, respondents were provided with a list of potential barriers to physical security playing a fuller role in tackling cyber threats. The respondents were asked to indicate their agreement with the statements and the results are shown in the table 1 below.

4.24 As can be seen, there were three statements that were agreed with by more than 7 in 10 respondents. On this evidence it would appear that cyber is defined as outside the remit of security, and then on the one hand cyber specialists tend to operate in silos, and physical security lacks the technical knowledge. Most disagree that cyber is not a priority; in fact of all the statements this received the highest level of disagreement.

4.25 It is striking that over a half of the sample agreed that cyber security experts do not want physical security experts involved in cyber security; over 4 in 10 agreed that physical security suppliers did not want to get

involved in cyber; and well over a third agreed that physical security suppliers did not see opportunities to contribute in this area.

4.26 In the physical security world, the dangers of selling on fear (scaring customers into buying) have long been highlighted; it is taboo. Yet there was a concern that this was not the case with cyber. This merits more research.

	Disagree		Neither agree or disagree		Agree		Total
	Frequency	%	Frequency	%	Frequency	%	Frequency
Cyber security is not considered to fall in the remit of physical security	36	17%	15	7%	161	76%	212
Physical security experts do not have the technical knowledge required for cyber	23	11%	39	18%	149	71%	211
In organisations information security specialists generally operate in silos	27	14%	32	16%	141	71%	200
Cyber security experts do not want physical security experts to get involved in cyber security	29	14%	61	30%	114	56%	204
Cyber security suppliers sell cyber security by promoting fear	42	21%	53	26%	107	53%	202
Physical security suppliers are not interested in getting involved in cyber	58	29%	60	30%	81	41%	199
Physical security experts aren't aware of cyber threats	83	40%	44	21%	83	40%	210
Cyber security is not seen as a priority	111	53%	20	9%	80	38%	211
Physical security suppliers do not see any opportunities for contributing to cyber	71	36%	54	27%	74	37%	199
Physical security experts do not want to get involved in cyber security	56	28%		37%	71	35%	201

Table 1. The extent to which the sample agreed that different factors pose a barrier to the physical security sector playing a fuller role in tackling cyber threats

Discussion: the need for convergence

4.27 So far, this section has served to critique the convergence argument, however, this section provides balance by examining the positive contribution convergence can play. Indeed, there is little doubt that in many instances convergence is alive and thriving.

4.28 However, and to emphasise a point discussed above, over a quarter of respondents (27%) said in the companies they discussed there was one overall strategy that included both physical security and cyber security and a half (50%) said they had separate strategies for each.[110] When asked whether there was there a senior person responsible for both cyber and physical security less than a third of cases (31%) said their was..

4.29 More positive news for those who support convergence emerged from responses to a list of statements to indicate their preferred way of managing security; here some of the sample referred to companies they worked with and some more generally. Well over a half, 56%, favoured some sort of converged approach (reflected in responses to the first four rows in the table below).

	Respondents preferences	
Management style	**Frequency**	**Percent**
A single converged team (cyber and physical security) under the leadership of an expert in physical security	17	7
A single converged team (cyber and physical security) under the leadership of an expert in cyber security	12	5
A single converged team (cyber & physical security) under leadership of one expert in physical & cyber security	83	34
A single converged team (cyber & physical security) under the leadership of one person who is not a security expert	23	10
Cyber security team headed	93	38

[110] 7% reported that there was a strategy for physical security only; 3% reported that there was a strategy for cyber security only; 9% reported that there was no security strategy and the remainder were 'not sure'.

by cyber security expert & Physical security team headed by physical security expert		
Unsure	14	6
Total	**242**	**100**

Table 2. Respondents' views on the preferred ways of organising security in corporations

4.30 Further analysis revealed some interesting trends. Comparing those who favored a converged team as opposed to a separate one, and counting just those who expressed a preference either way, those working in mainly cyber were more likely (63%) than those working in mainly physical (55%) to prefer a converged team, as were suppliers (61%) compared to clients (54%), and those working outside the UK (63%) compared to those in the UK (55%). If these findings are in any way representative of the security population generally it would suggest supporters of convergence need to focus more persuasive effort on those working in mainly physical security, amongst clients and in the UK.

4.31 So more than twice as many thought convergence was a good idea than is currently practised. Provided with the opportunity to feedback on why convergence was important, some interviewees identified a range of advantages, including a clear identification of security as an important entity in the business including at Board level; providing a form of rationalisation such as single risk assessments and a single budget (so avoiding duplication); and harmony rather than competition in the way in which security was practiced and perceived. Respondents also felt that it could help to avoid the risk of a threat falling between the two areas (it was argued that risk councils – that is individuals coming together to assess risks – generated a number of weaknesses including insufficient joined up thinking).[111] Some noted that fusing teams can and had generated energy and enthusiasm allowing staff to be more able to meet a broader range of challenges, in itself heightening the value of the security team to the organisation. Some indicative comments here included:

> *'I would say there is a huge advantage in a coherent presentation of requirements and not being competitive on the budget. You can offer a single story; there is no blurring of the lines'.* Head of Business Security, Service Supplier

> *'There are huge advantages bringing cyber and physical together, also for compliance. Compliance is a big part of*

[111] Although some noted that these had worked very well.

what drives multinational companies crazy, every complaint investigation has involved the information security team as a partner to help me assess the scope of the challenge. So good but for compliance reasons as well'. Associate Director, Global Security, Manufacturer

'Security is only good if you take all parts and take all fields into view'. Managing Director, Physical Security Supplier (Europe)

'We work with clients – one is [a large, global company whose product is based online] *– they have a fantastic set up with physical security and data all from one place – the command room looks like star ship enterprise, they call their guys 'security operations analyst', they have a background in physical security and have been trained in specific cyber security skill sets for the environment, for that business, and that's definitely the way to go. Because simply co-locating two otherwise separate teams will lead to friction between physical and cyber. You see it with public bodies – like the CIA – there is friction between underground operatives and analysts in the background – they don't really consider themselves the same team'.* Training Consultant

Concluding comments

4.32 Convergence is alive and well. For its supporters, this study provides encouragement that a converged approach has many merits. But the concept has different meanings for people. Despite a range of work that points to ways in which a convergent approach can be implemented[112] there is still a need to better understand how it can work in practice,[113] what the pros and cons of different models are, how managing different types of cyber and physical security specialists can be harnessed to best advantage. The role of ESRM with its core principles, and convergence with its focus on structure, both remain ways of doing things and there is a need to better guide practices with a greater insight into the pros and cons of different approaches. There is a need for those arguing a preference for one overarching security team or even close collaborative working to be able to better articulate and demonstrate the ways this can be achieved and how the potential dangers – including the risks that any reorganisation may be driven by a desire to reduce costs rather than improve overall security - can be guarded against.

[112] For example, see Tyson (2007) opp cite; PAP Standard opp cite. It is likely the concerns about the Internet of Things and the drive to SMART buildings and cities will further drive thinking.

[113] For a good discussion of the issues relevant here, see: Word Economic Forum (2016) Recommendations for Public-Private Partnerships against Cyber Crime. http://www3.weforum.org/docs/WEF_Cybercrime_Principles.pdf. The press conference around its launch also contains some helpful insights: https://www.youtube.com/watch?v=f0zMJ_C8YRU.

4.33 Finally, it's important to note that the case for convergence has not always been well made, and therefore, it may be difficult to determine what 'good' looks like when it comes to convergence models. This needs more work.

Section 5. The role of law enforcement

5.1 Respondents to the survey were asked to rate the capabilities of the police in responding to cyber crime. First they were asked to assess the level of effectiveness, and the results were striking; approaching 6 in 10 (58%) did not agree with a statement that the police were very effective at tackling cyber crime[114], and only 3% (6 people) strongly agreed. Secondly, people were asked to respond to the statement, '*the police are experts at tackling cyber'* and their responses were similar; 61% disagreed and only 4% strongly agreed.[115] Feedback provided here included:

> *'They don't understand it. They don't have the resources. They see it as a business issue. Stealing data from a business is not seen as a crime, it's seen…as a crime against business, not society'.* Director of Physical Security, Risk Management Company

> *'…we have tried to engage with police, and 60 percent of this is around fraud either against us or clients, and the only reporting mechanism is Action Fraud which is horrendous, and we don't get a response on most of that, perhaps about five percent. The police are a complete shambles, horrendous'.* Global Security Director, Security Supplier

> *'I attended a regional police cyber-crime workshop, and they were talking about stuff and then in Q&A they said they had no resources to deal with cyber. It is so specialised and the police have no idea. The realities of enforcement is that they won't pursue people in China, so it is a bit of joke'.* Consultant, Website Development

5.2 Those who worked mainly in cyber security were more likely to disagree (67%) than mainly physical security (52%) that the police were effective and more likely to disagree that the police were experts, (69% did so compared to 55%). However, the two were equally likely to disagree, less than half did so, that within the next five years the police will be able to be relied upon to tackle cyber crime. Suppliers were about as likely (62%) as clients (60%) to disagree that the police are experts.

[114] Generally the more senior in the organization were more likely to disagree and less likely to agree than those working at lower levels.

[115] Comparing just the numbers agreeing and disagreeing showed that over three quarters of those responding to each statement disagreed. There was a tendency for those who felt cyber was less important than physical security to be more likely to disagree with the statement (nearer 9 in 10 did so compared to three quarters believing that cyber was more important or they were the same).

5.3 Respondents were then asked to provide their response to the statement *'the police need to recognise that it is impractical to report all cyber crime'*. The results of those who answered are shown in table 3. It indicates that most people agree or strongly agree with the statement (55%), and only a quarter disagreed in some way. This puts in perspective what can be expected from data/information exchanges and the need for some clear rules and guidance about what is appropriate (for each side) and what is not. Those working for a supplier as opposed to a corporation were more likely to disagree and less likely to agree.

Response	Frequency	Percent
Strongly disagree	21	9
Disagree	36	16
Neither agree nor disagree	47	20
Agree	89	39
Strongly agree	38	16
Total	**231**	**100**

Table 3. Responses to the statement 'the police need to recognise that it is impractical to report all cyber crime'

5.4 The participants in the survey were then asked whether they felt that within the next five years they felt they would be able to rely on the police service more to tackle cyber crimes. Just under a half of the respondents to this question disagreed and about a quarter agreed that they would be able to. The responses are shown in table 4. Those working outside the UK were more likely to agree, as were those working for suppliers, those who worked at more senior levels were more likely to say they disagreed with the statement.

Response	Frequency	Percent
Strongly disagree	48	21
Disagree	56	25
Neither agree nor disagree	49	22
Agree	57	25
Strongly agree	17	7
Total	**227**	**100**

Table 4. People's responses to the statement, 'within the next five years we be able to rely on the police service more to tackle cyber crimes'.

What can be expected of the police?

5.5 It is important to identify and articulate the ways in which security professionals felt the police response could be improved. To this end,

the survey provided space for free feedback regarding key factors which would help the respondents in their industry.

5.6 Some argued for a much stronger and clearer narrative on what the police and business (including corporate and private security) can and should expect from each other. In terms of role, the police were clearly seen to be able to offer something distinct, in having:

- Powers of arrest
- The ability to close down websites
- Access to databases and intelligence
- The support of the law

5.7 It was noted in interviews that the business sector can offer information/intelligence and ultimately evidence, a key contribution to policing. This enables the police to build up profiles and understand trends, which when combined with other sources, facilitates the potential to offer a better oversight of the threats. Businesses generally and private security specifically, feel it could benefit from this. A key challenge to this process, reported by participants, is that all too often businesses report offences only to find there is no feedback from the police, and this acts as a disincentive to future reporting.

5.8 The police can potentially use their intelligence to predict where threats are coming from and enable users to take appropriate action. Examples were provided where this has worked really well. In future, the police response would benefit from better communication, for example, by making it clear what business reports are used for and providing feedback to individual victims.. Knowing that a report helps build a profile may be some comfort to business, but the police can, and are, recognising that where information they receive is helpful in a specific way – say in identifying an offender or new threat - they need to feedback to the victim (one sided communication leads to frustration):

> *'Companies report incidents but never get feedback and it is the same for the intelligence services; when we report intelligence, say about spamming, we send reports and call friends and contacts but we get no feedback. Only one side communication; we give but we don't receive. Everyone speaks about public and private partnership and it is only one way'.* Security Manager (Physical), Bank

5.9 However, sharing information is complicated. There is a fear from the business side that the police will fail to appreciate commercial sensitivities. This is one reason why some felt they would rather deal with a specialist private security supplier than the police. One interviewee, a security supplier in the USA, noted that while he felt the police are trustworthy, police organisations are big and complex and you cannot be sure everyone who manages data will understand the

significance of it, much less the associated commercial sensitivities, and you can't be sure someone won't be negligent, or even corrupt (also a concern when investigations were being conducted in some parts of the world).

5.10 One interviewee, who had helped initiate a Global Security Operations Centre (GSOC), was in the process of developing an information sharing agreement[116] with the police whereby intelligence would be pooled to mutual advantage. While the GSOC was too new to evaluate performance, the initial problems impacted mostly upon the centre rather than the police (albeit the information agreements took time to finalise). Firstly, because the staff were difficult to find, as there is more demand for skilled staff than supply *'and they are quite a commodity'* And secondly because although they have technological skills they were not always skilled at making judgments on what they found, generating some *'outlandish commentary'* on information they produced, leading the interviewee to highlight the crucial role of the 'human element'. As one Director of a cyber security consultancy noted:

> *'Why is security blooming in cyber? It is because of skill shortages, it takes three months to hire someone, we are all looking for people in the same pool…Why work in the police? They can't pay you enough'.*

5.11 Some argued for a much stronger and clearer narrative on what the police and business (including corporate and private security) could do. While there was an understanding that police lacked resources some respondents wanted a clearer insight into the implications, and one specific area and concern was police ability to respond quickly to incidents. Indeed, those who spoke about the potential advantages of private security here alluded to the speed of response, and the agility and flexibility it affords. The first quote below reflects a view about how the police need to be, and the second alludes to the potential benefits of private security yet in the last sentence highlights one of its main weakness too:

> *'The police need to set up an effective response to cyber crime, this means being agile and flexible; they need to be able to move quickly. They need to think in a different paradigm'.* Corporate Head of Security, Retail

> *'We were hacked in 2011. We learnt three things. First, everyone rushed to the point of the hack and left windows open for them to attack elsewhere. Second, every department was evaluating risk in different ways and we were not aligned in terms of response. Third, we have not identified our crown jewels and what was happening to them. We were on a flat trajectory. Now we have a*

[116] This was under the UK Government's CERT-UK initiative; https://www.cert.gov.uk/cisp/ (accessed 16th February 2016).

> *layered approach…We need to understand the adversaries, who is attacking you? Different sectors have different attackers, every specific group has its own code, and personality, and you can track these. It is all very specialist though. Technologies are very expensive'.* Director, Cyber Security Consultancy

5.12 The catch is that the tools to understand and track threats are very expensive and many would only be available to an elite. This was a central concern of a police interviewee. One senior officer noted that there were dangers here and they took two overlapping forms. The first point was that if the police left too much of the response to cyber to the private sector it might create a divide between the police and business in an area where the police needed to build up a rapport. Related to this was the point that the police should not be leaving vulnerable companies to the mercy of private security companies who might exploit them. When business and private security is being considered, the issue of trust is never far from any focal point. One respondent to the survey made the following point:

> *'Cyber crime has obvious differences from physical crime but there are different kinds of fingerprints to use as clues in an investigation. The main difference with private security involvement is cost, the police do not charge to investigate crime but private security, like some other professions, do, and that payment is not on a 'by results' basis. You have to pay to engage, then throughout the period of the contract and any final settlement fee at the end. There is also no guarantee of actually getting the service you pay for'.*

5.13 Despite all of the problems identified with the police response, some interviewees spoke very highly of the ability of the police to respond effectively. They spoke about those involved in specialist areas where a response form the police was prioritised or where they had struck up good relations. But one respondent noted that it was possible for business to take the lead here, and that the type of response businesses should expect from the police should be based on the type and quality of contribution it can make:

'I know the only way the police will respond is if we have done everything we can to prevent and thoroughly investigated it and provide the relevant information; if we don't then we don't get a response. We have learnt that the hard way. We have a fantastic relationship but we can demonstrate we are doing it right in the first place. And we provide a complete package of info'. Head of Resilience, Utilities

Discussion

5.14 There was general agreement that the police, like business generally and private security specifically, are playing catch up in understanding and responding effectively to cyber crime. For the police too, responding to cyber requires the acquisition of new skills and the establishment of new relationships with countries as well as organisations; these skills and relationships are very different to those needed to respond effectively to the traditional threats of street crimes, burglary and robbery. Some respondents could see and had benefited form the progress that had been made, but the ubiquity of cyber offences and the limited resources of the police led some to doubt that it was best placed to be a main (or the main) responder in the future. Indeed, there was a lack of clarity about how the police could best position itself to help business going forward. There was more certainty that police effectiveness in this area was not optimal.

5.15 It was noted that business, and its security parts, will need to take responsibility for cyber crime going forward. It can play a role in shaping the type of response it gets from the police by establishing how it can use its own resources to best effect, and it can engage in meaningful relationships based on data/information exchange. For many though, these aspects still need more work not least on the types of data that are likely to be most helpful and the ways in which this can be best communicated.

Section 6. Physical security and security patrols

Introduction

6.1 The study examined participants' beliefs about the role of physical security as part of the response to cyber crime. There was overwhelming feedback from the survey that it should play an important role, for example:

80% believed physical security measures had a role to play
79% thought that physical security was crucial to tackling cyber crime.

6.2 Of course, much depends on the type of physical security in question. For example, when shown a statement which said *'physical security suppliers do not see opportunities for contributing to cyber'*, 38% agreed, and only slightly less disagreed (36%). Yet it was clear that the sample differentiated between suppliers in its view about which groups could potentially make a contribution in the future. For example:

93% felt cyber security companies and experts could
91% felt security consultants could
72% felt security installers could
67% felt private investigators could
52% felt manned guards could[117]
38% felt facility management companies could

6.3 In comparison 70% felt the police could. A number of questions were asked about physical security experts. The majority (71%) thought that their technical knowledge for working on cyber threats was generally lacking, and asked whether physical security experts have knowledge of crime that can be applied to cyber over a fifth were neutral (23%), but more agreed (56%) than disagreed (21%).

6.4 As noted earlier, slightly over a third (35%) of the sample thought that physical security experts do not want to get involved in cyber, while over a half (56%) thought cyber experts didn't want physical security personnel involved in tackling cyber crime, many fewer disagreed with this (14%).

6.5 So, the general picture painted is one where the majority felt there were opportunities for most types of physical security suppliers, but amongst physical security specialists the lack of technical knowledge was perceived as an inhibitor, albeit their general crime knowledge can be useful. The difficulty of physical and cyber security specialists working

[117] Those working mainly in cyber security were much less likely (34%) than those working mainly in physical security (57%) to argue that manned guarding companies had a role to play in tackling cyber crime in the future; and suppliers (60%) were much more likely than clients (47%) to agree which is perhaps inevitable.

together can underlined by the hesitancy each may have about the other.

6.6 Some physical security experts don't want to venture into cyber security. As an example, during the research, an interview was conducted with the Chief Executive of a major manned guarding company, the individual was adamant that cyber was a different thing and saw no opportunities or wisdom in combining the two.

6.7 Some have not identified the commercial opportunity, confounded by a traditional view that the fields are very distinct and incompatible. As one interview noted, there are real danger for the physical security world if it does not respond:

> *'The industries that represent the physical security world are concerned because it is a largely virtual economy…Any physical security supplier saying 'We don't do digital security' will go bust…Is this an example of a declining industry looking inwards and complaining that no one is taking me seriously, rather than the world is changing and we need to change with it'?* Cyber security consultant

Or to put it another way:

> *'*[there are] *lots of opportunities for a bold security company* [to] *be a bit of a disrupter, and maybe they have to employ different people, and pay more, the size of the prize is high: any dinosaur that isn't adapting might struggle justifying what they do with the current group of people'.* Head of Resilience, Utilities

The need for security patrols

6.8 It was noted earlier – referencing Tyson's work - that security patrols can be seen as a crucial part of any response to cyber crime because they offer a physical response. The evidence from the survey is that not everyone is convinced. For example:

> *'There is probably not much patrols can do, it is a very different threat, the people who would do cyber attacks would not typically be at a premises'.* Information Security Consultant

6.9 When asked whether they felt security officers patrolling the premises might be able to identify some cyber risks and threats, over a third did not (35%), albeit over a half did think so (55%). Strikingly, and perhaps predictably, those working mainly in physical security (62%) were more likely than those working mainly in cyber security (37%) to agree with this.

6.10 Another question tackled the point in a different way by asking whether any approach to cyber that did not include a physical response was a weak one, the majority agreed with this statement (56%) and many less disagreed (16%).

6.11 During interviews the potential role of security patrols in helping with the response to cyber was underlined. The general point that emerged was that cyber threats are often facilitated by insiders or by intruders infiltrating the premises:

> *'If I can get physical access to your computer I can own it…I will attack it, that is easy. It is so hard to do it remotely if the target is remotely competent'.* Cyber security consultant

> *'It is not just wireless connectivity that creates a weakness, if you access cables you can get onto the network that way. This is where physical security comes in. I have known a phone in the lobby which when unplugged gave you access to the Ethernet. Now the security engineers should not have configured it that way, but looking out for this sort of thing is part of good security awareness'.* Product Security Consultant

6.12 Many interviews gave insights into the potential value of a good guarding service for cyber protection:

> *'Physical security can determine the relevance of anything that they notice. They have eyes and ears all over the building. CISOs don't have that'.* Director, Information Security, Manufacturer

> *'They do have a role. Physical human beings should be adequately trained to identify abnormal behaviours. This is relying on a physical response, say someone who is there and looking via bins, or being where they shouldn't. Sadly most attacks are done remotely. Sometimes supported and enabled by people on site'.* Head of Cyber Resilience, Security Supplier

> *'Hugely so – but it's more around making them aware of what risks are there…even in CCTV control rooms you see passwords left on notes on screens. Massively, they need to made aware'.* Training Consultant

6.13 Further evidence of the lack of consideration as to how security patrols could be of use was reflected in the way some people answered, that while they had not thought about this before, the interview made them think about the opportunity:

'Interesting question. Probably not so much, not a great deal. We get them to do things like energy saving, looking for restricted documents on staff desks, yes, that sort of thing. You have made me think for a moment, perhaps we could do more yes.[118] Head of Security, Construction

The value of security patrols

6.14 The evidence here is that there are opportunities for physical security experts to get involved in tackling cyber, because the response to cyber is invariably more than just a technical response, albeit this point is often not appreciated. There is scope for suggesting that many of those working in physical security, and manned guarding companies are not an exception, have underestimated the contribution they can make to tackling what is often considered the main security threat to business now and in the future.

6.15 During discussions it was noted that security patrols could have a range of tasks related to cyber security that are simple variations on their existing routine, for example, checking for passwords being left on or under desks (one Head of Business Security for a Service Supplier noted that manned guards can be particularly effective when there is a clear desk policy; it made it easier to notice if anything was missing). Additionally, patrols could be used to look for rogue devices, protect access to vulnerable products and areas, look for and identify suspicious people, and help train others in cyber awareness by alerting staff at appropriate times. Others added:

You could see patrols as quite important, maybe the detection of unwanted cars, say, near installations or critical facilities, they could be taught to pick up Wi-Fi signals, a guard can do this if trained. They can assess intruder protection systems and see whether they have been modified. The problem is our customers…look to firewalls, or think it is a landline attack from China but the reality is that it is far easier to get into a premises'. Managing Director, Physical Security Supplier (Europe)

'There is potential, and the Internet of Things is an example, like looking at thermostats, if there is blinking lights then there is an issue, we can encourage them to look for things providing they can be trusted. We need to be careful as some are low paid'. Convergence Engineer

'One way we can be effective, and I have been here with security officers, is being savvy as to what the issues are from the cyber threat. For example, what is the authority

[118] Interestingly, this was not the only interview where this type of response was generated. It underlines the point that there is a need for a greater discussion of the role of private security in this respect.

of people to be working in different areas? And more so, by knowing people going around the workplace and noticing if somebody is working on a desk that they would not normally be at, they must think, 'should that person be on that terminal?'…A lot can be done rather than filling up photocopiers. We have a team…they are being clued up on this and adding value'. Head of Resilience, Utilities

The internet of things

6.16 Earlier it was noted that one of the key developments in understanding cyber threats was that the security world was itself responsible for creating opportunities for offenders by its own lapse behaviour. In the survey, respondents were asked if weaknesses in physical security (e.g. IP Video, Access Control) and Building Management Systems created opportunities for cyber criminals. In the event 60% agreed, and 15% disagreed. Perhaps predictably those working mainly in cyber security (36%) were much less likely than those working mainly in physical (60%) to agreed with this. Although whereas over a half (53%) of clients agreed, this was true of two thirds of suppliers (66%).

6.17 Some noted that this was only true if security professionals and security companies lacked expertise in what they were doing. One corporate physical security interviewee, based in Europe, stated that this was becoming more of an issue now than in the past but was only just emerging. Clearly then, it is not an area where we should assume attention is paid.

'A large number of security system manufacturers don't get security. A large number of installers don't get security otherwise they would not install default user names and passwords…CCTV is compromised by default username and passwords. Also being produced with obsolete protocols in building management'. Owner of physical and information security consultancy

'It is a risk and generally business is not onto it, they don't appreciate the risk, they have not worked out the risk. In my world it is easy to do, apply a proper risk assessment methodology, but I would say that if it is not customer information then they are not worried'. Information Security Consultant

'Some products, like some anti-virus software can actually make you less secure. There is plenty of information on the web, you can download scripts. There again you need some sophistication if you want to avoid being caught'. Product Security Consultant

6.18 While it seems clear that not all of the security world has woken up to the risks it has created, this is not just a fault of manufacturers or installers, as another interviewee explained:

> *'There are three things. People, incompetent because they look at it as a dumb device, without thinking through all the consequences of linking devices to networks. Second, people, often millennials, are busy buying systems where they have always assumed they share info and not thought it through. Third, suppliers are trying to build a system for less money to meet the demands of the market and are making compromises. Any one can be a weakness and all three can happen…Those selling systems present solutions as less complicated than they are. So in private security they have people who put cameras on walls who don't understand networks. I don't think that person is doing anything wrong, that is what people who fix cameras to walls do. It is whoever told them to put that there who should understand the consequences'.* Convergence Engineer

6.19 There is, perhaps, one other point to be made here. Some interviewees noted that there was no substitute to the risks posed by the internet of things other than good security management, in systems design and implementation and then management. One noted a problem that different advisors may have *'conflicting views'*. Some noted that they had, as a direct response to this threat, changed their practices, vetting suppliers more carefully, and some had installed servers that were not connected to the internet:

> *'This is a risk we have managed. We have a network of plants that have their own operating system that is totally removed from the internet'.* Engineering Manager, Defence Organisation

> *'The facility I work at at the moment has 108 cameras, 200 access doors, on a dedicated network not open to the web, a decision made on the basis of the question you have just asked. We realised that the moment you have gold, as it were, you have a vulnerability.* Security Manager, Energy provider

Discussion

6.20 The physical security world, like the police service, is playing catch-up on cyber. The early response to cyber threats emerged from the information technology specialists who built up a considerable expertise, one that remains key today. As time has moved on though,

there has been a growing awareness that there are similarities in the principals governing the response to both physical and cyber threats. Moreover, that at least part of the response to any cyber strategy needs to take account of the human side. In this area, the physical security world generally (with some notable exceptions) has undersold itself and continues to do so.

6.21 Yet while the role of physical security experts and suppliers is largely recognised as having a place in the world of cyber, some need convincing. It is only obvious to some, for example, that security patrols act as eyes and ears on all security matters, including those that have a cyber link. On a general level, physical security experts are sometimes seen to lack technical expertise (and perhaps a general awareness of the threats posed by the internet of things), and a willingness to get involved. These matters are given rather less attention than they merit, and mark an opportunity for more developed thinking going forward.

Section 7. Final comments

7.1 This study took a rather different focus to others that have been conducted; it sought to examine the roles of corporate and physical security as they relate to cyber. It included a review of the issues that have appeared in previous research and reports, a survey and one-to-one interviews with corporate security personnel (with specialisms in physical and cyber security), as well as physical and cyber security suppliers.

7.2 The role of physical security in tackling cyber crime has received relatively little attention. Yet physical security suppliers are omnipresent and much of the national infrastructure is in private hands, and therefore corporate security departments play a part in protecting organisations and the country. It is far from clear that those who are advocates for physical security (in corporations and amongst suppliers) have articulated and promoted the case for it being a core part of the emerging cyber threat. This is all the more striking in the wake of a police force generally perceived to be lacking in expertise and resources (but with some notable exceptions).

7.3 The findings reveal general agreement that organisations are poor at preventing cyber crime, and even recognising cyber offences have taken place, despite recognising that cyber is a serious consideration on the threats agenda. As other surveys have found, many organisations have not yet fully appreciated the cyber threat nor developed an effective response.

7.4 A striking finding was that while technology is key to any response strategy so too are people. Most of the sample believed human factors were more important than technology and there was stronger agreement that an alert workforce was the primary defence mechanism. How strange then that the physical security world has not trumpeted its expertise in these areas.

7.5 Convergence is alive and well. There were many who saw it as the best way forward and some had very positive experiences of a converged approach. That said, it does not mean the same thing to all people, and despite the existence of documents that outline how convergence might work, there is still a need for better – and perhaps more accessible information on the pros and cons of different ways of implementing a converged approach.

7.6 Moreover, there are some clear barriers to partnership working and some of these relate to the way cyber security specialists operate (not least the perception they operate in silos) and some to operational physical security matters (including their perceived lack of expertise in technical areas).

7.7 There is a lack of clarity about how best to implement a converged response, what levels of merging, or overlap, or integration or

collaboration are necessary or desirable in what cases. Proponents of convergence, and there are many, need to move beyond advocating the case for shared working and avoiding silos - important though that is since it appears this remains an issue – and begin the process of advocating models of working, determining what is appropriate for different types of organisations in different circumstances.

7.8 The police have traditionally been seen as the key component of any response to crime. There was further endorsement here for the view that the police lack the expertise to tackle cyber crime effectively, and despite some excellent examples of good practice, and they are far from being able to be relied upon to coordinate a cyber response for the benefit of all and to the satisfaction of all. Business will need to take care of itself, or at least be the first and primary line of defence. But it can't be the only one, some of the responses are expensive and only available to the most wealthy. That is why an organisation like the publicly funded police service acting in the public good is important. Partnerships have a key role to play but more needs to be said about how these can work on a large scale (as opposed to the engagement of the elite few).

7.9 While it is clear that physical security is key to tackling cyber - the majority of the sample thought so - it is often understated. That said, there was some lack of awareness of the risks inherent in the internet of things.

7.10 Manned guarding, specifically, appears to have undersold itself, failing to see the overlaps between its traditional work and the new cyber threat. This is in no small part due to the tendency to see a cyber response in technical terms.

7.11 The security world, including its various parts – public and private, physical security, cyber security, clients and suppliers as well as the public police – are all still establishing how best to respond to the enormous and pervasive threat that has come with the cyber revolution. The findings from this study show that there is still some distance to travel before we fully understand the complex and interconnected roles of the many different groups who have an interest in this field, and are able to exploit what they can do to their full potential. Therein resides a key opportunity for the security sector.

Appendix: Methodology and sample

The approach
The study involved a review of existing literature on the role of physical security in responding to cyber crime, as well as that of information security and the police to identify key issues and themes.

This was followed by two main approaches: extensive discussions including semi-structured interviews with a range of security professionals about the topic, and an e-survey on the response to cyber crime within businesses. Both approaches sought the views of both physical security and information security professionals to understand their perspective and how best to respond to cyber crime.

One-to-one interviews
The approach in this work was to identify a wide range of individuals to help understand how cyber security is currently viewed within organisations and what the private security industry can do to respond to the threat posed. 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 and 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.

During the course of the research we attended many talks, and engaged in many conversations, over 50, directly related to this study. These are often not included in discussions of methodology but they can provide an invaluable source of information. In addition we formally interviewed a mixture of those who work for clients and those who work for suppliers, 13 who might most accurately be considered, ‘mainly physical’ and 12 who were ‘mainly cyber’.

Survey
The aim of the survey was to target a wide group of clients and suppliers from both physical security and cyber/information security backgrounds. It became

apparent when drafting the survey that there was some variation in the use of terminology such as ‘cyber security’ as opposed to ‘information security’. We therefore adopted both terms for the purpose of publicising the survey, while the survey questions (for simplicity) refer to ‘cyber security’. A definition of both physical and cyber security was provided at the beginning of the survey.

The survey addressed four key areas – the current approach to managing cyber security, the relevance of convergence between physical and cyber security, perspectives on law enforcement, and the potential role of private security in responding to cyber crime.

For the security profession, there is no defined population listed or recorded anywhere. The sample was, therefore, self-recruited. This means that no claims can be made about its representativeness. Attempts were made to publicise the survey widely, including via participants from previous research who had elected to be contacted for future research; links in the Perpetuity newsletter and social media; announcements made at conferences and other security events; and personal contact with a range of organisations who were informed about 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
- The ASIS European Convergence/ESRM committee
- SASIG (with thanks to Martin Smith)
- David Spinks and the Cyber Security in Real Time (CSIRS) (Linkedin group)
- The Corporate Security Management (Linkedin group) (with thanks to David Cresswell)
- EDUCAUSE (Higher Education Information Security Council)
- CDSE (Club des Directeurs de Sécurité des Enterprises)
- IEC 2 EMEA
- UK Cyber Security Forum
- Australian Security Industry Association Limited
- New Zealand Security Association
- ASIS Online
- Institute of Information Security Professionals
- ISACA London Chapter

We cannot be sure of the manner in which adverts were disseminated by these groups, but their contribution greatly enhanced the reach of our survey.

The findings of the survey helped gauge the status of cyber security and views on how the industry should be responding. The data though have primarily been used to provide a context to, and help frame, the interviews.

The survey ran from 2nd December 2015 to 16th March 2016.

Survey participants

A total of 289 replies were received although not every respondent completed every question in the survey. The data was analysed using SPSS. The data is categorical; therefore, it is not possible to assess the normality of data. It is important that this is borne in mind.

In all, 92% of respondents were male, a third (33%) were aged up to 34 years, over a third (38%) were aged 45-54 years, while the remainder were older (29%). The respondents worked for companies operating in 19 different sectors. About half the sample said they worked for an organisation based in the UK (48%) those who worked overseas did so on all continents although mostly Europe and the Americas. Half worked for companies up to 1,000 employees. A fifth of the sample described themselves as 'Board/Executive', and nearly a half (48%) as senior management, with the rest in approximately equal proportions as 'junior management' (175) or 'non management' (15%).

Of the 286 who gave details about their work, 161 (56%) were described as 'mainly physical security', and 83 (29%) as 'mainly cyber security', and 42 (15%) as 'other'. Of those who were 'mainly physical security' 161 gave further details, and of these 67 (42%) were 'suppliers', 75 (47%) were 'clients' and 19 (12%) were 'other'. Of those the 83 were 'mainly cyber', 27 (33%) were 'suppliers', 42 (51%) were 'clients', and 14 (17%) were 'other'.

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 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. More information on the SRI is available at: www.perpetuityresearch.com/security-research-initiative/

© Perpetuity Research and Consultancy International Ltd

About the Authors

Professor Martin Gill

Professor Martin Gill is a criminologist and Director of Perpetuity Research which started life as a spin out company from the University of Leicester. He holds honorary/visiting Chairs at the Universities of Leicester and London. Martin has been actively involved in a range of studies relating to different aspects of business crime including, the causes of false burglar alarms, why fraudsters steal, the effectiveness of CCTV, the victims of identity fraud, how companies protect their brand image, the generators of illicit markets and stolen goods, to name but a few. Martin has been extensively involved with evaluation research and with the offender's perspective looking at how they target certain people and premises and aim to circumvent security measures. He has published 14 books including the second edition of the 'Handbook' of Security' which was published in July 2014. Martin is a Fellow of The Security Institute, a member of the Company of Security Professionals (and a Freeman of the City of London), he is a member of the both ASIS International Research Council and the Academic and Training Programs Committee and a Trustee of the ASIS Foundation. In 2002 the ASIS Security Foundation made a 'citation for distinguished service' in 'recognition of his significant contribution to the security profession'. In 2009 he was one of the country's top 5 most quoted criminologists. In 2010 he was recognised by the BSIA with a special award for 'outstanding service to the security sector'. In 2015 he was nominated and shortlisted for the Imbert Prize at the Association of Security Consultants. In 2016 IFSEC placed him in the top five most influential fire and security experts in the world. In the same year he was admitted to the Charter of Security Professionals. He is the founder of the Outstanding Security Performance Awards – the OSPAs - (www.theospas.com).

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.

Perpetuity Research & Consultancy International Ltd
11a High Street
Tunbridge Wells
Kent, TN1 1UL
United Kingdom
Tel: +44 (0)1892 538690
www.perpetuityresearch.com
prci@perpetuityresearch.com