Covid-19 and the implications for the security sector: what happened and what has been and is being learned?

Security Research Initiative (SRI)

Professor Martin Gill
Charlotte Howell

July 2021

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

Copyright

Acknowledgements

We would like to thank everyone who has assisted us with our research. This work has been possible because of the ongoing support of our members and because the security sector has engaged with us. The members of the Security Research Initiative who sponsor the research deserve a very special mention. They not only sponsor, but their representatives also provide and share their experiences. They are: Steven Kenny (Axis Communications), Eddie Ingram (Bidvest Noonan), Mick Tabori and Joachim Ritter (Interr), Terry Hanley (Interserve), Clint Reid (M&S), Barrie Millett and Jason Towse (Mitie), Steven Gardner (OCS), Richard Stanley and Rich Stevens (PwC), Imogen Hayat and Tony Holyland (SIA), Simon Pears and Jane Farrell (Sodexo). 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. ADS (especially Jon Gray), ASIS (especially Rich Stevens), the BSIA (especially Mike Reddington and Andrew Cooper); the Security Institute (especially Rick Mounfield and Di Thomas); and The SASIG (especially Martin Smith and Danny King); they are valuable advocates of the Security Research Initiative. So too our longstanding enthusiasts from security media: Roy Cooper and Mark Rowe (Professional Security Magazine), Brian Sims (Security Matters) and Byron Logue (Infologue).

We would also like to thank those who supported the research by promoting the survey among their networks including Mike Hurst (IFPO), Chuck Andrews (Friends of Chuck), James Moore (IFSEC Global), Richard Jenkins and Dianne Gettinby (NSI). We would also like to thank all of those who took an interest in the topic and promoted the survey among their individual networks.

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

We would like to thank David Dickinson for insightful comments on a draft of the report.

Finally, thanks to our colleagues: Janice Goldstraw-White for proof reading the report; and Hannah Miller and Claire Tankard for administrative assistance.

SRI Members

Executive Summary

Recognising the significant issues faced within physical security due to the Covid-19 pandemic, the aim of the research was to understand the challenges, the successes and failings. It is based on the views of those involved in the provision of security (buyers and sellers and operatives) collected via an online survey and through one to one interviews.

Value

- Respondents felt that security may be more valued post pandemic than prior and that some types of security professionals had gained more status (cyber security professionals the most).
- However, physical security has not necessarily emerged in a better position compared to other types of professionals. A slim majority thought that other functions (such as risk management, health & safety, crisis management and cyber security) had a higher status than security prior to the pandemic. However this majority increased, with respondents increasingly likely to believe that post pandemic other functions would have a higher status than physical security. The biggest increase was seen for business continuity (rising by 21 percentage points); followed by crisis management (rising by 16 percentage points); risk management (rising by 15 percentage points); health & safety (rising by 13 percentage points); and finally cyber security (rising by 12 percentage points).

Performance

- 83% of survey respondents felt that overall security had performed well in the crisis, especially those in roles designated ‘essential’.
- 69% felt that generally speaking security had performed *better or much better* than other functions/departments. Further analysis showed that contracted security operatives less commonly held this view than those in other roles.
- The main reasons offered related to being versatile, flexible and working in trying conditions when most other workers did not have to do so.
- Those who had the opposite view argued that security roles had been lost; that the role of security officers had been reduced to that of ‘doormen’ required to enforce requirements but lacking the power to do so effectively; and that some security staff lacked the abilities to be effective in the required roles.
- 74% *agreed or strongly agreed* that security professionals have developed new skill sets during the crisis that will be invaluable going forward.
- 59% felt that security would retain a greater priority than held previously due to fear of future pandemics, although 57% believed that

the need to win contracts and cut costs post pandemic will exacerbate the 'race to the bottom'.
- 55% indicated that there are other service functions stood out more for their achievements than security did during the pandemic.
- 54% said that if/where the status of security has been enhanced this will last well into the future.
- 42% said that there had been a failure to explore partnership approaches in response to the pandemic.

Concerns and threats

- The primary concern focussed on a potential adverse economic climate.
- More specifically, 77% expressed concerns about the risks of an increase in levels of online crime, 69% in managing risks in the remote (online) working environment, and 63% in managing data security and privacy.
- About three quarters felt managing the mental health of workers generally and security specifically would be a greater issue than prior to the pandemic

Opportunities

- 79% of respondents thought there would be an increase or large increase in demand for remote monitoring; 62% thought so for mobile patrols; and 51% for security officers; 46% for keyholding; and less for security consultants (42%) and installers/integrators (40%).
- With technology, 79% thought surveillance/CCTV would be in greater demand, and 75% that access control; 63% physical barriers and 61% alarms would be.
- Some pointed to opportunities in offering additional types of training that were now more relevant (such as mental health awareness, first aid training, and communication training). Others noted more generally the need to offer specialised training in order to up-skill personnel; 64% indicated that the focus on the crisis has meant that usual staff training and development has been neglected.

Type of provision

- 65% reflected that the pandemic may *hasten a shift to more technology and less personnel*, this view was less common among contracted security operatives.
- Most respondents felt that moving forward the security sector would offer a broader range of services; 89% felt that the pandemic has demonstrated that things can be done differently.
- The greater focus on technology included, specifically more touchless technologies, and more relating to healthcare, including mental health

- 69% thought it was right to expect marked improvements and innovation in security from now on.
- 75% felt that despite good intentions, the financial constraints that are likely to follow the pandemic will undermine any progress made.
- 53% *agreed or strongly agreed* that redundancies in other sectors and a tough job market will bring fresh talent to security, although 45% thought it will be more challenging to recruit skilled and able individuals.

Table of Contents

Section 1. Setting the Scene

1.1. When the Covid-19 virus rapidly travelled the globe in early 2020 its impact on individuals, health services and businesses were overwhelming. Along with all sectors, security had to adapt very quickly to the threats posed and physical security, technology and cyber security all played a specific role in dealing with the varied challenges of both lockdowns and return to work leading to the so-called 'new normal'. Arguably the private security sector and corporate security, the focus of this study, has played a pivotal role in supporting operations that have been critical in responding to Covid-19 (such as hospitals, testing centres), as well as other 'essential' operations (such as supermarkets). Security has been at the forefront in environments where managing the virus has been difficult and more generally played a key role in facilitating operations in many settings.

1.2. Recognising the significant issues faced by the security sector, the aim of this piece of work is to understand what has been learned in responding to the Covid-19 pandemic – what were and are the challenges, the successes and failings? It examines the views of those involved in the provision of security, buyers and sellers, with consideration of the implications for security moving forward – what has changed, and what does this mean for the future of the industry?

Section 2. Understanding the context

Introduction

2.1. The threat of a pandemic has for some time been a prominent part of different government risk assessments. In the UK for example the National Security Strategy highlighted a health pandemic as a Tier One threat – the highest threat level.[1] In the US in 2019 the government conducted a simulation of a pandemic, which highlighted a limited capacity to respond.[2] Despite this and recent scares with swine flu (2009) and Ebola (2013), it is generally recognised that governments, businesses and the public were not prepared for a crisis of this nature, extent and longevity.[3]

2.2. There has been a wealth of speculation and also commentary on the pandemic[4], however there is little existing research from which to draw. This section explores what is documented on some of the key changes.

Changes in crime

2.3. Just as the pandemic signalled an 'overnight' sea-change for businesses, the same was observed in relation to offending.[5] There are indications that lockdowns prompted significant falls in acquisitive crimes, such as domestic burglary and robbery, due to reduced opportunities as vast numbers of the population spent the majority of their time at home.[6] While commercial buildings were potentially at greater risk of break-ins while empty, offenders may have been deterred by the lack of people present rendering them more noticeable.[7]

---

[1] HM Government (November 2015) *National Security Strategy ad Strategic Defence and Security Review 2015*, UK; and HM Government (July 2018) *UK Biological Security Strategy*, UK.
[2] US Department of Health and Human Services (October 2019) *Crimson Contagion 2019 Functional Exercise: Draft After-Action Report*.
[3] See for example: https://www.nato.int/docu/review/articles/2020/05/20/coronavirus-invisible-threats-and-preparing-for-resilience/index.html
[4] For good discussion on a wide range of Covid-19 related security issues please see the Outstanding Security Performance Awards series of webinars, available freely online here: https://www.youtube.com/channel/UC3ZsgjtdPBgJzs5yVzT-Lgw/videos
[5] For an excellent discussion of the impact of the pandemic on crime rates, see: Mawby, R. (2022) *'*Explaining the impact and implications of COVID-19 on crime rates: a criminological perspective'. In Gill, M., (ed) *The Handbook of Security*, third edition. Basingstoke: Palgrave. For informative discussions on specific crime types see, UCL - https://covid19-crime.com/
[6] See for example: ONS Statistical bulletin (August 2020) *Coronavirus and crime in England and Wales: August 2020.* Available online: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/coronavirusandcrimeinenglandandwales/august2020
[7] https://www.ucl.ac.uk/news/2020/apr/analysis-how-crime-changes-during-lockdown

2.4. There were also concerns about a rise in interpersonal violence as the pandemic had the potential to exacerbate known risk factors. Domestic abuse[8], and altercations in relation to compliance with Covid-19 requirements (such as at shops and hospitals) were thought to be increasing during the pandemic.[9] In a completely different way, a key issue for many security professionals, was the potential impact on mental health issues and suicide.[10]

2.5. Meanwhile, research has shown that cyber criminals were exploiting the Covid-19 pandemic[11] in wide and varied ways and that these crimes evolved in response to changing circumstances.[12]

> *'The critical dependency on virtual environments by organisations and individuals during the COVID-19 pandemic is being exploited by cybercriminals.'*

2.6. Many employees working at home did so outside the usual secure systems provided by their employer. To enable remote working many used personal devices, wi-fi and video conferencing technology for communication.[13] Covid-19 themed scams were designed to capitalise on the increased dependence on technology and electronic communication. One source for example reported a 667% increase in phishing attacks that used Coronavirus-related themes.[14] Social engineering was facilitated by the emotional vulnerability of people (in their personal and professional lives) at a time of uncertainty and challenges created by the pandemic. Meanwhile, the World Health Organisation has warned of the risks of infodemics, namely the malicious spreading of lies, misinformation etc in a medical emergency.[15]

---

[8] See for example British Medical Journal News (May 2020) *Covid-19: EU states report 60% rise in emergency calls about domestic violence*, BMJ 2020; 369: m1872. Available online: https://www.bmj.com/content/369/bmj.m1872

[9] See for example https://www.talkingretail.com/news/industry-news/central-england-co-op-reports-unacceptable-rise-violent-offences-18-05-2020/
and: https://www.securitymagazine.com/articles/93019-glasgow-hospitals-forced-to-increase-security-and-safety-procedures-after-rise-in-physical-attacks

[10] See for example QJM (June 2020) *The impact of the COVID-19 pandemic on suicide rates.* Available online: https://academic.oup.com/qjmed/advance-article/doi/10.1093/qjmed/hcaa202/5857612

[11] Bruno, D. 2020. COVID-19 and cybercrime: How rogue nations and cyber criminals are exploiting a global crisis. Northern Policy Institute: Briefing Note No. 17: 1-12. https://www.northernpolicy.ca/upload/documents/publications/briefing notes/bruno_crisiscybercrime.20.05.22.pdf. Accessed 26th March 2021.

[12] Naidoo, R. (May 2020) 'A multi-level influence model of COVID-19 themed cybercrime', *European Journal of Information Systems*, 29(3), 306-321.

[13] Cracknell, J. & McAuley, S. (July 2020) *Cyber security risks during a pandemic* - https://www.willistowerswatson.com/en-GB/Insights/2020/07/cyber-security-risks-during-a-pandemic

[14] Agarwal, R. & Karahanna, E. (2000) 'Time flies when you're having fun: Cognitive absorption and beliefs about information technology usage', *MIS Quarterly* , 24(4), 665–694.

[15] Gradon, K. (2020) Crime in the time of the plague: Fake news pandemic and the challenges to law-enforcement and intelligence community. *Society Register* 4(2): 133-148. https://doi.org/10.14746/sr.2020.4.2.10

2.7. Similarly, there were indications that serious and organised crime adapted to exploit the circumstances arising due to the pandemic.[16] While a range of different terrorist groups have used Covid-19 as propaganda arguing it has been caused by whatever section of the population it wishes to rally its supporters against.[17]

2.8. Beyond the immediate impact of lockdowns, the full impacts on crime remain uncertain. Sources suggest that the pandemic and associated lockdowns are '*causing a global economic crisis that is expected to rival or exceed that of any recession in the past 150 years*'.[18] While there is a need for caution in linking the existence of a recession to an increase in crime,[19] it inevitably heightens concern. In any event, there is some evidence that the '*threat landscape has broadened and diversified*'.[20]

Changes in demand & function

2.9. In some sectors demand for security staff fell as businesses were closed (such as event security at sport venues, door supervisors in hospitality, and non-essential retail); in others, demand was maintained or increased, such as in healthcare and in supermarkets. More generally there was logically a greater focus on business continuity and security teams were often central to any changing requirements. Research by ASIS Foundation tracked the response and recovery efforts of nine companies in detail.[21]

2.10. Exploring the possibility of a reduction in demand for security, The Security Executive Council in its 2020 Security Barometer[22] found that 14% of respondents had already experienced cuts, and another 45% were concerned about that possibility (of which 12% were very concerned, 21% were somewhat concerned, 20% were slightly

[16] Europol (April 2020) Beyond the pandemic: how COVID-19 will shape the serious and organized crime landscape in the EU.
[17] See, for example 'Covid-19 Fuelling Anti-Asian Racism and Xenophobia Worldwide', *Human Rights Watch*, 12 May 2020, https://www.hrw.org/news/2020/05/12/covid-19-fueling-anti-asian-racism-and-xenophobia-worldwide. Also for a good discussion see, Ramakrishna, K. (forthcoming, 2022) 'The Evolution of the Terrorism and Extremism Landscape in the Age of COVID-19'. In Gill, M (editor) *The Handbook of Security*, third edition. Basingstoke: Palgrave.
[18] Global Initiative Against Transnational Organized Crime (June 2020) *Aggravating circumstances: How coronavirus impacts human trafficking*, available online: https://globalinitiative.net/analysis/human-trafficking-covid-impact/
[19] See for example Pioneer Institute Public Policy Research (April 2020) *Will the COVID-19 related economic recession cause a spike in crime?* Available online: https://pioneerinstitute.org/news/will-the-covid-19-related-economic-recession-cause-a-spike-in-crime/
[20] Dark Reading for IFSEC Global (November 2020) *Dealing with insider threats in the age of COVID*, available online: https://www.ifsecglobal.com/security/dealing-with-insider-threats-in-the-age-of-covid/?elq_mid=4968&elq_cid=44966
[21] Gips, M. (2021) *Resilience, Business Continuity and Covid-19*, ASIS Foundation – available online: https://www.asisonline.org/security-management-magazine/latest-news/online-exclusives/2020/research/Final-Report-Resilience-Business-Continuity-and-COVID-19/
[22] Security Executive Council (2020) *Security Barometer: Is COVID-19 Putting Your Budget or Team at Risk for Reductions?* Available online: https://www.securityexecutivecouncil.com/spotlight/?sid=32219&sc=NX012_secbarCovidAtRiskRslts&utm_source=NX012&utm_medium=Email&utm_campaign=secbarCovidAtRiskRslts

concerned or not sure). Significantly, just a third (33%) were not concerned.

2.11. In the UK, the Security Industry Authority (SIA) conducted a survey of organisations providing private security shortly after the first lockdown was introduced. Of those with Approved Contractor Scheme (ACS) status[23] more than two fifths had seen a reduction in demand for services, while close to a third had seen an increase in demand. Nearly a quarter had redeployed staff to another sector, and nearly three quarters had 'furloughed' staff (to be paid via government funding).[24]

2.12. Security companies have highlighted the changing role of security officers, and the 'frontline' role that they have played. As well as their usual tasks, they were often required to fulfil a public safety role, adapting to tasks to meet requirements, such as limiting numbers accessing facilities, enforcing social distancing and the wearing of masks, and conducting temperature checks.[25] The 'Hidden Workforce' campaign in the UK by the BSIA, Security Institute and Security Commonwealth was initiated to raise awareness of the essential role that security officers play in public life and to increase respect for their capabilities.[26]

2.13. In much the same way as security officers have been in both less and more demand depending on the sector and context of their role, the technical security sector has faced lessening demand in some respects (such as due to delays in construction projects); but increases in others (such as solutions enabling requirements are met as employees initially adapted to home working and then later returned to work).[27] The use of access control systems have been extended as organisations increasingly seek to control not just who can enter and when, but how many people can enter at any one time, and to identify who was in close proximity to someone later diagnosed with Covid-19. While touchless technologies suddenly had an extra appeal. Installers, engineers and contractors have also had to adapt their working practices and have faced difficulties in following guidance[28] where the nature of their work means it can be impractical to either social distance

[23] This is a voluntary scheme for organisations providing private security in the UK to work to, that demonstrates key standards are being met, for more information see: https://www.gov.uk/guidance/learn-about-our-approved-contractor-scheme
[24] SIA (June 2020) *Covid-19 surveys; Summary*
[25] See for example: https://www.tracktik.com/blog/the-changing-role-of-the-security-guard-during-the-covid-19-pandemic-in-the-uk/; and IFSEC Global (2020) *Back in the game: How the return of spectators to sport may affect security and fire professionals* - https://www.ifsecglobal.com/critical-conversations/back-in-the-game-how-the-return-of-spectators-to-sports-may-affect-security-and-fire-professionals/?elq_mid=4327&elq_cid=49304
https://www.ifsecglobal.com/global/the-role-of-a-security-guard-during-covid-19/
[26] A survey carried out as part of the hidden workforce initiative showed the role of security officers is underestimated by the public. See: https://www.bsia.co.uk/hidden-workforce
[27] Omdia (May 2020) *Connecting the Dots: The impact of Covid-19 on physical security markets*, available online: https://technology.informa.com/api/binary/623409
[28] BEIS (2020) *Working Safely during coronavirus*

or “work side by side, or facing away from each other, rather than face-to-face”.[29]

2.14. The sudden switch to remote working and the growing rate of cyber attacks heralded an increase in demand for cyber security.[30] However this trend appears to be exacerbating the existing shortage of cyber security professionals. Further, many of those that were in post were noted to have been re-tasked in the early stages of lockdown to focus on IT support activities in the rush to enable employees to work remotely.[31]

2.15. Across the sector adaptability is considered key,[32]

> *‘To succeed in the post-COVID-19 era, technology providers must rethink their strategies and offerings to accommodate a new security landscape. And they must continue to monitor customers’ needs and adjust sales, service, and training accordingly.’*

Safety concerns

2.16. Concerns about safety at work were logically prominent.[33] Various guidance has been developed to advise a range of professions on how to operate safely.[34] Inevitably this has had to be interpreted and adapted with both changing circumstances and a greater understanding of best practices, and where concerns were most acute when managing those on the frontline. Of particular concern in the UK was a report from the Office for National Statistics in May 2020[35] that revealed that men working as security officers had one of the highest Covid-19 death rates. Independent research explored some of the reasons why security occupations may be at greater risk such as the

[29] Seymour, H. (2020) ‘Rethinking best practice? The impact of COVID-19 on installers, engineers and contractors’, *IFSEC Global* - https://www.ifsecglobal.com/installer-zone/impact-of-covid-19-on-installers-and-contractors/?elq_mid=4039&elq_cid=44966
[30] https://blog.isc2.org/isc2_blog/2020/05/study-pandemic-boosts-cybersecurity-demand-.html
[31] https://www.cnbc.com/2020/09/05/cyber-security-workers-in-demand.html
[32] McKinsey & Company (July 2020) COVID-19 crisis shifts cybersecurity priorities and budgets - https://www.mckinsey.com/business-functions/risk/our-insights/covid-19-crisis-shifts-cybersecurity-priorities-and-budgets#
[33] See for example Security Executive Council (June 2020) *The Top COVID-19 Concerns of Security Leaders*, Available online: https://www.securityexecutivecouncil.com/spotlight/?sid=32075&sc=NX006_spotCOVtopConcerns&utm_source=NX006&utm_medium=Email&utm_campaign=spotCOVtopConcerns
[34] See for example: https://www.cdc.gov/coronavirus/2019-ncov/community/guidance-law-enforcement.html ; https://www.cpni.gov.uk/staying-secure-during-covid-19-0 ; https://www.gov.uk/guidance/working-safely-during-coronavirus-covid-19
[35] Office for National Statistics (May 2020) *Coronavirus (COVID-19) related deaths by occupation, England and Wales: deaths registered up to and including 20 April 2020* – available online: https://www.ons.gov.uk/peoplepopulationandcommunity/healthandsocialcare/causesofdeath/bulletins/coronaviruscovid19relateddeathsbyoccupationenglandandwales/deathsregistereduptoandincluding20april2020#men-and-coronavirus-related-deaths-by-occupation

demographic characteristics of security officers and the nature of their work.[36]

Security trends emerging

2.17. Commentary from IFSEC Global[37] posited a number of future trends for security that may be likely to arise from the pandemic, these included:

- Building an agile, remote workforce, maximising the potential of technology to assist.
- Embracing new forms of outreach – online and virtual training, more webinars, virtual trade shows.
- Convergence – the need for a more unified operating environment and overlap between systems; the need to see an entire security posture in a single pane-of-view.
- Driving decisions through data – the need for innovative ways of collecting and analysing data into usable information to enable decision-making and assist the security response.
- Filtering information through intelligence – the use of machine learning and AI to enable more streamlined decision-making and response; the ability of technology to solve complex problems.

2.18. Other sources have suggested diversification of services is important in protecting security companies, where for example margins in security guarding are tight.[38]

2.19. There is evidence to suggest that Covid-19 has acted as a catalyst, creating more demand for technology such as touchless systems (as noted above) which were already gaining popularity, but now offer specific advantages in aiding safety measures in relation to controlling access and enabling social distancing:

> *'As a sector we should actively promote solutions that will help organisations to operate as 'normally' as possible while helping to reduce the risk of infection.'* [39]

2.20. Building on these foundations and themes, the next two sections consider the views of security professionals. The first reports on a

[36] Goldstraw-White, G., Gill, M. & Howell, C. (June 2020) *Why is the death rate of security officers comparatively high? Thinking about the reasons: A report commissioned by Corps* Security, Perpetuity Research; available via https://www.corpssecurity.co.uk/corps-security-news-information/corps-security-press-releases/2020/06/25/report-why-is-the-death-rate-of-security-officers-comparatively-high/

[37] Rawling, S (2020) 'The security trends set to arise from coronavirus', *IFSEC Global* - https://www.ifsecglobal.com/critical-conversations/security-trends-arising-from-coronavirus/?elq_mid=3815&elq_cid=44966

[38] IFSEC Global (2020) *Foremost Security: How diversification of services enabled growth, and life after the pandemic* - https://www.ifsecglobal.com/guarding/foremost-security-how-diversification-of-services-enabled-growth-and-life-after-the-pandemic/?elq_mid=4366&elq_cid=44966

[39] Jefferies, P. (2020) 'Touchless access control – improving both security and safety', *IFSEC Global* - https://www.ifsecglobal.com/access-control/touchless-access-control-improving-both-security-and-safety/?elq_mid=4435&elq_cid=44966

global survey of 500 security professionals, and the second on 39 in-depth interviews. They seek to explore:

- Are the changes noted above the ones security personnel consider the most salient?
- What are their implications?
- Are there ways in which the security sector can emerge in a stronger position, and find new opportunities?
- What have we learnt that can benefit the industry in the future?

Section 3. Survey Findings

The sample

3.1. A survey of security professionals was conducted in order to gain a better understanding of:

- Whether the pandemic has changed the perception and status of security;
- How well security has performed;
- The likely threats faced by security professionals post pandemic;
- The likely demand for security post pandemic; and
- The difficulties and opportunities to prepare for.

3.2. The overall aim was to understand whether security will emerge from the pandemic in a stronger, weaker or similar position to when it entered. The findings are based on 500 responses[40].

3.3. In the introduction to the survey it was noted that – *We have used the word 'security' to apply to the private security sector (i.e. the work of security companies providing security services and products to clients; and of security teams within corporate and public sector organisations).* The majority of questions were multiple choice, some of which posed statements which respondents were invited to indicate their level of agreement or disagreement with. Additionally, a small number of questions invited open text responses. All of the topics covered are condensed and summarised below.

3.4. In addition to the frequency responses to questions, analysis was undertaken to assess whether views differed by specific characteristics/sub-groups of respondents. Only those issues that were statistically significant are included in the discussion, evidencing a relationship between the variables (i.e. not occurring by chance). Key points are integrated into the main findings, and include perspectives by:

- Whether the respondent thought that generally physical security had performed better, worse or about the same as other functions/departments.
- Whether the respondent thought that generally physical security would be in a stronger, weaker or similar position post pandemic.

3.5. Notably the role of the individuals (i.e., whether a security supplier, buyer/customer, or an operative) and whether their organisation provided security in an 'essential' sector during the pandemic, very

[40] The number of responses to each question varies as some respondents dropped out part way through and some chose not to answer certain questions.

rarely related to how respondents answered. Where it did, this is noted within the findings.

3.6. Just over half of the respondents (56%, n=277) worked for a supplier; while a third (33%, n=164) indicated they worked for a buyer/customer.[41]

3.7. The remaining respondents were other security experts (e.g. academic, regulator, etc.) at 8% (n=42) of respondents, or other interested party linked to security at 3% (n=17). Table 1 displays these roles.

Table 1: Breakdown of respondents by role % (n=500)

Role	Type	% , N	Total
Supplier	Director, Manager, Consultant	28%, n=139	56%, n=277
	Contracted operative	28%, n=138	
Buyer/ Customer	Security Manager	10%, n=51	33%, n=164
	Intermediary	1%, n=3	
	In-house operative	22%, n=110	
Other	Other security expert	8%, n=42	11%, n=59
	Other interested party	3%, n=17	

3.8. The sectors most commonly indicated by respondents as those they provided security to (respondents could tick all that apply) were Retail (31%, n=157) and Property (27%, n=135). A full breakdown is provided in Appendix 2 (Table 2).

3.9. The majority of respondents (62%, n=308) indicated that they worked in a sector considered 'essential' during the pandemic (such as a hospital, food retail etc). 30% (n=147) did not and 9% (n=43) were unsure.

3.10. Over two thirds of respondents worked for organisations based in the UK (71%, n=352). A full breakdown is provided in Appendix 2 (Table 3).

The perceived value of security

3.11. Respondents were asked whether they thought that the perceived value of private physical security would change as a result of the pandemic, among a number of key groups. Predominantly respondents thought that the perceived value among those groups would either be more positive or stay the same.

3.12. More than half (55%, n=265) thought that buyers of security (clients) would have *a more positive or much more positive* perception of

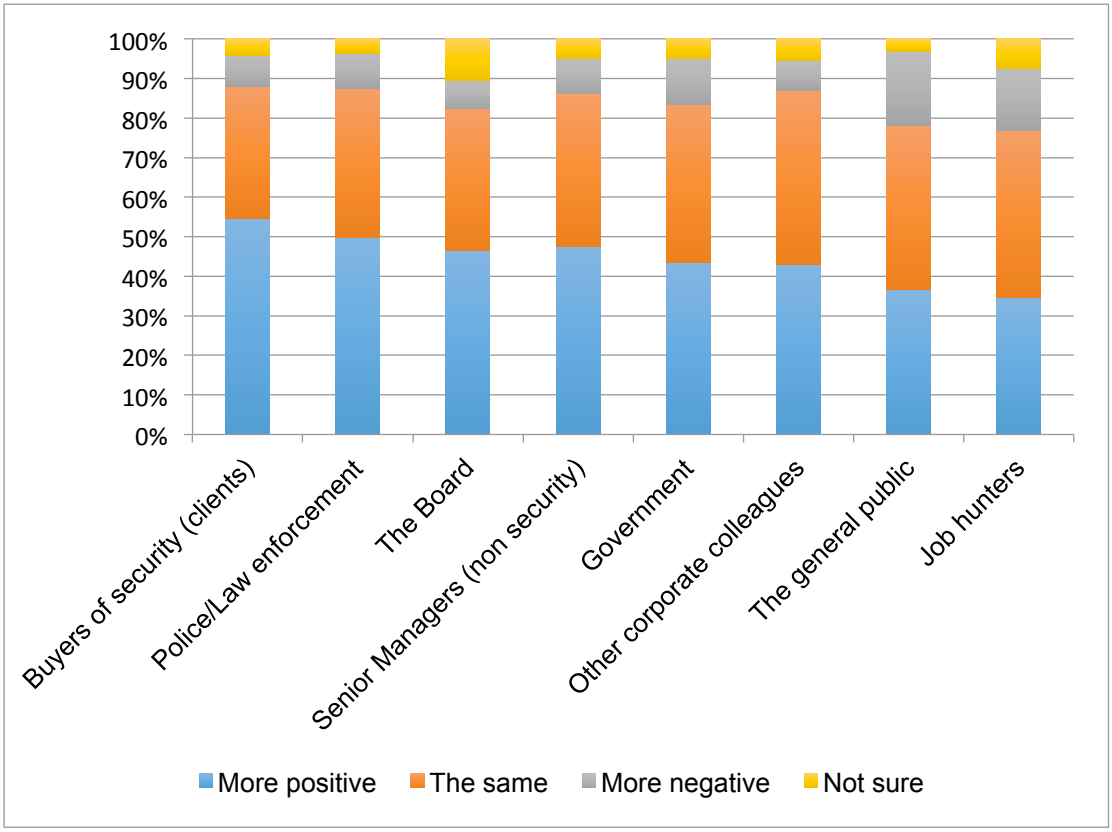
[41] It is unknown to what extent this reflects practice across the security sector. Determining this would be insightful.

security; 50% (n=245) thought that the police/law enforcement would and a further 50% (n=244) thought that the boards of organisations would.

3.13. A relatively small proportion of respondents felt that the perceived value of security would be viewed as *more negative or much more negative* post pandemic. This was thought to be more common (albeit still a minority view) among the general public (19%, n=92) and job hunters (16%, n=77) than any of the other groups explored.

3.14. Figure 1 displays the full results.

Figure 1: Change in perceived value of private physical security among certain groups post pandemic (n=485-492)



3.15. Further analysis of these figures showed the subgroup of respondents that believed that security had performed better than other functions/departments during the pandemic (a subsequent survey question), were more likely (than the group that believed security had performed worse than other functions/departments during the pandemic) to indicate that the perception of security among these different groups was more positive post pandemic.[42]

3.16. Similarly, the subgroup of respondents that indicated that on balance security would emerge from the pandemic stronger (another

[42] See Appendix 2, Table 4

subsequent survey question) were much more likely (than those that thought security would emerge weaker) to indicate that the perception of security among these different groups would be more positive post pandemic.[43]

3.17. In other words, those that were more positive about how security had performed during the pandemic, were also more positive that this had improved perceptions of security.

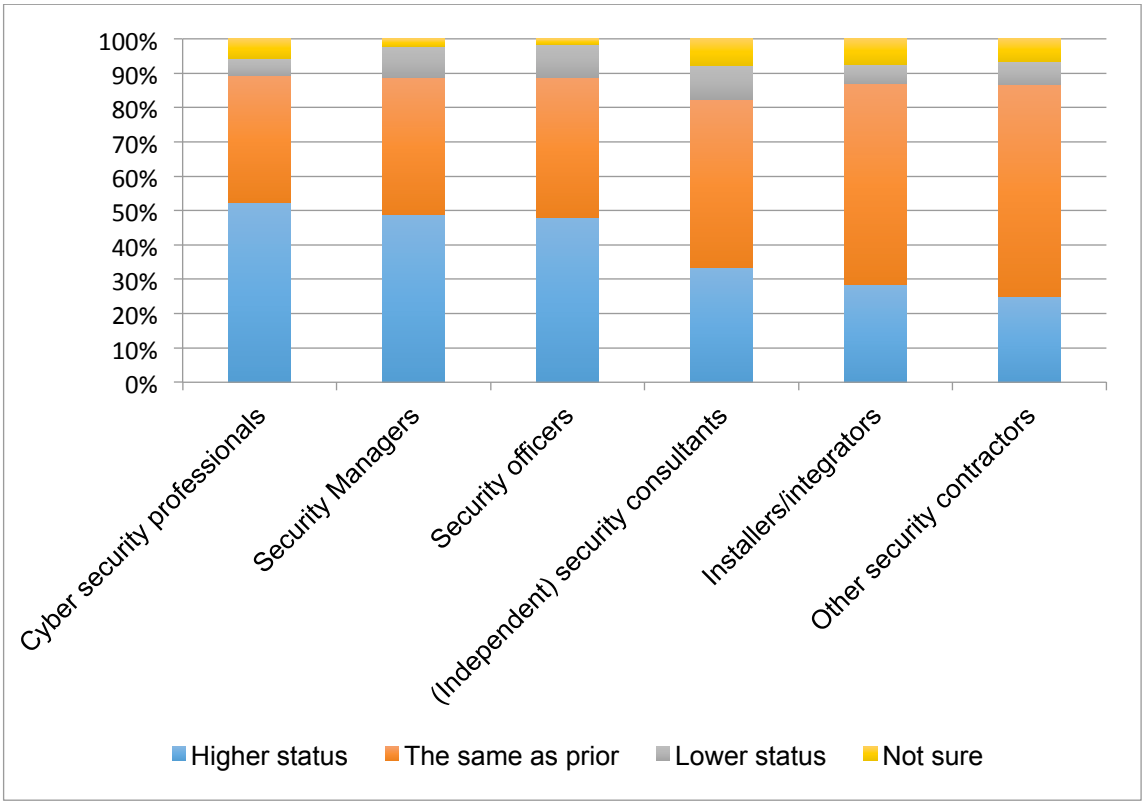
3.18. Respondents were also asked more specifically whether they thought the relative status within organisations of a number of security specialisms would be different post pandemic. Typically, the respondents thought that the status of those specialisms would either be higher/much higher or the same as prior to the pandemic.

3.19. A majority of respondents believed that cyber security professionals (52%, n=256), security managers (49%, n=241), and security officers (48%, n=237) would have a *higher or much higher* status post pandemic than prior. Meanwhile, the majority of respondents felt that other security contractors (62%, n=300), installers/integrators (59%, n=287), and (independent) security consultants (49%, n=239) would hold the *same* status as prior to the pandemic.

3.20. The results are displayed in Figure 2.

[43] See Appendix 2, Table 5

Figure 2: Perceived change in the status within organisations of security specialisms post pandemic (n=486-495)



3.21. Further analysis showed that the subgroup that believed that security had performed better than other functions/departments during the pandemic, were more likely (than those who believed security had performed worse than other functions/departments during the pandemic) to indicate that security professionals held a higher status than prior to the pandemic.[44] In other words typically those that were positive about how security had performed were more commonly the ones that felt the status of security professionals had increased.

3.22. The subgroup that thought security would emerge stronger from the pandemic were much more likely (than those that thought it would emerge the same or weaker), to indicate the status of *security managers* and *security officers* would be higher post pandemic.[45]

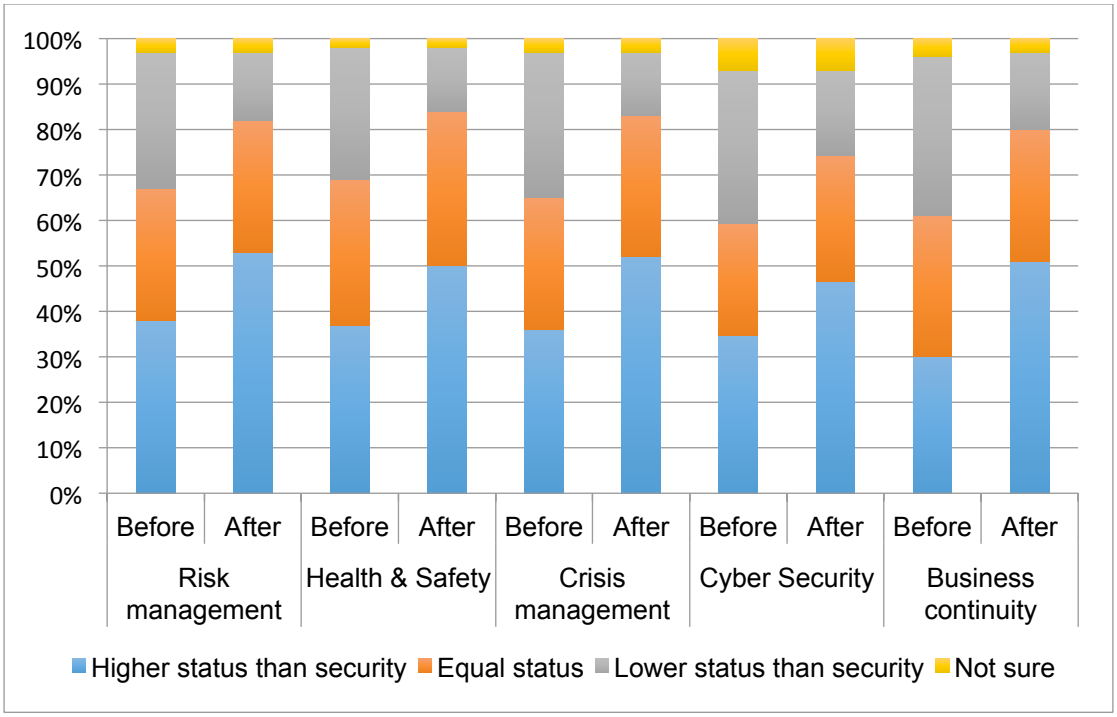
3.23. The status of private physical security professionals was also compared to other business functions. First respondents were asked whether each function had a higher, lower or equal status to physical security before the pandemic. The results were fairly evenly split across all three answer options. With the exception of business continuity, all of the other functions explored (risk management, health & safety, crisis management and cyber security) were viewed by a slim majority as having a *higher* status than security.

[44] See Appendix 2, Table 6
[45] See Appendix 2, Table 7

3.24. Next, respondents were asked what they thought the relative status of those other functions would be post pandemic. Respondents were increasingly likely to view other functions as having a *higher* status than physical security post pandemic. The biggest increase was seen for business continuity (rising by 21 percentage points); followed by crisis management (rising by 16 percentage points); risk management (rising by 15 percentage points); health & safety (rising by 13 percentage points); and finally cyber security (rising by 12 percentage points).

3.25. The perceived status of each function both before and after the pandemic is shown in Figure 3.

Figure 3: Relative status of other functions compared to physical security – pre pandemic ('before') and post pandemic ('after') (n=443-450)



3.26. So, although there was an indication that security may be more valued than previously and that some types of security professionals had gained more status, security has not overtaken the status of other functions – indeed it seems other related roles have gained more status from their contribution during the pandemic.

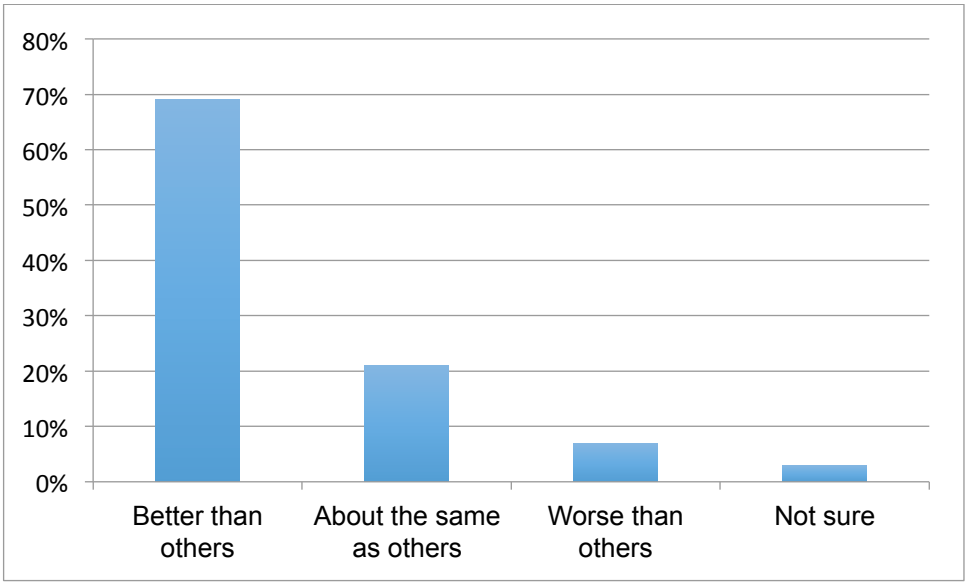
Performance of physical security during the pandemic

3.27. Respondents were asked to indicate generally speaking, how well or badly physical security had performed during the pandemic, compared to other service functions/departments. Nearly seven in ten (69%, n=293) felt security had performed *better or much better* than other functions/departments. Further analysis showed that contracted security operatives less commonly held this view, compared to those in

other roles, which given the open comments collected in relation to this question (see below) is likely to be due to the considerable challenges and concerns they had faced on the frontline.[46]

3.28. The results are displayed in Figure 4.

Figure 4: Performance of physical security compared to other functions/departments during the pandemic (n=424)



3.29. Respondents were asked to explain their answer (in their own words) and just over half did so (55%, n=233).

3.30. Of those that had indicated security has performed *better or much better* than others and provided a written explanation about this (n=178) the most commonly expressed reason was that security had shown high levels of adaptability (n=60), by taking on additional tasks both in relation to Covid-19 requirements, and covering tasks usually undertaken by others, who were not present during the pandemic;

> *'Continued delivery of core contractual roles, taken on additional roles, delivered more hours of service, adapted to change, rapidly mobilised new sites and services, all whilst under pressure and fear of contracting virus, and whilst others are sat at home either on furlough or safe behind a laptop!'*
>
> *(Survey respondent)*

> *'[Private] Security has become and remains more visible than ever before, providing deliverables at a pace that exceeds other business elements. Our team is tremendously more responsive and agile than others.'*
>
> *(Survey respondent)*

[46] 64% of contracted security operatives thought security had performed better or much better than other functions/departments; compared with 71% of buyers/customers, 75% of suppliers and 76% of in-house security operatives.

'For many environments, they took on roles vacated by others being the only permanent presence. Ample very positive feedback recognising the flexibility shown by individuals and teams.'

(Survey respondent)

'I would say that because it has had to adapt to massively different and constantly evolving operational challenges it has demonstrated its flexibility, resilience and adaptability to an unprecedented degree (and continues to do so).'

(Survey respondent)

3.31. Respondents also highlighted that security had played a pivotal role in the pandemic, working on the frontline in difficult circumstances (n=45), despite the threats to their own health and increased aggression from the public in relation to new requirements (such as wearing masks);

'We have been at more at risk to ourselves and family, we have had to work really long tiresome hours, we have to deal with extra abuse compared to normal from the public but we continue to do it as its our Job. And we don't really have much protection when it comes to ourselves.'

(Survey respondent)

'Operatives have continued to work in public facing sectors despite apparent risks and performed admirably in difficult environments.'

(Survey respondent)

'Security personnel have not had the luxury of sitting at home unlike most other employees. They have had to come in to work day in and day out, making many personal sacrifices and dealing with a lot of stress as a result. In addition, they have taken the brunt of the angry general population as a result of the decision making of government and public health authorities. They have been outstanding.'

(Survey respondent)

3.32. It was also highlighted that security had continued to function, maintaining a visible presence, protecting sites, and looking after buildings while others were working from home (n=27);

'As is often the case, Physical Security are a core facet of the response team, and they are the staff who can rarely work remotely.'

(Survey respondent)

'Security Teams have provided on-site support to their Clients throughout all of the Pandemic. Always there no matter how bad the spread of the virus has been. For many clients, their security teams have been the only ones on site to ensure the integrity of the building remains in place and fit for when their staff are able to return.'

(Survey respondent)

'The security sector have basically remained the only sector contributing to the client's sites, all other functions have been either reduced in number or all completely furloughed with no presence on the sites.'

(Survey respondent)

3.33. Some highlighted that security professionals had shown themselves to be more able and better prepared than others – playing pivotal roles in keeping businesses operational and designing and implementing new approaches in response to the pandemic (n=23);

'Availability, resources, mindset that suits most of the crisis other branches might not be prepared to deal with.'

(Survey respondent)

'More oriented to action, which set it apart from other departments.'

(Survey respondent)

'Client venues (both existing and new) extremely impressed with both management functions and DS [door supervisors] ability to operate to assigned protocols and assess risk etc. - when other 'entry level' in-house staff scared, struggling, ignoring protocols etc.'

(Survey respondent)

'Security was better prepared to handle the shift in workload, lock down of sites (as needed) and implementing COVID safe processes for essential sites / employees.'

(Survey respondent)

3.34. Those who offered a reason, as to why they felt security had performed about the *same* as others (n=31), highlighted that although they had adapted to changes, the work was essentially the same, and that the loss of security jobs in some sectors meant there was no opportunity to perform better or worse. Some felt regardless of their efforts security was still viewed the same as previously and some had seen examples of security performing both better and also worse than others.

3.35. Those who offered a reason as to why they felt security had performed *worse or much worse* than others (n=21) provided a variety of reasons, such as: that security roles had been lost in sectors that had shut down; that the role of security officers had been reduced to that of 'doormen', required to enforce requirements, but lacking the impact and power to do so effectively; and that some security staff lacked the abilities to be effective in the required roles.

3.36. To further explore how well security has performed, a number of statements were offered, for respondents to indicate their level of agreement/disagreement with.

3.37. The vast majority of respondents *agreed or strongly agreed* (83%, n=353) that overall security has performed well in the crisis. Further

analysis showed that this was a little higher among those working in a sector considered 'essential' during the pandemic, than those who were not.[47]

3.38. Close to three quarters (74%, n=316) *agreed or strongly agreed* that security professionals have developed new skill sets during the crisis that will be invaluable going forward.

3.39. Close to three fifths of respondents (59%, n=249) felt that security would retain a greater priority than held previously due to fear of future pandemics, although there was concern among a majority (57%, n=242) that the need to win contracts and cut costs, post pandemic, will exacerbate the 'race to the bottom' (where the quality of service provision is sacrificed in order to achieve a low price). Further analysis showed that this latter view was more prevalent among those who indicated on balance that security would emerge weaker from the pandemic, than those who indicated it would emerge stronger.[48]

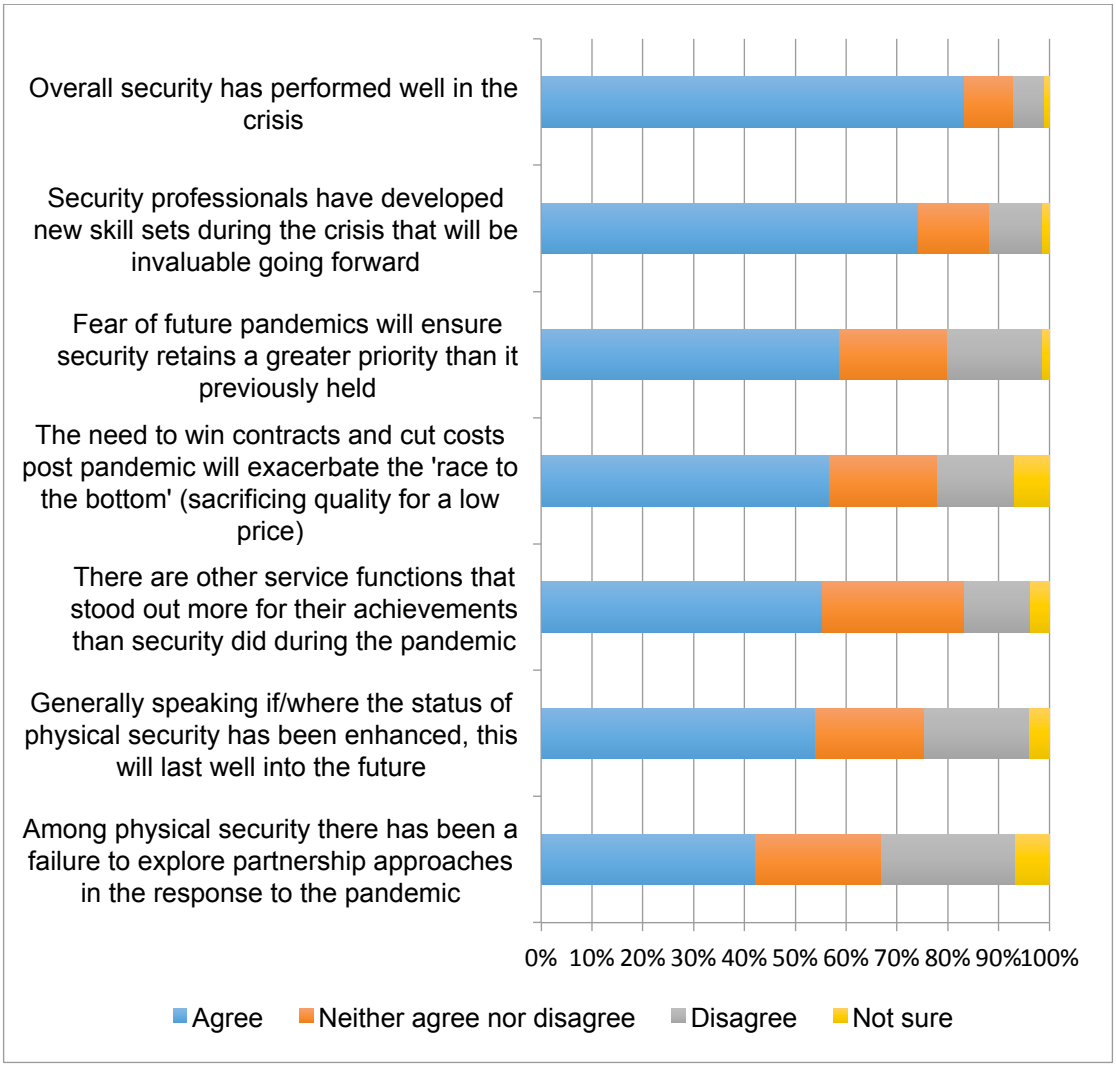
3.40. A majority (55%, n=235) indicated that there are other service functions that stood out more for their achievements than security did during the pandemic, which perhaps highlights that there are no guarantees that the good work performed by security during the pandemic will remain centre stage in the future. That said, a majority of respondents (54%, n=230) did indicate that if/where the status of security has been enhanced this will last well in to the future.

3.41. Over two fifths (42%, n=179) of respondents indicated that there had been a failure among physical security to explore partnership approaches in response to the pandemic, while a quarter (26%, n=112) disagreed. This would suggest there is some room for improvement here and something that organisations may want to consider further.

3.42. The findings are displayed in Figure 5.

[47] 88% of those working in a sector considered 'essential' during the pandemic agreed or strongly agreed; compared with 79% of those that were not working in an 'essential' sector.
[48] 73% of those that indicated security would emerge weaker or much weaker from the pandemic agreed or strongly agreed that the need to win contracts and cut costs post pandemic will exacerbate the 'race to the bottom'; compared with 62% of those that thought security would emerge the same, and 47% of those that thought security would emerge stronger or much stronger.

Figure 5: Level of agreement with statements related to performance during the pandemic (n=424-426)



3.43. Respondents from the subgroup that indicated that security had performed better than other departments during the pandemic, more commonly agreed with the statements above that reflected positively about security. Meanwhile those that indicated that security had performed worse than other departments, more commonly agreed with the statements that were critical of security.[49]

Concerns and threats

3.44. The survey explored to what extent a number of issues would pose concerns for the security sector post pandemic. Respondents were asked to rate their views on a scale from 1 to 5 where 1 means 'low', 3 means 'medium' and 5 means 'high'. The greatest concerns related to

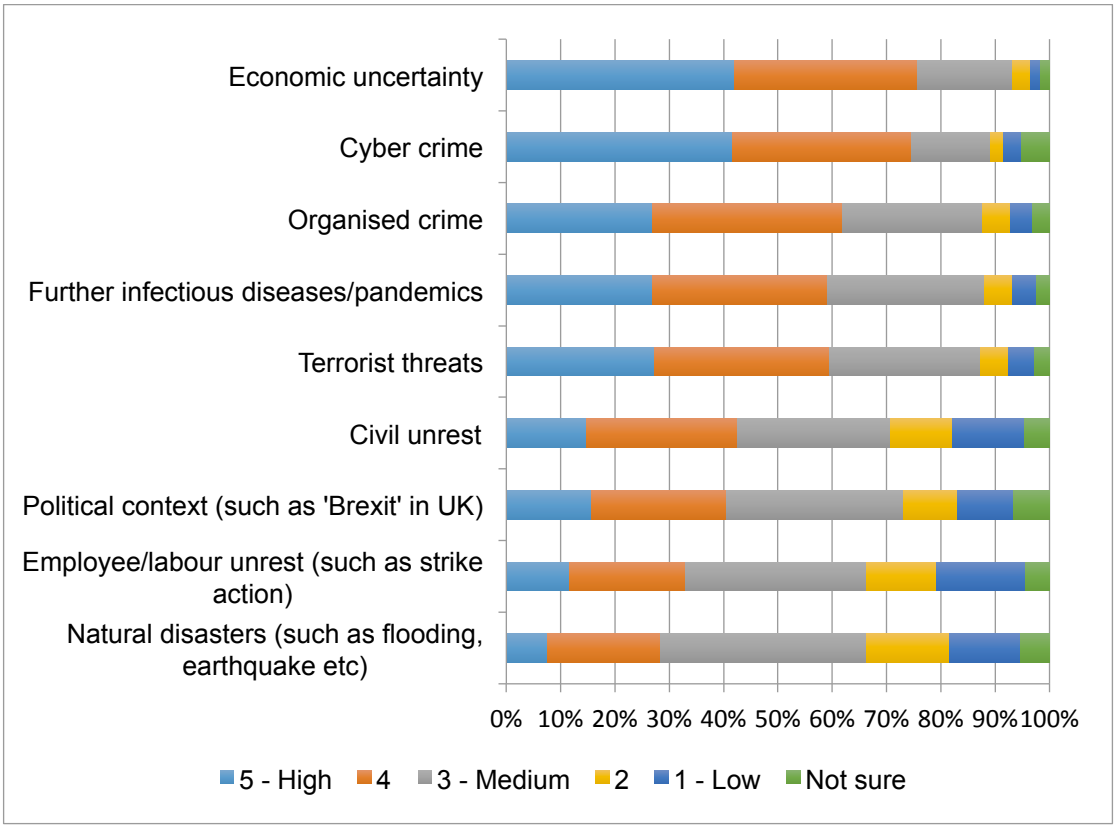
[49] See Appendix 2, Table 8

economic uncertainty[50] and cyber crime[51] – over two fifths rated each of these as 5 and a total of three quarters rated these as 4 or 5.

3.45. These concerns were followed by organised crime[52], further infectious diseases/pandemics[53], and terrorist threats[54] - with just over a quarter rating each of these as 5, and a total of around three fifths rating these as 4 or 5.

3.46. Civil unrest[55], political context[56], employee/labour unrest[57] and natural disasters[58] were of less concern. Figure 6 displays the full results.

Figure 6: Concerns for the security sector post pandemic (n=403-409)



3.47. Notably, further analysis showed that perceptions of how the issues described above may change in prevalence post pandemic, were unaffected by whether the respondent felt security had performed better or worse than other departments during the pandemic.

3.48. Respondents were asked to consider whether a number of potential threats to security within organisations would be different post

[50] 42%, n=171 rated economic uncertainty as '5 – high' concern.
[51] 42%, n=168 rated cyber crime as '5 – high' concern.
[52] 27%, n=109 rated organised crime as '5 – high' concern.
[53] 27%, n=110 rated further infectious diseases/pandemic as '5 – high' concern.
[54] 27%, n=111 rated terrorist threat as '5 – high' concern.
[55] 15%, n=60 rated civil unrest as '5 – high' concern.
[56] 16%, n=64 rated political context as '5 – high' concern.
[57] 12%, n=47 rated employee/labour unrest as '5 – high' concern.
[58] 8%, n=31 rated natural disasters as '5 – high' concern.

pandemic to pre pandemic levels. Across all the threats considered, very low numbers of respondents thought they would see a decrease in threats – the majority felt there would be an *increase or large increase*. This would suggest that if and when the pandemic has passed, it will have longer term consequences and considerations for security.

3.49. Most notable was the proportion of respondents – over three quarters, who felt that online crime (77%, n=312) and a focus on managing the mental health of workers across organisations (75%, n=307) would increase, compared to pre pandemic levels. Almost as many (70%, n=285) felt that managing the mental health of those involved in security would be a greater issue than prior to the pandemic.

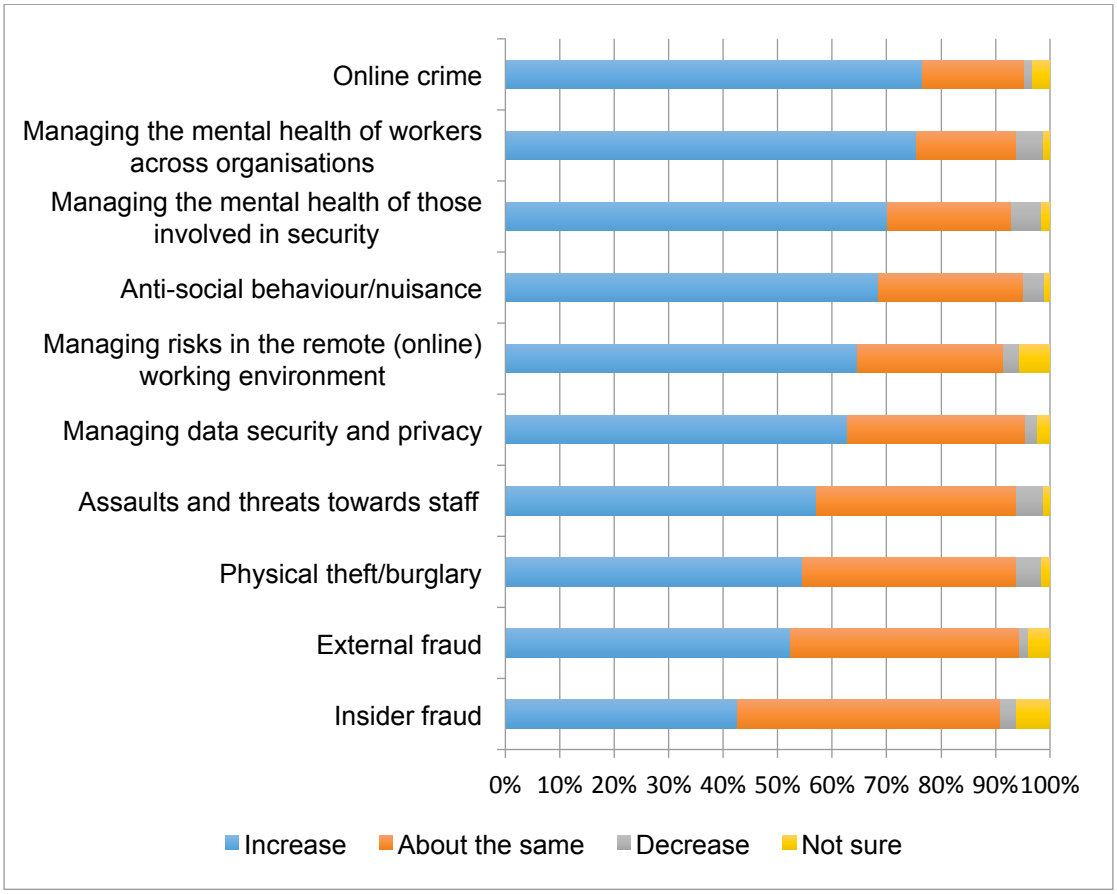
3.50. Notably, a potential increase in the threat of antisocial behaviour/nuisance (69%, n=279) was flagged a little more than managing risks in the remote (online) working environment (65%, n=263) and managing data security and privacy (63%, n=256).

3.51. A little under three fifths of respondents indicated that the issue of assaults and threats towards staff (57%, n=234) and physical theft/burglary (55%, n=221) would increase post pandemic.

3.52. A greater proportion of respondents indicated that the threat of external fraud (52%, n=212) would increase, than the threat of insider fraud (43%, n=172).

3.53. Figure 7 displays the full results.

Figure 7: Expectation of change in threats to security post pandemic (n=404-407)



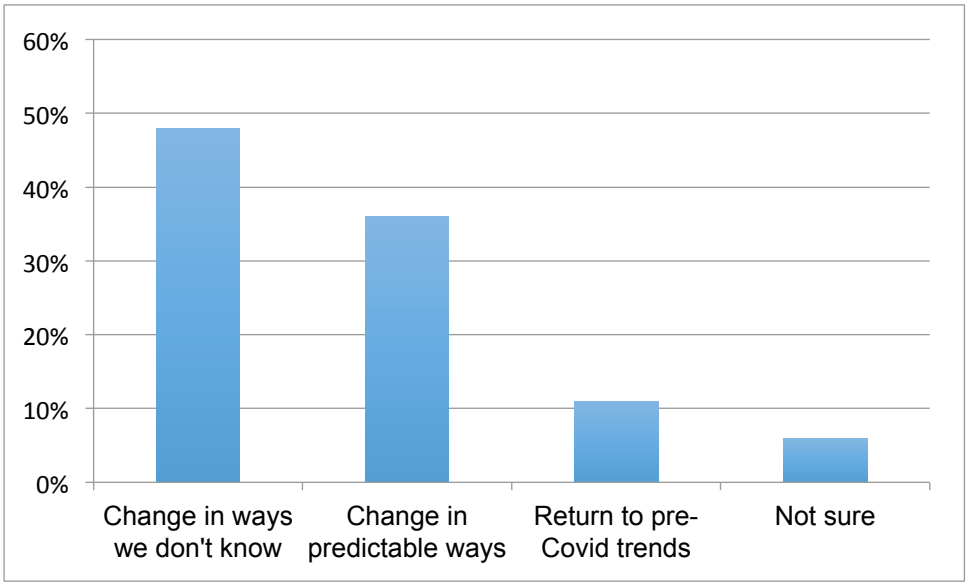
3.54. For the most part, the perceptions of these threats increasing was not affected by whether the respondents felt security had performed better than other departments during the pandemic. However, there were some exceptions. Those who thought security performed better were more likely to expect a focus on managing the mental health of those involved in security, to increase.[59] Similarly, they were more likely to expect a focus on managing the mental health of workers across the organisation to increase[60]; more likely to expect an increase in focus of managing data security and privacy[61]; and a little more likely to expect external fraud to increase.[62]

[59] 73% of those that indicated security had performed better or much better than other departments/functions expected an increase or large increase in the challenge of managing the mental health of those involved in security; compared with 67% of those that indicated security had performed the same and 54% of those that indicated security had performed worse or much worse.
[60] 79% of those that indicated security had performed better or much better than other departments/functions expected an increase or large increase in the challenge of managing the mental health of workers across the organisation; compared with 73% of those that indicated security had performed the same and 63% of those that indicated security had performed worse or much worse.
[61] 63% of those that indicated security had performed better or much better than other departments/functions expected an increase or large increase in the challenge of managing data security and privacy; compared with 68% of those that indicated security had performed the same and 52% of those that indicated security had performed worse or much worse.
[62] 54% of those that indicated security had performed better or much better than other departments/functions expected an increase or large increase in external fraud; compared with 53% of

3.55. Notably, perceptions of a likely increase in crime were greater among those who thought security would emerge from the pandemic weaker than those who thought it would emerge stronger. Meanwhile perceptions of a likely increase in a focus on issues, such as managing mental health of the workforce, managing the risks of remote working, and managing data security and privacy, were greater among those who thought security would emerge stronger from the pandemic, than those who thought it would emerge weaker.[63]

3.56. Given that security personnel are at the forefront of preventing and responding to crime, in order to draw on their insights, the survey also explored respondents' views more generally of how the pandemic may impact on crime. Close to half (48%, n=195) felt that crime would change in ways *we don't yet know or can plan for*; and over a third (36%, n=145) felt that crime would change, but *in predictable ways*. A tenth (11%, n=44) thought there would be a *return to pre-Covid crime trends,* and the rest (6%, n=24) were not sure. These results are shown in Figure 8.

Figure 8: Views on how the pandemic may impact on crime (n=408)



3.57. We might expect security personnel working closer to the public/crime interface than most others to have insights that may not be seen in official statistics. Those who offered an explanation of the changes they expected to see (n=100 did so) most commonly highlighted that:

- crime generally, or specifically would increase (n=31), such as cyber crime (due to new opportunities); violent offences (due to a more 'angry' public); and terrorism (for example where events resume);

those that indicated security had performed the same and 44% of those that indicated security had performed worse or much worse.

[63] See Appendix 2, Table 9

- criminals would adapt to available opportunities, meaning that some crime types would increase, while some would decrease (n=19);
- changes, such as economic depression and high unemployment would put further pressures on people and that may lead to more acquisitive crime and also aggression (n=14);
- new types of fraud were emerging directly in relation to the pandemic (such as fake vaccinations) (n=12).

3.58. Further analysis showed that the subgroup of respondents who felt security had performed worse than other departments/functions during the pandemic, were a little more likely than others to indicate that crime would *change in ways which we don't yet know*.[64]

Demand for security

3.59. Respondents were asked to indicate their views on whether demand for physical security services, technology that aids security, and cyber security protections would increase, decrease or stay the same post pandemic.

3.60. Almost four fifths (79%, n=303) of respondents thought there would be an increase/large increase in demand for remote monitoring. A majority also thought that demand for mobile patrols (62%, n=238) and security officers (51%, n=196) would increase.

3.61. For key holding and security management, the results were split evenly between those who thought there would be an increase in demand (both 46%, n=176) and those that thought demand would stay the same (46%, n=176 for key holding and 45%, n=173 for security management) – both at a little under half.

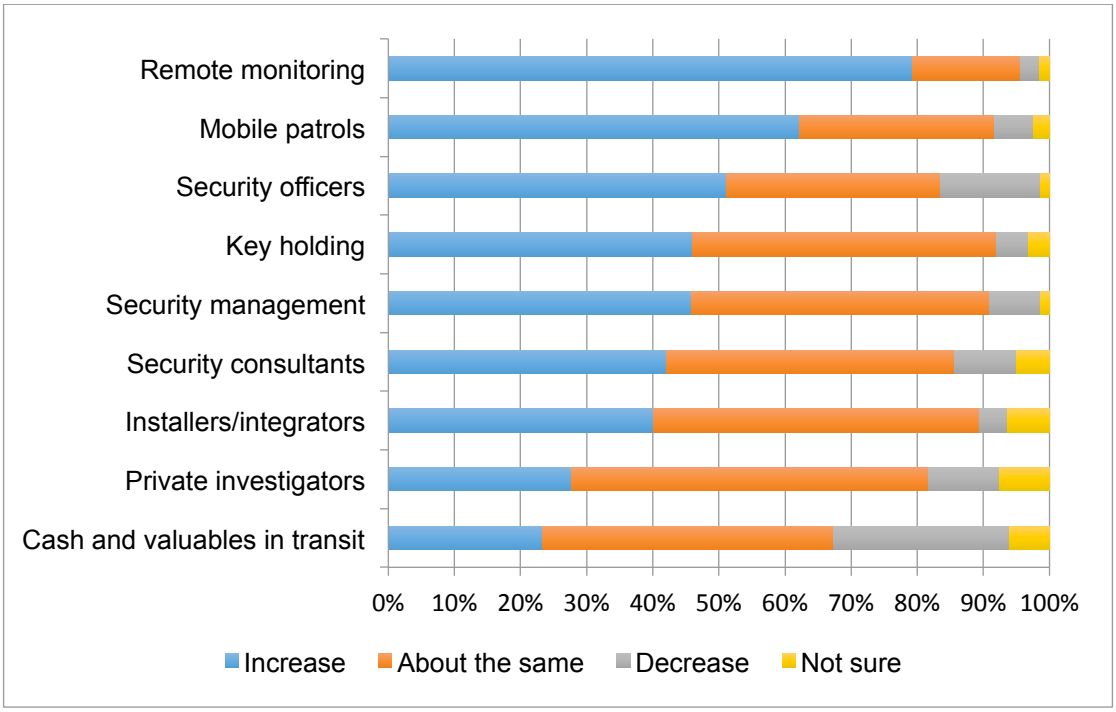
3.62. A slightly greater proportion of respondents thought that demand for security consultants and installers/integrators would stay the same (44%, n=166 and 49%, n=187 respectively) than increase (42%, n=160 and 40%, n=152 respectively).

3.63. Respondents most commonly regarded demand for private investigators (54%, n=206) and for cash and valuables in transit (44%, n=168) as likely to stay the same. In the case of cash and valuables in transit, it was also notable however, that of the remaining respondents (i.e. those that did not think demand would stay the same), a slightly higher proportion thought demand would decrease (27%, n=102) than thought it would increase (23%, n=89).

3.64. The results are shown in Figure 9.

[64] 56% of those that indicated security had performed worse or much worse than other departments/functions thought crime would change in ways we do not yet know; compared with 49% of those that indicated security had performed the same as others and 46% of those that indicated security had performed better or much better than others.

Figure 9: Perception of change in demand for security services post pandemic (n=379-384)



3.65. Respondents who indicated that security would emerge stronger from the pandemic more commonly believed that demand for security management[65] and security officers[66] would increase post pandemic, than those who thought security would emerge weaker. These subgroups were however, more closely aligned regarding the other types of physical security services explored. There was no notable distinction between the views of suppliers and buyers on this issue.

3.66. The majority of respondents thought demand for technology that aids security would increase post pandemic. However, very low numbers thought that demand would decrease.

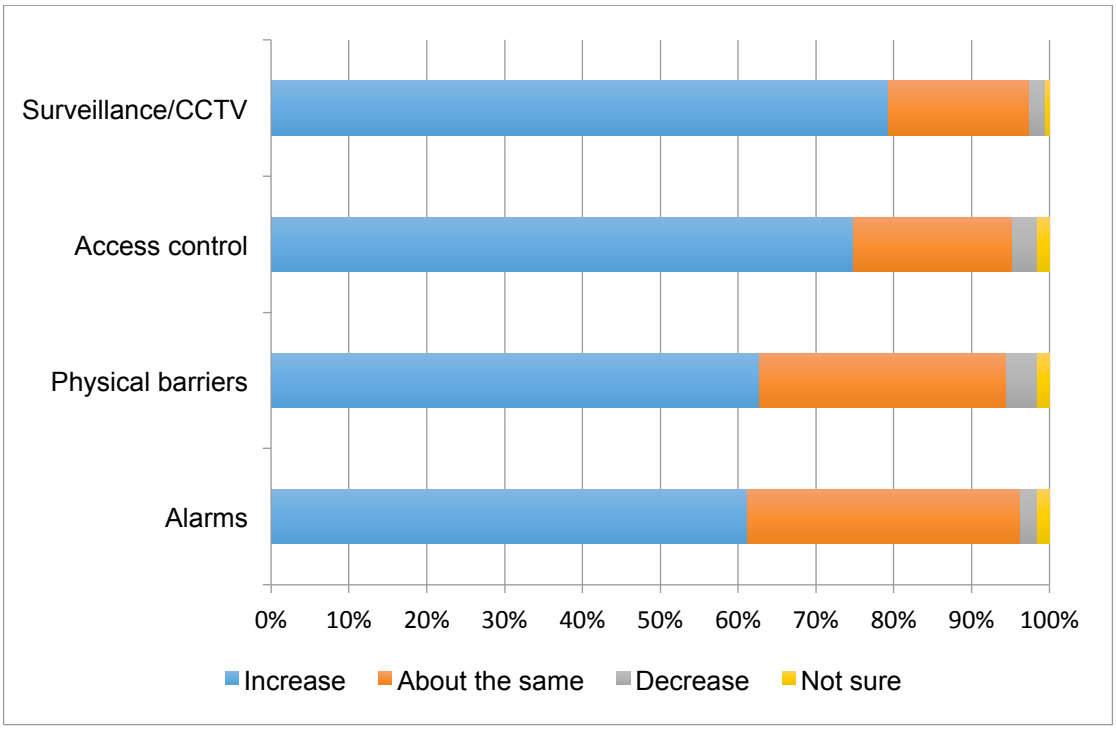
3.67. Almost four fifths (79%, n=303) thought surveillance/CCTV would be in greater demand, and three quarters thought (75%, n=285) that access control would be.

3.68. Over three fifths of respondents thought physical barriers (63%, n=239) and alarms (61%, n=233) would be in greater demand.

3.69. These findings are shown in Figure 10.

[65] 63% of those that indicated on balance security would emerge stronger or much stronger from the pandemic viewed there would be an increase or large increase in demand for security management; compared with 27% of those that thought security would emerge the same; and 26% of those that thought security would emerge weaker or much weaker from the pandemic.
[66] 65% of those that indicated on balance security would emerge stronger or much stronger from the pandemic viewed there would be an increase or large increase in demand for security officers; compared with 36% of those that thought security would emerge the same; and 34% of those that thought security would emerge weaker or much weaker from the pandemic.

Figure 10: Perception of change in demand for security technology post pandemic (n=381-382)

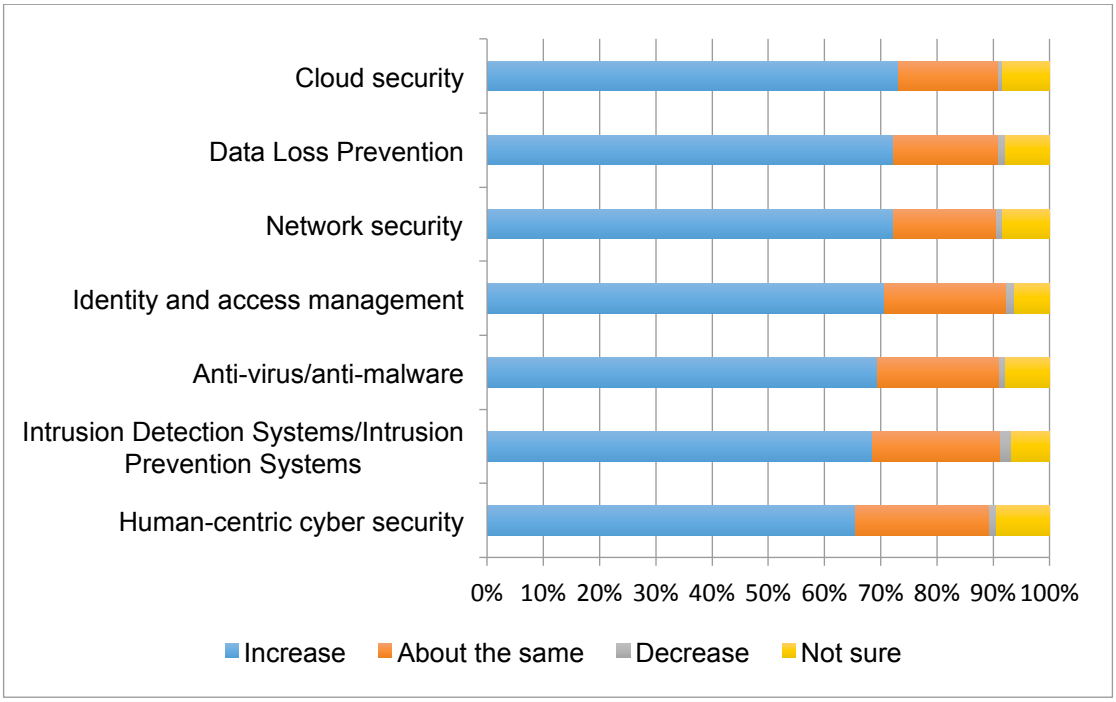


3.70. Perceptions on demand for security technology were typically unaffected by whether the respondent thought generally that security would emerge stronger, or weaker from the pandemic.

3.71. The picture was similar for cyber security – a majority of respondents thought demand for cyber security protections would increase post pandemic – and the numbers were very consistent across the different types explored. Very low numbers thought demand would decrease.

3.72. The results are show in Figure 11.

Figure 11: Perception of change in demand for cyber security protections post pandemic (n=381-384)



3.73. Notably then in terms of demand the general perception was that for both security technology and cyber security demand would increase for all of the types explored within the survey. However, the picture for physical security services was more mixed.

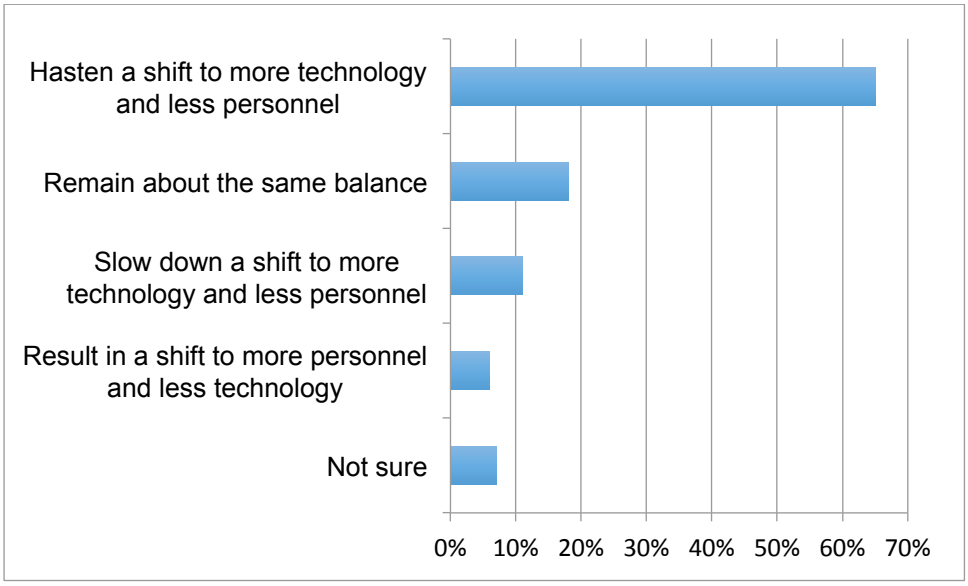
Type of provision

3.74. When asked about the potential impact on the balance between personnel and technology employed in physical security solutions, close to two thirds of respondents (65%, n=221) reflected that the pandemic may *hasten a shift to more technology and less personnel*. Further analysis showed that this view was less common among contracted security operatives than among other roles, perhaps reflecting their level of experience of the various ways in which an intervention by a person remains needed.[67] Less than a fifth (18%, n=60) thought the balance would remain the *same*.

3.75. The results are displayed in Figure 12.

[67] 40% of contracted security operatives indicated the pandemic will hasten a shift to more technology and less personnel; compared with 63% of in-house security operatives, 69% of buyers/customers and 69% of suppliers.

Figure 12: Potential impact on the balance between personnel and technology employed in physical security solutions post pandemic (n=361)



3.76. Views on this trend (that the pandemic may hasten a sift to more technology and less personnel) were mirrored between both those who thought security would emerge stronger from the pandemic and those who thought it would emerge weaker.[68] In other words, this trend is unlikely to relate to how effective the security sector was during the pandemic, and more likely to relate to other factors – such as economic concerns and the perception that technology can bring cost savings; and such as a change in mindset towards technology because of its prominence during the pandemic, and/or a change in need because of the consequences of the pandemic.

3.77. Respondents were asked to reflect (in their own words) on the main ways that the type of security provided by contractors and security teams would be different in the longer term (of which n=231 did so). The most common response (from a third of those who answered the question, n=78) was that security would offer a broader range of services than it had previously:

> *'Broader, to cover more eventualities.'*
>
> *(Survey respondent)*

> *'I predict broader services due to experience gained during the pandemic. The security sector has done well to learn from this pandemic.'*
>
> *(Survey respondent)*

[68] 65% of those that thought security would emerge stronger or much stronger from the pandemic and 66% of those that thought security would emerge weaker or much weaker – indicated that the pandemic would hasten a shift to more technology and less personnel. 56% of those that thought security would emerge from the pandemic the same, answered this way.

'I think the financial impact of Covid will cause most security personnel suppliers to try to cover more types of work due to loss of earnings.'

(Survey respondent)

'I think there will be a broader offer, with technology at the basis. I think the offer will include more customer service and integrated wrap around care for commercial settings.'

(Survey respondent)

'More expectation of Security professionals to cover a broader remit, seeing a requirement for the Security Manager to cover more aspects of Organisational Resilience.'

(Survey respondent)

3.78. The next most common response (from an eighth of those who answered the question, n=30) was that there would be a greater focus on the use of technology, for example:

'There will be different usage of technology but most have already been there for years but maybe used in different ways - e.g. CCTV to count occupancy or monitor social distancing.'

(Survey respondent)

'I've seen a large increase in robotics and AI being used to augment on-site teams (one operator can now effectively cover an entire campus through this technology).'

(Survey respondent)

'Security will have to diversify but I see a shift toward tech solutions to minimise cost and reduce staff risk.'

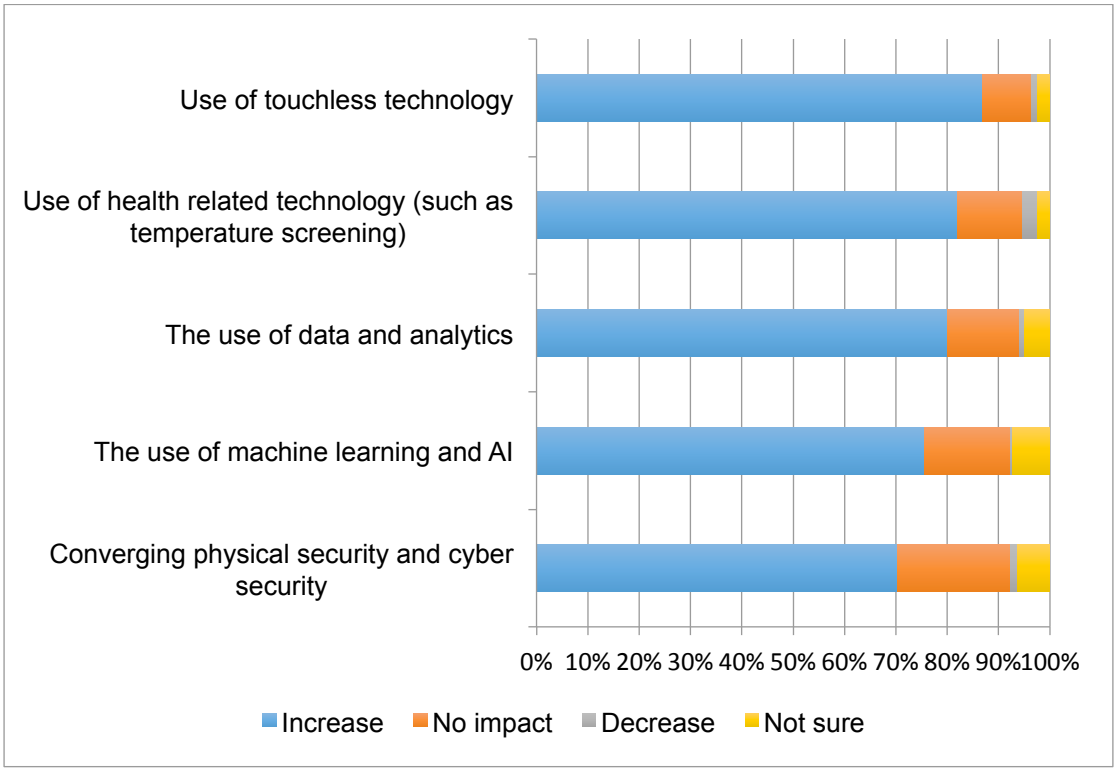
(Survey respondent)

3.79. Other themes evident, albeit in smaller numbers were that the services would remain the same as previously (n=13) and that services would become more holistic or blended (n=11).

3.80. Respondents were asked their views on the potential impact on a number of trends. The vast majority thought that the use of touchless technology (87%, n=313) would *increase* as a result of the pandemic. Four fifths thought the use of health-related technology (82%, n=295) and data and analytics (80%, n=287) would *increase*. More than two thirds believed that the use of machine learning and AI (76%, n=272), and the convergence of physical and cyber security (70%, n=254), would *increase*. Extremely low numbers of respondents thought that these trends would decrease.

3.81. The results are shown in Figure 13.

Figure 13: Impact of the pandemic on key trends (n=359-361)



3.82. Further analysis showed that across all of these key trends, the subgroup of respondents who thought security would emerge from the pandemic stronger, more commonly believed these trends would increase, than those who thought security would emerge weaker.[69]

3.83. A number of general statements were offered in the survey about the possible impacts of the pandemic on security provision, which respondents were asked to indicate their level of agreement with.

3.84. On a positive note, the vast majority *agreed or strongly agreed* (89%, n=319) that the pandemic has demonstrated that things can be done differently. More than two thirds (69%, n=247) thought we are right to expect marked improvements and innovation in security from now on.

3.85. Sounding caution, more than four fifths (84%, n=301) *agreed or strongly agreed* that even more will be expected of security for the same (or less) in the future; and three quarters (75%, n=271) believed that despite good intentions, the financial constraints that are likely to follow the pandemic will undermine any progress made. Close to two thirds (64%, n=228) indicated that the focus on the crisis has meant that usual staff training and development has been neglected.

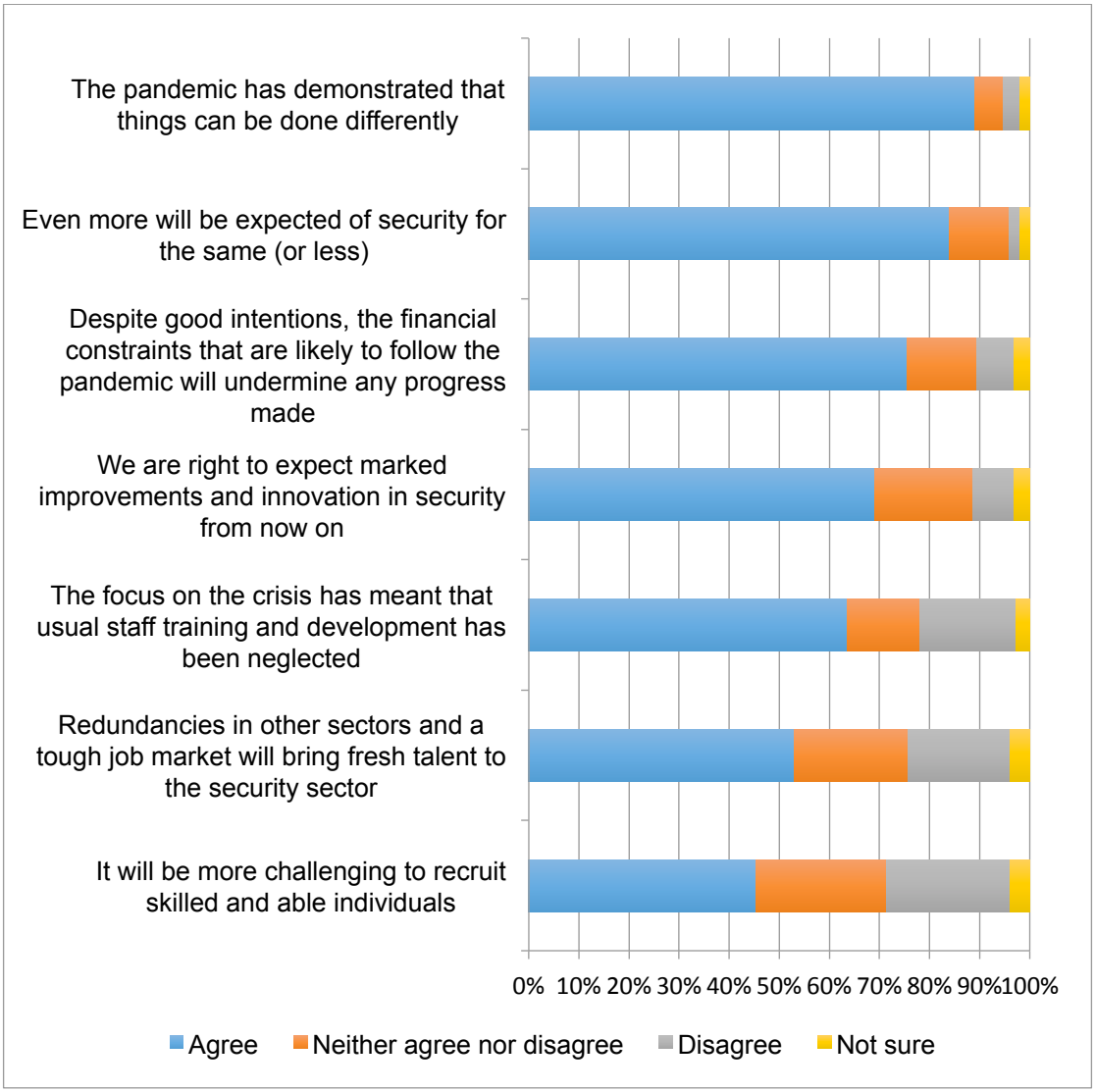
3.86. Thinking about the implications for recruiting capable individuals, just over half (53%, n=190) *agreed or strongly agreed* that redundancies in other sectors and a tough job market will bring fresh talent to the

[69] See Appendix 2, Table 10

security sector. However, under half (45%, n=163) thought it will be more challenging to recruit skilled and able individuals (a quarter – 26%, n=93 neither agreed nor disagreed and a further quarter disagreed – 25%, n=89).

3.87. The full findings are displayed in Figure 14.

Figure 14: Impacts of the pandemic on security provision (n=358-359)



3.88. There was correlation between the views expressed and whether the respondent expected security to emerge stronger or weaker from the pandemic. Those who thought it would emerge stronger more commonly agreed (than those that thought it would emerge weaker) that: even more will be expected of security for the same (or less)[70]; the

[70] 90% of those that thought security would emerge from the pandemic stronger or much stronger agreed or strongly agreed that even more will be expected of security for the same (or less); compared with 80% of those that thought security would emerge the same; and 78% of those that thought security would emerge weaker or much weaker.

pandemic has demonstrated that things can be done differently[71]; we are right to expect marked improvements and innovation in security from now on[72]; and that redundancies in other sectors and a tough job market will bring fresh talent to the security sector[73];

3.89. Meanwhile, those who thought security would emerge weaker, more commonly agreed (than those that thought it would emerge stronger) that: despite good intentions, the financial constraints that are likely to follow will undermine any progress made[74]; the focus on the crisis has meant that usual staff training and development has been neglected[75]; and that it will be more challenging to recruit skilled and able individuals.[76]

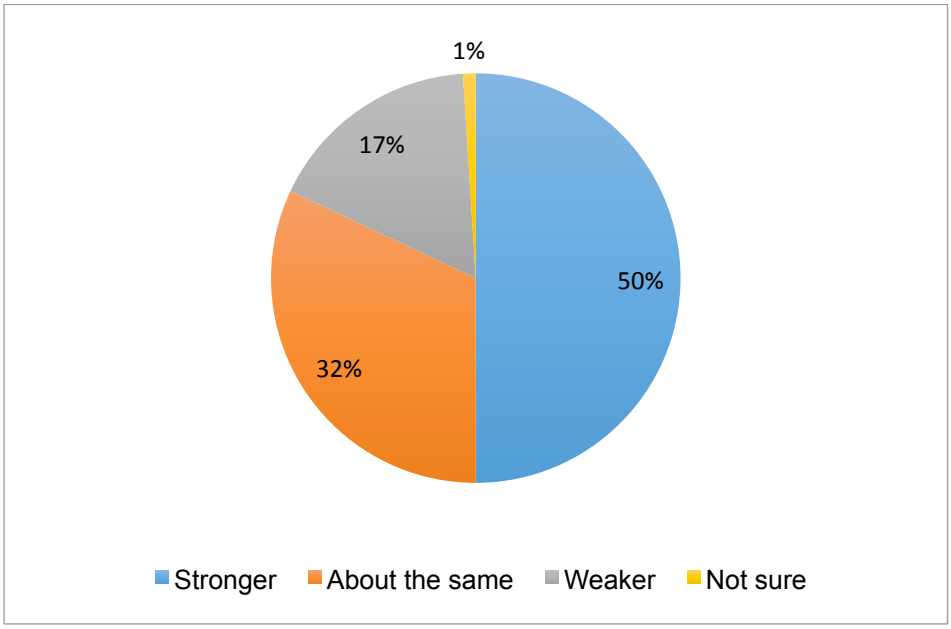
Overall impacts

3.90. Respondents were asked on balance, when emerging from the pandemic, whether the physical security sector will be in a stronger or weaker position than prior to the pandemic.

3.91. Half of the respondents (50%, n=260) believed the sector would emerge in a stronger position, a third (32%, n=113) about the same, and less than a fifth (17%, n=59) weaker.

[71] 94% of those that thought security would emerge from the pandemic stronger or much stronger agreed or strongly agreed that the pandemic has demonstrated that things can be done differently; compared with 89% of those that thought security would emerge the same; and 75% of those that thought security would emerge weaker or much weaker.
[72] 81% of those that thought security would emerge from the pandemic stronger or much stronger agreed or strongly agreed that we are right to expect marked improvements and innovation in security from now on; compared with 62% of those that thought security would emerge the same; and 51% of those that thought security would emerge weaker or much weaker.
[73] 71% of those that thought security would emerge from the pandemic stronger or much stronger agreed or strongly agreed that redundancies in other sectors and a tough job market will bring fresh talent to the security sector; compared with 36% of those that thought security would emerge the same; and 34% of those that thought security would emerge weaker or much weaker.
[74] 88% of those that indicated security would emerge weaker or much weaker agreed or strongly agreed that despite good intentions, the financial constraints that are likely to follow the pandemic will undermine any progress made; compared with 78% of those that thought security would emerge the same, and 71% of those that thought security would emerge stronger or much stronger.
[75] 66% of those that indicated security would emerge weaker or much weaker agreed or strongly agreed that the focus on the crisis has meant that usual staff training and development has been neglected; compared with 66% of those that thought security would emerge the same, and 63% of those that thought security would emerge stronger or much stronger.
[76] 65% of those that indicated security would emerge weaker or much weaker agreed or strongly agreed that it will be more challenging to recruit skilled and able individuals; compared with 46% of those that thought security would emerge the same, and 40% of those that thought security would emerge stronger or much stronger.

Figure 15: Post pandemic position of the physical security sector (n=355)



3.92. Further analysis showed that respondents who indicated security had performed better than other department/functions during the pandemic more commonly felt that security would emerge in a stronger position post pandemic (than those indicating that security had performed worse than others).[77]

3.93. Survey respondents were invited to comment (in their own words) on the main difficulties (if any) resulting from the pandemic that may impede the development of the physical security sector (n=245 did so).

3.94. The issue most frequently mentioned (n=87) was money. There were concerns that the pandemic has created significant strains on finances and this may impact on both the ability and appetite to pay for security. For example:

> *'Businesses will be looking to tighten budgets in order to stay in business and hopefully improve. Whether security has shown it's value or not during the pandemic will not matter as all departments will be forced to tighten up as the world may take years/decades to return to what was once normal.'*
>
> *(Survey respondent)*

> *'Availability of money, security is often seen as a luxury and reduced budgets may slow down or stop future developments and investment in security measures / staffing levels and training.'*
>
> *(Survey respondent)*

[77] 57% of those that indicated security had performed better or much better than other departments/functions thought security would emerge from the pandemic stronger or much stronger; compared with 39% of those that indicated security had performed the same as others, and 26% of those that thought security had performed worse or much worse than others.

'Budgets will be tight as unplanned spend on covid-secure and sickness impacts will be recovered.'

(Survey respondent)

'Cost- everyone will need to cut them and Security is a low hanging fruit when 'appearances' seem to suggest all is good in the world.'

(Survey respondent)

'Finance being allocated to a sector that doesn't produce a profit for the customer.'

(Survey respondent)

'Funding for change is difficult at this time, boards will be focusing on returning to pre pandemic levels of demand and security will be ignored to a great extent. However, it is now even more important that security progress their worth with the board, suppliers and other departments within their companies.'

(Survey respondent)

3.95. Related to this was some concern about how any potential reduced funding may impact on quality:

'The main difficulty will be the cost restrictions imposed across the industry. Contracts have been forced to run with less resource and in some cases expected the same level of service. Corporate service providers have had to demonstrate the same with less. This I fear will be exacerbated post pandemic.'

(Survey respondent)

'Financial constraints on businesses will lead to a return to cheapest gets the contract.'

(Survey respondent)

'Race to the bottom low price, low service security services.'

(Survey respondent)

'The state of the economy may force companies to implement security on the cheap, paying barely above the living wage, resulting in poorly trained and motivated staff.'

(Survey respondent)

3.96. On a similar note, another common theme was the potential impact on staffing (n=39). There were two key points here – one ensuring security staff are paid appropriately for the work they undertake both generally and especially now that some have taken on further responsibilities; and two – finding and attracting suitably qualified and experienced personnel. Some illustrative quotes include:

'Amount paid to staff, as wider range of skills have developed especially in the healthcare security sector.'

(Survey respondent)

'Companies will struggle for staff. Many have moved from smaller companies to larger ones that secured the initial pandemic contracts and smaller companies will struggle to retain staff or get old staff back.'

(Survey respondent)

'Low pay and poor working conditions means I and others will be leaving the industry for better wages and employment opportunities in other sectors.'

(Survey respondent)

'Market will be flooded with inexperience as security is seen as easy to get into and is pushed by job centres as an easy way to get people back to work, this will make recruiting calibre more difficult and likely to result in high turnover as people leave the industry to return to original trade as the economy returns to pre pandemic levels.'

(Survey respondent)

'Security needs to look after its welfare of staff.'

(Survey respondent)

3.97. The issue of a potential reduction in the number of sites requiring security in the future was also noted by a number of respondents (n=31). As the pandemic has led to a significant increase in remote working, it was highlighted that this may result in a shift in organisations occupying less building space in future; and similarly, the impact on some sectors (such as the Night Time Economy, Events industry and non-essential Retail) may mean business closures and result in less available work for security companies and officers. For example:

'Greater remote working will reduce the need for a physical security presence, compared to pre-pandemic numbers, at key business sites and assets locations.'

(Survey respondent)

'I think the fact the pubs, clubs or events such as Glastonbury already cancelled for 2021 will have a major impact on these sectors.'

(Survey respondent)

'Reduction of opportunity to grow with potentially many empty properties being remote monitored.'

(Survey respondent)

3.98. Other issues relating to the future development of security included:

- The challenges of the work itself (n=19), such as working within new requirements and guidelines as sectors re-open post lockdown (e.g., managing the number of people in spaces, maintaining social distancing, and potential health risks to officers and violence towards officers);
- The challenge of adjusting as circumstances continue to change (n=16), such as reduction in staff numbers; finding the right balance between technology and personnel; and adapting to a greater focus on cyber threats and business continuity concerns;

- Retaining a focus on the value of security (n=14), something which may be forgotten as businesses return to normal and other issues dominate;
- The potential difficulty of investing in staff, particularly training (n=14). It was noted that a lack of funding for security and other priorities may result in difficulties in maintaining and developing the level of training for officers.

3.99. Conversely, survey respondents were also invited to comment (in their own words) on the main opportunities (if any) resulting from the pandemic to be explored (n=222 did so).

3.100. The opportunity most commonly mentioned (n=60) was in relation to the demand for and capabilities of technology. Respondents noted that the need for reduced human contact and the increase in remote ways of working lend themselves to greater use of security related technology, such as access control, remote monitoring, data and analytics, AI, thermal and touchless. It was also noted that to provide security within shrinking budgets, security may need to use technology innovatively. For example:

> *'Expand in ways using technology we have not used prior.'*
>
> *(Survey respondent)*

> *'Greater use of technology and innovation that will help to shape a more sustainable business model not so commoditised.'*
>
> *(Survey respondent)*

> *'Temperature and improve access control solutions.'*
>
> *(Survey respondent)*

> *'There are opportunities for remote technology monitoring.'*
>
> *(Survey respondent)*

> *'Use of new technology; new ways of working to improve performance.'*
>
> *(Survey respondent)*

3.101. A number of respondents (n=30) highlighted opportunities where there would be greater demand for security than previously. Examples included the increase in vacant buildings (prompting demand for keyholding, remote monitoring and physical patrols), and the emergence of new sectors (or at least they were new to some security businesses such as officers in the night time economy shifting to essential retail):

> *'More key holder security and building checks, as buildings left empty, manned guarding placed on site for asset protection and prevention of squatters.'*
>
> *(Survey respondent)*

'Opportunity to provide key holding and remote security surveillance.'

(Survey respondent)

3.102. A number of respondents (n=24) suggested increased opportunities and benefits of working in a more holistic way, integrating services to better address overall security, or to carry out functions more efficiently. Mostly, references were made to integrating personnel with technology, and/or physical security with cyber security:

'Blended services technology and physical security, cross over training for officers to supply a greater range of services that include other roles such as traffic management and health and safety.'

(Survey respondent)

'Bigger emphasis on cyber and physical security collaboration. Better blended approach to key issues.'

(Survey respondent)

'Bring together Cyber and physical security + crisis management + ESH (integrated/holistic approach)'

(Survey respondent)

'Greater joint working between physical and technology.'

(Survey respondent)

'Interaction with cyber, vetting, access, monitoring etc to deliver a complete security solution to the identified risks presented.'

(Survey respondent)

'More integrated systems that can be managed and monitored by a small number of security staff.'

(Survey respondent)

3.103. A number of respondents (n=22) suggested there were opportunities in relation to training. Some noted additional types of training that were now more relevant (such as mental health awareness, first aid, and communication training). Other noted more generally the need to offer specialised training in order to up-skill officers. Some illustrative examples include:

'More first-aid qualified guards.'

(Survey respondent)

'On-line learning and skills updates.'

(Survey respondent)

'To up-skill those in the profession.'

(Survey respondent)

'Training to a more professional level.'

(Survey respondent)

3.104. A number of respondents (n=21) felt there were new opportunities related to the capabilities that security professionals had demonstrated or obtained during the pandemic. Respondents indicated that the range of skills demonstrated by officers, and their ability to take on additional

tasks relating to changing needs was something to be explored further. For example:

> *'Security experts have shown they are excellent in crisis response and planning and therefore are listened to more - hopefully this will factor into future decision making on security spend, pay rates, overall status of the security teams etc.'*
>
> *(Survey respondent)*

> *'They should be the main go-to people when an emergency occurs or response is required. Combining security with other functions e.g. receptionist who is also security trained.'*
>
> *(Survey respondent)*

> *'The willingness of staff to undertake whatever is required. But, this will be undersold by security providers and undervalued by clients.'*
>
> *(Survey respondent)*

> *'Taking over new functions related to the prevention of diseases.'*
>
> *(Survey respondent)*

> *'Skills obtained and increase in knowledge having been in and dealt with situations.'*
>
> *(Survey respondent)*

> *'Greater multi skilling of the workforce, and being valued for the multi faceted nature of tasks being undertaken.'*
>
> *(Survey respondent)*

Summary

3.105. It was notable that characteristics which we may have expected to impact on views, such as the role of the respondents (i.e. whether they are a security supplier or a buyer/customer or an operative) and whether their organisation provided security in an 'essential' sector during the pandemic, in fact very rarely correlated to how respondents answered. More often, there was correlation across perception questions – those that were positive in one way (such as that security would emerge in a stronger position post pandemic) were also likely to be positive in other ways. This would suggest that overall views on the impacts of the pandemic are influenced by a more complex interaction of factors and experiences than the broad type of work undertaken during the pandemic.

3.106. Generally speaking, the survey responses are indicative of a sector that believes it has played an important role during the pandemic, and that this may improve perceptions of physical security and in some cases the status of security professionals. Some positives that can be taken forward were highlighted and there was indication that demand for physical security would remain - particularly those types that reflect

new realities and ways of working post pandemic. However, this is tempered against the findings that security is not the only function that has played a prominent role, that some sectors have suffered significant blows and that there are concerns about how the financial impacts of the pandemic will influence the level and quality of physical security that can be maintained going forward. It was also clear that there will be little opportunity for the security sector to 'relax' post pandemic, as many different types of threats and issues were considered likely to increase in prominence or prevalence post pandemic. In short, it seems the sector may emerge with new capabilities and confidence in the skills and tools possessed, but with significant challenges to address, and against a backdrop of financial and other uncertainties.

Section 4. Experiences of Covid-19: lessons from one-to-one interviews

Introduction

4.1. As part of the research one-to-one interviews were conducted with 39 security professionals, facilitating the opportunity to explore some issues in more detail. We spoke to individuals from a range of organisations, sectors, and roles, including some that had worked in 'essential' sectors and some that had worked on the 'frontline' during the pandemic. The interviews were revealing. This section reports on the findings. We start by looking at the changes in role necessitated by the pandemic and the extent to which the sector could have been seen to be ready for a crisis. We then move on to consider the key challenges faced by the sector, and then the key factors that determined whether the reaction was a good one. Any discussion needs to take account of the skillsets that have been developed and this precedes an important insight into the range of opportunities that evolved from working during Covid-19, and then the shortcomings that were shown up and there were plenty of both. We end with consideration of the lessons learnt.

Role changes, readiness and the pandemic

4.2. Some respondents who worked say in the events sector or offering consultancy services to other areas rendered largely inactive because of the pandemic, found themselves without work. Others saw their role expand and/or they were given more responsibility. Examples included: managing social distancing requirements, temperature checking and enforcing mask wearing or queue management etc. Other more strategic roles included managing staff, either internally, or for clients (which included keeping them informed of new requirements and how it impacted them); developing new policies and procedures; training and awareness raising amongst key groups; managing the purchase and use of PPE; focusing on conducting risk (and health and safety) assessments (which were more frequent and built on Covid-19 related requirements); managing travel (given that more limited public transport hindered people getting to and from work, while travel away on business had obvious added dangers); protecting buildings that were empty rather than occupied (which sometimes required a different approach), or construction sites that still retained expensive machinery; managing staff changes, which sometimes meant coping with less staff (e.g. in airports) and sometimes in security speedily deploying more to needy environments (e.g. retail and healthcare); being involved in crisis management, and advising on the different elements of business continuity.

4.3. One consultant explained having to learn new ways of conducting risk assessments without visiting sites by using local staff to conduct work under very specific guidance, by taking photographs and using videos, and reporting back, and relying on prior knowledge:

> *Most of the places I have been to before, so if there are questions I can ask for pictures and I have found it is all possible to do remotely, and we will continue in that mode until the end of the year at least. In one area I had not been to and the accountant there talked me through it. We did it.*
>
> *(Security consultant)*

4.4. The conferring of 'essential' worker status was sometimes considered important; for example, it eased travel to and from work and rendered site visits by managers easier. One interviewee from an international corporate noted that because security staff working in the US were paid more to work in what was now a riskier environment, their UK colleagues were treated the same and 'essential' worker status helped the justification for this. All this said, some interviewees felt that beyond generating a positive perception that security mattered, the 'essential' status offered little practical advantage:

> *I agree it was a status thing, that key worker identified you as critical and others recognise that, but there was not much benefit beyond that.*
>
> *(Representative Government agency)*

4.5. Organisations displayed a 'mixed bag' of readiness to cope with the demands of the pandemic. Some felt that they were as ready as was realistic given this was something new. Certainly, if readiness was to be judged by adapting quickly and effectively, then the general view was that security had been ready:

> *For the most part security teams on ground really proved themselves – security were prepared as best you can be … good collaboration (with competitors) to mobilise at speed on behalf of the government (and we) made a good account of ourselves.*
>
> *(Senior manager, Security Supplier)*

> *I've had a few compliments over the months –thanking us for being there and working the frontline in shops and stuff. Aye … you're standing there in all weathers, rain and wind and all that. You get a lot of people appreciating you.*
>
> *(Security officer)*

> *Here security is still viewed as lock doors and kick out bad guys. That or the lazy security guard. They kind of make fun of guards and I am hoping we will see a more positive view now. How they have helped to police health*

and safety is important. Maybe a better perception will result.

(VP operations, security supplier)

4.6. That said, there were a number of key challenges that had to be managed.

Key challenges faced

4.7. It is important to be aware of a general context here; security personnel were not alone in working largely in unknown territory. It was noted that the speed with which '*Covid-19 went from being a Chinese virus to a global pandemic*' took many by surprise and posed real life challenges. As one respondent said, '*it was just a shock*', and another '*it kind of came out of the blue*', and it was a case of '*learning as we go*'. While the challenges varied, there are five key issues that featured prominently albeit not all are the types that are specific to the security sector.

4.8. The first was the need to manage remotely, which often required new methods of engaging, reporting back, following up and checking what was being carried out, was fit for purpose. One hospital security manager noted that security installers were often reluctant to come on site (where they were allowed) to update or improve security systems, which hindered progress, or large numbers of (supply) staff had been furloughed which presented challenges.

4.9. The second issue is that in being on the frontline raised concerns about staff safety and it meant managing people who were anxious or otherwise agitated and sometimes aggressive. It was noted that some staff were concerned about working (and travelling to and from work), but concerns were especially grave when work meant interacting with members of the public, not least in environments – such as at testing centres – which by definition were of higher risk:

> *Often we have people presenting who are symptomatic, are nervous about a test, heard that it's an invasive procedure receiving the test, (so it is about) allaying people's fears, directing them properly … Some are young. Some have never worked in security before … They are novices in security, so keeping on top of that, making sure H&S protocols are observed. I find that challenging.*
>
> *(Site lead, coronavirus testing station)*

4.10. There were many references to the difficulties for security personnel in having to manage an agitated public. Some pointed to having to deal with aggressive members of the public which took many forms:

Some had protestors filming, some had people trying to use a vehicle as a weapon, saw people posing as couriers to try and pick up testing kits (black market), trying to steal PPE supplies … we were able to recognise some of the patterns and give heads up on trends we were seeing and also on that call a rep from CPNI and NACSO –so true collaborative piece of work.

(Senior manager, Security Supplier)

A wee bit more aggression. I was working in (name) supermarket before the testing centres. Quite a bit of abuse because they had to queue up – I'm used to that though. But (it occurred) more than previously.

(Frontline worker, Security supplier)

We're getting a lot of 'anti' people – anti-vaxxers – people who don't want to wear a mask … I had to remove someone for not wearing a mask … We are used to dealing with relatives that have lost people but they had been able to see them, when they can't see them and the frustration of not being allowed to come in, you get them still turning up and then the confrontation, upset, angry.

(Healthcare Security Officer)

4.11. For some security staff and companies there was a concern, and a third issue here, about whether they would be paid or retain their jobs, either at all or in the role they were accustomed to:

Some got really stressed with worry about losing jobs. Budgets have been affected quite badly … so worries about job losses and job descriptions changing.

(Security officer)

Some colleagues lost their jobs overnight – including those at strategic level – they were seen as overheads – do they deliver anything if threat has changed? You see good people losing their jobs.

(Hotel security manager)

4.12. A fourth challenge was having to scale up supply speedily. In some cases, this was a blessing, staff who could not say work in airports could be redeployed to retail, but sometimes additional new staff were needed. Invariably this meant bringing other suppliers on board and only some companies had agreements in place for this already; fewer still had agreements in place that provided for the volume of staff required. But sub-contracting posed other challenges and not least when it has to be undertaken speedily as the following quote so poignantly illustrates:

It was done on a huge scale and logistically impossible. No security company can scale up that quick, the only way they could supply the labour needed was to sub contract and to sub-contract and to sub-contract. It was

> *ridiculous how many security companies there were involved. We worked to the main supplier, but often five companies supplied staff to the site. When you did that standards drop, the money people get is lower as you keep sub-contracting, so the standards are lower. Also managing those who don't work for you and don't get paid much, well, it was a challenge.*
>
> *(Manager, security supplier)*

4.13. A fifth and one of the biggest challenges, certainly in the early days of the pandemic, stemmed from continually changing Government guidance as world leaders adapted to the evolution of the pandemic. Largely because of this, organisations were slow to make decisions, or changed decisions quickly, meaning security departments and security staff regularly worked in an uncertain environment, on an already anxious frontline, continually making assessments about what policies were likely to evolve next:

> *More for me was the concern about client indecisiveness, we can roll with them, but they were unprepared, even when we asked them for plans early on, they were slow. They just had not prepared. They had had conversations and not looked at the details. A lot of other suppliers had not done anything either. It was difficult for us.*
>
> *(Chairman, security supplier)*

Factors that determined whether the reaction was a good one

4.14. There were four key factors that determined whether the response was a good one. The first was the quality of the business continuity plans already in place. For some, these were developed and practiced. Respondents noted that part of the difficulties they faced was that even a seemingly good business continuity plan could be dominated by a focus on cyber risks or terrorism, while the pandemic was a different challenge altogether. One respondent with experience in this area noted that where pandemics had been considered, this had been on a much less 'worst-case scenario'; in other words not one that was so enduring. Moreover, any discussion to relocate teams to home working would have been opposed and in the Finance Sector '*wouldn't get regulator sign off*', yet the '*vast majority have done it now*.'

4.15. Others though found that there were gaps, sometimes the business continuity plan generally was not good enough, and sometimes specifically with regards to Covid-19. Certainly, as far as the latter was concerned there was a feeling that this was new, impacting on an unprecedented scale, and for an extended period of time that was not predicted, there was a sense it was reasonable not to have predicted it and been ready. Indeed, some respondents felt that since no-one was ready, security was comparatively better off because it had faced other challenges in recent times and adapted well (e.g. terrorist incidents)

and/or crises was something security was good at. Others though were more self-critical. There was a sense that given the sector had faced dealing with other diseases; swine flu, bird flu, SARS, Ebola – it should have been more aware of risks. One respondent felt though that it had led to a false sense of security since their impact had generally not been as bad as might have been feared. Some typical comments here included:

> *A lot of people had pandemic in their minds, but didn't imagine one like this. I remember someone once said to be a good risk manager, you need a good imagination. Some of us, and I include myself in this, should have used our imagination a bit more.*
>
> *(Head of Operations, Security supplier)*

> *Every single BC plan was the Emperor's new clothes, it was never tested, it was abstract.*
>
> *(Enterprise Risk, Security supplier)*

> *Ours is very much a people business and as a people business we are dependent on good relationships and it is harder to do when you are not in the same room. That translates to other areas of the business, and how you work with clients. How you support staff and how you bring new people in and get the company culture to them. It is harder for new people.*
>
> *(Managing Director, security supplier (manned guarding))*

4.16. A second factor related to the use of technology and equipment. Some organisations were more advanced in what they already had, could buy, or had access to, and the extent to which they were able to use that well contributed to their level of readiness. The issue of technology and equipment featured in many ways: in being able to speedily support working from home; linked to this, in having forms of virtual communications which all had access to and could use; in being able to deploy quickly and effectively on the frontline, for example to test temperatures; in having access to appropriate PPE to protect workers, including security personnel:

> *This hit me in December 2019 with the teams in China, and I would say security was ready but technology was not ready, not in the supply chain. The ramping up of manpower was there, but what we struggled with was the response to get technology to the market in those first few weeks, such as temperature checking equipment, and there was a bit of panic. There was a delay. Then you were flooded as technology caught up.*
>
> *(Global security director, Security Supplier)*

4.17. One overseas interviewee noted how CCTV was harnessed to help police the underground and railways with regards to compliance with Covid-19 rules. It was effective in some ways; it could of course identify

whether people were standing together, but not whether they were permitted to do so because they were family members for example.

4.18. A third factor relates to the general competence of the organisation. There were a number of factors that differentiated those who were felt likely to perform better post the pandemic and they might best be characterised as those with more service lines; those who embrace technology and combine that with manpower; those who are focussed on staff well-being and invest in training; those with a good cash flow; those active in growth sectors and are less focused on service lines that have been hard hit (reception and mailroom duties were mentioned as examples here); and there is never a substitute for being a well-run business. Indeed, some felt that those who were efficient and competent before the pandemic, were generally more effective during it, and some felt that only those competent beforehand could be competent afterwards. Although it was noted that the pandemic was such an unusual event and therefore this did not necessarily always hold true. Others felt that competence related to the extent to which security was supported by the organisation/client:

> *It depends on the client. Where a client has a positive view of the contribution of security already, this has enhanced it and we have been entrusted with even more responsibility and activity.*
>
> *(MD, Security supplier)*

4.19. A fourth factor here was the context in which people worked. As noted, the pandemic caused redundancies, staff were furloughed, and some sectors stopped working altogether. The general view from respondents was that organisations they were familiar with did handle this well, but it was challenging. For example, there was a need to: redeploy staff (where possible) and manage their expectations and concerns; decide who to put on furlough and who not; allocate resources fairly and efficiently; train frontline workers in managing new responsibilities (like ensuring social distancing, managing queues, cleaning radios at shift changeover times); then there was the issue of having to write new Standard Operating Procedures, often from scratch and managing staff absences from illness, or having to self-isolate. One interviewee, who deployed staff across many client sites (including internationally), outlined the challenges of knowing who was where on a day-by-day basis. In short, organisations had to rethink their entire approach, even the basics:

> *Understanding the equipment and the terminology and also the working environment are all important, and even for example, the impact of air conditioning … you can't take the temperature of someone if they are in an air conditioned car … There was hand held temperature checking and remote temperature checking and not getting within two metres … we had to ensure we understood any risks to how security officers were doing*

checks, how to collect a visitor's badge which could be contaminated, the same with PPE being returned. Important this and really we learnt as they did.

(Global security director, Security Supplier)

Thinking about skillsets

4.20. There was a general recognition that security personnel were faced with many new challenges and this required the adoption of new skills, accompanied in some cases by the need for more training, more awareness, and new procedures to accompany new tasks.

4.21. For those on the frontline there was generally a need to engage with people more (and not everyone was accustomed to that) and most respondents pointed out the advantages of learning new skills, an issue which many in security emphasise as being important. This meant interacting with others more and offering customer service. One interviewee felt that this increased engagement would help staff deter those attempting hostile reconnaissance, if it encouraged staff to be more able and willing to approach people.

4.22. That said, and as noted above, approaching people in a pandemic carried risks. They need to be prepared and they needed to feel comfortable. There was a lot of discussion about managing people's mental health because some roles/demands at work were new and stressful; there were often safety risks, specifically of contracting Covid-19; and because working contexts changed. On this latter point, some staff faced a different challenge; rather than being on the frontline they suddenly found themselves working in empty, or near empty buildings:

Dealing with boredom, dealing with downtime. We've been able to do more on site – online training. Comms has been a key part. We've worked to increase and improve communication – be that visits from management, using (Microsoft) Teams, email – newsletters, updates or briefings for advice on dealing with Covid.

(MD, Security supplier)

If someone is unhappy and not getting support they become disgruntled and they have access to company data via homeworking and all this with limited oversight. That cocktail may lead to insider action.

(Advisor, Government sector)

4.23. As noted above, the need to manage conflict was seen as important. Here formal training could be given, and where this occurred it was invariably on-line. But a number of respondents pointed out the need to be good at communicating and keeping all staff abreast of what was going on and supporting them, specifically when trying to meet the needs of different personnel. Meanwhile, there was the concern of

managing the risk of distraction from regular duties, where these were being retained.

The opportunities from Covid-19

4.24. Interviewees noted a range of potential opportunities emanating from the pandemic experience, including new areas of business, new service lines, and new clients. Some had needed to shift their focus away from areas that were inactive to those where more security was required. So new opportunities had opened up and these took different forms. Some had had to work with other security companies, enabling a new rapport and reasoned that too could generate other collaborations post pandemic. Some security suppliers responded to the need to hire more staff quickly by approaching companies that were releasing staff and offering to engage them. This too they considered offered potential, albeit more in building up a rapport with the business concerned, than in it providing a model that could be routinely replicated for recruits. Another interviewee could see long lasting benefits from a forced role change brought about by the pandemic. Principally the role involved security officers acting as Safety Ambassadors, advising visitors about the need to wear masks, handing out free masks etc. The emphasis was less the role and more the significance of it:

> *We have worked with other companies and we have done coronavirus testing with them at schools and other places and that has opened up new markets. We may well collaborate with them again, it was one of the best collaborations we have had, another security supplier, we have got on well, and yes, it may continue.*
>
> *(Chairman, security supplier)*

4.25. For those who had performed well - suppliers and internal security teams - being seen to be valuable generated other business benefits:

> *The positives are they are seen now as a more integrated part of a client solution. Where as before [we were] seen as an obstacle for people to get past.*
>
> *(Account manager, Security supplier)*

4.26. Stemming from this, many had identified new ways of working and recognised, as many organisations did, that staff do not necessarily have to be in an office to be effective; if managed well this creates more time to focus on other priorities. As well as enabling a better work/life balance; the sector has gained an awareness of its ability to mobilise quickly at scale (e.g. the new testing centres and Nightingale hospitals); the sector can be effective lobbyists (e.g. achieving 'key worker' status); there is a wider awareness of the greater capability of what security can provide above basic provision; and similarly of the wide variety of services it can provide; it has highlighted how technologies can be used effectively (as well as learning from

ineffective technologies); the development of e-learning; then there is the improved perception of security as a credible career.

4.27. In a different way, one supplier was able to introduce an improved sick pay package and make it generally available, and also a death in service payment, both because of the impetus given by the virus and these will stay in place. Some pointed to benefits in organisations being more prepared to listen to new ideas. One respondent said his company were now much more focussed on staff and their well-being. Others pointed to unity of spirit, this was true within companies, with clients, and in some cases with competitors, especially where they had been required to collaborate. One interview added another benefit:

> *The role of security changed. In the short term … some security managers reached the very top of the organisational structure in an informal way because they were around, they got promoted in a way by their presence, while others were out of the picture, before companies learned to work in an agile way.*
>
> *(Responsible for a group of hotels in the EMEA region)*

4.28. Many pointed to longer-term opportunities that will benefit the security sector for having performed well in the pandemic, although the extent to which this was true varied. Many felt that while security had done well, it was not alone in this. Much depends it seems on the value put on security in the first place. One respondent felt that regulated sectors were generally more positive, while another comment focused on the advantages of providing multiple services which increased importance and recognition. Another stated that '*probably H&S still has the edge*', as well as those involved in business continuity, and many felt that frontline services generally – carers, refuse collectors, cleaners – '*have come off well*' in terms of how they are perceived. However, a number were cautious about the longevity of this status and some felt '*it is already forgotten about*':

> *Memories are short – in two years' time, everyone will try and wipe this year from their memories. Maybe I'm overly cynical. I'm in Business Continuity so I'm supposed to go for the realistic worst scenario. I'd like to think so. Some won't. But overall I'm fairly positive that security will be remembered for doing a good job and the extra work.*
>
> *(Head of Operations, Security supplier)*

> *I'd like to think they won't be forgotten but if we go back to normal – you'll go to a supermarket, the officer will be gone and forgotten … I'd like to think (there will be) a lasting impact but potentially may not be unfortunately … We are recognising people, within security it will. But not the wider public.*
>
> *(Head of security, Security supplier)*

> *I think it will be forgotten, bottom line is (clients are) paying for something you can't see, something*

preventative and (they are likely to) cut out costs if they can't see the benefit.

(Management consultancy to security companies)

Security as an industry or element within a company is not very good at selling itself. We have our guards, we stop people from breaking in. We alert people. We call the police if there is an issue. We make people wear badges. We tell everyone not to leave stuff on their desk. That's what people see that we do. We are not good at selling ourselves to the senior management to say we are not just doing this (we are) saving you money … Unfortunately I can see a lot of security going back to the way it was. Senior management don't see the added value of security in a pandemic or any other situation.

(Security consultant)

4.29. Some felt that the ultimate opportunity both for the sector generally and for their own organisations was to minimise the risk that any good work undertaken during the pandemic would be forgotten. There were various suggestions as to how this could be managed, by reminding stakeholders of the good work and the efficiencies generated by having good security:

We must highlight what we have achieved. In my report I will be saying what we have done and establish our priorities, last year we didn't do a lot of things and I don't want to say covid caused this and covid caused that, I want to explain what we have done, what efficiencies we have made, get that out, also any further efficiencies we are in to, but focus now on what we have achieved, all that we have done. Explain the risks too, especially if we can say, look if you were to be cut back then there is a danger of this.

(Head of security across hospitals)

If management, senior managers in the client company stood up and took more notice of what we raise. Right now any suggestions are emailed and are unnoticed.

(Team lead, pharmaceutical)

I don't think we have sold the story very well, I am not sure security gets out there … I am not sure buyers and end users understand … They don't care really.

(Head of operations, security supplier)

4.30. The general view was that technology was an opportunity that had been enhanced from experiences during the pandemic. One interviewee, from overseas explained how the pandemic had forced a more unified approach to surveillance of transport structures. This has led to greater cooperation, and the plan for moving forward is to harness this for managing other concerns, such as those related to terrorist threats or suspicious activity. In addition, improved camera performance necessitated by the need to identify people, even though

they were wearing face masks, has increased possibilities for security relating to facial recognition:

> *There is a much better option on cameras analytics, we can use the experience of detecting whether people are wearing face masks to help detect fare evasion, fights and other things are being considered now.*
>
> *(Manager of security for trains)*

4.31. As noted above, many saw opportunities to develop services via the use of technologies, while for some, this was inspired by the pandemic. For others, the trend of embracing technologies predates Covid-19 and some felt that a blended approach - of people and technology – still has some way to go to full development. The key here is the potential to link good intelligence, to the risk profile to the solution and to combine these elements effectively. There was no suggestion however, that this was easy. Some pointed to the opportunities for using Artificial Intelligence and machine learning to improve performance. This was presented as work in progress, so too were the use of drones and robots. One supplier who had previously been a buyer had contended that technology in time could largely replace personnel, but more recently had concluded that he had '*changed my mind on that now*' in favour of a more blended approach. Another interviewee saw clients favouring the use of technology compared to physical attendance at nights but considered a physical security presence essential during the day.

4.32. Some noted that not only was technology, and new ways of collating and delivering intelligence improving performance, but also that the pandemic had increased the availability of quality labour available to the sector, especially at more senior levels. Interviewees highlighted that as other industries subsided, security became more attractive as a career choice. In contrast, some noted that the competition for labour at lower levels was more intense than before the pandemic, as people who had previously worked in security or might have considered it as a career option, could find less onerous roles (away from the frontline), that avoided shift work/long hours, and sometimes paid better.

The shortcomings of security

4.33. For the most part the concerns raised by the interviewees tended to feature challenges that existed pre-Covid-19 and were not improved and may even have been exacerbated by the pandemic. The shortcomings identified were set against a context noted above that the good work undertaken throughout would be quickly forgotten and made worse by the '*multiple pulls and pushes*' of factors such as the pandemic, 'Brexit' (in the UK), and job markets changes leading to security cutbacks. One MD on the supplier side noted that clients '*don't want to invest to get the long-term saving, they want to shave bits off to make an instant saving*'. Beyond this five key issues were identified.

4.34. The first main shortcoming groups a range of internal concerns. Some of these were strategic issues, such as the lack of personal contact with some clients which had made some other programmes/investment programmes harder to achieve. One interviewee pointed to '*contract renewals which allows you to build in salary improvements*' that have not occurred, although others noted here the benefits in saving time and effort with tendering. Other issues were operational, so while some pointed to progress on online training many noted a reduction in physical training, that they will need to catch up on. For example, one interviewee noted that supervisor training for career development had '*taken a bit of a back seat*'. Another noted that penetration testing had not been undertaken because personnel were not allowed on site. Likewise, the lack of contact with some staff needed to be managed and there were concerns that mental health issues may only come to the fore later. Similarly, one interviewee noted the concern that people may have been radicalised while being relatively isolated from others, a danger not easy to identify and often comes to notice only when it is too late.

4.35. The second issue related to technology and the vast array of states of readiness to fully maximise its potential; a range of factors were discussed here. Organisational perspectives on technology generally and security specifically played their part; as did the state of legacy systems; and the levels of investments already made. Covid-19 had only sometimes speeded up change. More often it merely set in process changes that had already been agreed, and often, Covid-19 had distracted stakeholders from developing technologies. But there was more to this. One interview from a supplier felt that the technology arm within his company had been less than totally supportive in exploring opportunities during the crisis, '*I could have got them more business if they had put down egos and worked with us*'. One guarding company had identified a weakness in its internal deployment of technology and personnel and had therefore made a senior appointment to rectify this. For some, new investment amounted to no more than buying thermal cameras to check temperatures (and lamented that some suppliers overstated their potential) and PPE (and getting supplies were a challenge especially in the early part of the pandemic). Finally, one other point made frequently about shortcomings in the use of technology is summarised in this quote:

> *When we kicked everyone out to work from home, we paired back the patching and updates so there was a drop in security of the systems, and this has come to the fore as we return.*
>
> *(Enterprise Risk, Security supplier)*

4.36. A third issue related to financial viability. One interviewee working in a state sector organisation noted that the security team had been given a lot of finance during the pandemic, mostly for technology, and worried that this would come back to bite them as there would be demands to

reduce headcount as a result of a desire to curtail spending. Moreover, the use of agency staff had proved successful, further fuelling concern that there would be less need to keep so many security personnel on the books. Others echoed this theme, '*I think the long-term consequences are financial, there will be fewer businesses so fewer clients*', and '*Do you remember the banking crash of 2008? In the following years there was a huge increase in zero-hour contract work*', and '*it may create the feeling, do we need manned guarding?*'

4.37. A fourth issue concerned the security sector relationship with the police. In general, interviewees valued their relationship with the police service and pointed to a 'mutual respect' (especially at senior levels) and a range of joint initiatives such as: working together on operations (e.g. in relation to tackling terrorism) by giving police direct access to case files; developing information sharing agreements; joint initiatives on awareness raising; collaboration on training; and in response to a wide range of offences such as rural crime, financial crime, metal theft, retail crime and terrorism. Some felt that there was an opportunity to do more, much more, proactively helping the police in some routine tasks relieving them to focus on other priorities. That said, despite some clear exceptions, Covid-19 had often not made collaboration easier, it served more as of a distraction for both parties.

4.38. Moreover, some of the traditional impediments to collaboration remain (and also may have been exasperated). This includes the need to be persistent to engage police officers because they were busy; because there is a concern that otherwise '*they won't do anything*'; and because the police can be sceptical of collaborating with private security. Indeed, there was specific mention here about the profit motive or 'the commercial' realities that private companies must make a profit. Certainly, some felt this had not been sufficiently challenged and in two distinct ways. First, in the sector itself remedying its weak points; it lacks 'consistency' and suffers because '*there will always be someone who lets us down who has not been invested in*'. Second, in presenting a better case of its value, as one interviewee said: '*as an industry we are still unclear of the value we can bring*'.

4.39. A fifth issue is the buyer supplier relationship. The economic challenges impacted some and affected approaches to security. One interviewee from a corporate with a global reach felt that relationships with suppliers had been good, but it continued to pay all staff through the crisis and had worked hard at getting the right suppliers not on the lowest price. This is significant because some interviewees from suppliers pointed to what they saw as a lack of realism from some buyers. One company had completed an analysis of the pay rates of six security companies and found a pay spread is £6 an hour difference in one area and lamented the morals of those at the lower end, given the knock-on impacts on officer morale and low quality of service. One supplier lamented the attitude of a client who looked to what he saw as unfairly offloading the redundancy liability (as a consequence of Covid-

19) to the service company (or at least for trying to do so). Even those who topped up furlough pay during the first lockdown did not always in the second. Another challenge noted was getting clients to understand the dangers posed by the virus to security workers on the frontline. A typical comment here included:

> *Some clients aren't being realistic. There are different pay rates at different sites … You can't expect the same service. You will get a professional service. But you get what you pay for.*
>
> *(Senior manager, Security Supplier)*

4.40. One other point here was made by an interviewee that merits consideration. It focussed on the future and a possible concern. During Covid-19 the night-time economy collapsed, and given its nature there was a concern that companies who had found alternatives would stick with them, leaving a gap for less reputable enterprises to step-in; '*there is a danger for us in that the gap is filled by illicit suppliers*'. Finally, for one interviewee, the major shortcoming was simply not having faced anything similar previously:

> *So, appreciating the all-consuming nature and debilitating effects a pandemic can have is hard to appreciate, until you have lived it.*
>
> *(Managing Director, security supplier (manned guarding))*

Learning the lessons

4.41. Most interviewees felt that overall, security had performed well in the crisis. The key to moving forward was to manage the downside and promote the good. Specific lessons learned often focussed on having better business continuity plans, and always being prepared for the exceptional; building lessons learnt into operational practices, and ensuring they are captured; being good at communicating, internally with staff, not least in a crisis but also with other stakeholders; recognising that being good at security always has to be a priority, whether that be internal operations, external partnerships etc, they are always essential but especially when crisis beckons. The pandemic posed many challenges, not just for security of course. However, the very nature of security work gave it a special place, for example: security is usually key to managing crises; security staff are on the frontline and exposed to some of the most troublesome aspects of Covid-19, it is infectious and dangerous, it can kill; in a different way security personnel are amongst the first staff to be lost when there are job cuts to be considered.

4.42. While the pandemic identified some shortcomings, and exacerbated issues that existed beforehand – including with clients and the police - it also generated new opportunities, including new business via new clients, service lines and collaborators, and new credibility reflected for

some in the classifying workers as ‘essential’. In the final section we consider these issues further.

Section 5. Discussion and summary comments

5.1. Overall, the good news is that security professionals have gained more status as a result of the pandemic. There was a strong sense that the sector had been as ready as was reasonable - and half of our survey sample believed the sector would emerge in a stronger position (not least because of concerns about future pandemics); a third that the effect would be neutral, and one in six worse off. Moreover, over a half felt that where the status of security has been enhanced, this will last well into the future, and this was especially true for cyber security professionals, security managers and security officers.

5.2. That said, and this is important, it is also true that security has not necessarily emerged in a comparatively better position. Here the sample made a distinction between believing on the one hand security had performed well, especially those designated 'essential', and on the other hand that those working in the area of crisis/contingency management and risk/health and safety emerged better off.

5.3. The issue centred on a belief that not only is security not valued as much as other functions, but that its good work would soon be forgotten. Again, on the one hand there is a belief that the security sector generally is not good at promoting the good work that it does, not internally, not with clients, not with the public, and not with other stakeholders, such as the police and government. On the other hand, there was a belief that any post pandemic economic hardship could affect the security sector particularly adversely. Just as a characteristic of security is that in a crisis it shines, so it is also true for many that, in harder economic times it is one of the first to witness cutbacks, indeed three quarters of the survey respondents felt that ensuing financial constraints will undermine any progress made. Some felt that as a consequence the 'race to the bottom' in terms of quality of service that companies have worked hard to move away from, may be revived.

5.4. The pull of having performed well, albeit not as well as others, against the push of a crisis, was reflected in a discussion of the opportunities that have been generated, and there are quite a few. New business opportunities were frequently mentioned as some had found new service lines as a direct result of the pandemic, and close to 9 in 10 believed the pandemic had shown that things can be done differently and even better. This was particularly true for personnel and technology. There are two key points here. The first is, that more thought the greater reliance on technology, already apparent pre-crisis, had been hastened during it. Second that the integration of the two was always a challenge. Others pointed to new training opportunities (to meet new demands), and sometimes a need to fill gaps in what had been missed as a result of a focus on the demands of the pandemic and restricted face-to-face contact.

5.5. Although some felt that the pandemic had simplified the security task, in that there was much less crime and ready access to funding, many pointed to a range of challenges. At a strategic level, there was a concern that during the crisis disreputable companies may have entered the market, which would serve to undercut and undermine legitimate business. While some were optimistic that there were new labour pools to recruit from, others feared the reverse; that finding labour would be an issue. These concerns need to be tracked.

5.6. The pandemic itself posed the challenge of having to manage remotely, and many mentioned the difficulty of keeping up with changing official guidance and the knock-on implications of people making decisions slowly and changing them quickly, at least in the early days. Other challenges related to being on the frontline and the risks that were associated with that. Clearly the dangers of catching Covid-19, managing distressed people including a sometimes agitated and aggressive public, persuading clients and others of the dangers, and getting support, have been significant.

5.7. While for some there was a challenge in having to scale up quickly because of the demand for work, and for others, the risk of redundancy and managing this when security work disappeared (such as at airports). Some challenges are on-going. Prime amongst these are managing the implications of staff working from home and in isolation. The mental health implications are largely unknown, the dangers some might have been radicalised have not been realised yet, the abuse of (home) systems by rogue staff or offenders, may yet emerge and this could be serious. Over three quarters of survey respondents viewed an increase in online crime as a distinct risk, over six in ten managing data security and privacy issues, and nearly seven in ten the more general challenge of managing a remote (online) working environment.

5.8. The sample was clear that there are distinct factors that governed how well security performed during the crisis. An interesting context was set here, alluded to above, that by and large interviewees did not think that security could be blamed for not predicting the crisis. That it impacted on an unprecedented scale; for an extended period of time; and was not anticipated by any other groups, was warm comfort. Only some organisations had business continuity plans that were fit-for-purpose, and that was an issue. Even some that were considered good had an over focus on threats such as cyber crime, but in many cases, they were just not good at all, that is where they existed at all.

5.9. Indeed, and more generally, those who were efficient and competent before the pandemic were seen to be more effective during it. Linked to this was the skill of managing effectively during a period of change; scaling up or down speedily as the crisis evolved; managing staff and clients and other stakeholders including senior ones (who were often facing distinct challenges of their own); developing new procedures and

communicating them, in fact, being good at communication was rated highly; generating new business opportunities while retaining existing relationships all differentiated the good from the less good.

5.10. Because Covid-19 placed an emphasis on working remotely and the use of virtual communications, being good with technology and being able to deploy/use it speedily were factors distinguishing those who reacted well, from those that did not. Some invested in new technologies (touchless types and measuring temperatures were frequently mentioned) and that was an advantage.

5.11. Perhaps the ultimate takeaway from this research is that the security sector has an opportunity. In some countries its workers have been officially defined as 'essential', it has met demanding requirements head on and seemingly performed well. It will be judged on how well it can harness these good points. It will need to do so in a new tricky world where there may be cutbacks and a different type of upheaval as the working environment adjusts to new modes of operation. We know security can be flexible, but can it communicate its value and the positive difference it has made and can continue to make to diverse audiences, which often don't see security as a priority? Historically, security professionals have not been good at this, it's a bad thing to be bad at. That said, it can be addressed if the unified will is there to achieve it. Let's hope it is.

Appendix 1. Methodology and Sample

The approach

The study involved a review of available sources on the challenges posed by the Covid-19 pandemic for private physical security and also the changes in function and demand that have emerged so far. These were used to give context to the work of security during the pandemic and to help identify key issues and themes to explore in the consultation with security professionals.

The review of the literature was followed by two main approaches: 1) an online survey on security professional views of the impact of the pandemic on the security sector; and 2) extensive discussions including semi-structured interviews with a range of security professionals to gain a more in-depth understanding of the topic.

Survey

The survey examined the views of security professionals on a number of key themes: whether the pandemic has changed the perception and status of security; how well security has performed; the likely threats faced by security professionals post pandemic; the likely demand for security post pandemic; and the difficulties and opportunities to prepare for.

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 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 associations; 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. 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 13th January to 12th February 2021.

A total of 500 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

The approach in this work was to engage with security professionals from a range of roles and sectors that may be able to add insight. We engaged both

informally and formally with a wide range of professionals in conversation about the issues covered in this report. This included during our series of webinars on security.[78] 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 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 39 professionals.

[78] Please see the OSPAs Thought Leadership Webinars – recordings are available here: https://www.youtube.com/channel/UC3ZsgjtdPBgJzs5yVzT-Lgw/videos

Appendix 2. Additional Data Tables

Table 2: Sector that respondents provide security in (respondents could tick all that apply) (n=500)

Sector	N	%
Retail	157	31
Property	135	27
Public Admin, Other Services, Government	126	25
Health	114	23
Manufacturing	111	22
Leisure & the Night Time Economy	109	22
Transport	92	18
Education	91	18
Production	85	17
Construction	81	16
Energy	79	16
Finance	77	15
Hotel & Catering	66	13
Post & Telecommunications	48	10
Mining, Quarrying & Utilities	43	9
ICT	37	7
Motor Trades	35	7
Wholesale	35	7
Agriculture	28	6

Table 3: Country where the respondent conducts the majority of their work (where they are based) (n=493)

Country	N	%
UK	352	71.4
Canada	20	4.1
USA	16	3.2
South Africa	10	2
Kenya	8	1.6
Nigeria	8	1.6

Belgium	6	1.2
Germany	6	1.2
India	6	1.2
China	4	0.8
Iraq	4	0.8
Russian Federation	4	0.8
Australia	3	0.6
Ireland	3	0.6
Mexico	3	0.6
United Arab Emirates	3	0.6
Austria	2	0.4
Finland	2	0.4
Malaysia	2	0.4
Norway	2	0.4
Pakistan	2	0.4
Singapore	2	0.4
Spain	2	0.4
Switzerland	2	0.4
Bhutan	1	0.2
Botswana	1	0.2
Egypt	1	0.2
Greece	1	0.2
Iceland	1	0.2
Indonesia	1	0.2
Japan	1	0.2
Liberia	1	0.2
Lithuania	1	0.2
Qatar	1	0.2
Saudi Arabia	1	0.2
Slovakia	1	0.2
Somalia	1	0.2
South Sudan	1	0.2
Sweden	1	0.2
Thailand	1	0.2

Trinidad and Tobago	1	0.2
Turkey	1	0.2
Ukraine	1	0.2
Zambia	1	0.2
Zimbabwe	1	0.2

Table 4: Belief that perception of security amongst key groups would be more positive, by perception of how well security performed compared to others during the pandemic

Indicate this group will have a more positive perception of security post pandemic	Of those that thought security performed better than others	Of those that thought security performed the same as others	Of those that thought security performed worse than others
The Board	57%	44%	22%
Buyers of security	60%	50%	36%
Senior Managers (non security)	55%	39%	36%
Other corporate colleagues	49%	35%	25%
The general public	40%	35%	32%
Police/law enforcement	55%	43%	43%
Government	48%	42%	39%
Job hunters	42%	27%	14%

Table 5: Belief that perception of security amongst key groups would be more positive, by perception of how security would emerge from the pandemic

Indicate this group will have a more positive perception of security post pandemic	Of those that thought security would emerge from the pandemic stronger	Of those that thought security would emerge from the pandemic the same	Of those that thought security would emerge from the pandemic weaker
The Board	71%	35%	27%
Buyers of security	79%	39%	29%
Senior Managers (non security)	65%	37%	32%

Other corporate colleagues	60%	33%	25%
The general public	53%	22%	20%
Police/law enforcement	64%	41%	41%
Government	63%	35%	20%
Job hunters	51%	20%	27%

Table 6: Belief that the status of security professionals will be higher post pandemic, by perception of how well security performed compared to others during the pandemic

Indicate these professionals will have a higher status post pandemic	**Of those that thought security performed better than others**	**Of those that thought security performed the same as others**	**Of those that thought security performed worse than others**
Security managers	53%	54%	32%
Security officers	52%	47%	28%
Cyber security professionals	54%	61%	41%
Installers/integrators	30%	31%	17%
(Independent) security consultants	34%	34%	41%
Other security contractors	27%	24%	14%

Table 7: Belief that the status of security professionals will be higher post pandemic, by perception of how security would emerge from the pandemic

Indicate these professionals will have a higher status post pandemic	**Of those that thought security would emerge from the pandemic stronger**	**Of those that thought security would emerge from the pandemic the same**	**Of those that thought security would emerge from the pandemic weaker**
Security managers	65%	36%	38%
Security officers	64%	34%	29%
Cyber security professionals	56%	47%	59%
Installers/integrators	34%	22%	22%

(Independent) security consultants	38%	24%	37%
Other security contractors	32%	13%	19%

Table 8: Agreement with statements about how well security has performed in the pandemic, by perception of how well security performed compared to others during the pandemic

Agree or strongly agree with statement	**Of those that thought security performed better than others**	**Of those that thought security performed the same as others**	**Of those that thought security performed worse than others**
Overall security has performed well in the crisis	92%	71%	57%
Fear of future pandemics will ensure security retains a greater priority than it previously held	65%	50%	40%
Security professionals have developed new skill sets during the crisis that will be invaluable going forward	81%	61%	60%
Generally speaking if/where the status of physical security has been enhanced, this will last well into the future	59%	51%	27%
There are other service functions that stood out more for their achievements than security did during the pandemic	53%	57%	70%
Among physical security there has	40%	47%	63%

been a failure to explore partnership approaches in the response to the pandemic			
The need to win contracts and cut costs post pandemic will exacerbate the 'race to the bottom' (sacrificing quality for a low price)	57%	57%	63%

Table 9: Perception that the prevalence of crime and other key issues would increase post pandemic, by perception of how security would emerge from the pandemic

Indicate these issues will increase in prevalence/focus post pandemic	**Of those that thought security would emerge from the pandemic stronger**	**Of those that thought security would emerge from the pandemic the same**	**Of those that thought security would emerge from the pandemic weaker**
Physical theft/burglary	60%	40%	71%
Online crime	80%	69%	87%
Assaults and threats towards staff	57%	54%	71%
Insider fraud	45%	33%	51%
External fraud	57%	41%	61%
Anti-social behaviour/nuisance	71%	64%	80%
Managing risks in the remote (online) working environment	71%	62%	56%
Managing the mental health of workers across organisations	84%	71%	70%
Managing the mental health of those involved in	84%	58%	58%

security			
Managing data security and policy	70%	52%	64%

Table 10: Perception that key trends will increase post pandemic, by perception of how security would emerge from the pandemic

Indicate these issues will increase in prevalence/focus post pandemic	**Of those that thought security would emerge from the pandemic stronger**	**Of those that thought security would emerge from the pandemic the same**	**Of those that thought security would emerge from the pandemic weaker**
Use of touchless technology	93%	80%	85%
Use of health related technology (such as temperature screening)	85%	77%	80%
Converging physical security and cyber security	77%	65%	61%
The use of data and analytics	85%	74%	76%
The use of machine learning and AI	83%	67%	71%

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.

About the SRI

The Security Research Initiative (SRI) started 18 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

Professor Martin Gill is a criminologist and Director of Perpetuity Research which started life as a spin out company from the University of Leicester. He holds honorary/visiting Chairs at the Universities of Leicester and London. Martin has been actively involved in a range of studies relating to different aspects of security, private policing and business crime on topics including: organised crime and fraud; why offenders offend; the (in)effectiveness of different security measures; and the scope of security management. 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 and is currently working on the third 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 manages 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.

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

