The Evolution of Physical Security Measures: assessing the benefits and implications of using more advanced technologies

Martin Gill
Charlotte Howell
Caitlyn McGeer
Josephine Ramm

July 2019

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

Table of Contents

Acknowledgements

We would like to thank everyone who has assisted us with our research. This is the seventeenth year of the SRI and it has been possible because of the support of our members and because the industry has engaged with us. The members of the Security Research Initiative who sponsor the research deserve a very special mention. They not only sponsor, their representatives also provide and share their experiences. They are: Chris Sisson (ICTS), Mick Tabori and Russell Sharp (Interr Security), Jerry Nelson (KPMG), Jo Goulden (Kings Security), Clint Reid (M&S), Jason Towse (Mitie), Steven Gardner (OCS), Richard Stanley (PWC), Brian Riis Nielsen (Securitas), David Humphries and Imogen Hayat (SIA), Simon Pears and Jane Farrell (Sodexo), Paul Harvey and Eddie Ingram (Ultimate Security), Adrian Moore (VSG). In addition, Chris Smith personally supported the research which we very much appreciate. Clearly they are not responsible for any of the views expressed in this report which are exclusively our own.

Our key supporters were once again invaluable in promoting the work. ASIS (especially Dave Clarke, Mike Hurst and Graham Bassett), the BSIA (especially Mike Reddington and Andrew Cooper) and the Security Institute (especially Rick Mountfield and Di Thomas); they are valuable advocates of the Security Research Initiative. So too our longstanding enthusiasts from security media: Mark Rowe (Professional Security Magazine), Brian Sims (Risk UK) and Byron Logue (Infologue).

We would also like to thank those who supported the research by promoting the survey among their networks including Hugo Rosemont and Elizabeth Sheldon (ADS), Chuck Andrews, Adam Bannister (IFSEC Global), Richard Jenkins and Dianne Gettinby (NSI), Johanna Skinnari (The National Council for Crime Prevention Sweden), Karen Lott (ProSecureNewsOnline) and Professor James Calder.

We would like to thank those that helped in other ways and with specific advice, they include Professor Rachel Armitage, David Dickinson, Professor Paul Ekblom, Richard Fenton-Jones, James Willison and Geoff Zeidler.

We owe a special thanks to all those (anonymous) contributors who gave their time completing our survey and who contributed insights and took part on interviews. They, by necessity and agreement must remain nameless, but we acknowledge their important contribution here.

Finally, thanks to our colleagues Hannah Miller and Claire Tankard for administrative assistance.

SRI Members

Executive Summary

The focus of this report is on understanding the ways in which physical security measures are being enhanced by internet-enabled technologies which we refer to as 'advanced technologies' and the implications this has on security practice. While, of course, there are many benefits to advanced technology, which are the focus of many a conference talk, there has been less focus on whether and how the benefits are realised. This report is based on a survey of security professionals, and in-depth interviews with both security professionals and offenders involved in a variety of acquisitive crimes.

In summary, the report demonstrates how many of the traditional elements of good security are still important today and perhaps all the more so because of technological advancements. These include good products where security is designed in; a good security strategy guided by the broader needs of the business; recognition of the potential barriers to implementation and the need to chart a path for circumventing them; effective implementation and management; savvy security staff with skills in both security and business; and good user engagement with programmes. The report demonstrates how offenders adapt quickly to circumvent advanced technology and find ways to exploit it to their benefit, highlighting the fallibility of even the most advanced systems especially when they are not designed, installed and managed effectively.

Key findings

- Generally speaking, by investing in advanced technologies clients benefit from reduced expenditure and suppliers can often make just as much profit if not more (on a lower turnover). At the same time they are behaving in a way that is consistent with good practice and helps reduce contract churn (itself a contribution to profits). Other benefits noted include, for example, better equipping security officers – say in working with linked cameras and in being provided with more information more speedily; helping managers to be more efficient, in streamlining processes and releasing staff and resources; generating more and better information to make decisions; facilitating better engagement with other departments (such as IT, HR and compliance); generating quicker responses to incidents which are known about sooner and about which there are more details; in linking security technologies to the broader aims of the business it has enabled security to demonstrate its value to a wider organisational audience; in so doing it has enabled the best security people/teams/companies to develop new skill sets helping to reinforce and further highlight their value to the business;
- That said, many of the reported benefits of advanced security were seen by others as drawbacks. For example, advances can save costs but can be expensive to buy, maintain and keep up to date; they provide an opportunity to engage with the whole business, but that is

not always welcomed and can sometimes be resisted by other departments (IT was frequently mentioned); they can reduce some errors (automation for example improves the reliability of decision-making) but can create the scope for more diverse human errors; they can reduce administrative burdens but can be difficult to use and their complexity can render them difficult to procure, integrate, manage and maintain; they can reduce dependence on people but can send out a message that people are less important when they are not, in fact better prepared personnel are often required in consequence to their implementation; they provide more and better information but this has to be assimilated and built into operations, which can be challenging; they help to safeguard legal privacy requirements but they generate privacy issues and when breached create additional legal, reputational and loss consequences, and it is still tricky to authenticate authorised users; while measures can improve security so too they contain inherent weaknesses which are still being understood (IoT being a high profile example); there is more of an evidence base to provide better security but realising the potential of what is there is at least as demanding;

- Systems have become more complex. They offer enormous opportunities but ensuring the right systems are purchased and the full benefits obtained is challenging. So too to is the task of assessing and managing the often considerable risks of more serious consequences and ramifications if things go wrong. Never have there been bigger benefits in having omnicompetent business security professionals or indeed bigger dangers in not having them.

The key findings from each of the main components of the research are considered below: first, the views of offenders; second, the responses from the survey of professionals; and third, the responses from interviews with security professionals.

What offenders think

- Advances in security technology can deter offending. Key to this is the doubt that advances can foster in offenders' minds – this 'new security' is much less predictable;
- Important though technological advances can be to security, it is human intervention that offenders most fear. Where technology results in the presence of fewer visible security people, offenders often see more opportunity, offenders were primarily concerned with immediate apprehension, police were viewed as being uninterested, and unlikely to respond. The effectiveness of security systems in discouraging crime decreased when offenders perceived there would be no response;
- Offenders are used to having to adapt. Technology continually evolves and recent developments are accepted as a natural part of this. Much offending has been displaced online, where offenders feel less visible, there are more opportunities and access to victims is facilitated;

- Technology can be exploited by offenders to their advantage, not least when it is not designed, purchased, implemented, maintained and/or managed effectively;
- Offenders also view humans as being the weak link in the effectiveness of security technology, in being careless, untrained or corruptible for example, and they look for ways to exploit this.

Views of security professionals - survey results

The current state of security

- Unsurprisingly, more than four-fifths felt that there was a general trend towards the increasing use of advanced technology within physical security measures. Those who were not engaged with them were less likely to agree with this trend;
- Three quarters of the sample said they were using more security measures with advanced technology than five years ago (either within their own organisation or within their clients' organisations). This view was more common amongst current users/suppliers than those not currently using such technologies;
- Respondents felt that a key advantage of incorporating advanced technology into physical security measures was the increased collaboration with other areas of the business that resulted from technological advances;
- Nearly two-thirds felt that incorporating technology resulted in a need for fewer security officers and other staff, though few felt they could be wholly replaced;
- The majority, at least four-fifths, agreed that Boards did not fully comprehend the threat posed by savvy offenders nor weaknesses in companies' approaches to security;
- Moreover, just over half agreed that there are serious weaknesses associated with using advanced technology that are not being responded to.

Views on how offenders respond to security

- In terms of the perceived threat, respondents generally considered offenders to be creative, seeking the most lucrative rather than just the easiest targets;
- Over two-thirds agreed or strongly agreed that offenders will exploit technological weaknesses in security quicker than the security sector is able to respond, and eventually offenders find a way to overcome all security measures, no matter how sophisticated the measure;
- More than 3 in 10 agreed that offenders are the real experts on security.

Influences on investment

- Over four-fifths agreed that security purchases are based more on what can be afforded than what is needed: traditional concerns about the influence of cost have not disappeared with advances in technology;
- Less than half the sample felt that there was an abundance of evidence that measures using advanced technology work effectively;
- Close to half indicated that pressures to buy are generated by what competitors are doing, and because they do not want to get *'left behind'*.

Potential drivers of change

- When asked to indicate what/who are driving advances in security, the influences cited most often by the sample were: the creative commitment of security professionals (just over two-thirds), security manufacturers/suppliers (nearly three-fifths); and advances in technology in other sectors (just under two-thirds);
- The influence of customer demand was seen as important by those currently using advanced technology, and significantly less important by those not doing so;
- It is perhaps striking that only two-fifths of respondents indicated that the security sector has been good at adapting to changes in the way offenders behave.

Potential threats to effective security measures

- There was general agreement that some of the most common difficulties in using advanced technology related to ensuring privacy requirements are met (noted by over three-quarters) and securing methods to identify authorised users (nearly three-fifths);
- Another challenge identified was that of realising the benefits of any investments made (noted by nearly three-quarters);
- The inherent security risks of technologies themselves were deemed to be a concern by a significant minority (just over two-fifths).

Views of security professionals highlighted via interviews

- Investments in security technology often result in clients benefitting from reduced expenditure and suppliers retaining or improving profit margins;
- While this is important, the benefits are not limited to reduced security expenditure but, when done well, can be felt across the whole of the business;
- Advances in technology are requiring security professionals to adapt and develop new skill sets; to be able to understand technology and its potential to influence, and interpret this for different business audiences;
- Keeping up-to-date, having realistic expectations, having the right knowledge base and skills-sets (amongst all parties at all levels),

understanding the broader relationship between security technologies and other technologies and its broader relationship to the business, are all elements in the effective use of advanced technologies;

- Although investments in technology may result in fewer staff members, many interviewees emphasised that it will generally involve the necessity for an increase in more skilled staffing, representing, of course, a cost increase;
- Cost is always important not least when the benefits are not always tangible and many technologies remain to be proven in the harsh realities of the commercial environment;
- Interviewees identified a range of practical problems highlighting the concern that technological opportunities did not always accord with the practical realties of business life;
- Some interviewees were concerned about an over-reliance on technology generally as well as security technologies specifically;
- There were concerns that security technologies can be undermined by malicious governments/companies; that good technologies can be installed on poor infrastructure and create new vulnerabilities; that technologies themselves contain inherent security weaknesses; and that some corrupt people undermine security;
- Thinking forward about the potential of technologies such as Artificial Intelligence, there is some optimism they may generate a marked improvement in security capability, but still many of the same concerns apply here too;
- Interviewees did not underestimate the ability of offenders to innovate, and that any good response was only ever temporary, highlighting that there is an increasing need for security responses to be able to adapt in response to increasingly rapid change in technological advances.
- It was noted that no matter how impressive the advances in security technology, this was undermined by a perceived lack of law enforcement response. This is an important reminder that technologies that are good at alerting security to the presence of offenders do not operate in a vacuum.

Section 1. Setting the Scene

1.1 Technology has changed the way we eat, sleep, work, and interact with each other. The first Industrial Revolution brought mechanised manufacturing in the 1760s, the second birthed mass production in the 1870s, and the third involved the development of internet technologies in the 1990s. Since 2015, we are in the throes of a fourth Industrial Revolution. *Industry 4.0*, as it is coined, is characterised by the dissolution of the boundary between technology and everyday life: the digital has become conjoined with the biophysical[1]. The fourth Industrial Revolution builds on the third and is unique to its predecessors in how quickly it has emerged. This period of time, on-going from the 1990s is colloquially termed *the digital era*.

1.2 This report explores the impact of this era on physical security measures. At many conferences one can hear talks about the different positive ways technology is enhancing security. There is much less focus on the potential drawbacks or more specifically the key factors inherent in maximising its potential.[2] This report seeks to cover territory which addresses that gap. It incorporates the views of security professionals on current trends and how they are impacting and taps into their experiences of learning about and integrating technologies.

1.3 It also incorporates the views of offenders on how they are responding to the advances in security technology. Are they, for example, developing more technological skill sets, and if so how? Or, are they being deterred because for example the new technologies are too complex to manage or because they fear they have increased their risk of getting caught? A comment on offender research helps sets the scene for what follows.

1.4 In the 1970s, criminological researchers began to recognise the value of incorporating offender-perspectives to truly understand the appropriateness of different responses to crime.[3] Research with offenders affords the opportunity to challenge assumptions and

[1] Lasi, H., Fettke, P., Kemper, H.-G., Feld, T., Hoffmann, M., 2014. Industry 4.0. Business & Information Systems Engineering 6, 239–242, https://doi.org/10.1007/s12599-014-0334-4; Schwab, K., 2016. The Fourth Industrial Revolution: what it means and how to respond. World Economic Forum. Available from: https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

[2] Although for interesting discussions see, Willison, J. and Sembhi, S. (2019) *Smart GDPR Assurance for a Smarter World*. http://www.axis-communications.com/smart-assurance-wp; also, https://www.ifsecglobal.com/ifsec-international/how-we-see-the-future-of-enterprise-risk-in-the-corporate-world/

[3] Nee, C. 2008. The Offender's Perspective on Crime: Methods and Principles in Data Collection. In Needs, A and Towl, G (eds). *Applying Psychology to Forensic Practice.* Blackwell Publishing: Oxford: pp 3-17

theories about the effectiveness of different measures and lay the foundation for improving the response.[4]

1.5 The value of such research[5], however, has often been thwarted by the difficulties involved in identifying and engaging a sample (which can be time-consuming[6]) and eliciting valid insights.[7] Studies use different approaches including interviews, either in prison or in the community, and focus group discussions. [8] Some studies return offenders to crime scenes to understand their motivation, decision-making, and methods adopted to overcome or mitigate the effectiveness of different measures.[9] Difficulties of such research aside, the importance of it cannot be overstated.

Offender responses to security measures

1.6 Offender-based research has recognised the broad range of environmental and other factors that influence offender decision making, including coming up with the initial idea and then decisions at the scene and on the way to and from it. Cornish and Clarke's seminal work[10], followed by Felson and Clarke's development of situational crime prevention techniques, provide a framework for conceptualising offending. Felson and Clarke reasoned that if one takes away the opportunity for crime then crime takes place less often. In other words, a cause of crime is the existence of an opportunity.[11] Felson and Clarke's techniques have been used to guide the security response. These techniques are based on five principles which are: 1) increasing the (perceived) effort that it takes for offenders to commit an offence thereby, incentivising them to stop; 2) increasing the (perceived) risk to offenders if they do persist, encouraging them to stop; 3) reducing the (anticipated) rewards, making it less worthwhile to offend; 4) removing excuses for crime; and 5) reducing provocations so that some of the reasons for offending are eliminated altogether.

---

[4] Nee, C. 2008. *Op cit*

[5] See, for example: Gill, M. 2011. Learning From Offenders' Accounts of their Offending. *Prison Service Journal. March*, 194, pp. 27-32.

[6] Hearnden, I. and Magill, C. 2004. Decision-making by house burglars: offenders' perspectives. *Research, Development and Statistics Directorate*. Home Office: London. Available from: https://webarchive.nationalarchives.gov.uk/20110218140054/http://rds.homeoffice.gov.uk/rds/pdfs04/r249.pdf

[7] Bernasco, W. 2010. *Offenders on Offending.* Willan: Cullompton; Jacques, S. and Bonomo, E. (2017) Learning from Offenders' Perspectives on Crime Prevention. In Leclerec, B. and Savona, E. (eds). *Crime Prevention in the 21st Century*. Springer: Switzerland; Nee, C. (2008). The Offender's Perspective on Crime: Methods and Principles in Data Collection. In Needs, A and Towl, G (eds). *Op cit*

[8] Nee, C. 2008. *Op cit*

[9] Nee, C. 2008. *Op cit*; Sanders, A. N., Kuhns, J. B., and Blevins, K. R. (2017). Exploring and Understanding Differences Between Deliberate and Impulsive Male and Female Burglars. *Crime and Delinquency*, 63(12), pp. 1547-1571.

[10] See Cornish, D.B., and Clarke, V.R. eds. 1986. The reasoning criminal: Rational choice perspectives on offending. Springer-Verlag: New York.

[11] Felson, M. and Clarke, R.V., 1998. Opportunity Makes the Thief. *Police Research Series Paper 98, Policing and Reducing Crime Unit. Research, Development and Statistics Directorate.* Home Office: London.

1.7 This work on how to influence offenders' decision-making has led to the development of a range of approaches under the different but overlapping subject areas of (for example) environmental criminology,[12] rational choice perspective and routine activities theory,[13] situational crime prevention,[14] Crime Prevention Through Environmental Design (CPTED),[15] the Conjunction of Criminal and Opportunity,[16] game theory,[17] script analysis,[18] and behaviour sequence analysis. [19]

1.8 While a discussion of the merits and limitations of each of these approaches is beyond scope here, it is important to recognise that:

> *The decision to offend is a complex process, which may be influenced by situational context; timing; individual differences in intelligence, education, financial stability, and experience; and one's perception of the associated risks, costs, and benefits.*[20]

1.9 One could add to this, a person's psychological state, the presence and influence of co-offenders,[21] the availability of victims, habits, and precipitating factors, to name but a few.

1.10 Traditionally, the potential of security measures to be effective has been viewed as being, in part, determined by the extent to which an offender weighs up the pros and cons of committing or desisting from an offence. When there is some degree of rational choice, so the argument goes, it can afford the opportunity for security measures to increase the level of risk for an offender and encourage them to desist or commit a lesser offence.[22] The more the offender weighs up the pros and cons the greater potential to influence that decision, although of

---

[12] Nee, C. 2008. *Op cit*; Kang, M. and Lee, JL. 2013. A Study On Burglars' Target Selection: Why Do Burglars Take Unnecessary Risks?. *American International Journal of Social Science*, 2(4). Available from: https://www.aijssnet.com/journals/Vol_2_No_4_June_2013/3.pdf

[13] Cornish, D. B. and Clarke, R.V. 2008. The rational choice perspective. In R. Wortley and L. Mazerolle (eds). *Environmental Criminology and Crime Analyses.* Willan: Cullompton, UK.

[14] Felson, M. & Clarke, R.V. 1998. *Op cit*; Clarke, R.V. 2005. Seven misconceptions of situational crime prevention. In Tilley, N (ed). *Handbook of Crime Prevention and Community Safety*. Willan: Cullompton, UK; Wortley, R. 2013. Rational Choice and Offender Decision Making: Lessons from the Cognitive Sciences. In B. Leclerc and R. Wortley (eds). *Cognition and Crime: Offender Decision-Making and Script Analyses*. Routledge: London.

[15] Armitage, R. 2013 *Crime Prevention through Housing Design*. Palgrave: Basingstoke.

[16] Ekblom, P. 2011. *Crime Prevention, Security and Community Safety Using the 5Is Framework*. Palgrave: Basingstoke.

[17] See, Rauhut, H. (2017) Game Theory. In W. Bernasco, H. Elffers and J-L Van Gelder (eds) *Oxford Handbook of Offender Decision Making*. Oxford University Press: Oxford.

[18] Haelterman, H. 2016 *Crime Script Analysis.* Palgrave: Basingstoke.

[19] Keetley, D. 2018. *Understanding Patterns of Action: Behaviour Sequence Analysis in Crime Research*. Palgrave: Basingstoke.

[20] Collins, M,E. and Loughran, T. (2017) Rational Choice Theory, Heuristics and Bisases. In, Bernasco, W., van Gelder, and Elffers, H. (2017) (Eds) *The Oxford Handbook of Offender Decision-Making*. Oxford: Oxford: University Press. P,19.

[21] For example, Tillyer, M. and Tillyer, R. (2015) Maybe I Should do this Alone: A Comparison of Solo and Co-offending Robbery Outcomes. *Justice Quarterly*. 32,1064-88.

[22] Kang, M. and Lee, JL. (2013) *Op cit*

course even if a would-be offender is not rational he/she may still be prevented from committing an offence.[23]

1.11 That said, recent research has questioned the rather simple way that rational choice has been discussed in the context of crime decisions inviting (amongst others things) recognition of the importance of the decision-making process not only when the offence is being committed but also when the offence is first conceived.[24] Further complexity is derived from understanding the time gap between when the decision was made to commit the offence and the actual commission of it. [25] Another researcher has lamented attempts to over simplify decision-making in offending by highlighting the multiplicities of choices offenders have:

> *Usually we treat decisions by offenders (and others) as binary – commit crime/do not commit crime –- when in most circumstances there are far more than two choices – commit crime A, commit crime B, delay committing a crime for some time, recruit a co-conspirator, or do not engage in crime.[26]*

1.12 An article by Eck and Madensen (2017) which focuses on public policing also has relevance for private security: they argue there are four factors that determine the quality of the influence that policing can have, in what they present as a RDFC (Reasonable, Disarming, Focussed, and Consistent) model. [27] This model focuses on policing (or security) interventions and how they impact offending.

1.13 The first factor is *Reasonable*, in terms of whether an intervention is necessary and can be justified in terms of doing more good than harm, and whether it protects citizens' rights. In short, the intervention is reasonable if it stops only 'harmful' behaviours. The second factor is *Disarming*, which refers to the way an intervention is managed so it induces compliance and does not generate resistance. The third factor is that an intervention must be *Focussed*, so that only those who are a threat are targeted. The fourth is to be *Consistent*, on the basis that this will generate trust.

1.14 These conceptualisations shed light on the context in which security measures must operate. It is a very complex picture. Before grappling with how the changes to security measure are impacting offenders, it is

[23] For discussion, see Sidebottom, A., and Tilley, N. 2017. Situational Crime Prevention and Offender Decision Making. In W. Bernasco, H. Elffers and J-L Van Gelder (eds) *Oxford Handbook of Offender Decision Making*. Oxford University Press: Oxford.
[24] Sidebottom, A., and Tilley, N. 2017 *op cit*
[25] Hearnden, I. and Magill, C. 2004. *Op cit*
[26] Eck, J. and Madensen, T. (2017) Police and Offender Choices: A Framework. In W. Bernasco, H. Elffers and J-L Van Gelder (eds) *Oxford Handbook of Offender Decision Making*. Oxford University Press: Oxford.
[27] Eck, J. and Madensen, T. (2017) *op cit*

first important to establish what the changes to security measures have actually been.

Changes to Security Measures

1.15 There have been numerous advances in security technologies over the last decade and more advances are forecast. The global security market is expected to grow to $112.43 billion USD by 2021,[28] and technology is key to that development.[29]

1.16 Physical security is becoming digital and the distinction between cyber and physical is becoming blurred. The ability to combine new developments in technology with easier access to a variety of sources of data and intelligence, internally and externally is enabling more informed security (and business) decision making, even helping companies to predict crime and model their security response accordingly. As physical security has converged with digital technology, it has become more complex. [30]

1.17 The ways in which security is incorporating new technologies are diverse, so much so that it is more appropriate to give examples of relevant developments than try to assess the scope. The Internet of Things (IoT), much discussed, has generated a wide range of opportunities for security. The increased level of connectivity facilitates a range of potential security benefits for example real-time security alerts, a log of security events, and geofencing capabilities.[31] At the heart of many of these new and emerging technologies that are part of the IoT are Artificial Intelligence (AI)[32] and Cloud technology.

1.18 One of the most crucial aspects of AI is the ability for continual learning. AI applications can filter through a mass of information to hone in on key issues, present them in a user-friendly way, and thereby facilitate more informed and evidence-based decision-making.[33] In theory, AI can lead to increasingly better predictions as to where, when, and how crime will take place, affording an opportunity to prevent future offending.

---

[28] Ingram Micro Advisor. N.D. 3 Physical Security Trends We're Seeing This Year. *Ingram Micro Advisor*. Available from: https://imaginenext.ingrammicro.com/integrated-solutions/3-physical-security-trends-were-seeing-this-year-1

[29] A good discussion of the technical and other changes affecting the security sector can be found in the ASIS Foundation project *Scouting the Future*. It was published by ASIS International in 2018. https://www.asisonline.org/globalassets/foundation/documents/research/asis-scouting-the-future-exec-summary-revised.pdf.

[30] Trend Micro. 2017. Protecting Physical Security Systems against Network Attacks. *Trend Micro*. Available from: https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/protecting-physical-security-systems-against-network-attacks

[31] IoT For All. 2018. Is IoT Making Physical Security Smarter? IoT For All. Available from: https://www.iotforall.com/iot-physical-security-technology/

[32] Colombo, A. 2017. Top Security Trends and Technological Advances of 2017. *Campus Safety Magazine*. Available from: https://www.campussafetymagazine.com/technology/security-trends-technological-advances/

[33] Reinhard, S. 2018. 5 AI Trends You Should Be Using to Improve Physical Security. *Security Magazine*. Available from: https://www.securitymagazine.com/articles/88943-ai-trends-you-should-be-using-to-improve-physical-security

1.19 AI also has the capacity to understand human behaviour through video and audio footage. This provides a much increased potential to, for example: identify a person via traits[34]and/or a face among the masses, even in unwieldy environments[35]; decrease the number of false alarms[36]; and improve operational efficiencies and decision-making.[37]

1.20 Cloud technology has changed the ease of flexibility and connectivity of security. It has expanded access control and Cloud authentication and credential management has enabled machine-to-machine digital certification in the IoT.[38] These certificates enable more devices to be connected with unique digital IDs.[39] Physical Identity and Access Management (PIAM) is one such area of growth. PIAM focuses on converging physical and digital security into a single credential. Such identity models use Cloud authentication to, for example, have mobile devices validate digital and physical IDs.[40]

Consequences of changes to security measures

1.21 In the rush to embrace the benefits of technological development, the potential pitfalls are often overlooked.[41] They include improper design and/or management, as well as accuracy and accountability concerns including privacy issues[42]; generating threats to critical data, including third party providers; and crucially human factors, recognising that cyber security ultimately relies on people, and all people in an organisation, not just the security personnel.

1.22 It is an often under-acknowledged feature of security measures that they can, if not properly designed and managed, result not just in them being ineffective but also increasing levels of potential harm.[43] An improperly designed or poorly managed interconnected security measure can be cloned and hacked,[44] providing access to entire

[34] See, https://www.bbc.co.uk/news/technology-38235584
[35] Reinhard, S. 2018. *Op cit*
[36] Neemuchwala, M. 2018. How 'Industry 4.0' Technologies Are Impacting Physical Security. *Security Sales and Integration*. Available from: https://www.securitysales.com/columns/industry-4-physical-security/
[37] My Tech Decisions. 2018. Top 5 Access Control Trends for 2018 According to HID Global. *TechDecisions*. Available from: https://mytechdecisions.com/physical-security/top-5-access-control-trends-2018-according-hid-global/; Reinhard, S. (2018). 5 AI Trends You Should Be Using to Improve Physical Security. *Security Magazine*. Available from: https://www.securitymagazine.com/articles/88943-ai-trends-you-should-be-using-to-improve-physical-security
[38] My Tech Decisions. 2018. *Op cit*
[39] My Tech Decisions. 2018. *Op cit*
[40] My Tech Decisions. 2018. *Op cit*; Lanner. 2018. 7 Physical Security Trends in 2018. *Lanner America*. Available from: https://www.lanner-america.com/blog/top-physical-security-trends-2018/
[41] Beyond the scope of this project a threat is posed by inadequate cyber laws which are gradually being updated and discussed at least in the UK. For a discussion on this issue see The Paper, 20-5-19, p 6.
[42] As part of its Industrial Strategy Challenge Fund the Government is seeking to generate new ideas and ways of designing in security. For discussion see, The Paper, 25-2-19, p10.
[43] Gill, M. 2016. Learning from Offenders: Some Iatrogenic Effects of Crime Prevention Measures. In B. Leclerc and E.U. Savona (eds). *Crime Prevention in the 21st Century: Insightful Approaches for Crime Prevention Initiatives*. Springer: Switzerland.
[44] Zenitel. 2017. Are you aware of the threats to your physical security system?. *Zenitel*. Available from: https://www.zenitel.com/news/are-you-aware-threats-your-physical-security-system; Sharp, N., and

systems, including via lights[45] and cameras[46], but also drones which can if hacked relay incorrect information back or engage in unsanctioned actions.[47]

1.23 In a different way a third-party provider contracted for design or build elements for intermediary technology, web interfaces (API's), and cloud infrastructure could also prove to be a threat to critical data, as Sharpe and Gollan highlight.[48] They outline that mitigating this threat involves a high level of care in drafting the supply agreement, perhaps incorporating a right-to-audit clause to ensure all aspects of security protocols are adhered to. These protocols can be secured through, for instance, applying strong cryptography methods to protect critical data alongside stringent management procedures for the cryptographic keys.[49] The theory though is often easier than the practice.

1.24 Numerous studies have shown that smart home systems are particularly vulnerable because they are highly interconnected. At the University of Michigan, for instance, in a study of connected smart home systems, researchers were able to hack into all the widely available smart home systems on the market and open locks, change pre-sets, and trigger fire alarms.[50] It has been shown that humans can be ill-prepared or ill-trained to identify and manage the IoT-associated security risks.[51]

1.25 Indeed, it is significant that many of the key strategies for combatting offences that involve technology, for example, good corporate governance; alert/engaged/prepared/ staff; authoritative and engaged leadership; effective standards; the implementation of appropriate security that is well managed and maintained; a focussed and effective risk culture (to name but a few) all largely depend on people. So the key elements of a cyber defence system are dependent on one of the main weaknesses. It is not surprising then that human factors feature prominently.

Gollan, N. 2016. Whitepaper: Internet of Everything. How to Secure the Internet of Everything. *Sense of Security.* Available from: https://www.senseofsecurity.com.au/sitecontnt/uploads/2016/04/Sense-of-Security-Whitepaper-How-to-Secure-the-IoE-v1.0-01Apr16.pdf

[45] UL. 2017. Cybersecurity Considerations for Connected Smart Home Systems and Devices. *UL*. Available from: https://industrie-4-0.ul.com/wp-content/uploads/2018/02/UL_Cybersecurity_SmartHome_White_Paper_en.pdf

[46] A report by Beaming, noted that security cameras were amongst the most frequent target of hackers. See a report in The Times, 9 July 2019, p12.

[47] Lanner. 2018. *Op cit*

[48] Sharp, N., and Gollan, N. 2016. Whitepaper: Internet of Everything. How to Secure the Internet of Everything. *Sense of Security.* Available from: https://www.senseofsecurity.com.au/sitecontnt/uploads/2016/04/Sense-of-Security-Whitepaper-How-to-Secure-the-IoE-v1.0-01Apr16.pdf

[49] Sharp, N., and Gollan, N. 2016. *Op cit*

[50] UL. 2017. *Op cit*

[51] Merella, A. 2018. IOT Security Issues and Risks. *Apiumhub.* Available from: https://apiumhub.com/tech-blog-barcelona/iot-security-issues/. See also, SIA (2019) *Future Scoping of the Private Security Industry*. Published by SIA, research conducted by IFF. SIA (2018) *The Provision of Industry Skills: Profiling Research*. Published by SIA, research conducted by IFF.

1.26 Of significant concern, then, staff engaged in security-related work have been found to be short of the requisite skills.[52] A study by Claranet, published by McAfee, highlighted the human challenges in Cloud security, this included in-house teams (working with partners) lacking expertise in the changes/developments they instigate.[53] Touching on the importance of cyber security considerations, an (ISC)[2] 2018 Global Security Workforce study found that the majority of departments that responded to their survey admitted they lacked staff dedicated to cyber security; indeed well over half (59%) felt that companies are at least at moderate risk of cyber-attacks as a consequence. One study has highlighted some of the vulnerabilities that IOT has given rise to:

> *1) Vulnerabilities in communication interfaces between the user and internet of things is insecure, where the user can bypass, access and control the device; 2) Weakness in the authentication process; 3) There are not enough methods to identify the authorized users, and this allows unauthorized people to log in to those devices; 4) Insecure software occurs when programmers focus only on the speed of transfer data neglecting the security aspect; 5) Using insecure protocols for data transfer; 6) Easiness of scanning and knowing the devices connected to the internet*[54]

How new security measures are impacting offenders

1.27 There is a tendency to think that the more advanced the security the better it is. Such a link is simplistic.[55] Already offenders are making use of AI, it enables them to more easily avoid detection while at the same time generate greater rewards.[56] Indeed, they can up-skill and adapt.[57] To illustrate, while traditional offender entry tactics involve lock picking, impressioning, and copying, new methods involve 'man in the middle'[58] and relay attacks, here is an example of how this works:[59]

---

[52] Moreover, some white-hat, or 'ethical' hackers, for example may not only lack the requisite skills, but may also not be so ethical after all. See, Pickup, O. (2019) Should you employ a former black hat hacker? *The Sunday Times*, 24 February, P10. Special section on Cyber Security.

[53] Taken from a discussion in The Paper (Business News for Security Professionals), 19-11-18.

[54] Tawkif, M., Almadni, A.M., and Iharbi, A.A. 2017. A Review: the Risks And weakness Security on the IoT. *International Conference On Recent Advances In Computer Science, Engineering And Technology*, pp 12-17. Available from: http://www.iosrjournals.org/iosr-jce/papers/Conf.17003/Volume-1/3.%2012-17.pdf

[55] See, Blythe, J. M. & Johnson, S.D (2018) The consumer security index for IoT: A protocol for developing an index to improve consumer decision making and to incentivize greater security provision in IoT devices. Conference; 2018; IET Conference Publications, Living in the Internet of Things: Cybersecurity of the IoT, 14/06/2018.

[56] Ismail, N. (2019) Fighting Fire with Fire: the Dark Side of AI. *The Sunday Times*, 24 February, P2. Special section on Cyber Security.

[57] Sanders, A. N., Kuhns, J. B., and Blevins, K. R. (2017). *Op cit*. See also, *The Theoretical and Geopolitical Implications of AI.* https://www.ifsecglobal.com/ifsec-international/the-ethical-and-geopolitical-implications-of-ai-and-machine-learning/

[58] Of course, these should more accurately be termed 'person in the middle attacks'.

[59] Moses, S., and Rowe, D. 2016. Physical Security and Cybersecurity: Reducing Risk by Enhancing Physical Security Posture through Multi-Factor Authentication and other Techniques. *International Journal for Information Security Research*, 6 (2), pp. 667-676. Available from: https://infonomics-

> *For a man- in-the-middle attack, an attacker is essentially acting as a middleman intercepting a transaction and then passing it on. The attacker acts as a card reader taking the information on the card then relaying the information to the true reader. This allows the attacker to sniff the traffic between a card and a reader stealing its access credentials, which would allow an attacker to impersonate the card. A Man in the Middle attack makes is possible to alter data as its passed through. This attack may thus provide higher privileges than those held by the legitimate card owner…A relay attack is where an attacker relays communication between the reader and the authentication card or token. A successful relay attack allows an attacker to possess a copy of the card. For a relay attack, one needs two devices to act as the card and the reader. They establish a relay channel and establish a connection which the reader and card is unable to distinguish from the true one*[60]

1.28 What is readily apparent from studies of offenders is that they adjust to new measures by finding new approaches of their own to mitigate the effects, which in turn requires newer measures or updates on existing ones.[61] But how do offenders learn about technologies when applied to physical measures? How, if at all, are they assessing risks? And what are the trends in advanced security as they relate to physical security measures and how do security professionals perceive the threat and opportunity here? The rest of this report focuses on these issues.

society.org/wp-content/uploads/ijisr/published-papers/volume-6-2016/Physical-Security-and-Cybersecurity-Reducing-Risk-by-Enhancing-Physical-Security.pdf

[60] Moses, S., and Rowe, D. 2016. *Op cit*. Page 671.

[61] Ekblom, P. 2011. *Op cit*

Section 2. Views of Offenders

Introduction

2.1 We interviewed 15 offenders. Cumulatively, their experience covered a number of different crime types such as shoplifting, burglary, robbery, and fraud – all had committed offences for financial gain against businesses and all had experience of overcoming security measures in order to commit their offences. The aim here was to focus on the more general perception of whether and the ways in which technologies associated with physical security measures, including on traditional crimes, had impacted on offending. While all credible measures can pose a threat, the aim here was to gain an insight into the ways in which advances in security impact on offending behaviour. It starts with a focus on the ways offenders learn about security technology and how to overcome it, and then moves on to consider the impact of technology on offending behaviour; how technologies can sometimes work in offenders' interests; the significance of visible security personnel; and the perceived risks presented by technology.

Learning about technology

2.2 We asked interviewees where they and/or others had learnt about overcoming technology. A number of methods were provided, some traditional (e.g. in prison) and some more novel and reflecting an increased use of technology and the resources it provides.

Employing accomplices

2.3 Sometimes offenders chose to involve accomplices because of their specialist knowledge (e.g. one offender talked about a network of 'middle men' who worked in a non-technical role for a primary offender who dealt with these aspects of the offence, such as creation of bank cards, circumventing bank security protocol) or they may be asked to join in on a crime and learn on the job, there was some evidence that organised crime groups recruited, through online advertising using channels the public can see, for people with technical skills. This shows how traditional paths into offending were shown to be disrupted by the advent of the internet, and how potentially, it has become easier for offenders to recruit those with the right skills to commit an offence and for those with no criminal background to be drawn into offending:

> *If you needed help then you have to bring someone with you that was their speciality – but you don't really want that because that is more money going their way – so when they help you watch them and then you don't need them again next time – I learnt it by watching them in action.*
>
> *(Interviewee 9)*

Education and online tutorials

2.4 There was evidence that for some, learning from educational courses, sometimes advanced, had since been employed in the commission of crimes that required circumvention of security systems (e.g. access control systems linked to a database). There was also a view that some previously complex technical crimes, involved in overcoming security protocols (e.g. both on and offline credit card fraud) were now more achievable due to a proliferation of websites providing advice on how to accomplish them, or resources that enabled them (e.g. video tutorials or product manuals):

> *There's always going to be ways round things, there's like tutorials, like you'd get on Youtube on how to do it these days, the carding sites are still in their prime. It's all online now, there's more help for people wanting to do it. It can be an amateur game now, everyone's an expert, it's all online now.*
>
> *(Interviewee 6)*

> *… really, to be honest, you could do anything you want with a search on google. To completely disassemble and replace an access system you could do* [disassemble and replace] *in 1-2 hours.*
>
> *(Interviewee 4)*

2.5 Some of the offenders talked about how their offending career had spanned periods of technological development and how their offending had evolved from physical to online offending, employing new techniques facilitated by the development of internet technologies and increasing use of the online marketplace:

> *You don't need to buy from the high street, everything's online now, and that's where we went… you don't need the risk.*
>
> *(Interviewee 6)*

Other online sources

2.6 Some pointed to learning from stories in the media, in all its guises, or engaged with online groups or forums which were either purposely dedicated to certain types of offending (e.g. hacking forums) or had relevance for the skills required in their offending (e.g. coding forums).

> *We used to watch Watchdog and we used to see people do stupid things so we thought if we did not do this it might work. We used to watch that a lot and get a lot of ideas.*
>
> *(Interviewee 12)*

> *On the news yesterday there was a story about how easy it is to steal new cars -- all these electronic key fobs. You just need a system with a scanner and to stand by their*

door and it picks up the signal and someone stands by the car and it opens it. If you make something, you can always make something to counter.

(Interviewee 8)

Observation

2.7 Some of the offenders talked about the process of learning about a specific target – e.g. a shopping centre's security arrangements, or how to de-tag items. Some of these answers showed how offenders would assess the capability of targets to respond, or their use of connected security systems and make decisions based on these assessments:

> [In a favoured offending location] *You used to be able to just fill up your trolley and push them out… there was no alarms.*
>
> *(Interviewee 6)*

> In some shops in the morning or late at night there was no one watching the changing rooms – I just noticed at that particular shop that is what happened.
>
> *(Interviewee 11)*

> What we used to find a lot is that you would have different security, different days, you could go three times a week and they wouldn't recognise you.
>
> *(Interviewee 7)*

> If you get (name of company), you know the foam is no good [to disable an alarm]. So for that if you knew someone who could cross wire it or short circuit it or something you would get them – so really it would depend on what the alarm is.
>
> *(Interviewee 9)*

Inside knowledge

2.8 Inside knowledge was invaluable to some of the offenders we spoke to. There was some evidence from the interviewees that family and friends working in security were used as highly valuable sources of information, both with regards to new developments in security technology, and how to circumvent them:

> *I worked in security…I still do work – in the shopping centre, as a caretaker, so the security people tell me what they do. I go to the CCTV room with them – but they don't know that I'm a shoplifter so I get training from them.*
>
> *(Interviewee 14)*

> *I had people and friends in security firms – so I knew what was up and coming and what was the new thing and how it worked – without them a lot* [of the offences] *wouldn't have happened.*
>
> *(Interviewee 9)*

> *A lot of the time it's people working in retail that give those tips as well. So over time they would find a way and like learn more about the technology.*
>
> *(Interviewee 13)*

2.9 One interviewee even reported that knowledge had been gained about how a shop secured its products from the security staff who caught them:

> *You talk to security while they are waiting for the police to arrest you and you have a bit* [of] *banter with them – you ask, what happened?... One time when I asked, they said, 'no it wasn't us* [who set off the alarm in order to apprehend the interviewee] *– look – you forgot to take one* [tag] *off'. That makes you more cautious for next time – you make sure you go over more thoroughly next time.*
>
> *(Interviewee 7)*

Impact of technology on offending behaviour

2.10 One route to determining the effectiveness of security measures (not just technological ones) is to consider the extent to which offenders say it impacts on their behaviour. The interviews conducted here showed that in the case of technology certainly, this is not a straightforward calculation.

Acting to avoid security

2.11 It did not always hold that offenders would avoid targets with improved security and pick easier targets. While some offenders indicated that they would avoid certain targets, that employed certain security measures (some feared for example the risk of being seen on CCTV), or businesses that they perceived to have good security; they also found ways to avoid the security that was in place and in some respects it did not matter whether it was a traditional physical security measure or one adopting more advanced technology:

> *CCTV is not entirely useless in these cases, but to be honest you could be a postman,* [or] *there to check the gas, it's easy … I'd look for which direction* [CCTV] *is pointing, what scope it is, so I'd know where to stand to be out of the field of vision, these are all things that you can learn.*
>
> *(Interviewee 4)*

2.12 Some felt that digital evidence of a crime – often CCTV footage was not always a deterrent because even if they were unsuccessful at avoiding detection, they made sure that they had a 'story' if they were caught or their behaviour was viewed as suspicious; this held across a number of offences, including shoplifters, credit card fraudsters, and an offender circumventing access control systems. For example, one petty shop thief said that she would use a self-scanner and when weighing

an item key in that it was something cheaper; her behaviour did not look criminal and that gave her confidence, and she had a ready explanation if challenged that she had accidentally pressed the wrong button.

2.13 One female in her early twenties noted that security measures of any kind, advanced or not, were not important if offending was organised and imperceptible to cameras (even advanced systems with face recognition) or staff. It was possible to avoid items that were tagged, or *'acting'* within the gaze of cameras, and offend only where there were insufficient security officers to pose a real threat:

> *It's not hard to look like you're not stealing, and if you don't look like you are, they're not looking at you… they've got enough to deal with.*
>
> *(Interviewee 2)*

2.14 One offender talked about the way in which scams could mitigate the likelihood that security technology already in place would be used to detect their crime. In this example, the offender working with an accomplice conducted a returns scam where their accomplice would purchase the same items as they put in the basket, then return to provide him with a receipt so that he could walk out of the shop confident that if he was challenged he would be able to provide 'evidence' of his purchase:

> *… there's no way they check CCTV or anything, the man at the front, if you've got a receipt he's not going to think anything, he's not going to say, 'oh hold on'.*
>
> *(Interviewee 6)*

Finding weaknesses

2.15 Problem solving to overcome some of the challenges for offenders that have been introduced by technology were evident and viewed as a normal aspect of offending. Offenders revealed how they could employ relatively low-level technology (or no technology at all) solutions to exploit weaknesses in security-related technologies. Traditionally this may involve breaking or removing what is there, and just because it was advanced did not mean it could not be broken or removed.

2.16 Interestingly, one offender, adept at manipulating access control systems, reported that very expensive systems were often very vulnerable, and while viewed by companies as very secure were easy targets. This offender indicated that there was often a, *'false sense of security'* in those places where advanced systems were installed. More generally, however, these complexities highlight that technology presents merely an opportunity to impact on offence related decision-making, it is not a given that technological security measures focussed on the sorts of offences they committed, and had built up an expertise on, were impediments.

Limited impact

2.17 A few interviewees talked about how technology could only catch 'low hanging fruit' or disorganised offenders who were committing crimes through desperation or opportunism, and not those who had developed a workable modus operandi:

> *Security might have some clever tricks but there's always ways around it, or … it just catches people that don't think.*
>
> *(Interviewee 6)*

> *…but if someone is smart enough, there's nothing you can do if they want to get in,* [but] *if they are regular people just a standard lock and CCTV would deter a regular criminal.*
>
> *(Interviewee 7)*

2.18 Others talked about how security and visibly 'high-tec' security may be indicative of something valuable to protect which can increase their interest in a particular target.

2.19 Interviewees noted the limited impact of security given that some offences could simply be committed quickly without any real need to avoid or overcome security. Shop theft and burglary were examples where there was a perception that police were not likely to turn up, and rarely quickly, and that although technology may alert security, if they were quick enough it would not matter:

> *It takes seconds and by the time they know what's going on we're done and off and anyway… there's nothing they could do.*
>
> *(Interviewee 2)*

> *If the alarm has gone off, and there is something there you can grab quickly and make your getaway.*
>
> *(Interviewee 3)*

> *I used to walk in – in and out quickly – don't hang about – walk in as though doing nothing wrong and leave within a minute. In and out.*
>
> *(Interviewee 15)*

Deterrence undermined by a lack of response

2.20 Crucially, a number of interviewees talked about how a lack of an effective response prevented security measures from being a more effect deterrent:

> *I've been in the room where they caught the person – usually youngsters – they let them off anyway.*
>
> (Interviewee 14)

2.21 Despite being aware of security measures being in place e.g. CCTV, or linked shop radio systems, for some, because they had not been caught, their confidence increased, and their perception of risk reduced. This demonstrates how the effectiveness of security systems can deteriorate when there is no visible response to offending behaviour – in the following example the interviewee shows how while cameras can introduce an element of doubt as to whether they are being watched, a lack of response led to an assumption that they were not and increased confidence in offending:

> *You can tell when security* [person] *is watching you, you can't if there's a camera, and 'cause I haven't been caught, I figure they're not.*
>
> *(Interviewee 2)*

> *People get away with lots of things. Cut backs, shops close, taking security out, money is tight, cutting back on security. Like where I…they radio whenever there is shoplifting, but by the time they get there the person has gone.*
>
> *(Interviewee 14)*

2.22 Offenders were concerned primarily with immediate risk, perceiving that if they were not caught at the time then the chances of getting caught later were rarely high enough to worry about. Indeed, it was also highlighted that some offenders, such as those motivated by drug use, sought only to get their target in order to fund their habit, and cared little about the possibility that the evidence generated by advances in security technology may increase the chances of them being subsequently caught and convicted. This again, is a reminder of the limits of security.

2.23 Similarly, some relied on technology being unreliable such as images being of too low quality to identify or convict them, and alarms not working properly:

> *They would put ink tags on their clothes, but they wouldn't work when you left the shop – they wouldn't set off the alarm so they were no deterrent. It was really easy to remove the tags. Once you are away from the shop you can take as much time as you want to remove it. One of the ways was to put it in the freezer and then take it off.*
>
> *(Interviewee 7)*

2.24 A number of interviewees noted that there was not much enthusiasm for tackling crime generally and anything involving technology specifically. There were general comments about the reduced police resources and the sheer proliferation of offences and offenders – many committing offences without being at the scene and therefore not visible, that rendered crime a relatively safe way of obtaining money, noting on lower-level crimes, '*the banks don't investigate, you don't get caught'*:

> *No, I'm not worried, the police care, but they don't care enough about it, and like, I don't think it's enough evidence - to pull out an investigation they need secure evidence.*
>
> *(Interviewee 5)*

2.25 One offender noted how the online sites that facilitated offending were sometimes uninterested in preventing it, and how despite carrying out an offence with a well-known modus operandi (so well understood that other users of the site would sometimes send him angry messages telling him to stop targeting victims using it) the website itself did nothing to prevent his offending:

> *No, other people used to flag it down, the adverts, people* [other users] *knew what we were doing, I've actually had messages saying, 'what you're doing is disgusting, I know what you're doing' – but never any action from the website…really they should* [change], *but it keeps them popular…*
>
> *(Interviewee 5)*

Career criminals are used to challenges

2.26 One 57 year old man who has extensive experience of offending, especially burglary, including 5 prison sentences and hundreds of offences, made the point that good preparation was key to being successful at crime and that this has not changed, even with the introduction of new security technology. He highlighted that being confident there was something worth stealing, understanding what security measures were present and having a plan for mitigating them were always important and always will be. This offender noted that technology has always been a challenge. Even the early burglar alarms – seen as an important new technology in their day - were always something that needed managing, so rendering them dysfunctional or acting quickly so that he disappeared before anyone could intervene were always a priority.

2.27 In short, technology does not operate in isolation and is only one factor in a network influencing offending decisions. These are both within the control of organisations (e.g. how do they respond to a detected threat) and out of their control, (e.g. if the sanctioned response to a crime is absent or low, there is little motivation to desist):

> *Shoplifting sentences are low…when they* [other people] *got caught not a lot happened.*
>
> *(Interviewee 6)*

Technology works for offenders too

2.28 There was evidence that offenders had concerns about technological advances and that this impacted on their offending behaviour. These

are detailed in 'Impact of technology on offending behaviour'. However, another important finding from the interviews was the way in which the advent of technology generally had influenced offending, and been co-opted (even security technology) into the commissioning of crime.

How offenders used the internet to facilitate crime

2.29 For some offenders, developments in technology had resulted in their offending being carried out online – this included developments in security technology, for example, one fraudster talked about how credit card fraud had become difficult with the introduction of chip and pin, and how they had moved to offending online because it was a less risky environment to offend in. This sentiment was shared amongst other offenders, with the internet viewed as having provided the dual advantage of generating more opportunities while reducing the chances of getting caught - by engaging in forms of offending that were perceived as less visible to authorities. One interviewee, whose offences included duping people into allowing their bank accounts to be used to process money, and in some cases taking over accounts to apply for loans in the victim's name which were then stolen, noted that the internet had greatly facilitated crime. It made it easy – '*too easy*' - to find victims, and then to commit offences without ever being seen. This offender talked about how the offence would not be possible without the internet; the individual sought victims online with perceived impunity, and was sometimes able to commit their entire crime virtually – through convincing vulnerable victims to take photographs of their bank cards, for example. This offender did not fear being caught because it was felt that the websites were not interested in improving their security, and police were unable to police digital environments.

2.30 There were numerous references to the ways in which technology had been used to facilitate crimes, and reduce risk, for example, offenders used social media channels to assess the value and risks at targets, and encrypted channels to communicate and share locations:

> *I hear that a lot of people are using Facebook if they are going to burgle.*
>
> *(Interviewee 7)*

> *There's a forum on* [name of website] – *I think they closed it but it went in to detail on tricks and how to get away with it.*
>
> *(Interviewee 11)*

> *If the forums and online communities are still going they would pool that information together.*
>
> *(Interviewee 13)*

2.31 Some of the interviewees talked about how by offending online they no longer had to face their victims, which was viewed as an advantage, lowering their concerns about victimisation and confrontation. One interviewee who had previously been involved in credit card fraud both

offline and later online talked about how online offending reduced the need for certain skills when committing a crime:

> *I was a good talker, I could talk my way out of any sticky situation…online you don't have to act.*
>
> *(Interviewee 6)*

2.32 In addition, some noted how new technologies and encrypted communication helped prevent them from being convicted, even when they had been identified as an offender:

> *…Used WhatsApp* – [it's] *encrypted and when police got the phones they couldn't work it out.*
>
> *(Interviewee 15)*

Security measures can be used for illicit purposes

2.33 A few of the interviewees noted how they had adopted more advanced security devices for their purposes, to reduce risk and identify targets. One talked about how they had purchased and used a GPS tracker to follow the whereabouts of a security car, and talked about how trackers were used by offenders at one carwash to identify the whereabouts of a target for later crimes:

> *They* [offenders] *don't want the risk, they're very aware...you think its a security device, so do they... we've used a tracker before when we needed to see where* [security] *was … It's safe, no one's going to see it*, [GPS tracker] *you've got a reason* [washing a car], *put them on and see where they go, if it's obvious they're not going to miss it* [money], *I never was involved but you hear it and you think, yeah, I can see that.*
>
> *(Interviewee 10)*

People factors

2.34 A key finding about security technologies evident from speaking to offenders was that while they were a potential deterrent through their potential to increase the risks, for example, by alerting others that an offence is taking place meaning that it has to be aborted; or reducing the rewards from the crime if you have to leave the crime scene before you have obtained all that is available, this potential can either be undermined or not fully realised due to a number of factors relating to human involvement in security.

2.35 Offenders were generally concerned that a person would intervene during the commission of a crime, some talked about their fear of *'confrontation'.* In its most effective guise, technology was viewed as a tool that can potentially trigger a response that will stop the offence, or make it more difficult, and both of these are negative, but most importantly, only people can detain you, and this was a big driver – the use of technology with visible security presence was most effective as

a deterrent. Generally speaking, people were more concerned about security staff than security technology and dogs too:

> *Well it was not really the type of alarm. But if it had a security guard, yeah. Yeah because then you cannot make no noise and then the chances of that … It can come up unexpected.*
>
> *(Interviewee 1)*

> *If there is security guard in a shop, it makes it more difficult. There are dogs at home, it is unpredictable.*
>
> *(Interviewee 8)*

2.36 Offenders also talked about how important the people who were employed to look after security were and how poor staffing could undermine it:

> *You can have the best system in the world, but if people don't care it's not going to help … If you know the guy watching the screens he knows where not to look … that's how it happens.*
>
> *(Interviewee 10)*

2.37 And importantly, while technology generates a wealth of information, it still has to be managed effectively:

> *What are you going to do with all the information?* [it] *doesn't provide a solution,* [you] *need to do something with this.*
>
> *(Interviewee 10)*

2.38 Another interviewee who was an expert at overcoming access control measures in buildings made three distinct points. The first was a very determined technologically minded niche criminal can always find a way. While refusing to give precise details the key point was that signals to transmitters can be intercepted and programming can be manipulated. The second was to note that the major general flaw of security systems, not least technologically advanced ones, is their maintenance, or the lack of it. Therefore, some basic measures were sometimes better than more advanced ones because they required less upkeep; and third that people can be a systems' strength or weakness:

> *The technology is smart enough, the technology doesn't need to get smarter, it's the people that do* … [you need security] *people who are really interested in your safety…. With systems, with the database, they lose it* [access to the database], *they lose the laptop it gets destroyed, they lose access, and then, if you found a trespasser and you want to change the key fobs you can't, that's the problem with connected advanced systems … If you have a concierge, that's a deterrent ... on the other hand … you can walk straight past a*

concierge and say hi, and they'll say hi back and not check who you are or even look.

(Interviewee 4)

2.39 Other offenders talked about how an organisation's security was damaged by other business priorities, for example, one offender spoke about 'high end' shops wanting to avoid projecting an air of suspicion on their shoppers which made stealing easier:

I think in some places, the higher end, they were more scared about looking like they thought you were stealing, and that makes it easier.

(Interviewee 2)

2.40 Others talked about how consistency of security staffing was a significant deterrent because the security staff built up a knowledge of their pattern of offending. It is notable that building up an understanding of patterns of offending is one of the benefits of AI, and while that has advantages it doesn't have the immediacy of impact people doing it has:

Some knew us, there were places where they had the same faces, and they'd cause us trouble.

(Interviewee 2)

We were going there for a few weeks – one day the security guard gave us a knowing look as we went in the door and he seemed to follow us and he said I've seen you here, I know what you are up to and we were quite disappointed because we had done really well in there.

(Interviewee 7)

Security technology and the increased risk factor

2.41 It is important to stress that technologies increase risks. So while some of the time interviewees focussed on the limits of new developments other times they outlined the potential dangers, not least going forward if and when there is effective interaction between technologies and people:

Definitely does – a lot of people are definitely getting caught more. A long process – but people will start realising that, 'I can't go to Oxford Street because people are information sharing', radios linked to cameras. Once it has become a mainstay of security, it will put people off. People will only go on for so long, if every time you are getting arrested, because internet, security and stuff – it will take a few times to realise and for that to sink in and then you decide not to go there.

(Interviewee 7)

2.42 The interviewees narratives described how the nature of offending was changing and that to be a 'successful' offender these days required more intelligence and ability:

> *Yes, you have to be quite a smart person and criminal minded these days, there's lots of things to deter, but if someone is smart enough, there's nothing you can do if they want to get in,* [but] *if they are regular people just a standard lock and cctv would deter a regular criminal.*
>
> *(Interviewee 4)*

> *You've got to be very clever to be a successful criminal – got to be on the ball with everything – alarms, locks, so many different things – if you've not made it and don't know enough people you can't do it. Successful criminals know a lot of people in a lot of different trades – in it for the long game. But now, with technology I think more will get caught.*
>
> *(Interviewee 9)*

> *It's harder now … everything's encrypted.*
>
> *(Interviewee 6)*

2.43 For some, the key point about technology was that it increased one of the factors that offenders feared most, *unpredictability*. The very fact that there is so much more technology posed a risk because there was often a fear that something had been improved or developed that they were not aware of that would prevent them from carrying out the offence or increase the likelihood of them being caught. Moreover, a technical record of a crime taking place (pictures with an ever increasing amount of detail, or dyes connecting offenders to scenes) were much more difficult to challenge, and were viewed as a significant deterrent (albeit the internet provides a good way of finding a solution):

> *You don't know anymore, that's the thing... you'd know if an alarm had worked,* [now] *has it gone off, are they watching, you don't have that... that element of doubt'*
>
> *(Interviewee 10)*

> *Security guy may be sitting, looking. If walking around that's better you have more chance. But if* [they're] *looking on the screen that's harder as they may be watching you.*
>
> *(Interviewee 14)*

> *Technology is off-putting because things are more documented. Also the unknown of what it can* [do].
>
> *(Interviewee 11)*

> *The domes [cameras] – you can't tell where they are looking so feel exposed.*
>
> *(Interviewee 15)*

2.44 Other offenders talked about specific fears:

A lot are more linked up. More if you are in a town or city, they are monitored. But at home there are ones that are monitored -- alert to your phone.

(Interviewee 3)

[would avoid] *If it was more technical like an alarm linked to a call centre that would send police response or stuff like that.*

(Interviewee 3)

If there is something where your face is shown, that would be an issue. CCTV, the new doorbell thing … that's a really big issue, you wouldn't want that. I might pick somewhere else.

(Interviewee 9)

I got caught on the facial recognition – it can get a tiny part of your head, ear – and it can only be yours.

(Interviewee 9)

In summary

2.45 The individual contexts in which security-related technologies operate vary markedly. There are many factors that govern whether it is effective or not; it is not just about how good the technology is. Interviews with offenders have generated insights that certainly set technology in perspective. There is nothing new about technology advances, nor therefore in the need for offenders to respond to them. It has always been thus and to that extent nothing has changed. Technology can make crime more difficult, some crime at least, but it has also generated many more opportunities.

2.46 Technology increases risks where offenders don't know about it, underestimate or misunderstand it, and/or don't have any form of mitigation of their own (technical or physical). But they do have options, those mentioned in interviews included using co-offenders; seek a less well protected target; cultivating an insider; researching the target including accessing online sources; and focussing on a different type of crime.[62]

2.47 It has been argued that in a more general sense, technology has in some ways worked in offenders' favour. For example, the increased amount of technology viewing our public areas has driven crime to less visible places where it is more difficult to detect creating an unintended and not much discussed drawback. And the principles of crime have not changed. Offenders like easy access to the goods, with low risks of being caught and arguably technology has made that easier too. Certainly offenders are quick to adapt, and always have been:

[62] They would rarely give up altogether. Some said they committed crime because of an addiction, especially drugs, others because it provided money, one interviewee said he was an offender because it was fun and he was successful.

> *It has always been that a security company will build a 10-foot wall and then a criminal will build a 12-foot ladder and find a way over it or around it. I am not saying just because it is has got more difficult it is impossible, there is always a way.*
>
> *(Interviewee 1)*

2.48 Yet perhaps what is most striking about talking to offenders about advances in technology is that discussions about people are never far away. Indeed, when they were asked how their crimes could be prevented there was much more of a focus on processes and especially people in the answers given. One interviewee warning about the dangers of victims being duped, emphasised the need to raise awareness amongst people generally so they could spot a scam easier, generating alerts (banks, websites, police) so that people were more armed with information about the dangers at the key moments when this was important:

> *Particularly for young people when they turn 18 and they can get credit, when big transfers happen they should freeze accounts … It would be really good to advertise exactly what I told you, tell the stories* [used to scam people]*, or any communication material, and introduce it into schools at 16 or 17 year olds.*
>
> *(Interviewee 5)*

2.49 Others stressed the importance of good practices, and how investment in security personnel and maintenance was vital:

> *Make sure your access control system is maintained…you'd be surprised how many doors you … just bypass with a Mastercard.*
>
> *(Interviewee 4)*

2.50 Ultimately technology is designed, developed, manufactured, implemented, maintained, managed, used by people and each of these stages (and others besides) affords the opportunity for people to be corrupted and/or make mistakes and offenders can be good, very good, at exploiting these. In a different way one interviewee argued that more sophisticated systems can work in offenders' favour where they gave companies and staff a false sense of security, even resulting in them being complacent; where they contained in-built weaknesses either from the start or at a later point which were not addressed; or because the people operating them were incompetent or corruptible.

2.51 What emerges most about interviews with offenders is that word about the quality of security, be that relating to individuals, companies or communities, spreads fast. It underlines again why good security is so important. Whether it is good or whether it is bad offenders will quickly know:

Word spreads like wildfire through the criminal community — do not go there because you will get caught, for example.

(Interviewee 1)

Section 3. Views of Security Professionals: A Survey

The sample

3.1 A survey of security professionals was conducted in order to gauge their views on how offenders respond to technologically advanced security measures as well as gain an overview of the topic by looking at current use and the implications of using advanced technology in physical security measures, drivers of change, trends that may be influencing investment as well as the key benefits and drawbacks of using advanced technology in physical security measures. The findings are based on 225 responses[63].

3.2 In the introduction to the survey the following definition was provided – *For simplicity and readability we use the terms 'advances in technology' and 'advanced technology' to encompass internet enabled technologies/the internet of things.* Various statements were posed which respondents were invited to indicate their level of agreement or disagreement with. Additionally, some questions invited open text responses. All of the topics covered are condensed and summarised below.

3.3 Within the overall sample of respondents, responses were categorised according to their relative perspective – as buyers (and separately intermediaries acting on behalf of buyers), suppliers or other security expert, to compare whether views differed in accordance with the professionals' role. Included are only those issues that were statistically significant, evidencing a relationship between the variables (i.e. not occurring by chance). Differences in view by role were however rare.

3.4 Just under half of the respondents (49%, n=110) worked for a supplier (n=78 were Director, Manager or Consultant at an organisation that supplies security goods and/or services to corporate organisations and a further n=32 were contracted security operatives); while over a third (37%, n=82) indicated they worked for a buyer (of which n=44 were a Security Manager in a corporate organisation with in-house and/or contracted security, n=29 were in-house security operatives and n=9 were intermediaries acting on behalf of a buyer/customer).[64]

3.5 The remaining respondents were other security experts (e.g. academic, regulator etc.) at 9% (n=20) of respondents, or other interested party linked to security at 6% (n=13). Table 1 displays these roles.

[63] In total 243 started the survey however 18 responses were removed due to none of the main survey questions having been answered. The number of responses to each question varies as some respondents dropped out part way through and some chose not to answer certain questions.
[64] It is unknown to what extent this reflects practice across the security sector. Determining this would be insightful.

Table 1: Breakdown of respondents by role % (n=225)

Role	Type	% , N	Total
Supplier	Director, Manager or Consultant	35%, n=78	49%, n=110
	Contracted operative	14%, n=32	
Buyer/ Customer	Security Manager	20%, n=44	37%, n=82
	Intermediary	4%, n=9	
	In-house operative	13%, n=29	
Other	Other security expert	9%, n=20	15%, n=33
	Other interested party	6%, n=13	

3.6 Respondents worked for organisations that are operational in a wide variety of sectors. Nearly two thirds of the respondents worked for organisations based in the UK (64%, n=140). A full breakdown of both sector and country is provided in Appendix 2 – Additional Data Tables.

Use of Advanced Technology

3.7 Respondents were asked a number of questions to gauge their level of familiarity with and their current use of advanced technology in security measures. Nearly three quarters (73%, n=163) indicated that in their role they use or supply security measures that use advanced technology and the responses from this group were compared with those who did not do so. Included below are only those issues that were statistically significant, evidencing a relationship between the variables (i.e. not occurring by chance).

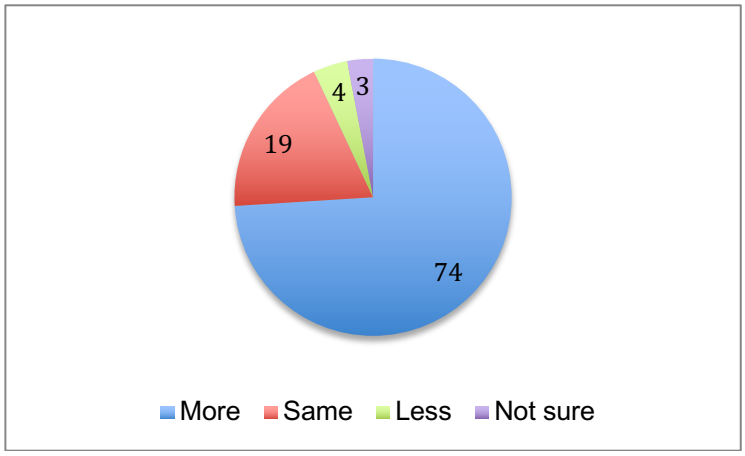
3.8 Perhaps unsurprisingly more than four fifths (84%, n=189) felt that there is a general trend towards the increasing use of advanced technology within physical security measures with those that use or supply security measures that use advanced technology (referred to from here onwards as 'current users/suppliers'), more commonly agreed that there is a general trend towards its increasing use. Indeed, those who are not current users/suppliers of security measures that use advanced technology [referred to from here onwards as 'non current users/suppliers'], were much less likely to do so.[65]

3.9 Three quarters of the sample (74%, n=165) said they were using more security measures with advanced technology than five years ago (either within their own organisation or within their clients' organisations). This view was more common among current users/supplier than non current users/suppliers, although it was still reasonably prevalent among non current users/suppliers[66]. Very few

[65] 93% of current users/suppliers agreed or strongly agreed, compared with 52% of non current users/suppliers.
[66] 83% of current users/suppliers indicated 'using more', compare with 48% of non current users/suppliers.

(9%, n=4) said they were using less. Nearly one fifth (19%, n=43) were using the same amount as five years ago. Figure 1 summarises the findings.

Figure 1: Amount of advanced technology used in security measures now compared with 5 year ago (n=224) %



The current State of security

3.10 Respondents were asked to indicate their agreement with a number of statements designed to gauge the current state of the security sector in relation to the use of advanced technology.

3.11 Most respondents agreed or strongly agreed that advances in technology that accompany physical security measures require security departments to collaborate more closely with other areas of a business (88%, n=186).

3.12 While there was a very high level of agreement with the suggestion that advances in technology provide enormous opportunities to improve physical security (86%, n=183), agreement was equally high that technology can never wholly replace officers when it comes to securing businesses (86%, n=183). The level of agreement was lower, but still a majority, with the idea that using advanced technology in physical security is reducing the number of security officers needed on the ground (64%, n=136).

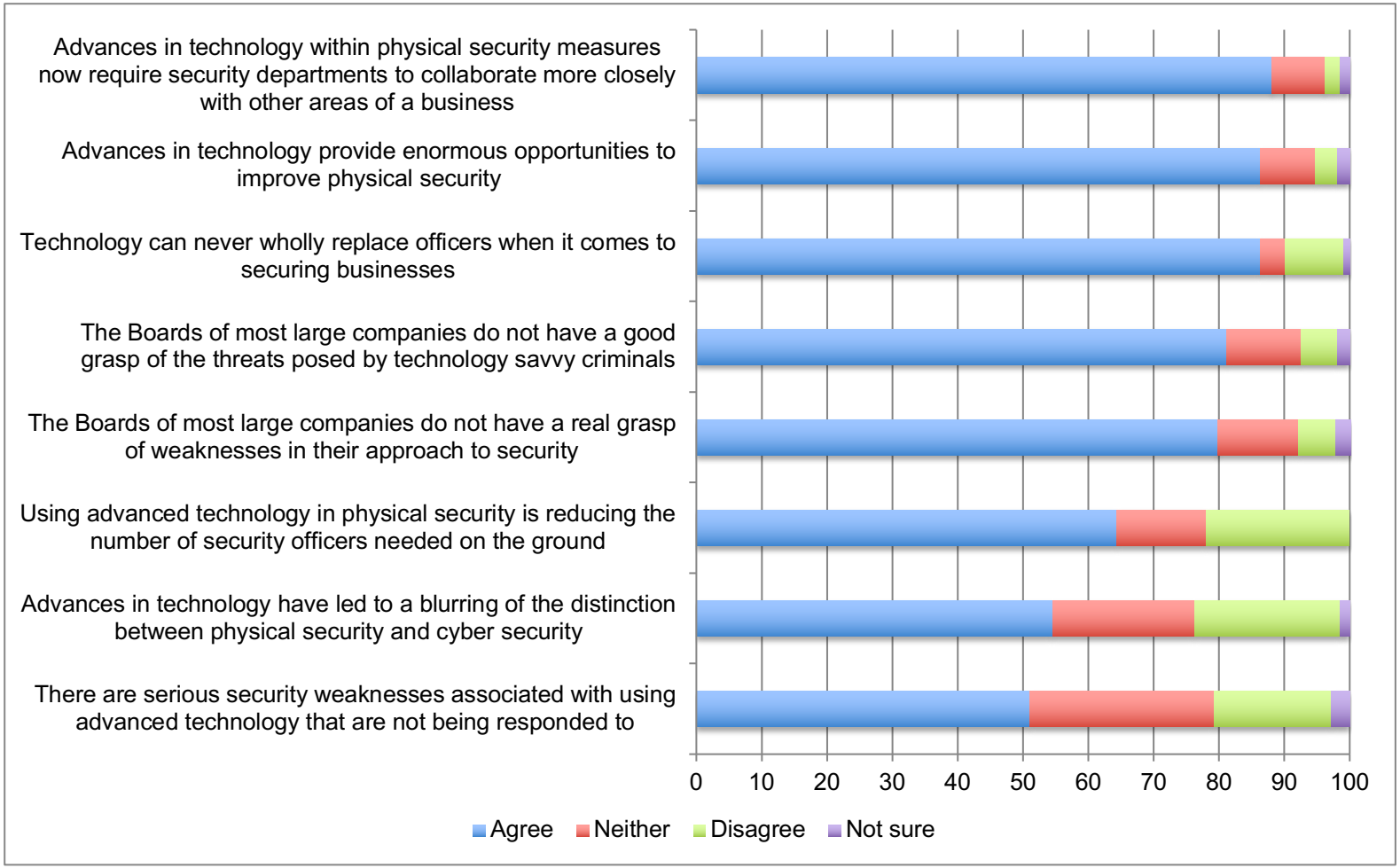
3.13 The findings paint a somewhat disappointing, if familiar picture in relation to Boards' views on understanding both the threat and the response, not least given previous research findings that highlight the importance of Board level understanding to the success of security[67]. Most notably:

[67] See for example Gill, M., Taylor, E., Bourne, T. & Keats, G. (2008) *Organisational perspectives on the value of security*, Security Research Initiative report, PRCI Ltd: Leicester.

- 81% (n=172) agreed or strongly agreed that the Boards of most large companies do not have a good grasp of the threats posed by technology savvy criminals.
- 80% (n=169) agreed or strongly agreed that the Boards of most large companies do not have a real grasp of weaknesses in their approach to security.

3.14 That over a half (51%, n=108) agreed that there are serious weaknesses associated with using advanced technology that are not being responded to suggests that there is much more learning to be done. Indeed, this may be viewed as all the more complex as a majority agreed that advances in technology have led to a blurring of the distinction between physical and cyber security (55%, n=115). These findings are summarised in Figure 2.

Figure 2: Level of agreement with statements about the state of the security sector in relation to technology (n=211-212) %



Views on how offenders respond to security

3.15 Another focus of the survey was understanding how security personnel perceive the threat posed by offenders. The findings suggest that the answer is 'considerable'.

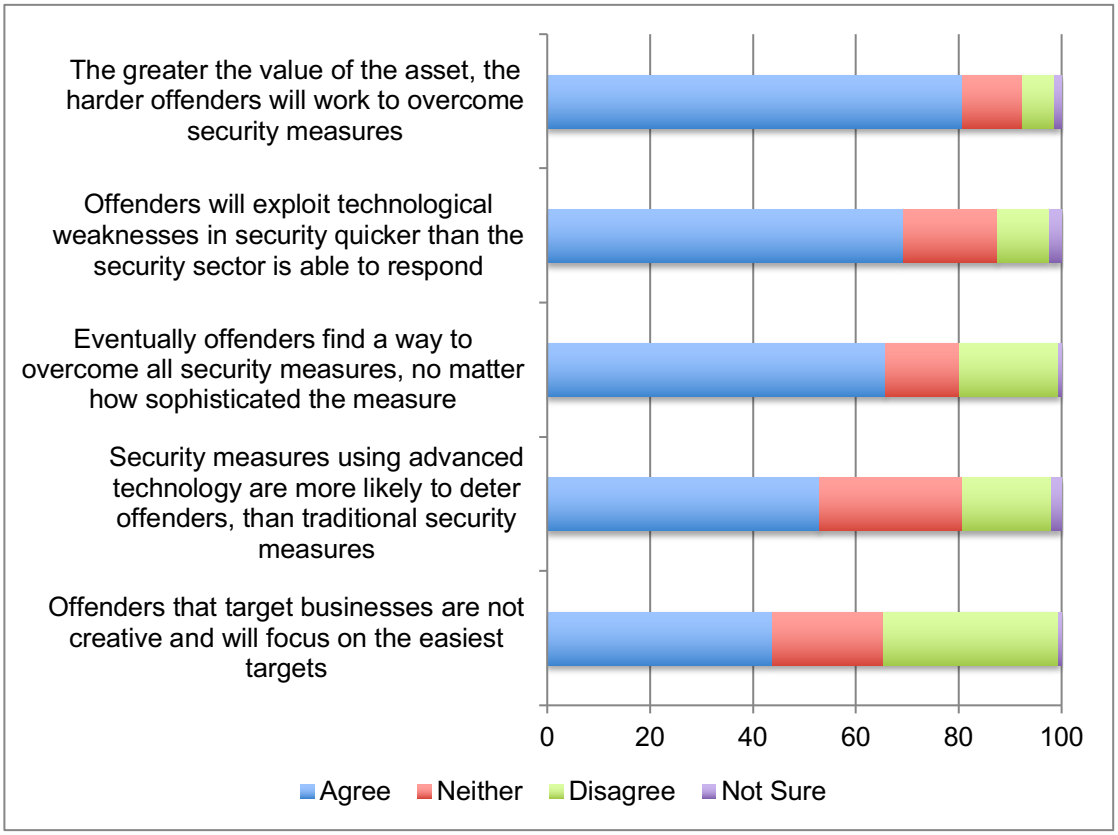
3.16 Most respondents indicated that the greater the value of the asset, the harder offenders will work to overcome security measures (81%, n=168). Conversely less than half agreed with the notion that offenders that target businesses are not creative and will focus on the easiest targets (44%, n=91). This suggests respondents feel offenders are not just out for an easy win and will work hard to get to what they want.

3.17 Over two thirds agreed or strongly agreed that offenders will exploit technological weaknesses in security quicker than the security sector is able to respond (69%, n=144) – although this view was more prevalent among current users/suppliers than non current users/suppliers[68]. Two thirds also agreed or strongly agreed that eventually offenders find a way to overcome all security measures, no matter how sophisticated the measure (66%, n=137). This underlines the constant need for security to evolve.

3.18 More than half indicated that security measures using advanced technology are more likely to deter offenders, than traditional security measures (53%, n=110). This is a somewhat muted response which perhaps suggests that creating a deterrent value is not a primary purpose of using advanced technology. The findings here are summarised in Figure 3.

[68] 70% of current users/suppliers agreed or strongly agreed, compared with 56% of non current users/suppliers.

Figure 3: Level of agreement with statements about how offenders respond to security (n=208) %



Influences on investment

3.19 A crucial component of good security involves the procurement process. Given this it will be viewed as disappointing that agreement was highest (compared to responses to all options here) that what security gets purchased is based more on what can be afforded than what is needed (83%, n=167). The long held view that cost is a primary determinant in the purchase of physical security[69] has not disappeared with advances in technology.

3.20 At least part of the difficulty, noted by over a half of the sample, is that is difficult for buyers to be sure of exactly what they are getting when they purchase physical security measures using advanced technology (57%, n=116) – notably though buyers agreed with this less commonly than suppliers and other security experts[70].

3.21 Reasons for this were revealed in other responses. Most notably, in that just over a half agreed that security measures with advanced security offer greater return on investment (55%, n=112) – current users/suppliers agreed with this a little more commonly than non

[69] See for example Ford, D. & Gill, M. (2007) *Introduction to Purchasing Security*, The Chartered Institute of Purchasing & Supply: Stamford.
[70] 50% of Buyers agreed or strongly agreed, 58% of Suppliers and 73% of Other Experts.

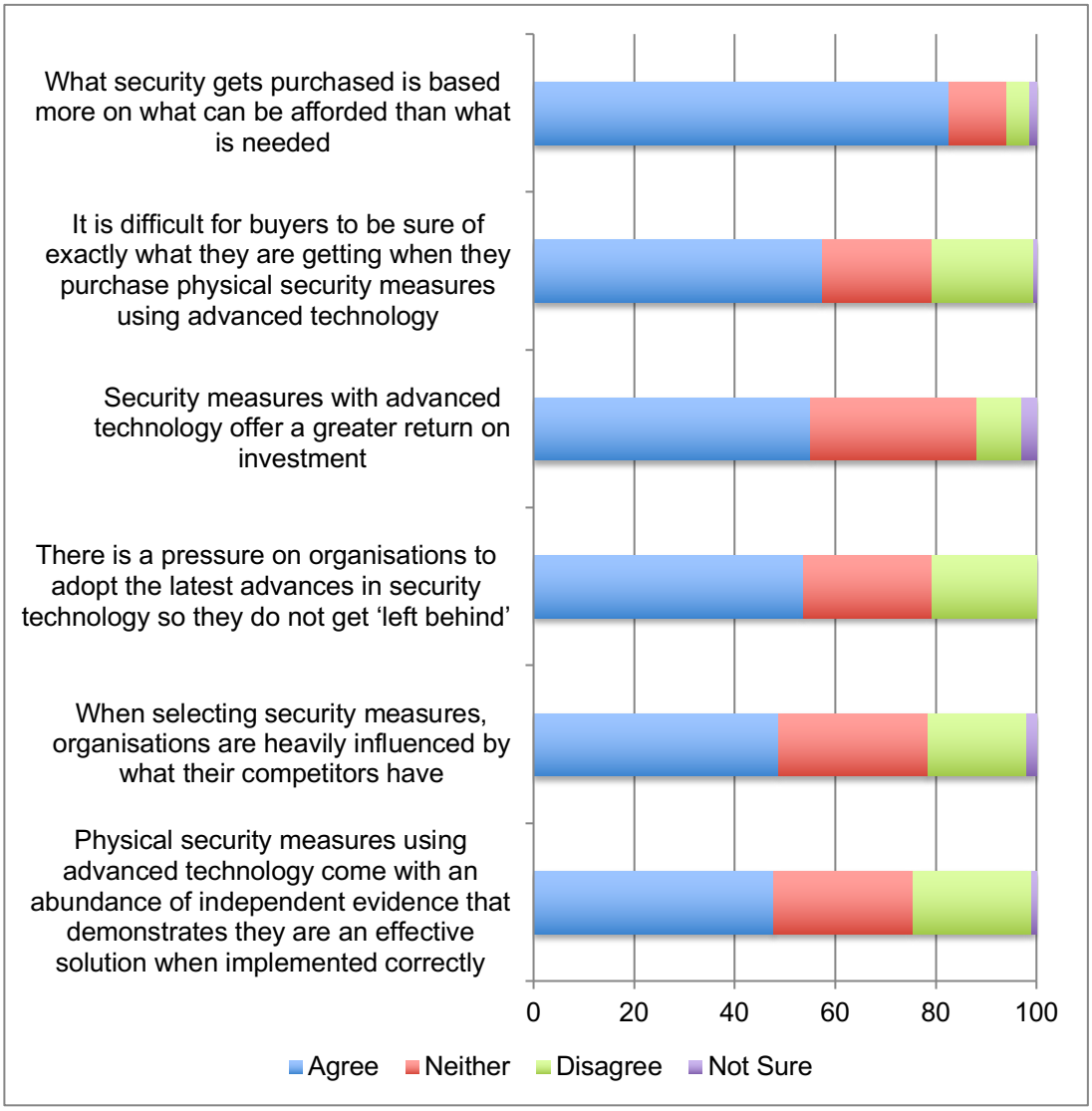
current users/suppliers[71]; while less than a half felt that security measures using advanced technology are accompanied by an abundance of independent evidence that demonstrates they are an effective solution when implemented correctly (48%, n=97).

3.22 The pressure to adopt the latest advances in security technology so they do not get 'left behind' (54%, n=109) – non current users/suppliers agreed with this more commonly than current users/suppliers[72]; and to a slightly lesser extent to keep abreast with competitor behaviour (49%, n=99) are notable.

3.23 In short, the sample highlighted that buying good security, even with the advent of new technology, has not solved traditional problems not changed many of the common influences on purchasing. The findings here are summarised in Figure 4.

[71] 60% of current users/suppliers agreed or strongly agreed, compared with 52% of non current users/suppliers.
[72] 72% of non current users/suppliers agreed or strongly agreed, compared with 55% of current users/suppliers.

Figure 4: Level of agreement with statements about trends that may be influencing investment in security (n=202-203) %



Potential drivers of change

3.24 We were keen to understand what the security sector feels to be the main drivers of change.

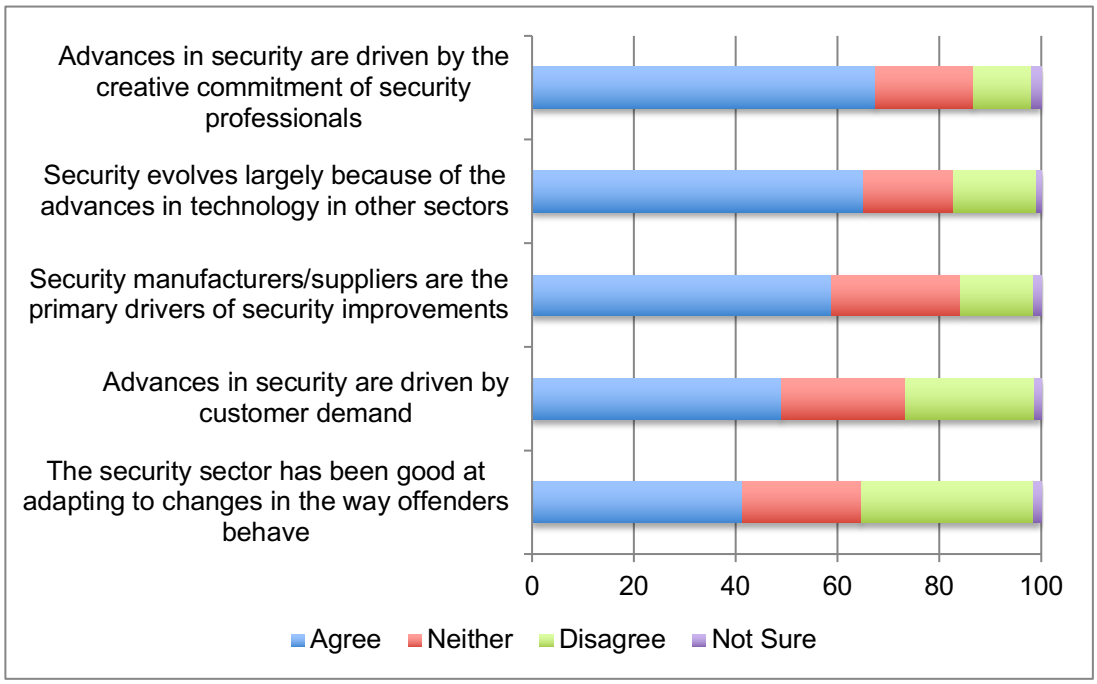
3.25 Of the options suggested three received majority support: they were with the statements that advances in security are driven by the creative commitment of security professionals (68%, n=137); because of advances in technology in other sectors (65%, n=132); and that security manufacturers/suppliers (59%, n=119) are the primary drivers of security improvements.

3.26 Interestingly, less than half of the respondents felt that advances in security are driven by customer demand (49%, n=99) – although this view was more common among non current users/suppliers than

current users suppliers[73]. So customers have a big influence where they are interested in it.

3.27 Strikingly, given the level of support for other options here, only two-fifths of respondents indicated that the security sector has been good at adapting to changes in the way offenders behave (41%, n=83). The findings on this issue are summarised in Figure 5.

Figure 5: Level of agreement with statements about potential drivers of change in security (n=201-203) %



Potential challenges to good security

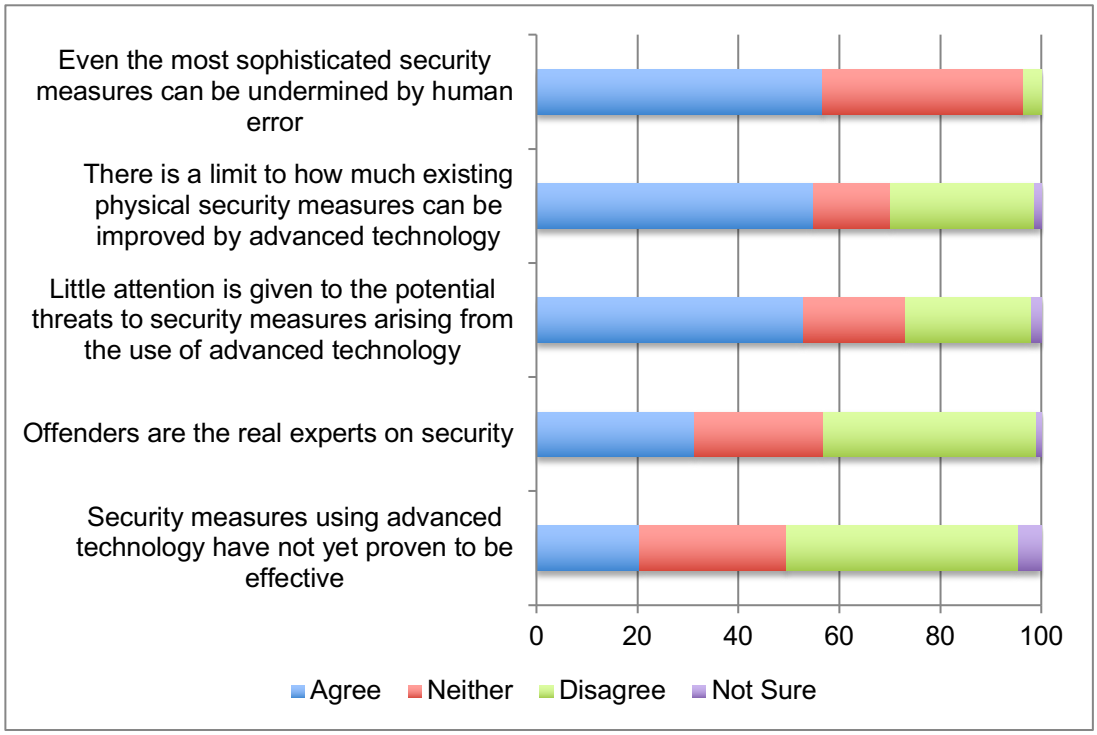
3.28 There are many challenges to good security. It has long been recognised that human error has the potential to undermine technology and this was supported by the sample (57%, n=114). And while overall the majority felt that there were limits on the extent to which physical security can be improved by advances in technology, (55%, n=110) this view was more prevalent among non current users/suppliers than current users/suppliers[74] suggesting again there is a caucus of personnel involved in security who are not convinced by advances in technology.

3.29 At least one explanation maybe the lack of attention given to the potential threats to security measures arising from the use of advanced technology, supported by over a half of the sample (53%, n=106). And more than 3 in 10 agreed that offenders are the real experts on security

[73] 64% of non current users/suppliers agreed or strongly agreed, compared with 50% of current users/suppliers.
[74] 75% of non current users/suppliers agreed or strongly agreed, compared with 51% of current users/suppliers.

(31%, n=63). While most disagreed that measures using advanced technology have not yet proven to be effective still over a fifth did so (21%, n=41). The results are shown in Figure 6.

Figure 6: Level of agreement with statements about potential challenges to good security (n=200-201) %



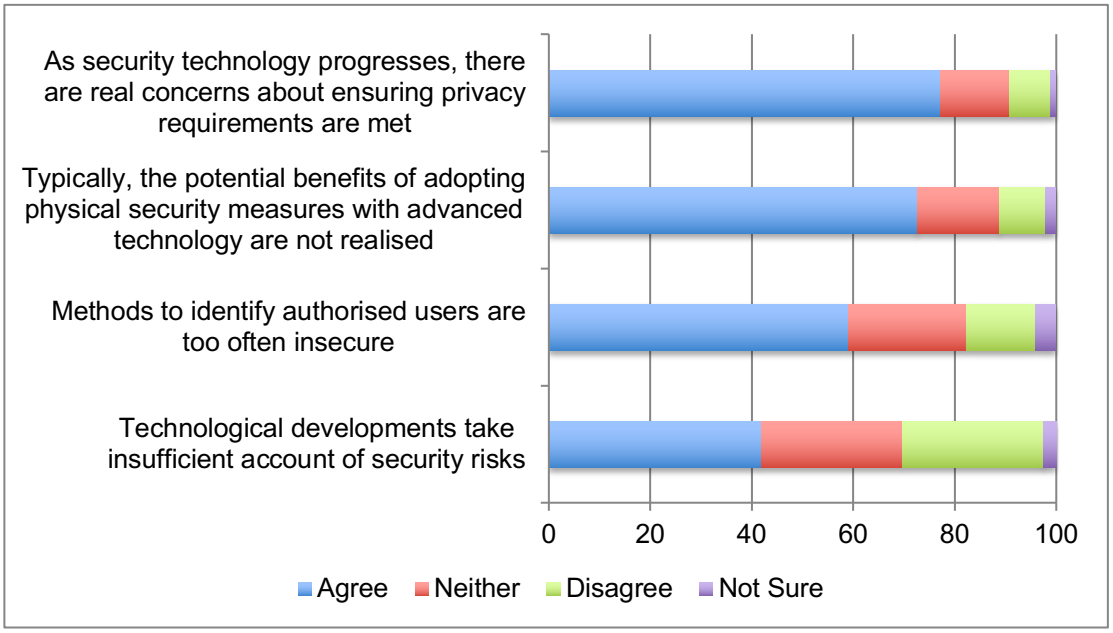
Potential threats to effective security measures

3.30 Sometimes, and not least at presentations at many conferences, advances in technology are presented as unqualified goods. Here there was widespread agreement that some of the most common threats were real ones.

3.31 Concerns about ensuring privacy requirements are met (77%, n=152) featured prominently and was perhaps to be expected. Although the difficulty and perhaps dangers of realising the benefits of any investments made were also widely supported as concerns. (73%, n=143).

3.32 Close to three-fifths of respondents agreed that methods to identify authorised users are too often insecure (59%, n=117) presents a specific challenge Once again the inherent security risks of technologies themselves were deemed to be a concern by a significant minority (42%, n=83). The findings are summarised in Figure 7.

Figure 7: Level of agreement with statements about potential threats to effective security measures (n=197-198) %



3.33 Towards the end of the survey two open ended questions were included to elicit comments from respondents on two key issues; the benefits of using advanced the technology, and then the drawbacks. These are discussed below.

The benefits of using advanced technology in security

3.34 In total, 157 respondents commented on the key benefits of using advanced technology in physical security measures. Where respondents described more than one type of benefit, these were treated as a unique response.

3.35 The benefit mentioned most frequently (n=37) was in relation to cost. Not all respondents were specific about how cost savings would be achieved although suggestions included that advanced technology in physical security measures could reduce manpower or reduce administration/back office which would result in cost savings.

> *'Manpower savings, decisions on mundane tasks can be taken by a machine.'*
>
> *(Supplier)*
>
> *'Cost savings to client for reinvestment.'*
>
> *(Supplier)*
>
> *'Can act as a real mid-long term cost saving.'*
>
> *(Supplier)*

3.36 It was also suggested that a key benefit was to enhance security (n=33) - primarily advanced technology was described as a tool which assists security officers and augments their capabilities.

'Technology can assist the human guard force operate effectively using the tools provided.'

(Supplier)

'Can complement the role of a guard.'

(Supplier)

'Tech should be seen as an aid to better physical security.'

(Contracted security operative)

'Mixture of human and technology combined will be more effective in prevention …'

(Buyer/Customer)

3.37 Similarly, the use of advanced technology in security measures was also seen as creating efficiency (n=26). It was suggested that it could streamline processes for basic/repetitive tasks and free up officer time to focus on aspects of work best suited to their skills, such as responding to incidents.

'Advanced technology enables security managers to streamline processes for repetitive tasks and enables basic jobs to become automated.'

(Buyer/Customer)

'Frees up time for Security Officers to conduct their business and takes the load of some of the more onerous aspects of their roles. It supplements but does not replace a physical presence.'

(Buyer/Customer)

'Replace mundane tasks.'

(Buyer/Customer)

3.38 The information provided by advanced technology was also cited as a key benefit (n=21). It was felt that the use of such technology in security measures increased the available data which could be analysed to inform the approach and provides evidence and a better reference point for an audit trail. Examples were given of how this information could also be useful beyond security to other aspects of business, for example by providing information on customer behaviour.

'Variety of reports, MIS data can help plan effective management in other areas of the business/organization too – it can help better shape future policies and strategies to respond to crimes and criminals.'

(In-house security operative)

'Clear audit trail, detailed reporting.'

(Supplier)

'Being able to measure what is done allowing security to "prove itself" to the organisation.'

(Supplier)

'Advanced data analysis leading to better risk identification and better decision making.'

(Buyer/Customer)

'Added value extras at no or low cost – people counting, dwell time, visual verification.'

(Supplier)

3.39 An improved response time was also cited as a benefit (n=20), particularly in terms of identifying threats so action can be taken but also the continuous accessibility of real-time data while responding to an incident.

'Reduced response time to threats.'

(In-house security operative)

'Access to real-time data brings possibility to respond to incidents/emergencies at the time those events occur and are in progress (Immediate distribution to stakeholders) …'

(Supplier)

3.40 Other benefits included the reduction of bias/error (n=16) associated with humans; more proactive detection of issues (n=15); integration with other systems such as cyber security and also other business systems (n=12); deterring offenders (n=10), improving accuracy (n=8); enabling compliance with procedures/requirements (n=8) and less dependence on manpower (n=6).

3.41 Benefits mentioned by very low numbers included the ability to provide 24/7 service (n=4), greater transparency (n=3), future proofing systems (n=3), flexibility (n=3), diversification of security roles (n=1), resilience (n=1), and increased employee confidence in security (n=1).

Drawbacks of using advanced technology in security

3.42 Respondents were asked what, in their view, are the key drawbacks of using advanced technology in physical security measures. In total, 156 respondents submitted an answer, however, as above, where respondents described more than one type of drawback, these were treated as a unique responses.

3.43 Despite cost savings being outlined as a key benefit, costs were also most commonly cited as a drawback (n=33). Specifically, that technology is expensive to procure, install (not just the cost of the equipment but also training staff and revising procedures) and maintain.

'Expensive.'

(Buyer/Customer)

'It requires maintenance which are overlooked in many cases.'

(In-house security operative)

'Initial costs will be higher (purchase, training, infrastructural adjustments) before costs steady.'

(Buyer/Customer)

3.44 Difficulties with implementation were also cited (n=16) such as reliance on other departments (such as IT) to provide reliable networks, the complexity of bringing staff up to speed with new approaches and procedures, the potential rigidity of systems – making it hard to customise it to a specific business; and having the necessary skills to adopt new systems and ensure they are effective.

> *'Reliance on networks that fail or drop out.'*
>
> *(Supplier)*
>
> *'Lack of process management for adopting change.'*
>
> *(Supplier)*

3.45 There was also concern about the potential changes resulting to workforce (n=15) particularly the implications of a loss of manpower and the importance of the human element, but also the greater competence and skills needed among officers to interact with technology; and further the need for involvement from more personnel (such as IT, HR, Compliance).

> *'Loss of manpower.'*
>
> *(Contracted security operative)*
>
> *'It can lead to a false impression that manpower is not needed to bolster physical security measures.'*
>
> *(Buyer/Customer)*
>
> *'The risk of the human factor (procedural matters) being "forgotten" with the introduction of intelligent systems.'*
>
> *(Other security expert)*
>
> *' … you are often relying on security staff who are sometimes out of their depth in how to use it. Measures only make sense if the staff are capable and trained in use and then the follow-up and fall back situation are well drilled.'*
>
> *(Other interested party)*

3.46 Concerns about vulnerabilities including failure in technology and the potential for systems to be hacked and for data breaches to occur was flagged (n=17), as was a lack of available training to use the product (n=12); the danger of over-reliance on equipment and software (n=12); and the potential that the system is not used to its full potential (n=12).

3.47 It was suggested that a drawback is that technology remains subject to human error (n=8), that it raises ethical issues (n=7) including the possibility that it could be misused and that its use creates negative connotations of suspicion and distrust. The relative complexity of systems was noted generally (n=7) and similarly, specifically, some flagged that end users struggle to use the systems (n=6).

3.48 Drawbacks mentioned by very low numbers included that the pace of advances in technology means systems soon become out-dated (n=5); the relative difficulty of establishing the cause of problems e.g. whether

it is the end user, the network, both (n=5); being sold poor or unsuitable products (n=5); the possibility that technology creates complacency (n=4), privacy concerns (n=4); that expectations are not met (n=4); and that offenders find a way to overcome it (n=3). One respondent for example cautioned that offenders do not have to be able to 'match' the sophistication of the technology used since in some circumstances they use speed and aggression to overcome technology e.g. ram raids, gas attacks on cash dispensers, destroying telecom/data networks.

Summary

3.49 The overall picture emerging from those taking part in the research is that the use of advanced technology within physical security measures is increasing and with it opportunities to improve physical security. While there was some indication that technology can replace security officers in respect of some tasks, a large majority of respondents felt it could never wholly replace people and indeed that people were crucial.

3.50 Views expressed on how offenders respond to security, suggested there is an impression that offenders: are not just out for an easy win and will work hard to get to what they want; are quick to respond to technological weaknesses; and typically overcome all security measures in time, no matter how sophisticated. The impression given is that there is a constant need for security to evolve and always to recognise that good security is only ever temporary.

3.51 Although a majority agreed, there was a comparatively muted response to the suggestion that advanced technology is more likely to deter offenders than traditional security measures; and similarly that it offers a greater return on investment than traditional security measures. This would suggest that generally speaking these are not primary drivers for its use and the key benefits may lie elsewhere. Indeed the benefits mentioned most often included cost, enhancing security provision, creating efficiencies and an improved response time, as well as increasing the amount of useful data to inform the approach to security.

3.52 There was some concern about potential weaknesses and limitations of advanced technology used in security measures, but this was moderate (typically falling close to 50%) rather than high. A large majority of respondents flagged belief that the Boards of most large companies do not have a good grasp of the threats posed by technology savvy criminals or of the weaknesses in their approach to security. The drawbacks mentioned most often included the relative expense of introducing and maintaining technology, the complexity of implementation, and the implications of a loss of manpower and the level of skills required to interact with technology.

3.53 It is ironic and important that some of the benefits provided by advances on security technology can also be drawbacks. It is developing fast and offering considerable scope but identifying which

technologies are best and keeping up to date remain inherent difficulties. Technologies can be cost effective, and often can be procured because of savings in manpower – and not just efficiencies – but the costs of change can be considerable, so too the resources needed to manage and maximise benefits. The next section adds depth to a discussion of these issues.

Section 4. Security Professionals in Their Own Words: Getting Realistic About Advanced Technologies

Introduction

4.1 This section is based on interviews with 21 security personnel, including suppliers and clients. The main purpose of the interviews was to explore in more depth some of the key issues that govern the use of advanced technologies and to present it using the interviewees' words; this is an insight into some of the key issues they deemed relevant. The context is set by discussing some of the benefits of implementing advanced measures that accrue and facilitate the making of a business case for their implementation. The chapter then considers why developments are not an unqualified good, and the difficulties of realising the full potential that technological advances offer. It moves on to consider the difficulties of preventing advanced technologies themselves. The chapter ends with a note on offenders and how they are perceived to be adapting to 'new security'.

The benefits and the key components of a business case

4.2 The business case for security technology improvements is there to be made, and one interviewee characterised it as *'easy'* to do so. This is perhaps an unsurprising conclusion from interviews with security sector personnel. That said some interesting points emerged.

4.3 During the interviews there were many examples of the benefits that can be accrued from advances in security technologies, just for example in improving operations by linking different technologies; facilitating the better capture of more diverse information to inform decision making and generating a speedier and more efficient response; and in being more reliable and less prone to error. We have quoted extensively here to emphasise the point:

> *Arrive at our office in* [city], *you arrive at the gate, ANPR recognises your car registration then an arrow directs you to your parking space, then as you get to the building a door opens because we have facial recognition, and then in reception your pass is waiting, you have not seen a security officer, that is where you can make progress.*
>
> *(Security supplier 4)*

> *We have a smart phone with an App, any sort of incidents within your areas can be reported, trip hazards, or an occurrence that happens while on patrol, say a beggar needs moving on, you can log it and send an email or text to whoever is affected, but it will also give a heatmap of*

areas and time for each event, and the AI can help you to develop work patterns and say you should patrol this area at a certain time. This handheld device has brought down liabilities with health and safety because there is more awareness of the issues, and they can respond quicker, it means they can get cheaper insurance.

(Security supplier 6)

We have invested in a head set that was about making people feel safer, they can communicate easier, and because of IP you can link technologies better, so there is no more security technologies sitting on their own in a silo, we want ones that run together. It identifies the speed people move around queues and headsets can communicate where staff need to be deployed.

(Security manager, client 8)

If I look at it with a software company lens – really it is the ability to capture data. Facial recognition, analytics in cameras and so on – the ability to capture. We've always had the data, but it has been buried somewhere – whether that be a paper report – whether it be on reams of videotape somewhere. It is really the ability to put that on your fingertips and show that to others.

(Security supplier 17)

As the technology develops it takes away the human error aspects. There is always the opportunity for a physical security officer to be put in a position to make a decision that isn't in line with corporate policy or strategy through duress. Technology doesn't suffer that pressure. Reliability – impartial reliability.

(Security manager, client 19)

4.4 That said, there was an important caveat to the clear enthusiasm for advancements in security technology, that is, security technology can never totally replace the need for security personnel. Some responses noted that this was always a challenge; while new technologies can improve security and save money, organisations do not always appreciate that in order for these to be effective staff with different and typically more advanced skillsets are needed:

In one site we are looking at upskilling and paying more for control room than officers on the ground because they are the brain of security. So we do need good people there.

(Security supplier 6)

I think businesses think you can do away with manpower, but look, it [technology] *can reduce manpower, but in the cost savings there you need to employ people with more skills and pay them more money, that needs to be part of it.*

(Security manager, client 11)

> *Clients expect the same level of service from technology alongside manpower. But someone in the building is more constant than a mobile response. So they need to understand they save money but the response can't be as immediate…Also,* [you need to ensure that] *the people that are monitoring are sufficiently equipped that there are enough of them especially when you are busy.*
>
> *(Security supplier 12)*

> *They may say, 'we used to have 10 guards, we want to go to 6, save X dollars and put in 42 cameras'. Maybe you can, but does it mean you need an operations centre? There are questions to ask.*
>
> *(Security supplier 17)*

> *It may reduce manpower at the site, but in doing that, you may have to up the numbers in the control room. But if lose 4 people at site A, you don't need 4 extra in the control room so there is a reduction. But you don't want an overflow of information and not enough people to deal with it all – you have to get that balance right.*
>
> *(Security manager, client 19)*

4.5 This last point is an important one, generating more and better information is one thing, ensuring that it is acted upon in an effective way is quite another. It will be recalled offenders felt they benefited from this gap in organisations. Moreover, there are limits to what new technologies can do; there are things that only people can do, such as offering personal support or treatment:

> *It still takes a human person to assess the response, people need to do that.*
>
> *(Security supplier 13)*

> *I ask* [the client]*, are you evacuating people, are you first responding? If so, then technology can speed up communications but it cannot respond to the individuals that need help.*
>
> *(Security supplier 14)*

4.6 For clients, technology provides the opportunity for more cost savings and a better service, and for suppliers – where it involves replacing, say, security personnel with technology – the almost inevitable loss of revenue but generally a greater profit margin. However, there were other key points here, and these were the recognition that meeting the needs of the client was good for business, as were the savings associated with the (considerable) costs of contract churn, and setting an example of good practice:

> *Your turnover is reduced and so are costs…you can make profit. If you had 10 buildings with 24/7* [coverage] *and now* [technology with] *two officers doing patrols, then you will make less money, but it is a marketplace where*

you need to reduce costs. So you have either to accept it or you can't bid.

(Security supplier 12)

We have two sites with 200 guards…and the country is saying if we reduce guards we will lose revenue, but with technology the profits can be the same…[we ask] *what is the right solution for the client?…We prefer the longer-term profit that comes with a client relationship. The longer we can have that client, the more we can make profits…doing the right thing for the client is better business.*

(Security supplier 14)

4.7 Approaches to profit making are, of course, dependent on many variables. One interviewee noted that his very large company was not dependent on making money from security; it could help other parts of the business to win contacts for broader Facilities Management offerings.

4.8 There was general agreement that the profit margin on technologies such as CCTV and access control is better than it is for security many types of personnel and especially security officers. One supplier posited that it was around 25%, whereas cleaning (sometimes purchased alongside security) was about two thirds of that, and guarding was much less, half, if that, and typically in single figures. So what are the components of a business case and the key requirement of establishing a return on investment (ROI)? Here interviewees noted that there was a strong need for a full understanding of all the benefits, not just to security but to the broader business. Many felt that this was unrecognised, and a far too narrow focus was adopted without thought for the very diverse ways that benefits can be realised by other departments.

To get a ROI for security on its own is difficult, so it is better to improve the customer journey, that is where we have a case; queue management, service points, how to improve the effectiveness of stores from an operating model, that analytic…What are the hard benefits and soft benefits? Key are, how much can we save, what costs can we offset, what does it do for our risk profile?…Then to the softer side, you have colleague welfare, improving the customer view…The last business case was around CCTV we had about 30 benefits, about how it will work in future. I declared the ones needed to get it across the line, so I don't put them all on the table…I may need to use some more down the line.

(Security manager, client 8)

> *while presenting we should not just present costs, but cost-benefit analysis – how these systems are going to benefit the business overall – what will they get out of that?*
>
> *(Security manager, client 18)*

> *you have to be able to demonstrate …a return on investment and a reduction in cost. Physical guarding goes on and is a continual cost. Technology is a capital cost written off over a number of years and then you start to become in profit.*
>
> *(Security manager, client 19)*

4.9 One interviewee underlined the importance of showing how savings can be used to improve security:

> *The way I would pitch it is I would say 'we can make a 10% saving and reinvest 6% in people', and they would be happy with that. That is the opportunity, enhancing benefits for the client and increasing our margin through technology. I would happily take out £100k and add £30k technology because the EBIT would be greater.'*
>
> *(Security supplier 2)*

4.10 A few interviewees noted that some organisations are reluctant to invest in advanced security technology and it merits a comment here. One interviewee noted that in some parts of the world there is a scepticism about technology. In some cases this is because there is a lot of regulation governing what can be used and how it can be deployed. In other cases there was a lot of faith placed in personnel, because there was a plentiful supply of inexpensive labour (especially compared to the perceived costs of technology) and it had become endemic in the ways businesses operated. One interviewee summarised the point this way:

> *The interesting challenge about that – in parts of the world where manpower is cheap, it is difficult to justify that. In the Middle East and Africa, labour costs are unbelievably low…So in some locations there is a reluctance to adopt it because they have already got manpower in the loop and don't see the benefit* [of technology].
>
> *(Security consultant 15)*

Why advancements in technology are not an unqualified good

4.11 Interviewees demonstrated how the adoption of advanced security technologies introduced a new and unanticipated set of issues (that is new security issues, including opportunities for theft) for organisations to deal with. For example:

In retail there has been some resistance, it can be seen as an aggressive tactic, some youngsters, say 15-25 [year olds] *who cause trouble are attempting to steal cameras, stopping the cameras from working.*

(Security supplier 4)

Door supervisors were asked to fill in forms on tablets, this was a challenge, putting shift work on an app, or digital platform rather than piece of paper. Small changes required a lot of learning.

(Security independent 5)

With this smart app we have had issues, when a client thinks a security officer is on his phone and therefore not working. Some clients see the mobile phone or hand held device as a distraction. But they are inputting not speaking.

(Security supplier 6)

The shop team becomes over reliant on it...rather than shop member saying don't bring alcohol in here they use the system (involving an announcement from a remote centre directly into the shop)*. It is slightly disruptive to the shop ambience.*

(Security manager, client 10)

4.12 This last quote underscores some of the inherent dangers in replacing people with technology in some cases. Three interviewees extended this point and raised the issue of technologies reducing human interaction and at the same time lessening the effect of security measures by failing to recognise the crucial role that people can do play. This is how they voiced their concerns:

For a long time my concern has been to keep the human presence, making use of advances is fine, but replacing people with AI, is dangerous. There needs to be a balance. In terms of new ideas, this creativity question is key, machines can't build relationships, they are not emotional.

(Security consultant 9)

Technology can't replace human intervention and it is not good to take human interaction out, it is a key part of living a quality life.

(Security supplier 13)

Clients are looking at technology as the silver bullet. Yes, good. But there is also the human side and it is a bit like remote working as there were cost savings but there is loneliness, isolation, lack of networking, good at first and then they feel isolated… feeling secure is a vital need… escorting, evacuation under emergency, responding to a specific need, can technology replace that? Humans can be seen on screens and that person can be 500 miles

> *OK, that might work. But we need to think…The industry has not done well in communicating the skills of people, and so we are easily replaced by a microchip. We have ourselves to blame because we have not shown how good they are … They are all saying cut, cut, cut, it is endemic, they don't value security, even if the corporate do and resist change they are also being side-lined by their corporate strategies to reduce cost.*
>
> *(Security supplier 14)*

Some difficulties in realising the benefits of advanced technology

4.13 A key issue that emerged from the interviews was that while advanced security had many benefits it could be challenging to realise them fully. For example:

> *Security teams need to think differently, where there is spending on advanced technology how much is being used? I would guess 30%, so what happens when those who have funded it find out that (say) only 50% of the systems' capability is being used? Then they will ask why have we spent so much?*
>
> *(Security manager, client 11)*

> [investments in advanced security technology] *may solve 50/60% of the problem but not the 40% which is very difficult/expensive and therefore doesn't get done.*
>
> *(Security consultant 15)*

4.14 When it comes to the ever-evolving world of technology, the scope for improvement and innovation is matched by misunderstanding and frustration when it comes to buying and using new security technologies. One interviewee conceded that some clients had been *'burnt before'* and were now less open to new innovations and ideas, or as will be shown, were perceived to be putting barriers in the way, whether that be completely new initiatives or refinements of current ones that could potentially realise additional benefits.

4.15 One client pointed to the difficulty of ensuring there was internal buy-in regarding what was being proposed. Many interviewees made the point that generating funding for security-related technology (or for anything else) inevitably involved justifying a ROI which for the most part was best achieved by showing how what was proposed for security impacted and benefited other parts of the business. Some client interviewees noted that their role was more than security providing them with an opportunity to interact and demonstrate their value more broadly:

> *I head a risk function, so more than just the silo of security. That gives me a visibility. This makes it easier for me to put on different hats dealing with different*

issues. We are retailer and sell, to look purely from security is one dimensional, we say we co-work and we can all benefit from collaborating so that is how we practice our mantra.

(Security manager, client 8)

4.16 Precisely because technology is helping to integrate security with other parts of the business. IT featured prominently in discussions about working with other departments and there was a positive mention of the role of procurement. For example:

We guys, as security guys are not fully qualified to assess those systems, what is required, even at a project stage – there are a lot of requirements that are not our strengths. A lot of coordination is required with IT and the information security department…I personally definitely see it as a positive. I do have an IT background so it is quite easy for me to collaborate but I have seen that it can be challenging as well – understanding jargons and language can be challenging for some people.

(Security manager, client 18)

So, in terms of a relationship with a procurement person this can be much better. Historically you only saw them when it came to renegotiation. So take the top social-media companies, procurement will be involved, and maybe even at monthly meeting and they play a part too, and they won't drive down the price and you can get over to them what you are doing better.

(Security supplier 1)

Some places it is still siloed. Others bring colleagues and come to a joint solution. In many cases the threats are similar but manifest differently…In the long run I think it is ultimately a good thing. You've got to go to the top of the hill to be able to coast down the other side. If you don't bring them in – you will eventually – if you bring them in later you may have already created vulnerabilities, so ultimately it is a good thing.

(Security supplier 17)

4.17 However, caution is required in interpreting this increased collaboration as an unqualified good. It was noted that the need to consult more broadly can distract security professionals from focussing on security specific requirements. Some noted that internal security departments had lost decision making power over security spend in some cases as a direct consequence of security technologies being part of a broader spend. For example:

Also, you are expected to do more than just security, Corporate Social Responsibility (CSR), environmental issues for the whole site.

(Security supplier 6)

For decision making on spend absolutely, they have lost the ability to veto corporate supply chain initiatives, they are influencers but not the decision maker. I would say of all big companies I can name, they don't hold the budgets.

(Security supplier 14)

4.18 Other interviewees underlined the importance of setting up the contract effectively in the first place:

If you built the case in advance, and you are rigorous and sensible, be realistic, then it is not a difficult task…The business case is key…If you want a security product there are plenty out there but a successful ROI needs much more…Can the products be linked, enhance user experience or take data to a new area?

(Security manager, client 8)

Again, it's selling the solution to people – in many aspects of business – why do we need to do it? Nothing may have happened. How do we identify that realisation? You have to be able to present that. It needs to be a business related justification…so you always relate it to a business solution if you can.

(Security manager, client 19)

4.19 Notwithstanding that interviewees frequently discussed successful projects, still there were many references to different types of skills gaps, amongst all parties at all levels in providing security. There was reference to consultants, end users and suppliers not fully understanding the causes of the problems they were trying to solve; specifying solutions they were comfortable with rather than what was best because of a limited ability to keep abreast of all that was available or because of a restriction of the types of products they were qualified or permitted to recommend; a lack of understanding of an organisation's ways of working which took many forms from its culture to the needs of the end user. In short, there was a lack of skills sets in order to realise the full potential of the security technologies available.

I think some [technologies] *are advancing so much that the skills gap is growing and skills are not keeping pace.*

(Security manager, client 11)

The vast majority of consultants have relationships and associations and with specific product manufacturers. So the solution offered is not solving the problem – it is making money. They make commercial relationships with manufacturers to fulfil that goal. So although integrators are often well intentioned – it's flavoured by the range of tools they have in the toolbox to fix the problem. That limits the amount of innovation – they don't want to re-train and adjust their business package – they want to re-use the investment they have already made in staff,

equipment, resources, so they are locked down a specific track, so it doesn't offer end users the best solution.

(Security consultant 15)

80% of the guys were not geared up to have the kind of knowledge where they could operate and manage these types of technologies, so that is the need of the hour – we need to upgrade ourselves.

(Security manager, client 18)

4.20 This latter point, that skills need to be upgraded alongside technology, was echoed in many of the conversations held with interviewees about this issue. One interviewee felt that the security sector had been, '*slow to react'* but that it was adapting adding that his own suppliers had moved from trying to sell him products to, '*listening to what I need as a business'.* Another client interviewee felt that the biggest problem he had faced in developing security technology – in this case to better protect against break-ins – was his own security department that, '*did not get it'.*

4.21 The dominant view was that technology may require fewer people, but to maximise the benefits of technology those that are engaged need to have more advanced technological skills. This is true of security personnel at all levels amongst both clients and providers. For example, security officers may be better equipped but they need to learn, use and be able to assimilate more information in order to make better judgments as a consequence. Senior managers, likewise, need to keep abreast of the latest developments and need to be able to understand points where barriers may occur and be able to respond to them effectively. Keeping and developing existing staff, recruiting new people with the right skills and integrating them, and then keeping them, were all noted as a challenge.

4.22 Interviewees also felt that a lack of skills was compounded by the ways in which organisation managed purchasing and implementation:

There is a fundamental problem in the way some contracts are set up – particularly new-build projects – quite often it is a design team that start a project – audio visual consultants – they design an integrated solution – identifying synergies between systems incorporating various services, as they should. But when the project goes to execution, the main contractor has to find contractors that can execute it. So they get a physical security contractor and an IT contractor, but not one company that can do both, so at execution, it is divided up and goes to different companies – they have a different SLA, different warranty period, so by the time the site is handed to the end user, they have a mishmash of different contracts that can't be pulled apart – they have to live with that so they are not in fact integrated. So there

are fundamental ways the contract is won that makes it difficult.

(Security consultant 15)

'The communication between the estate director and consultant at the time was reasonable, but once cameras were put in problems started to occur. Then they are trying to put Christmas lights up and all that, which breaks the whole system, in different ways, including the cameras not being able to see, the supplier and the installation teams are caught out and then questions get asked like, 'why don't you know you can't you move cameras', now that was simple, but major. The communication was faulty, they were not saying that at Christmas it will be different and they had not discussed this with the engineers.'

(Security supplier 1)

4.23 One interviewee related a problem faced in getting clients to accept improvements and new technological innovations because clients are placing strict procedures in place for any products proposed for their systems:

Innovations or solutions are delayed because of internal protocols, so far we have none back as fully signed off. None. They want innovation and then they do all these tests…[or] *then the clients don't really know how to test it, almost a ticking a box and then I sense they don't have the expertise or balls to make a decision to say 'good to go'. There is naivety at local level at who has responsibilities for what element. Do these internal customers really understand the risks? Or are they just responding to a programme? Some are really not a problem but we still need to jump through 330,00 hurdles.*

(Security supplier 14)

4.24 Many interviewees admitted that one of the biggest difficulties was keeping abreast of developments. Interviewees pointed to industry publications, conferences, talks and trade shows, peer groups, suppliers/clients/consultants, rivals, partners, colleagues, as some of the key ways that they tried to keep up-to-date, but it was a challenge:

I attend meetings and I have chats with my peers, somebody who has my role will say it is virtually impossible to keep up-to-speed, you need someone focussed on it.

(Security manager, client 11)

I do go to IFSEC, I know people, speak to peers, I get stuff in my inbox, and it is not rocket science you don't need to be a blinking astrophysicist to know what is coming forward, we have good consultants, the company has engaged good people, got people properly hooked in.

(Security manager, client 20)

4.25 Suppliers were sometimes seen to oversell or promise too much, and clients to be unrealistic about what technologies could do. Once again, (and a theme echoed throughout the whole research) enhanced technology was always viewed as increasing demands on some people – it is not a complete replacement, and indeed may require more skills:

> *You must have the right people using the technology and knowing what it is for. I have seen this, they have not had the right training, not shown what the use is, and basically it just does not get used and they start to think we are paying for rubbish. You must show the benefits.*
>
> *(Security supplier 6)*

4.26 A different difficulty, but also stemming from the lack of knowledge, was a concern that security technology potentials were not being fully realised because of concerns about privacy and data protection. There were two key points made here. On the one hand, that systems were being deployed and used that either did, or were close to, breeching privacy without sufficient protection by careless or incompetent companies. Some had encountered resistance from staff - concerned that they were being unfairly tracked, watched or otherwise monitored. Then on the other hand, the great potential of different technologies were being undermined by a lack of understanding about the proper controls that could be implemented to support its use. For example:

> *A lot in the press about facial recognition, police, manufacturers, or anyone* [who] *is using this needs to be a lot clearer about the controls around its use. They need to let the public know what can be done with the cameras, what the benefits are and what controls on privacy there are, there is no education out there…We are hoovering up information and there must be controls to restrict access and we must ensure there is a governance process in who can and how they access it for security, and people need to know about that.*
>
> *(Security manager, client 11)*

> *Expectations of what it will do and how it will do it. What it will deliver…The other point to that would be being ready for future vulnerabilities – being able to be current enough to avoid future issues.*
>
> *(Security supplier, 17)*

4.27 Sometimes the problem was not a lack of knowledge, it was more that some clients were unwilling to deploy advanced technologies. This was sometimes because they could not see the benefits, and/or were unable to do so typically because they had not the funds or strategy to support engagement with security technology. This is of course inevitable. One interviewee felt that problems were especially acute for clients who were '*not security focussed*', and another noted that where they were dealing with clients without security expertise in-house it complicated the potential to sell the benefits of new security. Some were put off by what they saw as real difficulties in integrating

technologies. This was a big point, that although technology integration was much easier than it once was there were still perceived to be limits and one always had to be mindful of these. Some felt that the security sector was behind the IT sector in being able to fulfil this potential:

> *It can take time to convince (clients) to allow us to collectively analyse and share information. Some embrace it more and some say, 'I can't see the point, not a lot goes on' and so on. A lot of the limitation is not wanting to embrace it…There are frustrations when systems are not flexible enough to do what you want it to do. There is a balance: what you can do, costs come into this. There is more technical flexibility, but still not 100%, so you do have to adapt to the technology in play and also to costs.*
>
> *(Security supplier 12)*

> *The biggest issue at the moment is that nearly everything in the world is a computer connected to a network. Physical security has still not caught up with the technical skills required to deploy computer systems in a secure and sustainable manner. Even in large-scale schemes with 1000s of cameras, it is rare to have the internal skills to design and install to the same standard you would see within the IT industry.*
>
> *(Security consultant 15)*

4.28 It is important to stress that one of the barriers to the implementation of advanced technologies is the need to work with systems designed for other purposes and/or those that are old and out of date:

> *If components are not designed to interface with other technologies they can get frustrated at things not being seamless as they hoped. There is still a way to go and it is getting better…Also we have to use platforms as flexible as possible.*
>
> *(Security supplier 12)*

4.29 Finally, and unsurprisingly, one of the biggest obstacles to realising the benefits of advanced technologies was their cost, not least when the benefits were not proven or tangible; the problem not sufficiently defined; and/or the effectiveness not sufficiently proven:

> *We can't get money for it…If you have a significant event then you spend money. What we suffer here is a lack of a serious incident.*
>
> *(Security manager, client 3)*

> *The stumbling block is the size of wallet. Some are expensive and untested so it is difficult to get a ROI.*
>
> *(Security manager, client 8)*

Do advanced technologies pose a threat?

4.30 Some of the interviewees were not concerned about protecting their systems, never because it was deemed unimportant, but typically because as far as their responsibilities went, they felt they were following due diligence and good practice. It was noted that the latest advanced security technologies often offered the same types of threats, for example from hackers, that already existed and were being responded to.

4.31 That said, it was recognised that in reality all technological systems were always open to being hacked, or misled, by well orchestrated attacks from criminals. In one conference discussion, the potential for social media to be used to fool systems into believing an incident was taking place (to distract attention and resources) was discussed. The key conclusion of the ensuing discussion was that ensuring the veracity and integrity of intelligence sources was as important as guarding against all other types of threats.

4.32 In discussion, there were four overlapping areas that were presented as offering key threats in this area. The first featured the threats posed by some foreign governments. Part of the concern here was that the threat is unknown:

> *You have companies in industry that have ulterior motives, some are state owned/funded – collecting information for purposes that you may or may not agree with…There is a mistrust of States and how they are using the information…This is going to become more and more important.*
>
> *(Security supplier 16)*

4.33 The second related to installing security technologies on a poor IT infrastructure. Some typical comments here included:

> *How do you maintain security on a network that may have weaknesses? Security can add a lot but it is a headache as to how to bring CCTV up to the required security, how to bring each one up-to-date. We have thousands of cameras, how do you do that? It brings on a whole new world of thinking...the most expensive resource we have is IT.*
>
> *(Security manager, client 8)*

> *You are limited by the internet. If you are relying on a service that moves data you need to ensure the components has redundancies so that if something goes down you have another solution. Also, you are only as good as the weakest link, nothing new, but you don't need to be aligned.*
>
> *(Security supplier, 12)*

4.34 The third focussed on the inadequacy, for various reasons, of the security products or technologies themselves. Every new security technology has the potential to create vulnerabilities alongside the new possibilities it provides, and the opportunities for good *and* bad in each was described by one interviewee as, *'mind blowing'*. A variety of explanations were offered, sometimes because manufacturers design in problems or were otherwise negligent, installers can be compromised, or products can be purchased carelessly; procurers may fail to understand the implications of cheaper alternatives:

> *As an installer we can take the precaution of buying branded products which have a reputation, we buy one for £300 and someone buying a similar spec will buy for £30, doing a similar job but does not come with all the protection and so it is price-led. They expect us to do due diligence but ultimately we are not embedded software engineers…Who knows what is going on?*
>
> *(Security supplier 13)*

> *Kit going in that is not ready for market – it may sound good, but from a wider perspective it is not right for the market…quite often procurement come in and replace like-for-like off a specification sheet. They are not doing their homework with providers. You have to be careful with an IoT device…Hackers are becoming increasingly aware…drug dealers and fraudsters are manipulating information to make money selling information quickly on the dark web…Some systems at schools and hospitals are put in by electricians who don't change the default username and password. That is a huge concern.*
>
> *(Security supplier 16)*

4.35 A final element, often mentioned was that security systems can be undermined by human factors and a specific point here is that people can and do sometimes behave maliciously:

> *There is a human factor, so if you had an operator wanting to be malicious and there was nothing in their security screening then they could get information and leave for their shift and pass things on.*
>
> *(Security supplier 12)*

Artificial intelligence and machine learning

4.36 During the interviews we asked about whether and how emerging technologies were being considered and managed, including the security threat they might pose. A case-in-point is AI and machine learning. This area was seen to be one that was becoming important on the margins rather than being a current major influence, although there were few who did not think this would be a higher priority going forward. It was recognised that it had the potential to impact many areas of security, some summarised their interest as follows:

We are looking at drones. It is coming up in iconic buildings and two have spoken to me about drones and counter drones and they are worried, I mean, they could have weapons. We spoke to a drone company and they were doing drone patrols inside the building…they…have cameras and speakers and they have a help button linked to a control room, the camera is 360, it has AI…we…use robots instead of humans for certain roles and they are a bit of a novelty.

(Security supplier 6)

We are developing facial recognition and that has AI built into it. It hones itself.

(Security manager, client 10)

Not massively, there are aspects of incident reporting, heat mapping and looking at situations on bigger scale that will impact the security of a building and AI looks at the circumstances and do this or that, but it is hit and miss at best.

(Security supplier 12)

We have some robots on tests, second generation. We are investing into to a point. But there is not the demand from the clients…We are looking at facial recognition… but we not yet fully there. Systems that predict are not there yet. We have engaged with those running systems and how they can predict crime and the next level of hostilities but it is not at a point sufficiently accurate.

(Security supplier 14)

4.37 There were also concerns here that the many technologies that include AI and machine learning are open to the same weaknesses. For example:

What I have picked up is a debate about what information are you putting into AI, is it biased, say racial or on gender against people? You need computer scientists to test this…the danger of…vulnerabilities in the coding. So you need a cyber secure technology, they are not necessarily secure and have in built design issues which is an age old problem of all security and all systems. Then the political issue about whether states are putting in insecure coding via the back door access. Some think countries are spying on us and doing it. Manufacturing is also an issue, why are they not designing it with security inbuilt from the go. The costs outweigh the need for security.

(Security consultant 9)

4.38 There is no doubt that AI will pose huge ethical problems which are still evolving. While these technologies present opportunities it does not mean that people will be replaced:

Interesting question – traditionally – its one of the de-motivations for security operatives – they are looking ahead and seeing their job role disappearing – see AI and think it means it will take over their job. There is an element of truth to that. The capabilities of deep learning while not completely stable yet, it is a matter of time before you can do predictive rather than actionable incident management. For example, [organisation name] *does AI based analytics and they were able to detect a leak in an air-con system quicker than the air-con system detected it. The camera was able to differentiate between the norm. All well and good but you still need someone to action that. People are still needed – someone still needs to go do something about it.*

(Security supplier 16)

4.39 There is one other point here that needs to be emphasised and presents another area where technology development needs to catch up with operations. During interviews a number of respondents noted that a key aim of technology was to improve practice and that this aspect was still evolving. For sure it had to be cost effective, be compatible with other technologies and align with strategy, but it also has to offer practical benefits. Two interviewees summarised their experience:

But as an aside, in our world we did a lot of work on people's behaviour in store, identifying the differences in behaviours between those buying and those committing theft and we did that via machine learning, and got some good results from an emerging technology. But you [an offender] can be in and out in 50 seconds and what do I want the interaction to be, and am I creating violence, so what are you going to do with the information when you have got it? The people selling were great, but they were not saying how I could deploy it and that is where they failed in my view.

(Security manager, client 8)

They need to relate their technologies to how we work, how do they relate to our environments? And then we can picture how that can work. But this is not even on their radar.

(Security supplier 14)

A note on the threat posed by offenders

4.40 There was widespread acknowledgement that any good response in using advanced technologies was only ever good for a limited period:

Heat maps show theft every Thursday at 3pm, the kids are stealing and you can set your work schedule to cover

that, but once offenders are aware that you have 3pm covered they will do it at 4.30 instead.

(Security supplier 6)

You have a step forward in technology that gives you the upper hand but they quickly adapt and they catch up and then you look for the next step forward to counter the impact of them getting around it.

(Security supplier 12)

It's a constantly moving target and it is never going to change. There is always going to be a way around it. Something we do – we were asked by a large financial – for cryptographic storage of credentials on board the camera – so you can't plug in to it and jump on the network. That, at the moment, is secure. But it is only a matter of time, before something comes out that catches up with it.

(Security supplier 16)

4.41 Moreover, the point was made that however good the technology it always depended on a good response, and interestingly, many felt that this was a key limitation:

We do patrols…they caught some pickpockets, there were two of them caught in a shop, with evidence, the victim was there giving evidence, but there was no response from police after 5 hours, so they were let go. So now they will tell others that you can do what you like. Technology is great, but ultimately if you don't get a response from the police then it can't work. I did think why didn't they just march them down the police station but that has dangers of course.

(Security supplier 6)

I think it is becoming complicated for them but there are people out there that spend their life doing it – people can hack in to NASA. Technology can certainly deter people at different levels. You can have the ability to detect early but if you have a bad response time to that detection – what do you achieve? It just means you know they've been there but you would have been able to see all your laptops were missing anyway. It's got to work and speed up detection of a violation, but you have to match that with a timely response to catch them in the act. People talk about perimeter defences – put a wire on top. But a reasonably fit person can get over a 2-metre fence in 17 seconds. That will set off an alarm but you still have to catch them before they get anything.

(Security supplier 16)

> *They may have tested it – rattled it to see how quick the response is – if no one responds they may think no body is monitoring - I can get over and get closer.*
>
> *(Security manager, client 19)*

4.42 One interviewee made the point that what technology will enable is the opportunity to prepare a more convincing case for prosecution, with more and better evidence to be presented in a form that the police can use with minimal work:

> *Because we are providing case level document packs with all the images, everything they need…Offenders are thinking twice, so we prosecute again and again so they avoid us* [it was] *slow going to get police on board and now this is being welcomed.*
>
> *(Security manager, client 8)*

Summary

4.43 This section has reinforced the points raised earlier. There are many benefits to advanced technologies, when done well. And that is the key. Advances in technology are a route to better security and not an end in itself. There is a skill set to making the business case, not just with technological knowhow but also in relating that to different business audiences, while recognising that while staff numbers may be reduced those who remain typically need to be better equipped.

4.44 Some drawbacks were examined, not just costs and the technical difficulties of integration, important though they are. A range of practical problems and the challenge of linking what is possible to what can be achieved; the implicit dangers of an over reliance on technology; managing a range of potential threats to the technologies themselves; and maintaining vigilant and avoiding complacency as offenders work out a way of circumventing what is in their way, as they always do (helped by a reducing police commitment to business crime). The final section summarises these and other key findings from the research.

Section 5. The Findings in Perspective

5.1 This report set out to assess the use of advanced security measures in physical security, a somewhat under-researched topic. Conference talks, in abundance, present advances in technology as an unqualified good. This work sought to evaluate this perspective within the context of their real-world application.

5.2 The findings suggest that there have been notable positive advances in the ways security technologies have developed; the majority of security professionals agreed that such measures were more common and most pointed to a range of advantages that can be accrued. The key reasons why advancement has taken place include the creative commitment of security professionals, as well as the work of security manufacturers/suppliers.

5.3 Moreover, some offenders noted that the more difficult the target (both in reality and where that was the perception) the less likely it was a good choice to victimise and advances in technology can pose risks, not least in adding unpredictability and rendering a target unworthy. There was a general view that acquisitive offences, at least those conducted in person, were becoming riskier for offenders.

5.4 On the other hand, the interviews with offenders documented how security devices, or an increasing reliance on technology had created new opportunities for offending, for example, those offenders who employed GPS trackers to track security vehicles, or those who adapted their offending behaviour to go unnoticed by cameras. Additionally, the same interviewees noted that the development of physical security had driven crime online, where security and prevention was far less developed, there were more opportunities, and less perceived risk of being caught.

5.5 Strikingly, while offenders recognised the threat posed by technologies, especially ones with developments they are unaware of or could not predict, it was humans and the increased risk of immediate apprehension their presence posed that offenders most. It is perhaps ironic that human factors were also viewed as the mostly likely vulnerability of advanced security systems.

5.6 There were other findings suggesting technology has not changed some things. For example, advances have not solved the problem that Boards are too often disengaged, at least this is the case when physical security measures are the focus; and there is still a focus on buying on cost. Many felt there was a lack of evidence that advanced measures work effectively; they are developing rapidly, and evaluations have not always kept up.

5.7 Many of the reported benefits of advanced security were seen by others as drawbacks. For example, advances can save costs but can

be expensive to buy, maintain and keep up to date; they provide an opportunity to engage with the whole business, but that is not always welcomed and can sometimes be resisted by other departments (IT was frequently mentioned); they can reduce some errors (automation for example improves the reliability of decision-making) but can create the scope for more diverse human errors; they can reduce administrative burdens but can be difficult to use and their complexity can render them difficult to procure, integrate, manage and maintain; they can reduce dependence on people but can send out a message that people are less important when they are not, in fact better prepared personnel are often required in consequence to their implementation; they provide more and better information but this has to be assimilated and built into operations, which can be challenging; they help to safeguard legal privacy requirements but they generate privacy issues and when breached create additional legal, reputational and loss consequences, and it is still tricky to authenticate authorised users; while measures can improve security so too they contain inherent weaknesses which are still being understood (IoT being a high profile example); there is more of an evidence base to provide better security but realising the potential of what is there is at least as demanding.

5.8 Interviews with security professionals largely reinforced these points. They highlighted some of the many advantages of technology, and prime amongst them was the potential for efficiencies and reduced manpower and costs. The positive here is that, generally speaking, the clients benefit from reduced expenditure and the suppliers can often make just as much profit if not more (on a lower turnover) and crucially act in a way that is consistent with good practice and help reduce contract churn (itself a contribution to profits). But there are two important caveats. The first is that the business case often depends on demonstrating benefits to the whole business and not just security. That requires a different skill set, not just technological expertise, but also the ability to understand different business or industry requirements and speak the language of business. The second is that there are limits to the ways in which investing in security technology can reduce staffing, with most saying that it will generally involve an increase in more skilled staffing, representing, of course, a cost increase.

5.9 The rapid development of technology was also viewed as a barrier to its successful integration. Keeping up-to-date, having realistic expectations, having the right knowledge base and skills-sets (amongst all parties and at all levels), understanding the broader relationship between security technologies and other technologies and its broader relationship to the business, all played their part in creating a barrier to successful implementation. Costs are always important, not least when the benefits are not always tangible, and many technologies remain to be proven in the harsh realities of the commercial environment. Indeed, it is a striking finding that a range of practical problems were evidenced

(even amongst this relatively small sample) that highlight the need to link the technologies with the requirements of practice. Additionally, some interviewees were concerned that an over-reliance on technology generally as well as security technologies specifically might be damaging if at some point it led to undermining/replacing human interaction.

5.10 While many felt that the potential threats to security that security technologies posed were being managed effectively, four overlapping key concerns were raised. That technologies can be undermined by malicious governments/companies; that good technologies can be installed on poor infrastructure and create new vulnerabilities; that technologies themselves contain inherent security weaknesses; and that some corrupt people undermine security.

5.11 With new developments, such as AI, two distinct messages emerged. The first was that many security professionals are not fully engaging with the potential here, not yet anyway. There is always the danger they will be left behind, not least as other areas of the business do so. In a different way, if such a trend is established, it will likely play to the benefit of Chief Information Security Officers (CISO) and the detriment of Chief Security Officers (CSO). Second, and somewhat countering the first point here, there is some optimism that with AI there may be a marked improvement in security capability, albeit that many of the same concerns discussed above apply here too. As one interviewee summarised:

> *With any technology, and I have fallen foul of this, there are always risks and I have yet to see a technology that is ground-breaking not have risks. The question is, 'where are the risks?' and then 'have we the right controls for those risks'?*
>
> *(Security manager, client 11)*

5.12 Interviewees did not underestimate the ability of offenders to innovate, and that any good response was only ever temporary. Many here noted also that another limit of technology was raised in talking about offenders, that no matter how good it was at identifying and enabling capture of offenders it was undermined if the response was lacking. Where security personnel are being reduced this needs to be heeded. Moreover, current restraints on police resources generally and the low priority of providing a response to business crime specifically serve as a reminder that technologies good at catching offenders don't operate in a vacuum.

5.13 Perhaps what was most clear - and another issue which remains prevalent, albeit an historic concern - is that while good security has always been dependent on having knowledgeable and effective individuals and companies, this is *even more important* today. The findings underline that there is a specific skill-set that correlates with effective modern security provision. The consequences and the

opportunities for getting it wrong are greater, and so too are the opportunities for offering more and better security.

Appendix 1 - Methodology and Sample

The approach

The study involved a review of existing literature on offender-based research; new and emerging security measures; and some of the key advances impacting the industry. These elements were used to identify key issues and themes to explore with those in the security sector and offenders.

The review of the literature was followed by three main approaches: 1) an online survey on security professional views of new and emergency technology advances in the sector, 2) extensive discussions including semi-structured interviews with a range of security professionals to gain a more in-depth understanding of the topic, and 3) interviews with offenders on the topics.

Survey

The survey addressed the key areas to determine how security measures are evolving and perspectives on the broader threat landscape. The sample was, self-recruited and clearly those with an interest in the topic were most likely to respond. While no claims are made that the survey is representative of the security industry as a whole, responses were received from a range of roles, sectors and countries. 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; security press; 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: ADS; ASIS (UK Chapter); ASIS International; Security Institute (SyI); British Security Industry Association (BSIA); IFSEC Global; Infologue; NSI; Professional Security Magazine; ProSecureNewsOnline; Risk UK; SIA; SyI; National Council for Crime Prevention (Sweden); Underwriters Security Council.

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 survey ran from 22nd February to 22nd March 2019.

A total of 225 replies were received although not every respondent completed every question in the survey. The data was analysed using SPSS. The data are categorical; therefore, it is not possible to assess the normality of data. It is important that this is borne in mind.

One-to-one interviews: Security Professional

The approach in this work was to identify a wide range of individuals to help understand which how technology has changed the security landscape. We informally and formally engaged a wide range of in conversation about the

issues covered in this report. This included at conference and trade shows, at meetings of security personnel, over professional dinners and other meetings and at different networking events. We contacted specific people by word-of-mouth and they sometimes referred us to others. We drew upon personal contacts and their networks; and some individuals who volunteered to offer more details after taking part in the survey.

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. 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.

We formally interviewed 21 professionals.

One-to-one interviews: Offenders

Due to the nature of the research, exploratory methodology was required in order to recruit participants willing to talk about their involvement in crime. Firstly, researchers exploited pre-existing relationships with potential participants. In addition, targeted advertising was used on a variety of online and offline platforms identified through research as potentially relevant. Finally, open source research was carried out in order to identify potential participants and contact them in relation to the interviews. It is important to note that during open source research techniques, strict procedures were maintained to ensure that no information was disclosed about our knowledge of the participants involvement in crime until the identity of the person had been confirmed and details of Perpetuity Research had been provided.

In order to improve the likelihood of participation and disclosure, the research team supported potential participants to employ methods with which they could remain anonymous to the members of the research team, should they desire. This included, for example, assistance on how to hide their identity from the researchers and how to receive payment without providing bank numbers. Additionally, flexibility was provided by the research team in order to facilitate the interviews, e.g. face-to-face or telephone interviews, or payment through various methods.

When sufficient interest in participation had been generated a sampling strategy was employed to attempt to generate a sample with a wide range of experiences. This was developed through open resource techniques concerning the nature of crimes though limited by the experience of the pool of participants. Additionally, attempts were made to interview a demographically diverse group and those with diverse motivations for the crime.

All participants were informed of the purpose of the study, and that personal information would not be recorded or used. Each participant was

recompensed for participating. Prior to interview each participant was screened to ensure criteria for interview were reached. At this point a research interview was organised and payment discussed. At interview, each participant was provided with consent information, given an opportunity to discuss consent and were required to provide verbal consent prior to commencing interview.

Similar to the interviews with security professionals, the interviews lasted thirty to sixty minutes and semi-structured interview schedules were used. We formally interviewed 15 offenders.

Appendix 2 – Additional Data Tables

Table 2: Main sectors that respondents' organisations are operational in (n=225)

Country	N	%
Retail	70	31.1
Public Admin, Other Services, Government	68	30.2
Property	51	22.7
Transport	49	21.8
Education	49	21.8
Health	48	21.3
Finance	47	20.9
Leisure & the Night Time Economy	45	20
Manufacturing	42	18.7
Other	40	17.8
Production	39	17.3
Energy	37	16.4
ICT	27	12
Mining, Quarrying & Utilities	25	11.1
Hotel & Catering	24	10.7
Post & Telecommunications	22	9.8
Wholesale	20	8.9
Motor Trades	17	7.6
Agriculture	6	2.7

Table 3: Country where the respondent's organisation is based (n=219)

Country	N	%
UK	140	63.9
USA	18	8.2
Netherlands	8	3.7
Australia	5	2.3
Ireland	4	1.8
Germany	3	1.4
India	3	1.4

Norway	3	1.4
Austria	2	0.9
Finland	2	0.9
France	2	0.9
Nigeria	2	0.9
Slovenia	2	0.9
Somalia	2	0.9
South Africa	2	0.9
Azerbaijan	1	0.5
Blegium	1	0.5
China	1	0.5
Costa Rica	1	0.5
Cote D'Ivoire	1	0.5
Denmark	1	0.5
Egypt	1	0.5
Guyana	1	0.5
Italy	1	0.5
Kenya	1	0.5
Maldives	1	0.5
Pakistan	1	0.5
Qatar	1	0.5
Romania	1	0.5
Serbia	1	0.5
Spain	1	0.5
Sweden	1	0.5
Switzerland	1	0.5
Thailand	1	0.5
United Arab Emirates	1	0.5

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 17 years 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 focused, for example, on police views on private security; tackling cyber crime – the role of private security; the broader benefits of security; aspiring to excellence; 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/

About the Authors

Professor Martin Gill

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 an honorary Chair at the University of Leicester. 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'. 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 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 and 2016 he was nominated and shortlisted for the Imbert Prize at the Association of Security Consultants and in the latter he won. In 2016 ASIS International awarded him a Presidential Order of Merit for distinguished service. In annual IFSEC listings he is regularly recorded as one of the world's most influential fire and security expert. In 2016 he was entered onto the Register of Chartered Security Professionals. Martin is the Founder of the Outstanding Security Performance Awards (the OSPAs) and Tackling Economic Crime Awards (the TECAs).

Charlotte Howell

Charlotte Howell joined Perpetuity in January 2009, and is currently the Research Manager – responsible for managing the delivery of research contracts, and our team of research staff. She also managed the Secured Environments scheme run by Perpetuity Research on behalf of Police CPI. Charlotte is an accomplished project manager with experience of working with a range of clients including businesses, associations, police forces, government organisations and charities. Charlotte's knowledge and experience spans the range of our areas of expertise – including crime prevention and community safety, security research, and the social aspects of health research. Charlotte is also actively involved in delivering fieldwork and has consulted with a range of individuals, including stakeholders (such as individuals from the police, local authorities, service commissioners and staff), offenders (both in prison and in the community) and clients accessing services (such as drug and alcohol treatment services, domestic abuse services and support services for sex workers). Charlotte is adept at quantitative analysis

and has a wealth of experience analysing survey responses, client data and performance/outcomes data.

Prior to working for Perpetuity, Charlotte graduated from the University of the West of England with a first class LLB (Hons) in Law. Following this she received an MSc in Criminology from the University of Leicester. 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.

Caitlyn McGeer

Caitlyn works as a Researcher, having joined Perpetuity Research after earning an MSc in Criminology and Criminal Justice from the University of Oxford with distinction. During her MSc, Caitlyn focused on criminal justice monitoring and evaluation protocol, cultivating an expertise in quantitative platforms such as SPSS and GIS. Caitlyn is equally skilled in qualitative methodology: interview, ethnographic, and visual methods. Caitlyn is currently completing a DPhil in Criminology at the University of Oxford.

Caitlyn has extensive research experience in both domestic and international projects, specifically focusing on facilitating strategic public sector development and the establishment of the rule of law. Beyond academia, her professional background has centred on public-sector communications, risk management, and project development, coupled with advocacy and campaigning capacities. She is a communications specialist and an intuitive project manager.

Caitlyn has worked with community development initiatives in Ecuador, Ghana, and Guatemala.

Josephine Ramm

Josephine is a highly adaptable social researcher with expertise in both qualitative and quantitative research methods. During her career she has conducted research on behalf of a diverse range of organisations including the Department of Health, Youth Justice Board, Alcohol Education Research Council, fpa (formerly Family Planning Association) and various private clients including national financial institutions and prominent academics. Josephine holds a BSc in Psychology from the University of Exeter, an MSc in Health Psychology from the University of Sussex. Josephine has extensive research experience in recruiting and working with offenders.

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

