The role of security in influencing the budget: the holy grail?

Security Research Initiative (SRI)

Professor Martin Gill
Charlotte Howell
Janice Goldstraw-White
Josephine Ramm

July 2022

CONFIDENTIAL

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 and Sarah Cork (Bidvest Noonan), Mick Tabori and Joachim Ritter (Interr), 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); IFPO UK & Ireland (especially Mike Hurst); IPSA (especially Simon Pears); the Security Institute (especially Rick Mounfield); 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).

In establishing an understanding of the key issues we conducted a range of exploratory interviews and we are grateful for all those who took part, including international authors on security, Brian Allen and Rachelle Loyear.

We would also like to thank those who supported the research by promoting the survey among their networks: James Moore (IFSEC Global), Matthew Bull (International Security Journal), Richard Jenkins and Dianne Gettinby (NSI), Chuck Andrews (Friends of Chuck). 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 Geoff Zeidler for comments on a draft of the survey questions.

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

SRI Members

Executive Summary

The aim of the research was to explore the extent to which security managers are able to influence the security budget, whether and why this matters, and how greater influence can be attained. It is based on the views of security professionals from both in-house and contract positions (predominantly those currently in a 'security manager' type role) collected via an online survey and through one to one interviews.

Key findings from the survey

- 76% agreed that being able to influence the budget is key to delivering good security.
- 67% believed that the buying process lacks sufficient input from security experts.
- 46% agreed or strongly agreed that the more powerful procurement professionals are the less likely it is the client will allocate an appropriate budget for security.
- Influence over the budget was considered important for several reasons including: giving status to security in discussions with other departments; enabling security advice and proposals to commonly be listened to; and being able to direct the allocation of resources using relevant expertise.
- A lack of influence meant that security managers could not: purchase basic and essential resources; could not plan effectively; and resulted in security decisions being made by non-security experts.

Experiences of those currently in a 'security manager' role

- 51% had a relatively high level of influence on the budget; of which 28% were 'responsible'; 23% considered themselves 'accountable'; meanwhile 21% had very limited involvement; of which 11% were merely 'informed' of the budget and 10% were 'not involved'.
- Predictably influence increased with seniority and with those with global responsibilities.
- 46% of security managers/directors thought that their current budget was 'insufficient'. Less thought that it was 'sufficient' (42%)
- Unsurprisingly, those with the highest levels of influence over the budget were the least likely to view it to be insufficient.
- Reasons for the budget being considered less than required included: the budget allocated did not reflect the risks faced; and did not cover key areas such as training, travel, basic equipment, contingencies; teams were understaffed; rising costs not covered; and being asked to provide more for less.

Factors influencing the budget

- The chances of being allocated an appropriate budget was – according to the sample – improved if: the security function was seen as core to business (86%); an organisation understands its security threats and

risks (85%); the security team has a high status (83%); operations take place in regulated sectors (67%); or there is a statutory requirement on clients to have a minimum standard of security (62%).
- 46% agreed or strongly agreed that the higher the reputation of the security supplier, the more likely it is that the client will allocate an appropriate budget for security.

Factors that influence how effective security is

- Only 14% believed that a reduction in spend was an indication that security is ineffective.
- 32% believed that excellent relationships between clients and suppliers are rare – but almost half (47%) disagreed that was the case.
- Over two thirds (68%) agreed that a nominated board member with responsibility for security improves security effectiveness (if the Board member is able and engaged that is).
- 58% believed that security personnel generally do not sell the benefits of security, although this view was less prevalent among current 'security managers' that had a high level of influence over the budget.
- 48% agreed that Enterprise Security Risk Management (ESRM) is the future of good security. Notably, few disagreed (7%) but nearly two fifths (37%) gave a neutral response.

Similarities between in-house and contracted security managers

- 60% felt a good security manager working for a security supplier would generally adapt well to being an in-house corporate security manager, whereas 45% agreed a good in-house manager would adapt well to a supplier company.
- 20% believed that in-house security managers see themselves as 'budding CEOs'.

Factors affecting the procurement of security

- Close to three fifths (58%) agreed that clients' buying decision are guided more by procurement professionals than security professionals. Contract managers in particular thought so, as did 'security managers' with less influence on the budget.
- Only 14% agreed that clients are good at allocating the right amount of budget to the level of risks they face; and notably, those with the least influence over the budget were the most likely to disagree.
- 37% of current 'in-house' security manager respondents *agreed or strongly agreed* that security suppliers are focused on hitting targets rather than offering the best security.

Factors that are important when purchasing security

- When looking at the factors considered to be important to organisations when buying security, both current 'in-house' and 'contract' security manager respondents gave similar responses.
- The key factors were: understanding and responding to the client's identified needs (92%); the expertise of the supplier (88%); the supplier having a good reputation (86%); having a proven partnership with other

clients (79%) and having a proven partnership with the current client (69%).
- Offering the lowest price was the least important factor of those explored (44%).
- The contract agreed between the client and contractor was rarely a 'very close' match (13%), most commonly they were considered 'close' (33%) or 'approximately similar' (35%).
- Reasons offered included: natural adjustments over time; unforeseen circumstances; clients may have underestimated requirements; or seek to add extras at a later date ('Mission creep'); suppliers may have over promised what can realistically be achieved for the price; poor project or price specification by one or other party.

Factors that increase the likelihood of a security manager influencing the security budget

- The more competent the security lead/team, the greater the influence. The status, credibility, and qualifications of the security lead matter.
- Being effective at building relationships was also frequently mentioned, particularly building a relationship with senior management, the Board and procurement.
- Key is the ability to be able to argue a business case and articulate the benefits of security and the 'Return On Investment'.
- The occurrence of an incident/crisis often increased security influence over the budget.

Key findings from the interviews

- Career progression to being a CEO would require security leads to take a sideways step outside of security.
- They are disadvantaged by: lacking as much business acumen as peer group professionals; being more operationally focussed than strategic; being less ambitious as many are in second careers in security.
- Moreover, their peers in other disciplines are not generally interested in security.
- Younger security professionals may represent a new approach.

Are contract and corporate security managers interchangeable?

- A broad view was that in-house professionals may need to develop their sales skills, while contractors would need to adapt their business language and learn to engage with senior management.

Who owns security budgets and how are they set?

- Rarely did ownership sit with security: finance, procurement and facilities management departments were frequently mentioned and in certain circumstances, local operational units.
- While there are variations in approaches to setting the budget, only a minority are thought to start from scratch each year.

- Some of the interviewees noted that securing an adequate budget was becoming increasingly challenging.

How do security managers influence the budget?

- Relating security spend to reducing business risks and improving operations was key; highlighting the dangers and risks in not meeting objectives; ensuring the risk owner understands and accepts the implications/risks; using data and ensuring arguments are evidence based; linking physical security spend to cyber security (generally viewed as a greater priority).
- For contractors, the same issues apply but in addition they need to have built a strategic relationship based on respect and trust.

Table of Contents

Section 1. Introduction

1.1. Around the world security is evolving, from being a marginal activity involved in protecting against danger to a core activity that is facilitating business operations. Security teams at their best are becoming more business savvy, understanding how the different parts of the business work to generate appropriate and competent measurements of risk, proposing mitigation that is proportionate and workable, and communicated in a way that leaders can relate to. There is a new buzz concept, Enterprise Security Risk Management (ESRM) which seeks to promote and formalise this.

1.2. Moreover, in a series of Thought Leadership webinars[1], which have included security experts across the globe, and many security managers, several issues have emerged, which were mirrored in the last SRI report[2]. These have included findings that:

- The perception of security management has changed positively from being seen to have responded well during the pandemic; managers have been seen to oversee the delivery of a good service in trying conditions, while showing themselves to be flexible and competent
- Security will be valued more post-pandemic from a new awareness about its attributes
- The appropriate funding of security is key and a condition of it being effective

1.3. This last point has long been the subject of extensive discussion, and general lament, principally that: funding has not kept pace with the changing and emerging role of security; that Boards are still only just becoming supporters; that procurement departments prioritise the lowest price, and frequently win arguments in price versus quality debates.

1.4. What has been left largely unresearched is the extent to which the security function is able to influence the budget. Is this the Holy Grail? Does it matter that much? What are the ways in which security professionals achieve this? What are the obstacles they face and how are they overcome? What skill sets are most valued by security managers in terms of influencing the budget; are there winning strategies, or losing ones? What are they? To what extent are suppliers at the mercy of the commercial acumen of corporate security managers and vice versa or do they have an influence? To what extent are the objectives of in-house security teams and their suppliers aligned? Do they have similar and complimentary skill sets and objectives to support any case that is put? Are managers working for security

[1] https://theospas.com/thought-leadership-webinars/
[2] Gill, M. & Howell, C. (2021) *Covid-19 and the implications for the security sector: what happened and what has been and is being learned?*, Security Research Initiative, Perpetuity Research.

suppliers viewed as partners of corporate security teams? To what extent do security managers see themselves as business savvy and how does this impact on the perceptions that others have of them and by association the security sector?

1.5. The report on which this research is based seeks to address these issues. It is based on a global survey and one to one interviews.

Section 2. Thinking about security managers

Setting the scene

2.1 Time has seen the role of security in organisations transition from being a largely policing role, protecting assets, to a more business-like role, helping the organisation to achieve its objectives by supporting business operations so they are secure, and/or so that they can take place at all. At least for some this is the case. Prima facie evidence would suggest this transition is important for influencing the budget. After all a 'merely' protecting role typically places security at the edge of an organisation, a business enabler role places it centre stage as relevant to core business, a much better strategic position for influencing budgetary decisions.

2.2 Certainly, there are a number of changes placing security centre stage; the pandemic has been one, a crisis generally places security centre stage. In a different way, earlier reference was made to the current emphasis placed by some on Enterprise Security Risk Management, focussing on '*the application of risk principles to manage all security risks ... in a comprehensive, holistic, all-encompassing approach*,'[3] which crucially requires engagement with business operations. However, it is far from clear the extent to which risk principles dominate security practice or that security managers engage holistically.

2.3 Then there is the overlapping trend towards convergence – the engagement of security with other business functions especially cyber security and business continuity, although this too remains work in progress. One study for the ASIS Foundation found that less than 3 in 10 (29.3%) of respondents to a survey in different parts of the world reported that their function had completely converged, while 4 in 10 (39.5%) had not converged at all. When asked further about the impact of convergence less than half of business continuity (46%) and physical security (43%) respondents, and a little over a third of those working in cyber security (35%) felt security had been 'greatly strengthened'.[4]

2.4 Convergence is not a pre-requisite for ESRM, it is but one way of achieving it, a point that is sometimes confused. But the key issue here is that security management can be seen as different things. While some advocate a risk-based approach (ESRM), others focus on departments working collaboratively (Convergence), others hold dear to the belief that security is ultimately about the protection of assets, some see physical security and cyber security as distinctly different areas of expertise, others see them as both being about managing similar types of risks for the same ultimate purpose, protection.

---

[3] Allen, B.J. and Loyear, R. (2018) *Enterprise Security Risk Management: Concepts and Applications*. Connecticut: Rothstein Publishing, p4.

[4] ASIS Foundation (2020) The State of Security Convergence in the United States, Europe and India. *www.asisfoundation.org*.

2.5 The key point though about any move from a primarily protection role, to one that emphasises the best route to achieving this being for a business focussed approach, requires that senior security managers are skilled in business. One recent report[5] based on the views of global security executives has recommended a greater focus on training and education in this area, evidence, that this still work in progress.

The complexities of good security

2.6 The word 'security' has been referred to as being 'slippery', 'contested', and 'confused'.[6] Perhaps unsurprisingly then, getting security right is difficult, very difficult. Understanding and specifying the threat[7]; agreeing a strategy and then developing an effective response and implementing it; engaging peer groups and stakeholders (who may have different perceptions of what security is and/or should be); ensuring the right people and teams have the right skills sets (being effective communicators, security experts, business savvy to name but three); earning respect from decision makers on the one hand and implementors or doers on the other; generating effective relationships (personal and professional); building effective partnerships; generating the right information for the right networks in sufficient quantities; are nearly always an essential element of good security but arguably none of these are easy to achieve.[8]

2.7 This list is far from exhaustive, but it is illustrative. Indeed, to take one example, the relationship between internal security teams and security suppliers, research has shown the range of issues that can complicate 'getting things right'. These include the difficulties of establishing the much valued qualities of trust, honesty and transparency; equalising the balance of power; agreeing the security requirements and how they should be met; ensuring internal security teams are not too distanced from procurers such that they are unable to impart their security expertise in making buying decisions; challenging the lack of status of security professionals amongst peers; while providers need to avoid what is easy at the expense of what the customer needs; and then there is the issue of cost.[9] None of this then means that the ability for security professionals to be able to influence the budget is a given.

---

[5] Peterson, K. & Roberts, J. (2021) *The State of Security Management – 2020; A Baseline Phenomenological and Empirical Study*, ASIS Foundation. www.asisonline.org/foundation

[6] Forbes-Mewett, H. (2018) *The New Security*. Basingstoke: Palgrave.

[7] For a discussion see, Chen, C. and Reniers, G. (2022) Security in the Chemical Industry: theory and practice. In Gill, M, (editor) *The Handbook of Security*, third edition. Basingstoke: Palgrave.

[8] For an excellent discussion see, Whelan, C. and Molnar, A. (2019) *Securing Mega-Events*. Basingstoke: Palgrave

[9] Gill, M., Howell, C., and McGeer, C. (2018) *The Barriers to Effective Buyer-Supplier Relationships in the Security Sector*. Tunbridge Wells: Perpetuity research.

Security expertise and the security budget

2.8 There is a range of studies that have looked at the myriad of factors that can impact on the amount of budget allocated to different functions. Thinking about those that might apply to security, they include: the profitability of the company; the power and influence of the relevant professionals; the relationship of the departmental head to the executive power holders; the extent to which the issue under budget consideration is perceived as core business;[10] the extent to which new risks are understood and accounted for;[11] to name but a few.

2.9 Yet there is relatively little work that has focussed on the extent to which security managers can and do influence budgets, and the relative importance that security suppliers – as partners of corporate security teams – have on decisions. Certainly there is reason to believe that challenges exist here. One piece of research sponsored by the ASIS Foundation, for example, found that 'obtaining resources' was the top challenge faced in performing the security management role[12].

2.10 Costs are of course always a central consideration in discussions about the value of security. The somewhat traditional notion that the benefits of security are intangible has given way to a wealth of studies that have examined the cost benefits of security using a variety of methodologies. Although in practice these are rarely used.[13] Of course each organisation makes a judgement on how much it wants to spend. The problem for the security sector is that it is littered with examples of organisations wanting the lowest price at the expense of quality, which may itself be a reflection of the lack of understanding of the benefits of good security compared to the limitations and dangers of bad security.

2.11 It raises a fundamental question, what factors are key in influencing the security budget? To what extent does internal security expertise – in-house teams – and external security knowledge, security suppliers, influence the budget process? What are the limitations and barriers to effective working and how they might be addressed? It is these central issues that are the focal point of this study.

---

[10] For example, see, Breunig, C and Koshi, C. (2020) Topping Off and Bottoming Out: Setting Budget Priorities Through Executive Power. *Policy Studies Journal*, Vol.48 (2), p.342-366. Cheong, Y, Kim, K and Kim, H. (2013) Advertising and promotion budgeting during volatile economic conditions: Factors influencing the level of decentralization in budgeting and its relations to budget size and allocation. *International Journal of Avertising*, Vol.32 (1), p.143-162

[11] Beebe, N. L., Young, D. K., & Chang, F. R. (2014). Framing information security budget requests to influence investment decisions. *Communications of the Association for Information Systems*, *35*(1), 7.

[12] Peterson, K. & Roberts, J. (2021) ibid.

[13] For a good discussion of approaches see, Manning, M., Fleming., C.M. and Pham, H-T. (2022) Making an Economic Case for Security. In Gill, M, (editor) *The Handbook of Security*, third edition. Basingstoke: Palgrave. For an example of applications in a specific context, see, Chen, C., Reniers, G., Khakzad, N. (2020) Cost-Benefit Management of Intentional Domino Effects in Chemical Industrial Areas. *Process Safety and Environmental Protection*. Vol 134, 392-405. 10.1016/j.psep.2019.10.007

Section 3. Survey Findings

The sample

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

- Factors that influence the security budget;
- Factors that influence how effective security is;
- Whether there are similarities between 'in-house' and 'contracted' security managers; and
- Factors that are important when purchasing security.

3.2. The overall aim was to understand the obstacles faced by security managers/directors. The findings are based on 338 responses[14].

3.3. In the introduction to the survey it was noted that – *For the purposes of this survey, we define a security manager/director broadly, as someone who is in charge of a function that is engaged to protect a location against crime and other threats. The role may vary widely depending on the nature and size of the environments they are employed in; the number of supporting security officers; and the threats and risks faced. Typically duties may include advising on security risks; recruiting, supervising and training staff; writing the security strategy and related plans; monitoring the security budget; and producing and presenting security reports.*

3.4. 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, comment boxes were provided to enable respondents to expand on their multiple choice answer if they wished to. A small number of questions invited open text responses. All of the topics covered are condensed and summarised below.

3.5. 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:

- Type of security manager role
- Type of locations the security manager is responsible for
- Level of influence over the security budget

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

- Satisfaction with level of influence over the budget
- Perception of sufficiency of the security budget

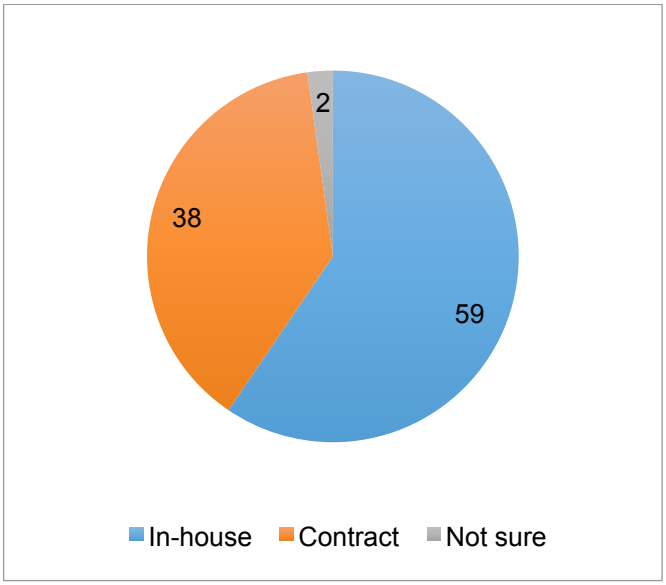
3.6. The sectors most commonly indicated by respondents as those they provided security in (respondents could tick all that apply) were Public Admin, Other Services and Government (25%, n=84), Property (23%, n=77), Retail (23%, n=76) and Health (22%, n=74). A full breakdown is provided in Appendix 2 (Table 1). Over three fifths of respondents worked for organisations based in the UK (62%, n=208). A full breakdown is provided in Appendix 2 (Table 2).

3.7. The majority of the respondents indicated that they are currently employed as a security manager or director – 81% (n=274). Of those that were not currently working as a security manager/director (19%, n=64), two fifths were a security operative (42%, n=27), over a quarter were a security consultant (28%, n=18), around an eighth were from another key role at a security supplier company (director, business development, sales, marketing etc) (13%, n=8). The rest were another type of security expert or interested party (17%, n=11).

Security Manager/Director respondents

3.8. Those that indicated that they are currently employed as a security manager or director were asked a number of additional questions to gain a more in-depth understanding of their work and experiences. Close to three fifths of the Security Manager/Director respondents reported they were 'in-house' (59%, n=163) and almost two fifths reported they were 'contract' (38%, n=105). This is shown in Figure 1.

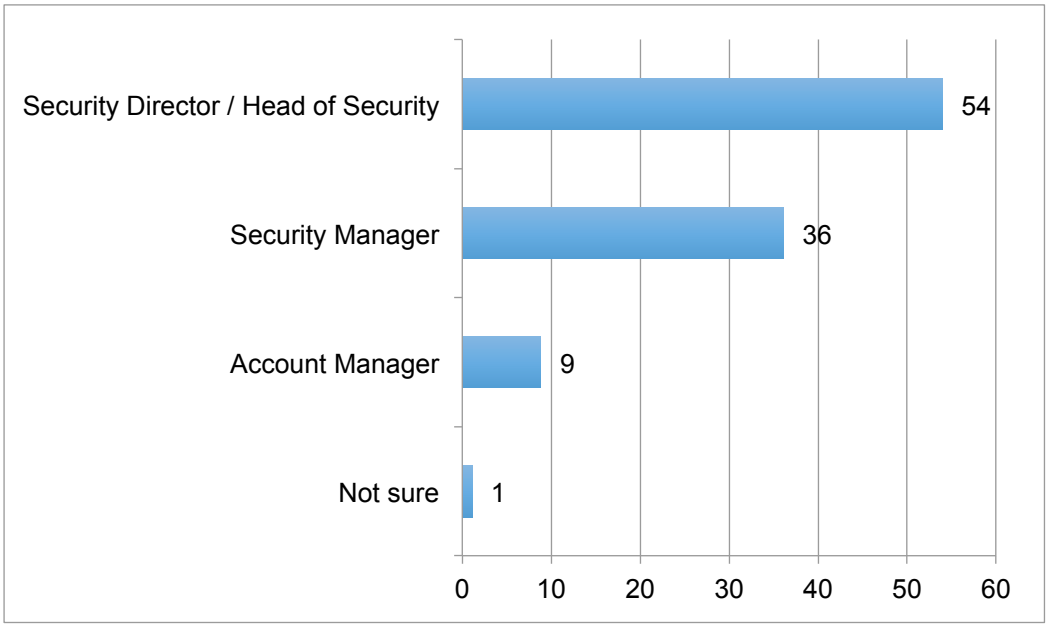
Figure 1: Employment Type (n=274) %



3.9. Asked more specifically about the type of security management undertaken, over half indicated they were 'Security Director / Head of

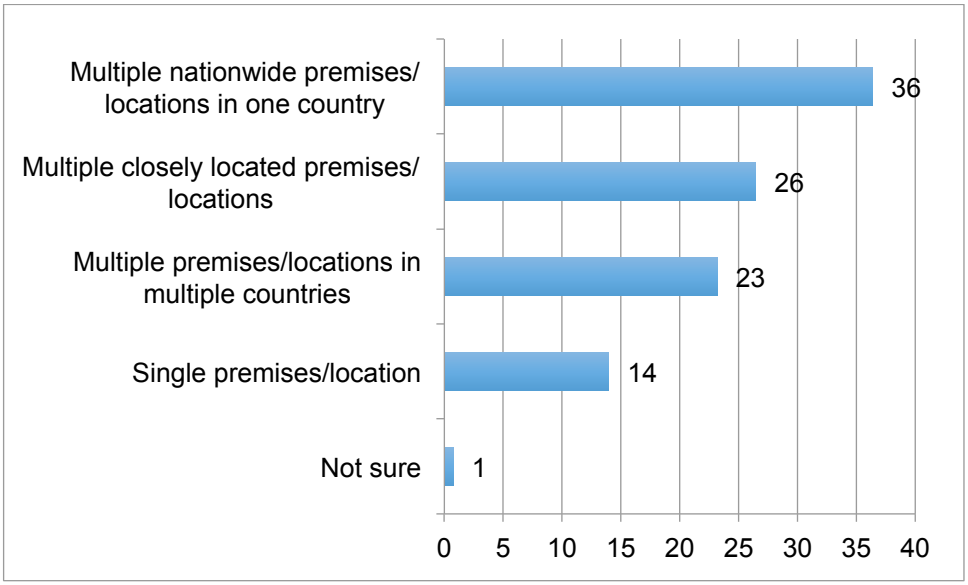
Security'[15] (54%, n=148), over a third indicated they were 'Security Manager'[16] (36%, n=99) and close to a tenth indicated they were an 'Account Manager'[17] (9%, n=24). Figure 2 shows the results.

Figure 2: Type of Management undertaken (n=274) %



3.10. The respondents represented those with responsibility for single as well as multiple premises. Figure 3 displays the breakdown.

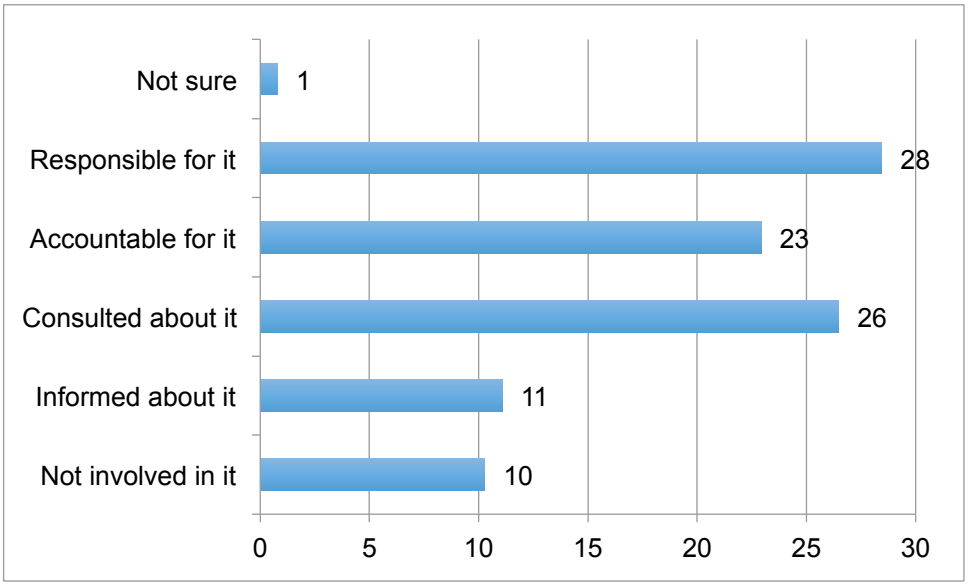
Figure 3: Locations that respondents are responsible for (n=272) %



[15] We described this as: the person with overall responsibility for the strategic direction of a security function.
[16] We described this as: supporting or running the day to day function of security.
[17] We described this as: overseeing the performance of the security team(s) contracted to deliver services to the client(s).

3.11. Respondents were asked to indicate their level of influence over the budget allocation for security in the organisation(s) they manage security for. There was considerable variation. Just over half (51%) had a relatively high level of influence; over a quarter (28%, n=72) were 'responsible' for the budget and less than that (23%, n=58) were 'accountable' for the budget. Meanwhile a fifth of respondents (21%) had very limited involvement (11%, n=28 were 'informed' about the budget and 10%, n=26 were 'not involved'). Figure 4 shows the results in full.

Figure 4: Level of influence over the security budget (n=253) %

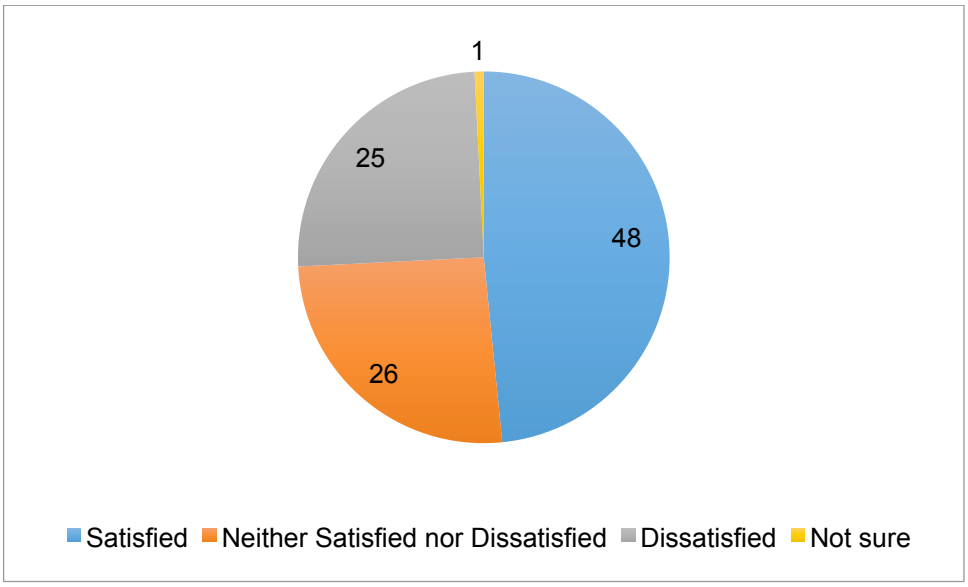


3.12. In terms of the characteristics of those that had most influence, those in a 'Security Director' type role more often indicated they were **responsible** for the budget than those in an 'Account Manager' or 'Security Manager' type role[18]. Also, as the number and geographic spread of sites the manager was responsible for increased, so did the proportion that indicated they are **responsible** for the security budget[19].

3.13. In respect of the level of influence over the security budget held by respondents who were currently working as security managers/directors, just under half were satisfied or very satisfied with their level of influence (48%, n=122), a quarter were neutral (26%, n=65) and a quarter were dissatisfied or very dissatisfied (25%, n=63). This is shown in Figure 5.

[18] 43% of 'security directors' indicated they are *responsible* for the security budget, compared with 13% of 'account directors' and 5% of 'security managers'.
[19] 40% of managers responsible for 'multiple premises/locations in multiple countries' indicated they are *responsible* for the security budget, compared with 26% of those that manage 'multiple nationwide premises/locations in one country', 21% of those that manage 'multiple closely located premises/locations', and 16% of those that manage a 'single premise/location'.

Figure 5: Level of satisfaction with influence over the security budget (n=252) %



3.14. There was a strong correlation between the level of influence held by the respondent, and their satisfaction with that level of influence. Perhaps unsurprisingly, those with the highest levels of influence were the most satisfied, while those with the lowest levels of influence were the least satisfied[20]. Notably, there was a relatively similar level of satisfaction between in-house and contract security managers[21].

3.15. Respondents were offered the opportunity to explain the reason for their level of satisfaction with their influence over the security budget. 107 provided a response. Among those who were satisfied with their level of influence, reasons included that:

- They had a high level of influence and therefore were able to direct and influence the allocation of the budget ensuring security needs can be met.
- They indicated their organisation prioritised security and recognised the level of funding required to address the risks.
- They felt that their advice and proposals were typically listened to and/or accepted by those controlling the budget.
- Despite challenging budgets, working closely with clients to find effective solutions gives contracted security managers a competitive advantage.

3.16. Among those who were dissatisfied with their influence over the security budget, reasons predominantly related to them having a lack of involvement in deciding the budget and in some cases not even being

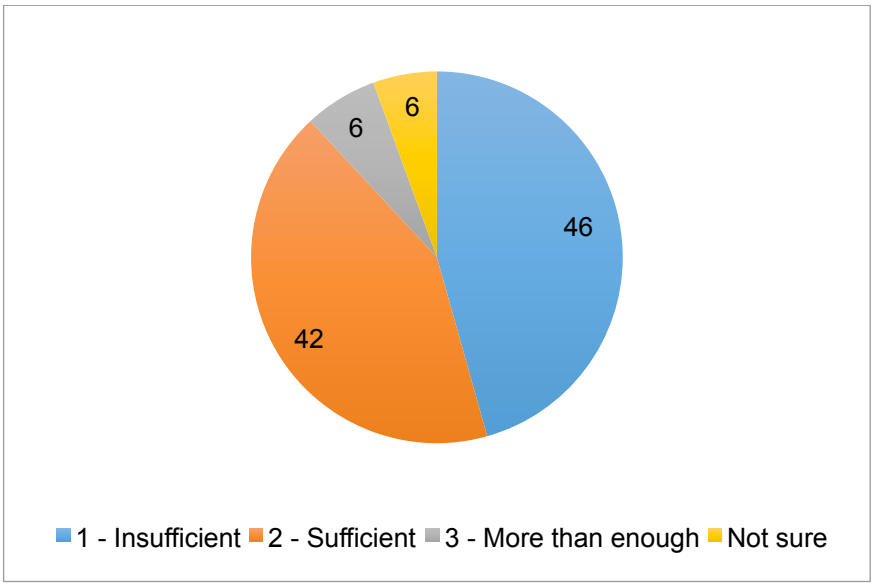
[20] 83% of those 'responsible' for the security budget indicated they are *satisfied or very satisfied* with their level of influence, compared with 55% of those 'accountable', 34% of those 'consulted about it', 14% of those 'informed about it', and 8% of those 'not involved'.
[21] 45% of 'in-house' security managers and 43% of 'contract' security managers indicated they are *satisfied or very satisfied* with their level of influence.

informed what the current budget is. Problems that respondents expressed as arising from a lack of involvement included:

- They could not purchase basic and essential resources (such as uniform) without first explaining why they are needed and gaining approval.
- They could not plan effectively for training security staff and for cover for security staff.
- They could not measure the performance of their department.
- Budget decisions were instead being made by people who sat above them but are not security experts and therefore are less able to make the case for developing security provision.
- Security not being valued or prioritised by the organisation.
- Decisions being made that were not beneficial to the operation of the security function.
- Projects being poorly thought out, with the security manager subsequently being relied upon to fix the problems (whereas involving them from the outset could have prevented or reduced the difficulties).
- Security being tailored to fit the budget, rather than an appropriate budget being allocated on the basis of the security required, or the available budget being targeted to best effect.
- Costs can end up being greater if the budget is allocated reactively to deal with issues, rather than proactively to prevent issues.
- Security budgets are often being seen as a place to seek savings.
- The opportunity to make savings being missed when budget decisions lack input from a security expert.

3.17. Turning the attention to the budget itself, approaching a half of the security manager respondents thought that the current budget available for security was ‘insufficient’ (46%, n=115). Over two fifths thought that it was ‘sufficient’ (42%, n=107). Very few thought that it was ‘more than enough’ (6%, n=16). Figure 6 displays the findings.

Figure 6: Level of satisfaction with the current budget available for security (n=252) %



3.18. In terms of the characteristics of those that felt the budget was insufficient, both contract and in-house managers were equally likely to view the budget to be insufficient[22]; however those in a 'security manager' type role more commonly viewed the budget to be insufficient than those in a 'security director' and 'account manager' type roles[23]. There was also correlation between views on the sufficiency of the budget and the number and geographic spread of sites the manager was responsible for - as the number and geographic spread of sites reduced, the perception of the budget being insufficient increased[24]. Further, those with the highest levels of influence over the budget were the least likely to view it to be insufficient[25]. And unsurprisingly, those that were the least satisfied with their influence over the budget, were the most likely to view the budget to be insufficient[26].

3.19. Respondents were offered the opportunity to explain their answer. 90 provided a response. The main reasons expressed as to why respondents felt the budget was insufficient included:

- It did not reflect the risks faced.

[22] 42% of 'in-house' and 43% of 'contract' managers viewed the budget as *insufficient*.
[23] 54% of 'security managers' viewed the budget as *insufficient,* compared with 36% of 'security directors' and 33% of 'account managers'.
[24] 50% of managers responsible for a 'single premises/location' viewed the security budget to be *insufficient*, compared with 49% of those responsible for 'multiple closely located premises/locations', 40% of those responsible for 'multiple nationwide premises/locations in one country', and 32% of those responsible for 'multiple premises/locations in multiple countries'.
[25] 31% of those 'responsible' for the security budget indicated it is *insufficient*, compared with 45% of those 'accountable', 51% of those 'consulted about it', 64% of those 'informed about it', and 58% of those 'not involved'.
[26] 95% of those that are 'very dissatisfied' with their level of influence, viewed the budget to be *insufficient*, compared with 62% of those that are 'dissatisfied', 51% of those that are 'neither satisfied nor dissatisfied', 35% of those that are 'satisfied', and 20% of those that are 'very satisfied' with their level of influence.

- A failure to allocate funds to aspects such as training and travel; and in some cases to basic equipment (with staff expected to purchase their own).
- Security teams being understaffed.
- A failure to manage and maintain security equipment and technology which resulted in a large spend on repairs and replacement that was not planned into the annual budget.
- Increased costs not being matched by additional funding.
- A failure to recognise the losses that could be outweighed by investing in additional security (which could also bring wider benefits).
- Wanting more provision for a lower spend.
- A disparity between the level of pay for security officers and the calibre of officers required.
- Being insufficient to meet minimum legal requirements.
- A lack of contingency for unexpected events.

3.20. By contrast the main reasons expressed as to why respondents felt the budget was sufficient included that there was good investment in security; that the budget was a good reflection of operational and strategic requirements; and that there was flexibility to adapt to changes and developments.

All respondents

3.21. The remaining questions were asked of all respondents, irrespective of whether the respondent was currently a security manager/director or in another security related role. They were designed to explore views and experiences on a range of topics.

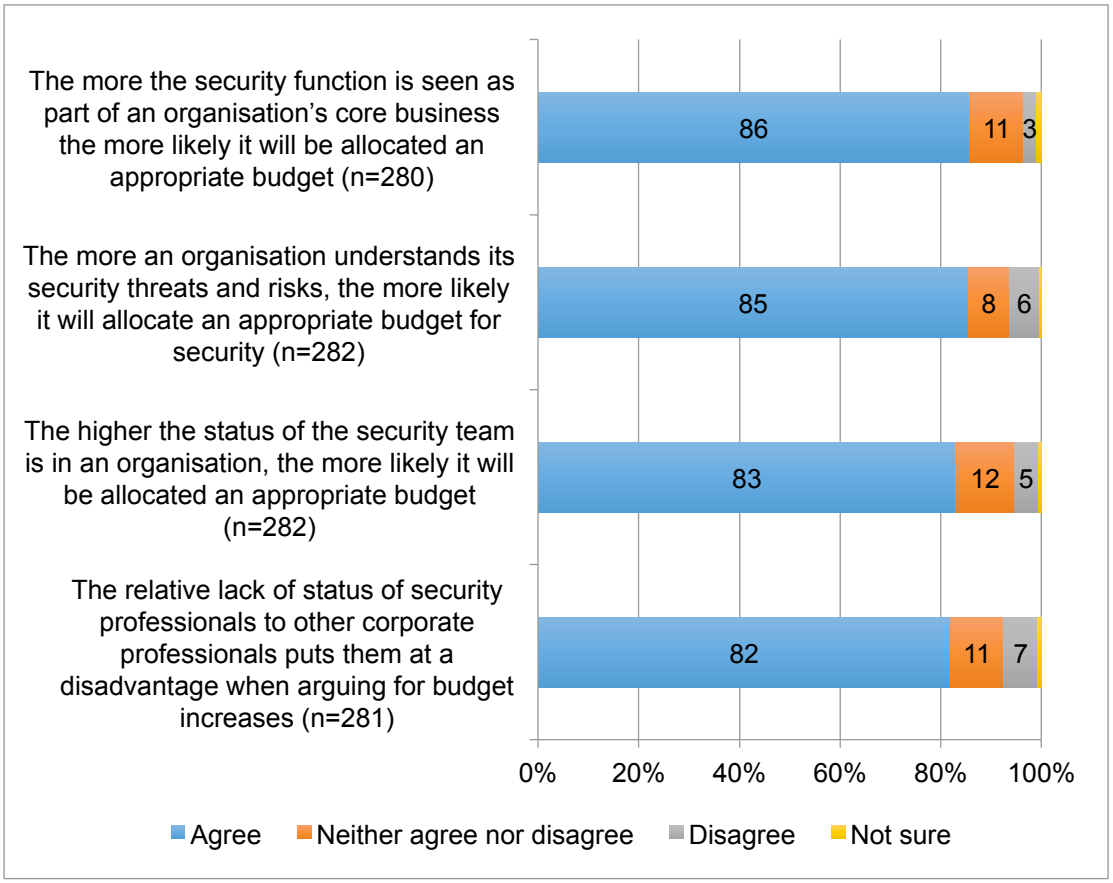
Factors affecting the allocation of an appropriate budget

3.22. A number of statements were presented to explore the factors that may influence the amount of budget allocated to security. The statements that received the highest level of agreement – all above 80% of respondents – were:

- 86% (n=240) agreed or strongly agreed that **the more the security function is seen as part of an organisation's core business** the more likely it will be allocated an appropriate budget.
- 85% (n=241) agreed or strongly agreed that **the more an organisation understands its security threats and risks**, the more likely it will allocate an appropriate budget for security.
- 83% (n=234) agreed or strongly agreed that **the higher the status of the security team** in an organisation, the more likely it will be allocated an appropriate budget.
- 82% (n=230) agreed or strongly agreed that **the relative lack of status of security professionals compared to other corporate**

professionals puts them at a disadvantage when arguing for budget.

Figure 7: Statements on allocation of an appropriate budget, with the highest level of agreement %



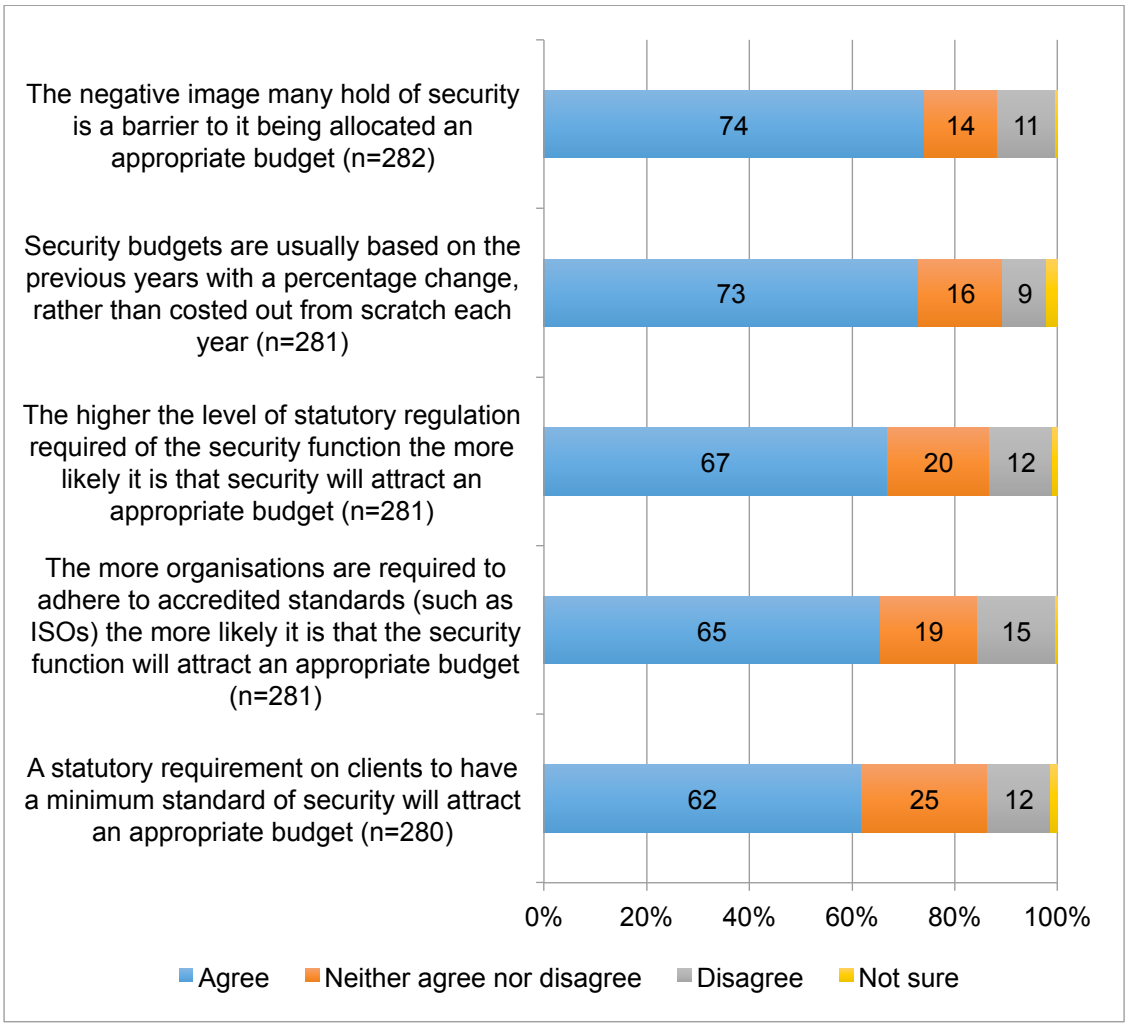
3.23. Agreement was a little lower – around 70% - with the following statements:

- 74% (n=209) agreed or strongly agreed that **the negative image many hold of security is a barrier** to it being allocated an appropriate budget; notably, security managers that indicated they are 'responsible' for the security budget were considerably less likely to agree with this statement than those who were 'not involved'[27].
- 73% (n=205) agreed or strongly agreed that **security budgets are usually based on the previous years** with a percentage change, rather than costed out from scratch each year.
- 67% (n=188) agreed or strongly agreed that the **higher the level of statutory regulation required of the security function** the more likely it is that security will attract an appropriate budget.

[27] 57% of security managers that are 'responsible' for the security budget *agreed or disagreed* that the negative image many hold of security is a barrier to it being allocated an appropriate budget, compared with 91% of security managers that are 'not involved' in the security budget.

- 65% (n=184) agreed or strongly agree that the **more organisations are required to adhere to accredited standards (such as ISOs)** the more likely it is that the security function will attract an appropriate budget.
- 62% (n=173) agreed or strongly agreed that **a statutory requirements on clients to have a minimum standard of security** will attract an appropriate budget.

Figure 8: Statements on allocation of an appropriate budget, around 70% agreement %



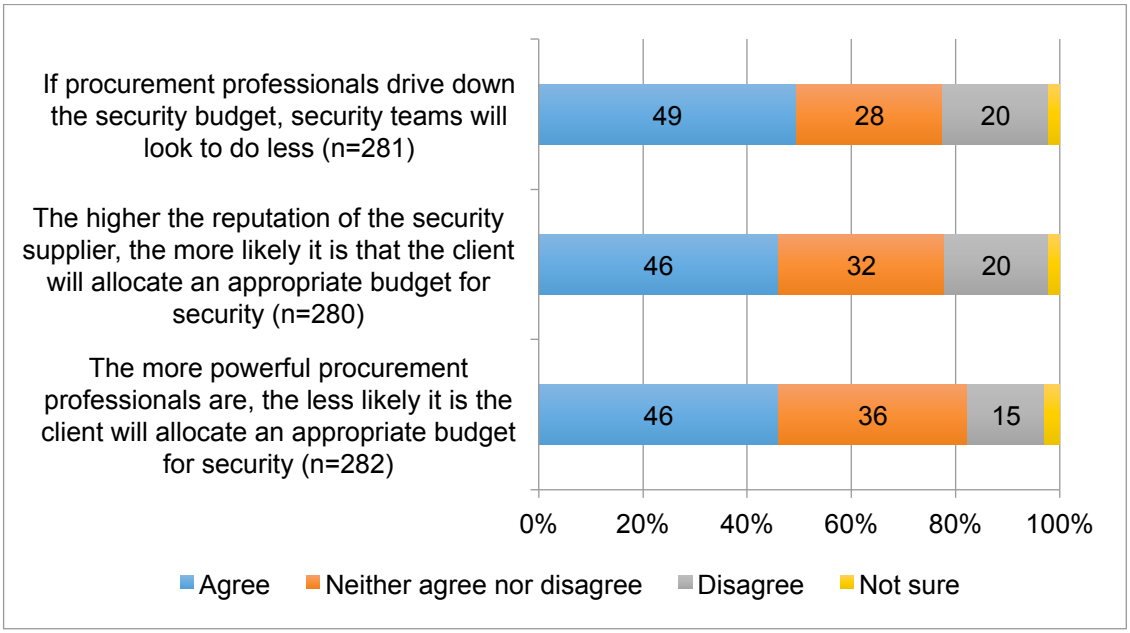
3.24. Agreement was lowest – under 50% - with the following statements:

- 49% (n=139) agreed or strongly agreed that **if procurement professionals drive down the security budget, security teams will look to do less**; security manager respondents that are 'not involved' in the budget were more likely to agree with this statement than those with any other level of influence over the budget[28].

[28] 65% of security manager respondents that are 'not involved' in the security budget *agreed or strongly agree* that if procurement professionals drive down the security budget, security teams will look to do less; compared with 39% of those 'informed about the budget', 49% of those 'consulted' about the budget', 38% of those 'accountable' for the budget and 35% of those 'responsible' for the budget.

- 46% (n=130) agreed or strongly agreed that **the more powerful procurement professionals are**, the less likely it is the client will allocate an appropriate budget for security.
- 46% (n=129) agreed or strongly agreed that **the higher the reputation of the security supplier**, the more likely it is that the client will allocate an appropriate budget for security.

Figure 9: Statements on allocation of an appropriate budget, with the lowest level of agreement %



3.25. Generally speaking, security manager respondents that were 'dissatisfied or very dissatisfied' with their own level of influence over the security budget, were a little more likely to agree with the above statements, than those who were 'satisfied or very satisfied' with their level of influence. There was one exception – for the statement 'the higher the reputation of the security supplier, the more likely it is that the client will allocate an appropriate budget'; agreement was higher among the group that were satisfied with their level of influence[29]. Similarly, security manager respondents that felt their budget was 'insufficient' more commonly agreed with the statements than those who thought their budget was 'sufficient'.

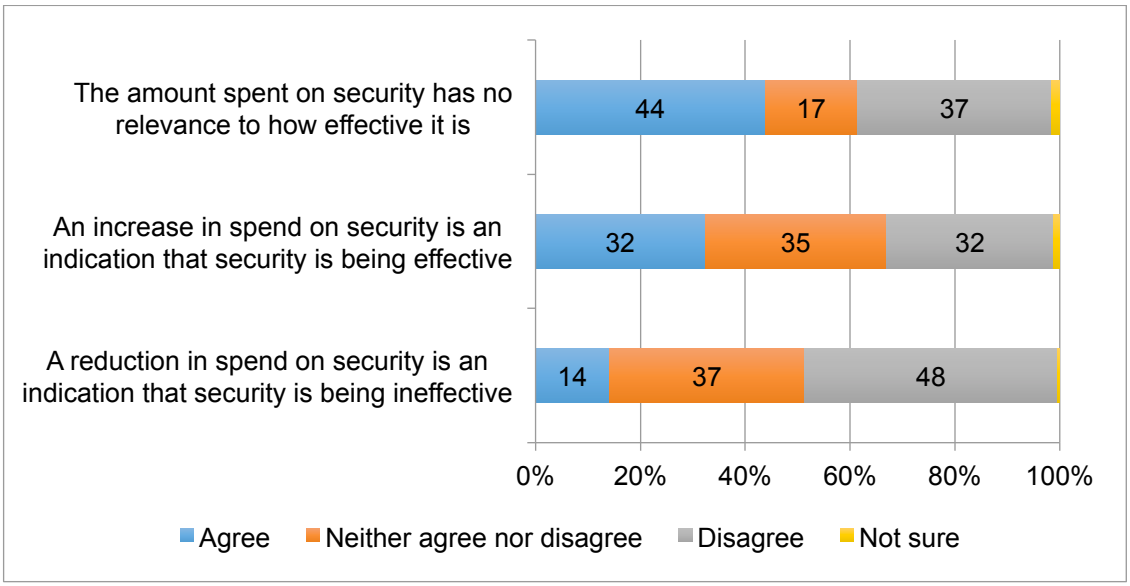
Factors that influence how effective security is

3.26. A number of statements were presented to explore some of the factors that may influence how effective security is.

[29] 42% of security manager respondents that are 'satisfied or very satisfied' with their influence over the budget indicated that they *agreed or strongly agreed* that the higher the reputation of the security supplier, the more likely it is that the client will allocate an appropriate budget for security, compared with 32% of security manager respondents that are 'dissatisfied or strongly dissatisfied' with their influence over the budget.

3.27. First, when asked whether increases or reductions in spend on security was indicative of how effective security is at an organisation was explored only 14% (n=38) believed that **a reduction in spend** was an indication that security is ineffective, suggesting that predominantly, reduction in spend is attributable to other factors. There was an even split in respect of whether **an increase in spend** on security indicates security is effective (32%, n=87 agreed, 35%, n=93 were neutral, and 32%, n=86 disagreed). Over two fifths (44%, n=118) indicated that increases or decreases to the amount spent **was not related** to how effective security is. Figure 10 provides a breakdown of the results.

Figure 10: Statements on whether changes to the amount spent on security is indicative of how effective security is (n=269) %



3.28. Some comments made by respondents provided context as to why changes in spending are not a simple reflection of how effective security is, for example:

> *'An increase or decrease in security spend is not the yard stick. It is how a budget is allocated, managed and spent in the right areas linked to risk and standards.'*
>
> *(Survey respondent)*

> *'Budget only provides staff and equipment. Training and good management is the driving force behind security effectiveness.'*
>
> *(Survey respondent)*

> *'I have had my budget cut because I was 'too effective' because I could show to my boss that I could extend the life span of a piece of equipment far beyond its normal life span while other departments who could not were rewarded with more money because they were incompetent. This is not a simple cause and effect here. Sometimes money is granted or taken away that has nothing to do with operational considerations but are*

sometimes emotion based. In one of the buildings I managed, I was given a larger budget than the risk profile warranted because of the emotional attachment the president of the company had towards the property.'

(Survey respondent)

'The suggestion that low security budget is a reflection on poor security, and that high security budget is a reflection of good security is a poor measure. Often security budgets are reduced when security are performing well, and increased after a period of poor investment and a significant failing.'

(Survey respondent)

3.29. Second, factors such as the relationships between individuals, and the influence of individuals were considered.

3.30. The vast majority of respondents (87%, n=235) agreed that **an effective relationship between those engaging internal security personnel and security suppliers is fundamental for good security**. Notably though, close to a third (32%, n=87) agreed that **excellent relationships between clients and suppliers are rare** – but almost half (47%, n=127) disagreed that was the case. This is an important finding and should be heeded.

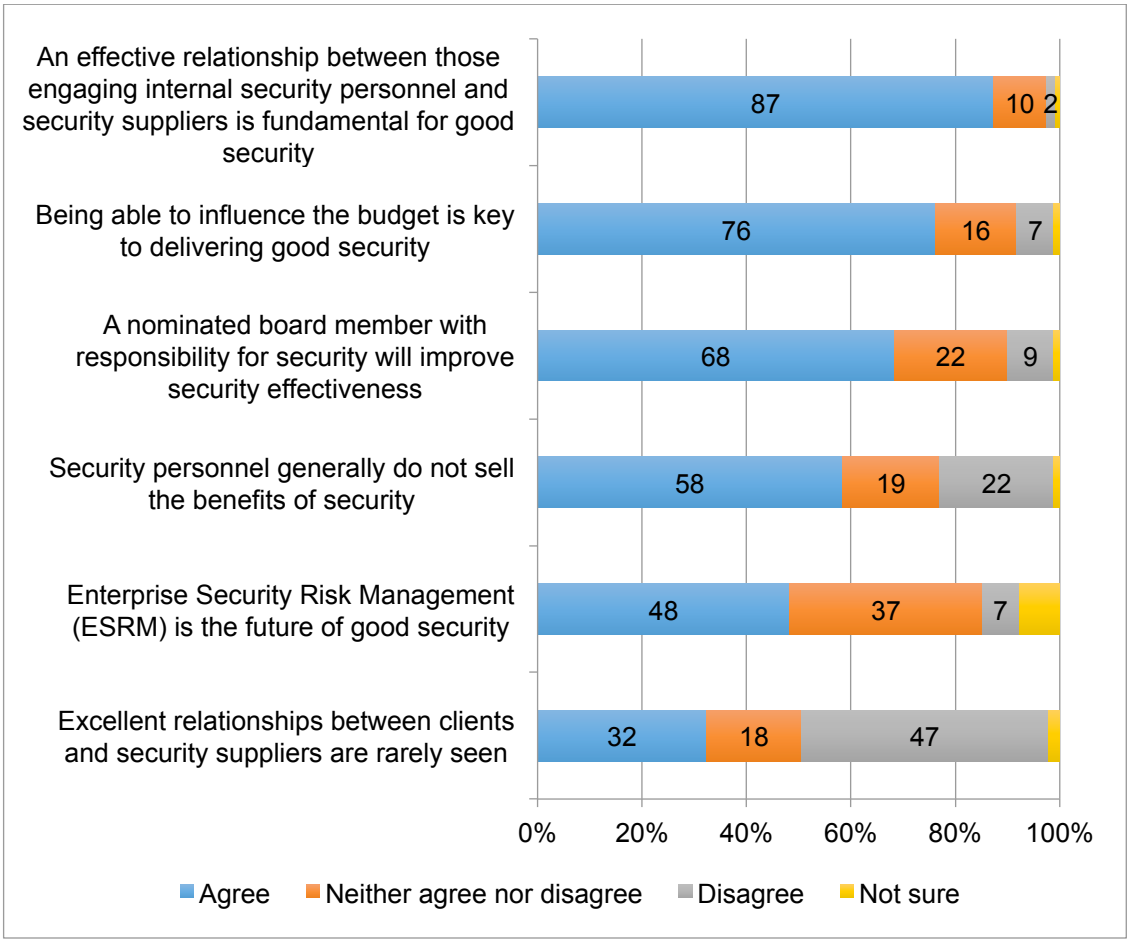
3.31. Over three quarters of respondents (76%, n=204) agreed that **being able to influence the budget is key to delivering good security**; and over two thirds (68%, n=183) agreed that **a nominated board member with responsibility for security will improve security effectiveness**. A small number of respondents explained that the skills and understanding of the nominated board member were critical, and that they would only have impact if they had a good understanding of security.

3.32. Close to three fifths of respondents (58%, n=157) agreed that **security personnel generally do not sell the benefits of security**. Here, there was correlation among security manager respondents, with those that were most satisfied with their level of influence over the security budget, the least likely to agree with this statement, and vice versa[30].

3.33. Close to half of respondents (48%, n=130) agreed that **Enterprise Security Risk Management (ESRM) is the future of good security**. Notably, few disagreed (7%, n=19), but nearly two fifths (37%, n=99) gave a neutral response. One respondent noted that while the principle works well, ESRM isn't currently '*sufficient to articulate a fully functioning framework for security*'. The full breakdown for these statements is shown in Figure 11.

[30] 34% of security manager respondents that were 'very satisfied' with their level of influence, *agreed or strongly agreed* that security personnel generally do not sell the benefits of security; compared with 62% of those that were 'very dissatisfied' with their level of influence.

Figure 11: Statements on factors that influence how effective security is (n=268-269) %



Similarities between in-house and contracted security managers

3.34. A number of statements were presented to explore some of the similarities and differences between security managers based on their employment type and perceptions of their relative influence on the budget.

3.35. There was a higher level of agreement that **a good security manager working for a security supplier would generally adapt well to being an in-house corporate security manager** (60%, n=157 agreed) than the other way around - for an **in-house manager adapting to a security supplier organisation** (45%, n=119 agreed). Although, as one might expect, current supplier security managers agreed a little more than current in-house security managers that a manager from a supplier would adapt well to in-house[31], whereas current in-house security managers were a little more likely than the current supplier

[31] 50% of current security manager respondents that indicated they are 'contract', *agreed or strongly agreed* that a good security manager working for a security supplier would generally adapt well to an in-house corporate security manager role, compared with 45% of current security manager respondents that indicated they are 'in-house'.

security managers to agree that in-house security managers will adapt well to a security supplier organisation[32]. In other words, each group was a little more inclined to view those in the same position as themselves to be able to adapt well.

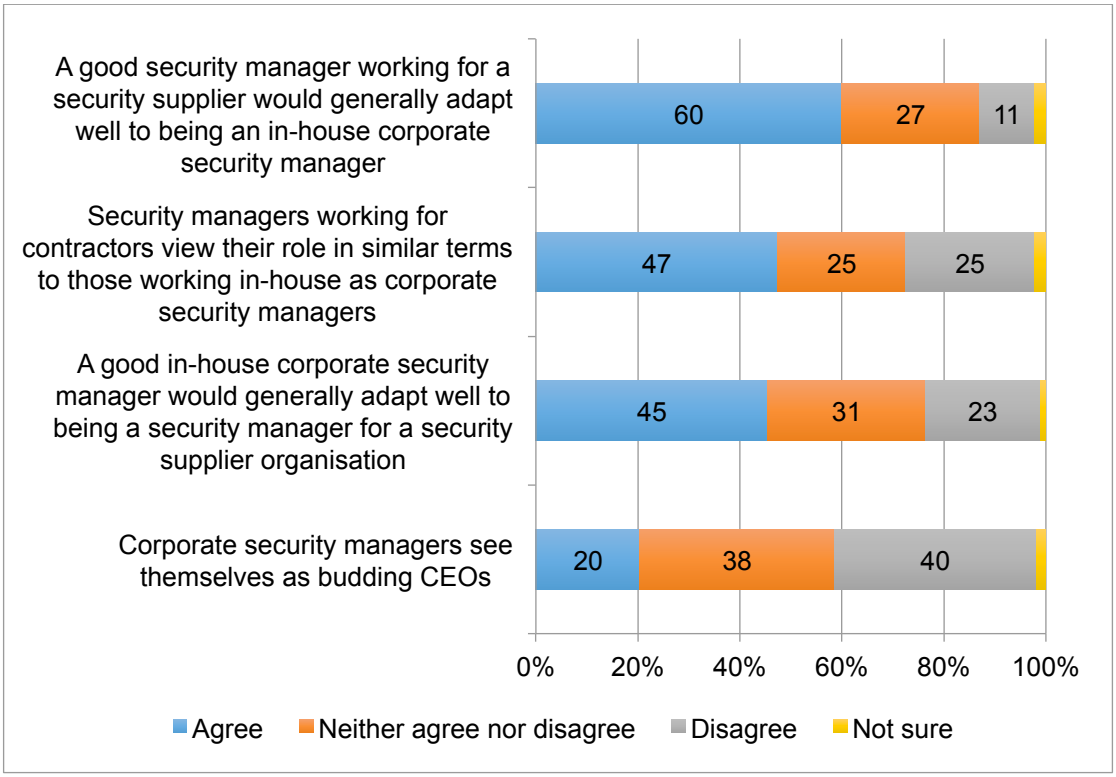
3.36. One possible explanation offered as to why it may be easier to adapt from contract to in-house, provided by a small number of respondents was that there are typically a higher proportion of ex police/military people in in-house security management and that such a background would mean they typically lack the commercial knowledge to be able to adapt well to a supplier organisation. One respondent noted that 'transferability' depended more on the specific individual and their 'willingness to adapt to a different culture'. Another highlighted some of the differences between in-house and contract security management:

> *'In house and contract skills required are vastly different on many fronts, internal politics, budget, business alignment, and accountability to multiple stakeholders drive the differences.'*
>
> *(Survey respondent)*

3.37. A fifth (20%, n=53) of respondents agreed that **in-house security managers see themselves as budding CEOs** suggesting that this is not a typical career aspiration. Figure 12 shows the results.

[32] 37% of current security manager respondents that indicated they are 'in-house', *agreed or strongly agreed* that a good in-house corporate security manager would generally adapt well to being a security manager for a security supplier organisation, compared with 32% of current security manager respondents that indicated they are 'contract'.

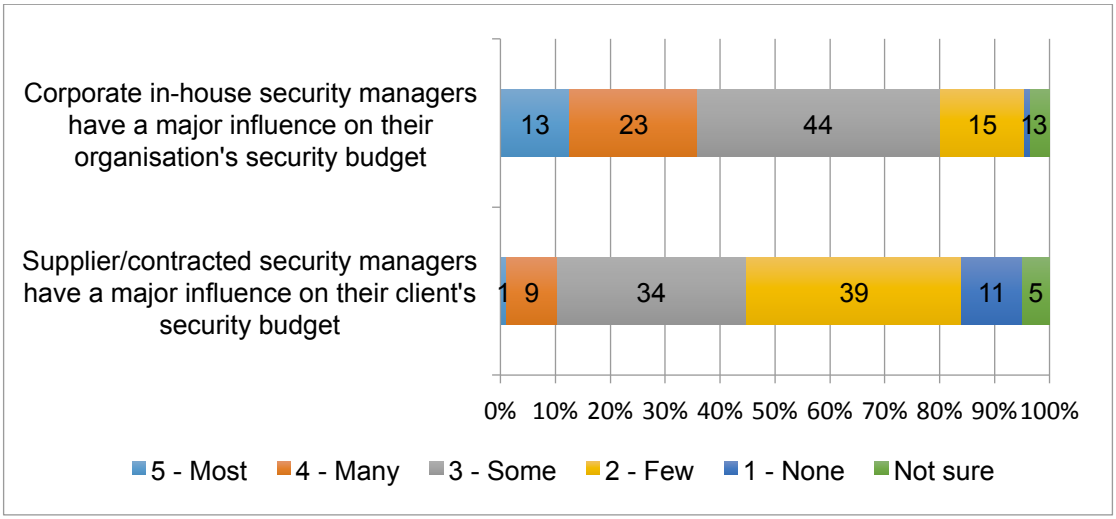
Figure 12: Similarities between in-house and contracted security managers (n=260-262) %



3.38. Respondents were also asked to indicate the proportion of security managers that have a 'major' influence on the security budget. Perhaps unsurprisingly in-house security managers were more commonly viewed to have a major influence on their organisations budget (13%, n=33 thought **most** had a major influence and 23%, n=61 thought **many**), than contract security managers on their clients' budgets (1%, n=3 thought **most** had a major influence and 9%, n=24 thought **many**).

3.39. However, it was also notable that for both in-house (61%, n=116) and contract security managers (85%, n=221), the majority of respondents felt that **some**, **few**, or **none** (as opposed to **most** or **many**) had a 'major influence', suggesting that overall when it comes to influencing the budget, a majority of security professionals do not have the level of influence that may be desirable. Figure 13 shows the results in full.

Figure 13: Proportion of in-house and contracted security managers that have a major influence on the security budget (n=261-262) %



Factors affecting the procurement of security

3.40. A number of statements were presented to explore key issues in the procuring of security services.

3.41. In respect of who may have an input on buying decisions, two thirds of respondents (67%, n=167) agreed that **the buying process lacks sufficient input from security experts** and close to three fifths (58%, n=145) agreed that **clients' buying decision are guided more by procurement professionals than security professionals**. On both of these points, current 'contract' security managers were more likely than current 'in-house' security managers to agree this is the case[33]. Further, on both these points, security managers that had the lowest level of influence[34], and security managers that thought the budget was 'insufficient'[35] were much more likely to agree.

[33] 54% of current 'contract' security managers *agreed or strongly agreed* that the buying process lacks sufficient input from security experts, compared with 39% of current 'in-house' security managers.
AND
51% of current 'contract' security managers *agreed or strongly agreed* that clients' buying decisions are guided more by procurement professionals than security professionals, compared with 34% of current 'in-house' security managers.

[34] 69% of current security managers 'not involved' in the security budget *agreed or strongly agreed* that clients' buying decisions are guided more by procurement professionals than security professionals, compared with 28% of current security managers that are 'responsible' for the budget.
AND
65% of current security managers 'not involved' in the security budget *agreed or strongly agreed* that the buying process lacks sufficient input from security experts, compared with 40% of current security managers that are 'responsible' for the budget.

[35] 51% of security managers viewing the budget to be 'insufficient' agreed or strongly agreed that clients' buying decisions are guided more by procurement professionals than security professionals, compared with 39% of those that view the budget as 'sufficient', and 25% of those that viewed the budget as 'more than sufficient.
AND
59% of security managers viewing the budget to be 'insufficient' agreed or strongly agreed that the buying process lacks sufficient input from security experts, compared with 42% of those that view the budget as 'sufficient', and 19% of those that viewed the budget as 'more than sufficient.

3.42. A number of respondents provided reflection on the input of procurement professionals, and the primary concern was that there was a lack of distinction between the 'cheapest' price and the 'best value' price which resulted in poor procurement decisions, for example:

> *'Procurement is normally weighted far too heavily on price. When you have 40% for quality and 60% for the price, the race to the bottom is inevitable.'*
>
> *(Survey respondent)*

> *'Many clients have shifted security responsibility to procurement, which in some respects is not a bad decision, however the procurement teams need to stop treating getting security delivered at the lowest cost possible as a success. Success will be paying a fair price that is linked to inflation as a minimum baseline standard.'*
>
> *(Survey respondent)*

> *'Procurement professionals need to appreciate that they do not manage the function, they have a role to get the best value for money but the final decision needs to be based on the end user - it is not always the cheapest'*
>
> *(Survey respondent)*

> *'The (adverse) influence of Procurement specialist is a major issue for us. Procurement people are specialists in procurement, not security, and are surprisingly ignorant about the complexities of the security industry. They will always tend towards the cheapest tender, which, especially in the labour part of the security industry, actually results in poorer outcomes and a poorer return on your investment.'*
>
> *(Survey respondent)*

3.43. The overall perception of respondents appears to be that there are weaknesses in the approaches taken to buying security:

- 63% (n=158) agreed that **clients are slow to adapt to changing security requirements**; current security managers 'not involved' in the security budget much more commonly agreed with this, than those that were 'responsible' for the budget[36].
- A half (51%, n=126) agreed that **clients are poor at securing the relevant security services for their security requirements.**
- Only a quarter (27% (n=68) agreed that **generally speaking, clients have an accurate grasp of their security requirements** whereas 45% (n=111) agreed that **suppliers have a much better grasp of a client's security requirements than clients do.** Although on the latter point this view was considerably more

[36] 58% of current security managers 'not involved' in the security budget *agreed or strongly agreed*, compared with 54% of those 'informed' about the budget, 49% of those 'consulted' about the budget, 47% of those 'accountable' for the budget, and 36% of those 'responsible' for the budget.

prevalent among current 'contract' security managers than current 'in-house' security managers[37].

- Only 14% (n=34) agreed that **clients are good at allocating the right amount of budget to the level of risks they face**; and notably, those with the least influence over the budget, were the most likely to disagree[38].

3.44. There was some criticism too of the focus of suppliers - just under half of respondents (48%, n=119) agreed that **security suppliers are focused on hitting targets rather than offering the best security**; and here it was the current 'in-house' security manager respondents that were more likely than the current 'contract' security managers to hold this view[39].

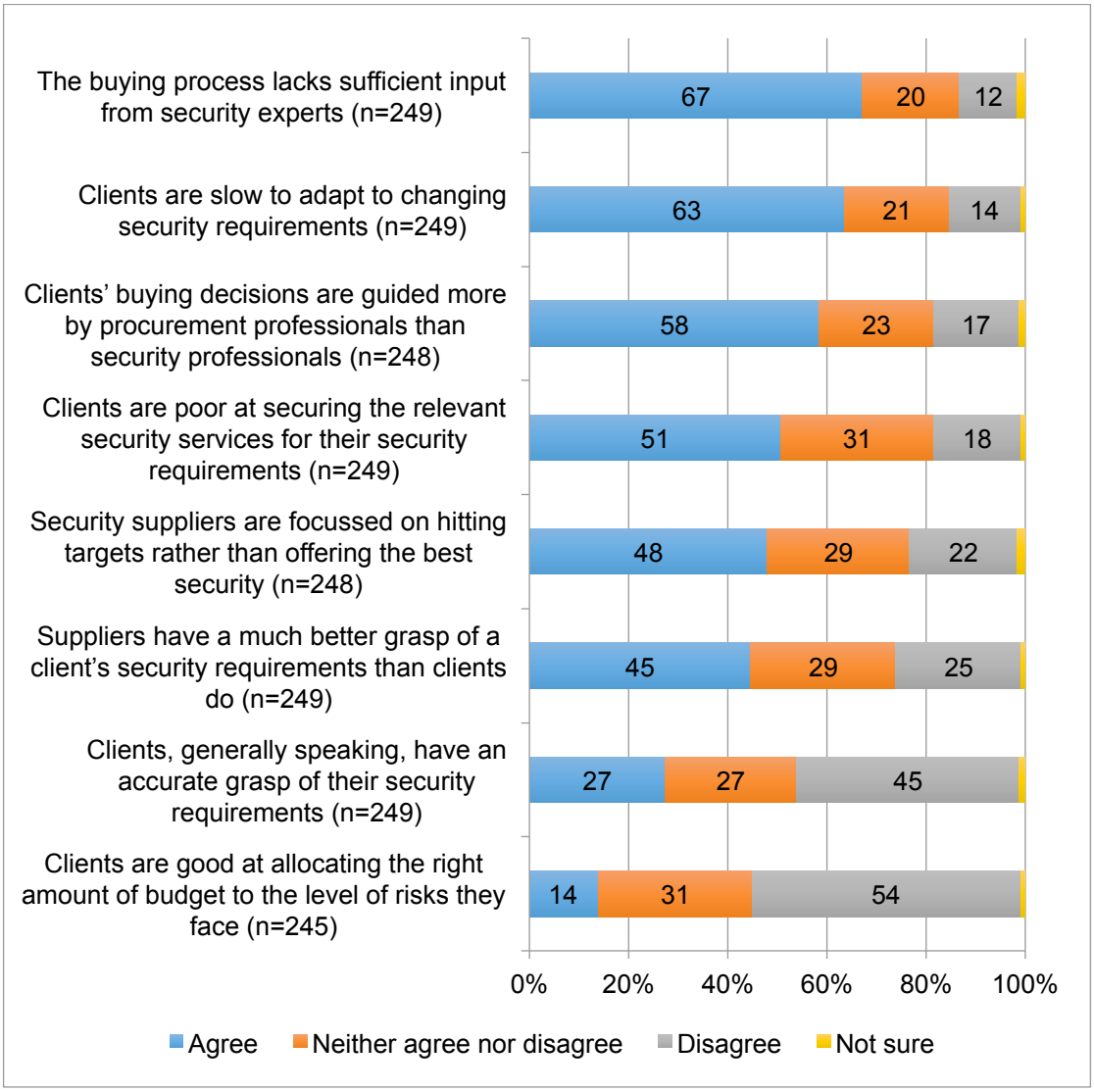
3.45. A number of respondents noted however that the procurement of security is an area where it was particularly difficult to generalise. Some acknowledged that some clients and suppliers were excellent in understanding requirements and procuring effectively, while some clients and suppliers were poor. Figure 14 displays the results.

[37] 41% of current 'contract' security manager respondents *agreed or strongly agree* that suppliers have a much better grasp of a client's security requirements than clients do, compared with 22% of current 'in-house' security managers.

[38] 55% of current security managers 'not involved' in the security budget *disagreed or strongly disagreed*, compared with 50% of those 'informed' about the budget, 48% of those 'consulted' about the budget, 36% of those 'accountable' for the budget, and 25% of those 'responsible' for the budget.

[39] 37% of current 'in-house' security manager respondents *agreed or strongly agree* that security suppliers are focused on hitting targets rather than offering the best security, compared with 29% of current 'in-house' security managers.

Figure 14: Factors affecting the procurement of security %



Factors that are important when purchasing security

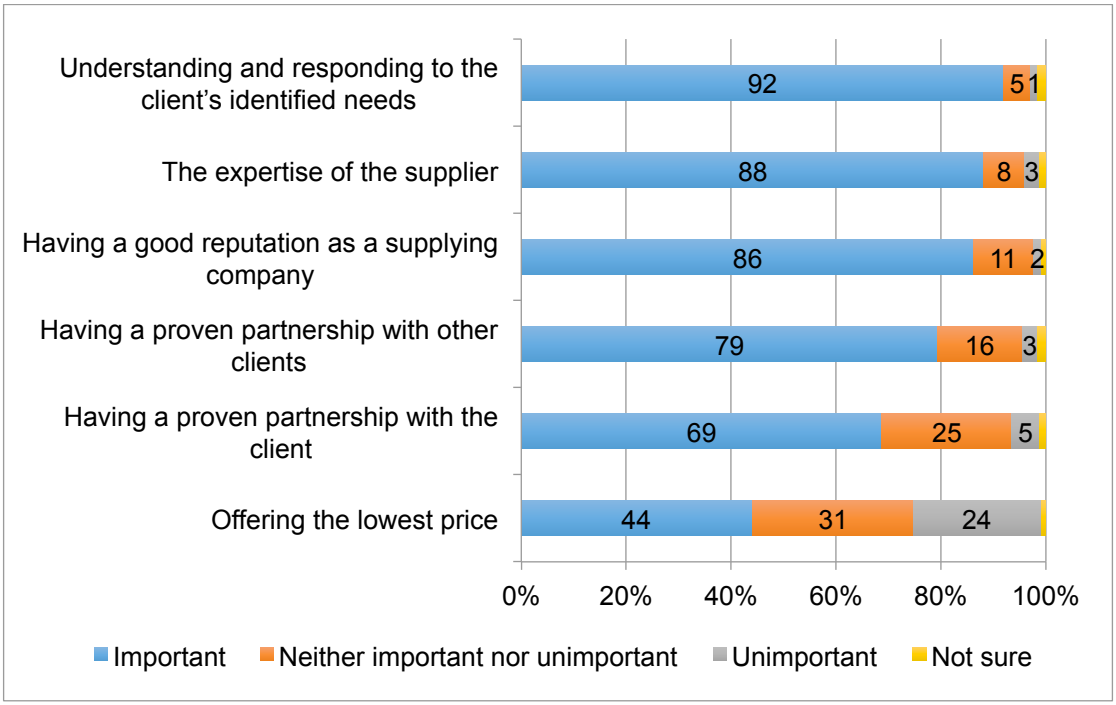
3.46. A number of statements were presented to gain an understanding of how important a number of factors are perceived to be, to a purchasing organisation, when security suppliers are responding to an invitation to tender.

- **Understanding and responding to the client's identified needs** was considered most important – 92% (n=226) indicated this is 'important' to the purchasing organisation.
- The **expertise of the supplier** (88%, n=216) and **the supplier having a good reputation** (86%, n=212) were also perceived by the vast majority, to be 'important'.
- **Having a proven partnership with other clients** (79%, n=195) was more commonly perceived to be 'important' than **having a proven partnership with that client** (69%, n=169), although both

were perceived to be important to a purchasing organisation, by a high proportion of respondents.

- **Meanwhile**, **offering the lowest price** was considered to be the least important factor of those explored to a purchasing organisation – less than half (44%, n=108). The findings are shown in Figure 15.

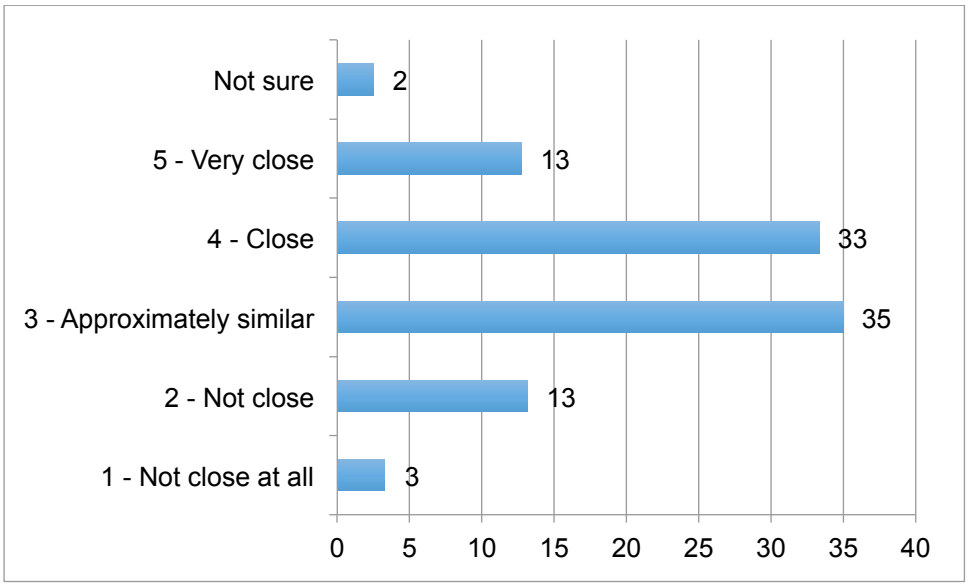
Figure 15: Factors that are important to a purchasing organisation (n=245-246) %



3.47. Notably, both current 'in-house' and 'contract' security manager respondents were aligned on the importance of these factors with very similar proportions rating each as important.

3.48. Respondents were also asked to what extent the security provision outlined in the contract agreed between the client and contractor, mirror what is implemented in practice. It seems that the two are rarely a 'very close' match (13%, n=31). Most commonly they were considered 'close' (33%, n=81) or 'approximately similar' (35%, n=85). This is shown in Figure 16.

Figure 16: How closely the provision outlined in the contract, mirrors what is implemented in practice (n=243) %



3.49. The current security manager respondents with the greatest level of influence over the security budget[40], and those that were the most satisfied with their level of influence[41], and those that viewed their current budget to be sufficient[42], were far more likely to indicate provision was a close reflection of the contract.

3.50. The main suggestions offered by respondents on why the reality may differ to the provision described in the contract included:

- There may be adjustments that need to occur when the contract commences, and theory becomes practice, in order to best meet requirements; similarly not all requirements can be foreseen.
- Requirements naturally change over the life of the contract, therefore the contract is a starting point.
- Clients may have underestimated requirements; or may have overestimated what is realistic within the price.
- 'Mission creep' - clients may seek to add duties subsequently.
- Suppliers may have over-promised what can realistically be achieved for the price.
- There are cases where an alternative to the technology specified is implemented for example due to a supplier looking to make a saving, or due to the technology specified not being compatible with existing systems.

[40] 45% of security managers 'responsible' for the budget considered provision to be *close or very close* to the contract, compared with 19% of those 'not involved' in the budget.
[41] 49% of security managers that are 'very satisfied' with their level of influence over the security budget considered provision to be *close or very close* to the contract, compared with 24% of those that are 'very dissatisfied' with their level of influence.
[42] 44% of security managers that viewed their current budget to be 'sufficient' considered provision to be *close or very close* to the contract, compared with 29% of those that viewed their current budget to be 'insufficient'.

- Those overseeing performance are not always familiar with the content of the contract or otherwise lack the knowledge or capacity to effectively manage the contractor to ensure requirements are met.
- Information used to create the specification and subsequent contract (such as risk assessments) may have been out of date or inaccurate.
- Security may be part of a larger contract of provision (e.g. total facilities management) and therefore the security element may be vague and/or poorly specified.

Factors that increase the likelihood of a security manager influencing the security budget

3.51. Respondents were asked to suggest in their own words, the factors that would increase the likelihood of a security manager having an influence over the security budget. 172 individuals answered the question, with some referring to a number of factors. All of the factors suggested were arranged into themes which are summarised below.

3.52. The most common factor raised related to being good at what you do (n=48) – delivering a good service, having a depth of experience and knowledge, and knowing how to provide security that best meets the requirements of the organisation:

> *'Experience and good knowledge as well as integrity.'*
>
> *(Survey respondent)*

> *'Having a clear understanding of what "good security" looks like.'*
>
> *(Survey respondent)*

3.53. This was closely followed by factors relating to the status, credibility, and qualifications of the security manager (n=40), for example:

> *'Credibility of the Security Manager - what other relevant qualifications, accreditations and industry memberships does the Security Manager have?'*
>
> *(Survey respondent)*

> *'Gravitas of the person, the department and the accountabilities for security at the C suite level.'*
>
> *(Survey respondent)*

> *'Having a seat at the table and being perceived as a valuable component of an organizational resiliency as opposed to being viewed as a cost center.'*
>
> *(Survey respondent)*

3.54. The need to be effective at building relationships was also frequently mentioned (n=29) – for contract security managers this was particularly important in terms of building a strong relationship with the client; but it also applied to in-house managers – particularly building a relationship

with senior management and the board, and also with procurement were seen as important steps to influencing the budget. For example:

> *'Having a good relationship with the procurement teams.'*
> *(Survey respondent)*

> *'A close and very good working relationship with the client (Decision maker).'*
> *(Survey respondent)*

> *'Board level engagement and operational stakeholder buy in to a detailed plan.'*
> *(Survey respondent)*

> *'Communication and relationship with the peers in the organization.'*
> *(Survey respondent)*

3.55. Almost as many (n=26) highlighted factors relating to having a business case and being able to articulate the benefits of security and the 'return on investment':

> *'Ability to communicate strategically in terms of cost effectiveness and return on investment; using appropriate data effectively to manipulate an argument.'*
> *(Survey respondent)*

> *'Being able to articulate a business case for security as part of value creation to the organisation. An enabler to retain and grow the business over a pure cost.'*
> *(Survey respondent)*

> *'Clear linking of budget with priorities and risks, clear articulation of value add for the business and how people are protected.'*
> *(Survey respondent)*

3.56. The security manager understanding the business, was also considered important (n=20) to being able to influence the budget – a number of respondents highlighted that demonstrating business acumen and financial knowledge were key:

> *'Knowing the business, looking at the holistic risks of the business, ESRM approach to the business cases that is ruthlessly focused on the business's value.'*
> *(Survey respondent)*

> *'High level of financial and commercial awareness.'*
> *(Survey respondent)*

> *'They have to understand the business and the only way that this can happen is by getting a seat at the table and adding additional value to the corporation that is not just about risk but about all aspects of the business.'*
> *(Survey respondent)*

> *'If the manager only speaks the language of security, they will never break out of the security bubble and convince*

others in the organisation of the need to buy into the concept and provide a suitable budget.'

(Survey respondent)

'Understanding and articulating security in terms of client business objectives.'

(Survey respondent)

3.57. The same number (n=20) noted that it is often the occurrence of an incident that can be the trigger to a security manager gaining more influence over the budget. A number of respondents felt that when things go wrong, organisations are more willing to take input from their security experts and allow security teams to request more budget:

'A company that has previously suffered loss will usually allow security managers to bid for a better budget.'

(Survey respondent)

'After a major loss caused by weak security CFOs and CEOs react with budget increases for security.'

(Survey respondent)

'Critical events that directly impact the business.'

(Survey respondent)

3.58. Although it was apparent across a number of the themes noted above, a small number of respondents (n=5) also specifically noted that the 'culture' of the organisation was significant, with those that value and prioritise security, more likely to value the input of the security manager.

Summary

3.59. The findings of the survey suggest that concerns remain that the purchasing of security lacks sufficient input from security experts, and that procurement departments continue to push for the 'cheapest' rather than the 'best value'. It was also apparent that relatively few respondents (especially suppliers) felt clients have an accurate grasp of their security requirements, and even fewer thought clients are good at allocating the right amount of budget to the level of risks they face. Almost half of the current security manager respondents felt their current security budget was 'insufficient' (and particularly those that had the least influence over the budget).

3.60. The majority of respondents felt that security having influence over the security budget was key to delivering effective security, and security managers with the greatest levels of influence were the happiest with their current budget, and were also less likely to agree with criticisms of clients' awareness and understanding of security needs and approaches to purchasing. In short, having an influential security manager can to some extent negate the concerns noted above.

3.61. The current picture suggests though that it is by no means commonplace for security managers to have a high level of influence over the budget. Just over half of the respondents that were currently working as security managers' believed they personally had a high level of influence ('responsible' or 'accountable' for the budget) and while the representativeness of the sample cannot be determined (i.e. it is not possible to assert that this is true of all security managers), this is in keeping with a different angle explored – the majority of respondents felt that 'some', 'few', or 'none' (as opposed to 'most' or 'many') security managers had a major influence over the budget.

3.62. Respondents pointed to the importance of the competency of security leads and their 'status' and credibility in an organisation as being key determinants of the extent of influence on the budget; but also to specific skills, such as relationship building (particularly with the board and procurement), and that they understand and 'speak the language of business' and crucially can articulate the revered 'return on investment'. In the next section we explore these points in more detail.

Section 4. One to one interviews

Background

4.1. This section contains the findings based on 33 one to one interviews carried out with security professionals. Interviewees came from a number of countries, and held a variety of positions, although most were current 'security managers', and both in-house and contract views were represented.

4.2. The semi-structured interviews covered several topics relating to the role and influence of security managers. These included; career progression for corporate security managers; the different challenges faced by suppliers and corporates; what enables or prohibits managers from exerting influence (including influence over budget), and the relationships between physical security and cyber.

Are corporate security managers budding CEOs?

4.3. We asked interviewees about the options for career progression within the security sector and their perception of ambition amongst their security peers. Many of the interviewees talked about **career limits and a ceiling to progression**:

> *'I've been 20 years working for corporate American companies. Our career path stops at Chief Security Officer.'*
>
> *(Interviewee 6, In-House Security Director)*

> *'In my experience…folks that have aspirations for executive positions are more likely to set up their own company or go to a contractor.'*
>
> *(Interviewee 3, In-House Security Director)*

4.4. Many interviewees felt that security professionals were **overlooked** regarding progression, for example:

> *'Quite often the corporate culture might overlook an individual's talent because they are from security.'*
>
> *(Interviewee 17, Supplier, Senior Executive)*

4.5. Some of the interviewees suggested ambitious security professionals would need to take **'sideways steps'** into other business areas in order to progress their career. They felt that this step would be **required to gain both skills and the recognition required** to progress:

> *'Probably be a necessity to take some sideways step to a different part of the organisation before you could get to*

CEO – to prove skills and get experience in other functions.'

(Interviewee 20, Security Consultant)

4.6. The interviewees identified ways in which limits to progression occurred. Generally, throughout the interviews people spoke about the difficulties that security professionals could face **integrating with wider business culture, gaining visibility and speaking the language of business**:

'…there are two parts to this – the businesses don't recognise or fully understand the security in the corporate environment because their work is based on profit and loss, whereas the security function is protecting/enabling this environment. Secondly, not enough security practitioners educate themselves in a business sense – they do in security, but not in general business.'

(Interviewee 22, In-House Security Director)

4.7. A prevalent theme to emerge was that where the security managers' work was focussed on **operations rather than strategy**, they were less likely than other business functions to gain the recognition needed to reach the highest level:

'To some extent this is because they are too involved in operations and not enough in strategy and so we don't have access to and presence amongst senior management.'

(Interviewee 27, In-House Security Director)

'We also have the problem that there are lots of folks in security where they are 'tactically-minded' rather than consider the business side of things (want to be the SWAT team) - so it's a bit of an uphill struggle to move up in an organisation with this attitude.'

(Interviewee 21, Supplier/Contract Account Manager)

4.8. Some felt that there was a **lack of ambition** amongst their peers, and that this may be due to the nature of people who were employed within the security profession, including people who entered security as a second career.

'I think in this company yes, but generally in security people are not attracted to it…people don't tend to aim that high.'

(Interviewee 18, Supplier/Contract Account Manager)

4.9. Related to this, some interviewees suggested that old fashioned views and **prejudices around people in the security** industry disadvantaged people who had ambition:

'No, security is a poor cousin, it was seen as an old man's job and is still seen in this way. It will be incredibly difficult to become a CEO against this background.'

(Interviewee 25, In-House Security Director)

4.10. Some interviewees highlighted **positive changes, and ambition in younger security professionals**. This included improved perception of their role within an organisation, improved confidence, and understanding of business:

'I definitely think that some see themselves in that fashion – some, not all…for the ones that do – they have a certain ambition and a very healthy somewhat perception of their role in their organisation. Those that don't, tend not to project a lot of confidence, just provide advice but often not taken that seriously…'

(Interviewee 17, Supplier, Senior Executive)

'Security practitioners need to understand how business works and there are some strong efforts happening here. Also, it (security risk management) needs to be a fundamental part of an MBA programme.'

(Interviewee 22, In-House Security Director)

'In the younger up and coming professionals, the career professionals, they do have that mindset."

(Interviewee 4, In-House Security Director)

4.11. Some talked about their personal experience and ambition coming from a security position, for example:

'In my current role I don't see myself as CEO. In retail or manufacturing I could see myself aspiring beyond the security role. I do see myself of the entrepreneur/CEO type mind set.'

(Interviewee 4, In-House Security Director)

4.12. A few talked about the difference between contract and in house security and career progression:

'In contract security you have a diverse portfolio to work from. For the in-house security the highest role you can get is the Chief Security Officer or Chief Risk Officer. You have a better chance in [contract] *security of progression because it is cheaper.'*

(Interviewee 1, Supplier/Contract Account Manager)

How do the roles of contractors and corporate security vary?

4.13. When asked about the relative similarities and difference between security managers that are in-house and contract, and whether for example it is easier to transfer from one to the other, some of the interviewees felt that these roles were broadly interchangeable:

'They are similar and interchangeable. It's no harder to move either way – I have been in-house before many years ago and then moved to a supplier - people do this all the time easily.'

(Interviewee 18, Supplier/Contract Account Manager)

'The fundamentals of security are all the same. What you learn as your professional skill it's the same. It's all risk based.'

(Interviewee 5, Supplier, Senior Executive)

'I think it's incredibly easy to transfer – it [security] *is growing but still seen as quite niche…Because it is a closed environment you will find people move from a government role, to consultancy, to a direct* [in-house] *role, back to consultancy.'*

(Interviewee 9, Security Consultant)

4.14. However, many of the interviewees highlighted the **different skills** that develop in people working in corporate or in-house security, and how, as a consequence, moving between these settings would be challenging and require adaptation. A broad view was that in-house professionals may need to develop their sales skills, while contractors would need to adapt their business language and learn to engage with senior management:

'The difference with supplier security managers is that they manage big teams, including the frontline. The benefit [corporate security managers] have is that they talk to the C Suite, well some do.'

(Interviewee 10, Supplier, Senior Executive)

'Either should be able to go either way – some in-house might have difficulties in selling services, and some contractors might find it a step change getting to grips with the business speak.'

(Interviewee 22, In-House Security Director)

'It would be challenging to swap roles as I think we work in different ways. In their world it is about being profitable and managing clients, whereas I am thinking board, operations and people. We would need to be better sales people they would need to be better at senior management engagement.'

(Interviewee 27, In-House Security Director)

4.15. Interviewees also drew attention to the **different objectives** of corporate and in-house security teams:

'Some things are similar, but the objectives are different. Mine in my corporate role is to protect the assets of the business but they as suppliers don't have such a wide remit and in their main objectives they have to make a profit and deliver and think about the next contract.'

(Interviewee 27, In-House Security Director)

'Contract security manager function, from my experience, is more akin to a HR manager – more to do with staffing and service levels, whereas in-house would focus directly on the security issues and requirements of the organisations.'

(Interviewee 20, Security Consultant)

4.16. Some of the interviewees felt there was a specific **direction in which it would be easiest to move**, but these views were generally mixed.

4.17. Some thought that the in-house role was **more challenging** and therefore it would be difficult for a contract professional to transfer because of a narrower business experience:

'I think it would be easier for an in-house to step into a contract role. For the inverse, they might not have had the same levels of visibility on the security detail and security postures, as there would be for an in-house employee.'

(Interviewee 20, Security Consultant)

'Massively different. Corporate security mangers can do what a supplier does but not the other way around…I can do their job. I do a lot of the managing them anyway and I feel I could click in easily. The other way is difficult because of a lack of understanding of the business.'

(Interviewee 25, In-House Security Director)

4.18. Conversely, though, some thought the nature of contract work required a **very different 'culture'** which was alien to in-house professionals, which would make it difficult to transfer. This included for example having to please clients and be very flexible and adaptable:

'I definitely think they are interchangeable, but not both ways as easily. An in-house manager coming into the contract management side of it – I think it would be very hard for them to understand – but definitely from the contractor side it would be an easy transition. I feel an in-house team see themselves as a cut above the rest – that is what would cause the issues - that superiority.'

(Interviewee 19, Supplier/Contract, Account Manager)

'Going the other way is virtually impossible for in-house security managers, because we are lazy, we don't do as much work as we think we do. If you look at what an account manager does for half your salary, we would run away screaming – when you look at the transfer the other

way. We don't know how lucky we are…In the vendor world, there is no safety net, they are at the whim of the customer. If they don't like your face, you will be removed from the contract…I know some that tried to move across but got themselves back to in-house as quick as they could. The money lured them in, company car, compensation but they didn't realise how many more hours it would be, how much more work – that's the difference.'

(Interviewee 6, In-House Security Director)

4.19. One interviewee saw it as a distinct advantage when **security professionals come to in-house security from a contractor background** where customer management skills were learned which could then be applied to good effect:

'I'm a great believer of the transition from vendor to in-house – if you get them at the right point in their career the transition can be fruitful.'

(Interviewee 6, In-House Security Director)

Are security managers as influential as other managers?

4.20. A few of the interviewees talked about their experiences of being **equally respected** as part of the management team:

'When I worked in corporate security I felt as influential as any other senior manager.'

(Interviewee 18, Supplier/Contract Account Manager)

'The vast majority of the management here do respect the in-house and my own [contractor] *bosses. That's not the case everywhere.'*

(Interviewee 8, Supplier/Contract, Security Manager)

'In an events scenario – the Security Manager is very important – just as important in management as anyone else. If you have a weak security manager you will have a weak event – it doesn't work.'

(Interviewee 2, Supplier, Senior Executive)

'…I had a conversation with a Vice Chancellor at a university and we were talking and she said, before you go, don't go out thinking you're not important [as a security professional]*. She said any conversation I'm having with someone who will cure Multiple Sclerosis or cancer – they want to know, is my car safe, am I safe, who is checking on me when everyone else has left. The most important person to him is that security man (sic). And I thought, what we are, is facilitators.'*

(Interviewee 2, Supplier, Senior Executive)

4.21. One interviewee was experiencing a positive change within their organisation, where a more systematic approach to identifying priorities was being undertaken:

> *'Things are changing, especially in the last two years here. They want to see a more homogenous alignments of…let's call them silos. To me this is a risk management process. They want to be able to compare and contrast (the silos) and for people to speak the same language. They want to know the top risks in the organisation and then be able to say why they are high risk. Having that same system of assessment across the organisation helps this, rather than just a stab in the dark. Moving from security being a bolt on to a more integrated function.'*
>
> *(Interviewee 23, In-House Security Director)*

4.22. However, many of the interviewees felt that security managers were **not as influential or visible as other management**. Overwhelmingly, this was perceived to be due to **a relative lack of interest in and value of security**:

> *'We just don't have an influence beyond security, people just are not interested and this company is better than the last one I worked at.'*
>
> *(Interviewee 25, In-House Security Director)*

> *'Security isn't seen as seriously as other functions – security is a very out of sight and mind – it's not the 'big sexy' – we don't add anything exciting – it's like having your house painted – it looks fantastic and is immediately noticeable. We're more like the guy who fixed your light switch – it's just not going to have that impact.'*
>
> *(Interviewee 21, Supplier/Contract Account Manager)*

> *'They don't see us.'*
>
> *(Interviewee 1, Supplier/Contract Account Manager)*

> *'Very little* [influence] *to be honest. I deal with a variety of stuff because I also have a compliance role, in part to get people to take me seriously. We are in the same bracket as cleaners and waste management.'*
>
> *(Interviewee 25, In-House Security Director)*

> *'Here it's quite separate standalone dept – we produce reports – people just see us there and keep things ticking over, we need a change in culture really.*
>
> *(Interviewee 16, In-House Security Manager)*

4.23. Some of the interviewees reported that **situational events**, for example recent global events, resulted in security having more influence, however, opinions varied as to whether this influence would remain:

> *'2 or 3 years ago I would have said more operational and less engaged. After the pandemic, Ukraine and other*

things that have been business critical, where what we do is critical to enabling operations, well now I get daily contact with senior managers.'

(Interviewee 27, In-House Security Director)

'I don't think quite as important as other managers. But once a disaster hits – everyone is asking why didn't we see it? They don't care until it happens and then it becomes super important…I think it [influence] *is just for the duration of the incident. They think it's cool that we've solved it – now you should go back to your recess and don't speak up.'*

(Interviewee 4, In-House Security Director)

4.24. Some of the interviewees attributed the level of influence held by security managers to **individual factors** and their 'soft' or interpersonal skills:

'You can put together the best business case and relevant data and present it well, but unless you have that real 'dynamic' skill of attracting someone's attention and making them interested in what you're presented you won't succeed. If you don't have the ability to do that, you're not going to be able to influence the people in the organisation.'

(Interviewee 17, Supplier, Senior Executive)

'It's an impossible question to answer. It is always going to be down to the individual's ability to influence the behaviour. If you don't have influencing skills it's going to be really really difficult.'

(Interviewee 3, In-House Security Director)

Who owns security budgets and how are they set?

4.25. The feedback from interviewees suggested that 'ownership' of the security budget **rarely sat with security**:

It tends only to be security when they are big enough – otherwise they are part of another department or function.'

(Interviewee 20, Security Consultant)

4.26. More commonly, it was owned by finance, procurement or facilities management departments and security was competing with other departments for a portion of whatever size pot was available. There were **variations** in the approaches to setting the budget, only some starting from scratch each year:

'Security budgets will depend on the individual entity – some have national sophisticated frameworks with generous budgets throughout the regions but others look

at a property they manage and literally just see what they can do as a minimum.'

(Interviewee 17, Supplier, Senior Executive)

'There are some clients who start with a blank sheet and ask you ok define what I need and let's build it up from there.'

(Interviewee 10, Supplier, Senior Executive)

'The percentage thing was the thing in the past. We're changing legislation regarding minimum wage – the cost of licensing – contract security staff – we have to build that in to our cost. To do that we have to be very open and go back on a yearly basis and say this is where we are, this is what it will cost us to do that, based on wages. And as long as we are open and honest.'

(Interviewee 2, Supplier, Senior Executive)

'Most clients have budgets that use previous data and use forecasts not withstanding capital budgets – operating budgets normally using historical data to forecast where they're going next year.'

(Interviewee 17, Supplier, Senior Executive)

'Procurement will say I have this budget what can you do? And we can discuss what is needed. If a security manager is in place, and they come from the contract sector they understand so it is not so much of a battle.'

(Interviewee 26, Supplier, Senior Executive)

4.27. Some thought there was a **lack of any strategic thinking** in regards to the setting of security budgets in their organisations:

Hand on heart I would say it is still probably finger in the air, and driven by tech or bits of kit – need for a new fence, new CCTV. Because security risks very rarely seem to appear on the business risk register; they tend to be at the operational/tactical level, rather than at the strategic level.'

(Interviewee 9, Security Consultant)

4.28. Some contractors talked about the difficulty of securing budget **based on risk**:

'It works on probability of occurrence. I can tell you if I went to a client and said we need another officer in this location because of a risk – I could do that until I'm blue in the face. Normally they won't budget for that.

(Interviewee 1, Supplier/Contract Account Manager)

4.29. Some noted that there was a focus on **cutting costs**:

'I think most of the time, they will say you had x amount last time, this time we'll take off 2% because of what is going on in the world.'

(Interviewee 9, Security Consultant)

'If your staff are just being tasked to drive down costs. Then it's a case of the old saying – they know price of everything and value of nothing. [As a contractor] You need the security manager on your side to say this is the value in what we are providing. With manned security the problem is showing that. It is not of case of showing we are making so many teacups or saucers. Its intangible. But I have to say, we have very few problems with this, because of the attitude we have to it.'

(Interviewee 2, Supplier, Senior Executive)

I have some big brands, huge conglomerates; organisations making billions of sales, but they will only give their facilities teams maybe minimum amounts to provide services and that team must cut what they have to meet all services, pest control, security and cleaning and they are all getting cut. So the starting point of the problem is companies internally not providing the budget holder with the right budget to deliver the service. It starts early on in this process. So by the time it gets to the RFP you are way past being able to influence.

(Interviewee 15, Supplier, Senior Executive)

We need to educate people on what security is. Otherwise it will always be a grudge purchase and always be about numbers.

(Interviewee 10, Supplier, Senior Executive)

4.30. Some of the interviewees noted that securing an adequate budget was becoming **increasingly challenging**:

'I went to the head of [a function] *and said, this is what we can do - if you can invest, it will go a long way to mitigate that risk. He gave us the money and we fixed it and we saved him a lot of money and he was very happy. But it does make it very difficult when instead of a uniform approach – this is the amount of money we need – to be told no – and have to go cap in hand to individual functions to say I need some money.'*

(Interviewee 3, In-House Security Director)

'I think personally speaking, I've never had too much of a problem getting what we needed. It is a challenge though and it gets harder each year, and we get better at saying why and where we need it… We have a proactive programme of upgrades – spread them over a 3 year period so they know its coming and can see it coming over the 3 years. The story you put with it, you've got to engage the board individually beforehand so when they get in the room they all know about it, then tick, done. But you've got to put the hard yards in.'

(Interviewee 7, In-House, Senior Role in Security)

Do security managers have enough influence over budget?

4.31. Predictably there were **mixed views** on this issue. Once again level of influence was linked to professional competence, which not all had, at least not all were skilled in the art of arguing for money compared to other business professionals:

> *'I don't see how you can set a budget without taking into consideration input from a security expert. It would be very foolish. If you don't have confidence in the security manager then you have the wrong one.'*
>
> *(Interviewee 2, Supplier, Senior Executive)*

> *I think it is factual we are low down, there are other groups who get the money whereas we have to fight. They are more central to business goals, anything that can impact on manufacturing is a bigger priority.*
>
> *(Interviewee 25, In-House Security Director)*

> *'A lot of Security Managers are timid – they don't want to upset the apple cart. But you can do it respectfully.'*
>
> *(Interviewee 1, Supplier/Contract Account Manager)*

4.32. Some reiterated the point that a serious incident can increase the budget, and had done so for many in the pandemic, but some felt that they were able to **proactively** secure the money they needed as long as they presented a strong business case:

> *'We put forward a business case if we need an increase. I would say we have a very good influence over the budget – we set our own budget and rarely is it rejected. We keep having to make savings, but we can accept that, or counter it with a good argument.'*
>
> *(Interviewee 22, In-House Security Director)*

4.33. There were though some tricks that increased influence and a key one was relating security spend to broader **business concerns.** Where an investment in security is linked to improved sales that can be an advantage, such as one retail loss prevention manager who linked having CCTV to making visible the 'customer journey' (i.e. routes taken via the store, time spent pausing at different sections, factors that may have influenced buying decisions, queue management). Another example related to health and safety:

> *'We had an old CCTV system and I said you will have losses, but my case is stronger when I say there are health and safety issues to this and that is always more persuasive where people may get hurt they care more which I understand. So I play the health and safety card when that is needed to get me what I want.'*
>
> *(Interviewee 25, In-House Security Director)*

4.34. Another tactic was to highlight the risks created in budget refusals:

'The budget is split between sites, four sites, and we will have more sites coming on, the budget is held by a senior manager at the site and we will sit down and say this is what we need for the year or they will tell us which is usually the case. My role is advisory … I will do surveys, I will make recommendations, if they refuse then I can put that into the risk register so I can refer this to the business. The risks registers are looked at every month.'

(Interviewee 25, In-House Security Director)

Contractor influence on budget

4.35. Interviewees were also asked their views on the extent to which contract security managers have an influence on the budget. Again, there was considerable variation. Some thought they had **no influence**, and that they simply worked to the specification they were required to deliver:

'They have no say and they don't understand it, they are part of the budget not a controller of it.'

(Interviewee 24, Security Consultant)

'We're not really influential because we're an external provider.'

(Interviewee 18, Supplier/Contract Account Manager)

4.36. Indeed, some in-house interviewees and some consultants saw it as important that contract security managers are **not allowed influence**, because of the possibility they will put their own interests first:

'I think if I'm honest they are going to have a very skewed approach to that – they are always going to think, how can I prolong the contract, get more out of it, and any input they have will be based around what their [supplier] *organisation can provide, rather than what the client really needs …. No contract security manager would ever say you would be better moving to in-house. I don't think they would make unbiased decisions, because it's not in their interest.'*

(Interviewee 9, Security Consultant)

'I think they certainly play a role in providing information about the efficacy of the equipment or resources but that whole decision piece – I don't think there's much influence. I think it's really around responsibility and accountability from who owns the budget and who is responsible and you couldn't or shouldn't give your contractor responsibility for the spending of the security budget.'

(Interviewee 3, In-house Security Director)

... you specify locations, hours and your assignment instructions and your requirements and they bid against

that. I don't need a manned guarding knuckle dragging provider to say actually I don't think you need that person there, or no person at all, we understand our business a lot better than any guarding provider, I would listen to what someone I respected says and if they were coming up with a spec or scope of works that they can price against then fine.'

(Interviewee 12, In-House Security Director)

4.37. Some suppliers indicated that they held a **small level of influence** with suggestions and recommendations being considered and sometimes taken on board, although these were more likely to be tactical than strategic:

'When first contracted I have some influence on wages but that's about it. I try to ensure that there's appropriate pay rates based on our budgets … what we would need to charge to cover our overheads and insurance etc. I factor that in just the security manpower part – other areas non-pay, I have no influence – I can offer some suggestions … but … offer recommendations based on relevant data and trends – but they are just suggestions.'

(Interviewee 17, Supplier, Senior Executive)

'Not a lot of influence at all - they have a budget when they go out to tender – they aren't going to go 10% above – the external company has little influence – we can suggest upping or the budget but nothing else otherwise.'

(Interviewee 18, Supplier/Contract Account Manager)

'Increases – we look at the national living / minimum wage – look at NI increases – SIA top up training for contract security officers – legislative increases and make an informed decision about pay and also an element for our overheads and profit, as they also increase in their background. We agree as a business how much we're going to be putting that up with our customers.'

(Interviewee 19, Supplier/Contract, Account Manager)

4.38. Some interviewees (both in-house and suppliers) felt that if there was a particularly **close relationship** between the contract security manager and the client organisation and/or where they played a **significant role** in the client organisation – for example where a client completely contracted out its security - they were more likely to have an influence:

'If you were an organisation that decided to outsource totally all of your security activity and you wanted a turnkey approach – say a small company with floor space in central London with 500 employees, and you just need a company to do security, 'tell me how much you need and what to do' I can see a contract security manager having influence within a pot of money determined by others.'

(Interviewee 3, In-House Security Director)

Yes [they can have an influence*] if he (sic) has a close personal relationship with the security manager and others in that business … we can get our two penneth in when we need to.'*

(Interviewee 2, Supplier, Senior Executive)

'if the relationship is right with your customers or decision-makers it is clearly valued, but that is different between clients. You have to make time to foster that relationship, whereas in-house it's already there.'

(Interviewee 19, Supplier/Contract, Account Manager)

'A contractor can still be visible but have to work hard to make that an invisible barrier … If you are employed by the company you are already there, you've already got that influence.'

(Interviewee 7, In-House, Senior Role in Security)

What helps security managers influence budgets?

4.39. We asked the interviewees about how they go about influencing the security budget and what facilitates this. A crucial aspect here was the ability to ***'speak the language of business'***. Those who felt they had good influence described proactively developing their knowledge and understanding of business by building relationships with senior management and developing their understanding of business goals:

'I have had to learn new skillsets. I did talk to CEOs and the senior management team and board members to see how they justify spend and the role of aims, mission statements and threats so that I too can talk the language they use. I don't think that this is common in my peer groups, I have a degree in business, albeit a long time ago and a good tutor.'

(Interviewee 27, In-House Security Director)

'Generally, they need experience of the industry and some have upskilled and trained in different areas of business operations – the more experienced ones I find are the ones making those decisions.'

(Interviewee 20, Security Consultant)

My experience coming up through the ranks, I was not an influencer in the early part of my career because I didn't understand business, I didn't build the correct relationships. [later in my career] *When I came in and met the senior leadership, I asked what are your pain points, where is security a pain for you and how can I fix it? I can fix those, build trust and then I had a seat at the table – it's about having that experience and self-awareness to engage with the right people and build trust.*

(Interviewee 6, In-House Security Director)

4.40. A few talked about the value of having **experience to draw on from working in other industries**:

> *'I would say experience – I have been involved in law enforcement and spent time overseas in Iraq and done all the fun stuff like this, but also spent 8 years working in service industry… Now you get some (recruits) from the police academy only 35 years old, so by the time their 50 years old and make their way up the ranks, all they know is law enforcement.'*
>
> *(Interviewee 21, Supplier/Contract Account Manager)*

4.41. Specifically, a crucial factor in the ability to influence budgeting, was being able to **create a good business case:**

> *'Identify the risk and the level and spread of that risk. That's the way we influence the budget here. You have to show why it's important you have this – that it is valid – not just somebody's bright idea, then support this with data to justify, then see if they are going to support this or not. It needs to complement the objectives of the organisation overall.'*
>
> *(Interviewee 23, In-House Security Director)*

> *'You've got to show the business in advance of taking the dollars that there is a role there and a risk that will be mitigated, these are my data points, what was achieved.'*
>
> *(Interviewee 6, In-House Security Director)*

> *'Those that really want to succeed really need to know how to communicate the strategic importance (of security) on finance and risk. Rather than saying 'we just need it' they need to put a business case forward addressing risks and costs – they need to hammer home the cost benefit and at the same time 'sell' security.'*
>
> *(Interviewee 17, Supplier, Senior Executive)*

4.42. More than just the ability to identify risk, was **the need to communicate the consequences of not responding** in terms that make sense for the business:

> *'If a manager wants to influence the budget, they will be using the risk register as their primary tool – this is where we are in the business world and this is what we need…you have to justify your spend.'*
>
> *(Interviewee 23, In-House Security Director)*

> *'Businesses grow but if your security doesn't you have increased risk, increased fatigue, it is going to fall apart on you. If you understand the game of finance for security managers, the easiest way to get money is provide them with a risk assessment and ask them to sign to say they accept that risk. It is the most successful technique I've ever used. You don't want to give me the money, here*

are the risks associated. I'm ok with that, but I need you to sign the piece of paper to say you don't want that.'

(Interviewee 6, In-House Security Director)

4.43. In setting out the business case interviewees described the importance of **selling positives and not focusing on negatives**:

'It's about how you present the business case for what you want to do. There is a tendency to over-emphasise the downside of not doing something - the doom and gloom stuff. While folk may listen they get bored when they hear it again. But if you emphasise the upside, that resonates better – change or influence on reputation – potentially creates revenue, that's always good.'

(Interviewee 3, In-House Security Director)

4.44. The basis for a good business case was invariably collecting good **data and using it effectively**. This was seen as a key aspect of creating a good business case:

'…but presentation skills again and a good business case – you cannot have too much data to make a case – real examples help as well.'

(Interviewee 17, Supplier, Senior Executive)

'I own it and am passionate about it, I can justify all the steps we've been through considering different options. You have to be really well prepared for all eventualities and present different options. We always present three. If you've got 3 scenarios, including the things that desperately need to be done, that'll keep the lights on.'

(Interviewee 7, In-House, Senior Role in Security)

'On the contract side. The key to influence is developing better metrics, showing the value that the supplier brings. When I talk to vice presidents and CEOs, they just don't know.'

(Interviewee 24, Security Consultant)

4.45. Interviewees talked about the need to **develop strategic relationships**, and the potential associated with **educating senior management** in regards to security:

'For Security Managers it is having ROI and partnership with budgetary leaders, so that they can understand why we are making the suggestions we have. Any time I enter a new role, I partner with executives, walk the property together, talk about things, so that they understand why I get passionate about it. I try the education piece, it doesn't always work but I feel better having gone through it.'

(Interviewee 4, In-House Security Director)

4.46. Against all this a few interviewees talked about there being **limited opportunities** for security professionals to be involved in budgeting decisions, resulting in a lack of experience, and henceforth, expertise:

> *'There is not enough exposure* [of security to budgeting decisions] *– and it is a problem because how can someone get experience if nobody gives them a chance.'*
>
> *(Interviewee 1, Supplier/Contract Account Manager)*

> *'The security managers do lack skills. In my experience the ones I work with are either ex police or military, probably have done security for years and there is nothing out there, say an apprenticeship where you can teach security managers.'*
>
> *(Interviewee 25, In-House Security Director)*

Relationship with cyber security

4.47. We asked the interviewees about the relationship between cyber and physical security, and whether the needs of cyber were more recognised within their organisations. Most of the interviewees felt that **the needs of cyber security were prioritised over physical**:

> *In some respects cyber is shouting louder. The information fed up to the director to make those decisions is often skewed.*
>
> *(Interviewee 9, Security Consultant)*

4.48. For many, cyber and physical security were very **distinct** within their organisations:

> *'I'm generally seeing these are separate functions with very little, if at all, overlap – and more IT driven for cyber security.'*
>
> *(Interviewee 20, Security Consultant)*

> *'With us it's two different entities – cyber security is an IT function and we don't have anything to do with it.'*
>
> *(Interviewee 16, In-House Security Manager)*

> *'I think people like to pretend that they are together, but really, they're not – they are different – they're just not … they are two groups working and thinking in different ways – we're not there. If you compare cyber security to physical, then cyber security is three-week old baby, very much in its infancy.'*
>
> *(Interviewee 21, Supplier/Contract Account Manager)*

4.49. A few interviewees talked about **integration** of the functions:

> *'We are fortunate that we have combined them in our organisation with info security – my boss is from a traditional (physical) security background. That's the way it should be (integrated). We've kept IT security separate*

though as a first line of defence and the rest seen as secondary parameters of prevention.'

(Interviewee 22, In-House Security Director)

4.50. Some interviewees noted there is an **ongoing evolution of security** and how roles within the field were changing, and how security professionals were either adapting to this change or resistant to it:

> *'Cyber in the next 10 years or so will be predominantly what the Security Manager focuses on. I have no background in cyber security but I'm starting to take classes and understand what that 'threatscape' looks like.'*
>
> *(Interviewee 4, In-House Security Director)*

> *'Cyber security is one of the reasons why a lot of managers have been scared away from positions. They are old school, not being familiar with technology. The cyber world is very scary. The virtual world is just around the corner. Clients will pay for that – those virtual pipelines allow the building of businesses. You have to get with the times and seek the best avenue.'*
>
> *(Interviewee 1, Supplier/Contract Account Manager)*

4.51. Explaining why they thought cyber security was higher profile, one interviewee noted that there was **more recognised interaction between staff and cyber** elements, so awareness of cyber needs was more prevalent. In contrast, people were less aware of physical security they were encountering and 'disconnected' with this:

> *'Once you have a bollard in place, it doesn't need continual tinkering. Physical security is quite static – it is all about protecting infrastructure. But people and boards go for cyber security – they are all using it, they understand it. Even though they walk through the* [access control security] *pod and see the guards, there is a disconnect there. Whereas they recognise they are using the laptop to do their job. …. People see themselves as interacting with the cyber element, but not with the security equipment.'*
>
> *(Interviewee 9, Security Consultant)*

4.52. Looking deeper at the disconnect between cyber and physical security within organisations, the interviewees spoke about their frustration about a **lack of organisational awareness** about the need for good physical security within cyber functions:

> *'… it's kind of a shame because good physical security concepts still apply to the cyber sec world – but it's where the allocation of funds is going… The amount a cyber-attack can cripple an organisation is very scary – even if one hacker gets in, they can shut you down and steal*

your data. It has a disastrous impact compared to a physical attack, so you can understand this somewhat.'

(Interviewee 17, Supplier, Senior Executive)

4.53. A few described their work to raise awareness of the links and importance of physical security to cyber security, and how they had worked to **partner with cyber** to improve their access to budgets:

'I think there is a huge emotional response by businesses to cyber security challenges and what is missing. I had this conversation with the VP of cyber security at my own company, about insider threat, about the risk of someone physically walking in to the building and getting access to our network. He thought 'oh shit, I never thought of that'. We forget, the easiest way to bring down a network is to get on site… The VP [of cyber security] *works in a separate vertical to me. He has bags of money, I can partner with him and attach my projects to him to get funding to enhance physical elements under the umbrella to a wider approach to cyber attacks.'*

(Interviewee 6, In-House Security Director)

'We keep saying it's great – need to fund [cyber security] *but we mustn't forget the physical side – but we're talking about people and people's behaviours – you need to frame the argument that the technical structure of cyber security is not the end of it, you need to spend money on changing people's behaviour – that always requires more money. Often you find you have got the technical solutions already, you just need to spend the money on educating people, it's a cheaper solution to solve the problem but it's a bigger / more difficult problem, but one thing we need to change. Rolls down into that thing – behaviours you seen online – you also see it in the physical environment – store things where they shouldn't etc. as an example.'*

(Interviewee 22, In-House Security Director)

4.54. In contrast to the majority opinion, a few interviewees felt that cyber was not dominating their organisations, for example, guarding contractors, and that they had maintained their distinction from cyber security:

'I personally am not seeing that – I'm not encountering that. On conversations they are tending to bring in other experts on cyber. I've always been a believer – maybe it has limited us – but we are a guarding company – not CCTV or alarms – it's easy to sound negative – that we don't do this or that. I believe stick to the knitting, know your job, know your bit and do that. I know good CCTV and alarm people and point them in that direction. I can't do that with cyber – we've had virtually nothing to do with it. Other people may be seeing that, but I'm not.'

(Interviewee 2, Supplier, Senior Executive)

Is there an incentive to perform badly in security?

4.55. We asked the interviewees whether there was a perverse contradiction inherent in the security field, where poor security resulting in incidents in turn highlighted the need for security investment. Some of the interviewees agreed with this, although more as a theory than in practice, in part because security personnel are ethical and motivated to protect, and also there is a growing appreciation of the value of security:

'If I go back many years I would have agreed, but the level of paranoia these days – I tend to think not. The covid thing has been a major changer of people's attitudes – in the past with the NHS – I said for 3 guards in A&E that'll cost this. They say, I can get a surgeon for that. And so they got the surgeon instead. But that's not the case anymore because that surgeon wants to be safe. The other thing is the police – the response is in most cases non existent – people are realising they have to protect themselves.'

(Interviewee 2, Supplier, Senior Executive)

I feel that we're almost incentivised to not be the best that we can. Most of the professionals are too ethical to do anything about that. It feels like we are punished if we are doing too well – why do you need more money if things are great.'

(Interviewee 4, In-House Security Director)

'Well, getting better is a risk but that is the way my job is, I want to get better so new risks come up and we do a good job, if it means less budget and influence then that is a price you have to pay…But events at the moment are massive and we are seeing high impact low probability ones like the war and pandemic so we can show value. So unlikely at the moment.'

(Interviewee 27, In-House Security Director)

> *My last job yes, this one no. My last job was about saving as much as possible. The role I have now, here security is still sufficiently important as all the deliveries are managed by my guys so that gives us a key role.'*
>
> *(Interviewee 25, In-House Security Director)*

> *Bad news sells newspapers – there is something in that. Its not something that I've particularly come across. I have seen the squeezing of budgets where whole organisations have had to go through cuts.'*
>
> *(Interviewee 9, Security Consultant)*

4.56. Interviewees spoke about how to circumvent the conundrum of good performance resulting in less investment. They identified that it was necessary to collect data, show value, and work towards **promoting organisational awareness and attitude change**:

> *'Catch 22, nothing ever happens because you are competent and they say they don't need you, which is why metrics are so important, you have to show value, responding to criminal activity was a small part of what I did, it is about so much more when done well.'*
>
> *(Interviewee 24, Security Consultant)*

4.57. Related to this, interviewees identified that security managers needed an awareness of change management processes and skills, because there was **resistance to change**, within organisations:

> *'Companies want to see their employees succeed as a whole but a lot are fearful of those that will replace them. I think people just generally do not like change at all. Make sure you stay in your place. Why approve a budget if you are doing the bare minimum with an acceptable amount. If something bad happens you have to save face, and show you have taken counter measures of putting things in to place.'*
>
> *(Interviewee 1, Supplier/Contract Account Manager)*

4.58. The next section of the report considers the implications of the findings from the surveys and interviews.

Section 5. Discussion and Summary Comments

5.1 What is clear is that having an influence on the budget is important, in part because security rarely own it, and so influencing is the next best possibility, and in part because, as 76% believed, being able to influence the budget is key to delivering good security. Logically because it enabled security managers to ensure that the spend was appropriately targeted using professional expertise and judgement but there was more to it than that. Control of the budget meant other professionals took more notice of their opinion, and that helps with engagement. Moreover, where security managers had influence it meant that the organisation prioritised security or at least took it seriously and that set a context for better security operations. Those who lacked influence pointed to not being able to buy basic and essential resources while watching helplessly as non-security experts undermined good security with poor decisions.

5.2 That said, survey findings revealed that just a half (51%) had a relatively high level of influence - being 'responsible' (28%) or 'accountable' (23%) for the budget. Still though a fifth (21%) had very limited involvement – either being merely 'informed' of the budget (11%) or 'not involved' at all (10%). Such a variation is perhaps not surprising, but more striking was the finding that 46% considered their budget to be 'insufficient' for a variety of reasons that included the budget not reflecting the risks that were being faced; a failure to include essential aspects such as training, travel, basic equipment, contingencies; some lamented teams were understaffed; rising costs not being reflected in increased in funding; and being asked to provide more for less.

5.3 A number of factors were seen to be important in determining whether an appropriate budget was allocated. Some noted in interviews that a serious incident was the best generator of more spend. That aside, prime amongst them were the organisation itself viewing the security function as core business and it understanding the risks and threats it faced. Where the security function has a high status that was associated with an appropriate budget; and where there was a requirement to meet statutory regulation requirements and/or adhere to accredited standards, that drove a focus. A less but still important factor is the quality of the supplier, a good one can increase the chances of meeting budget requirements from a security standpoint. That said, it is striking that close to a third (32%) believed that excellent relationships between clients and suppliers are rare.

5.4 It is striking too that close to three fifths (58%) believed that clients' buying decisions are guided more by procurement professionals than security professionals; that the buying process lacks sufficient input from security experts; while 46% of the sample associated a high level

of involvement of procurement professionals in the buying process with a less than adequate budget. Where security is influential, it seems that the power of the procurement teams can be managed or matched, they were sometimes spoken about as being good allies. It is where security professionals are not influential that procurement gains the influence that was viewed negatively.

5.5 Many of the open-ended comments in the survey stressed the importance of having competent security personnel and teams arguing the case effectively in order to achieve an appropriate budget. This was not just about security expertise, it was more than that, not least being able to build relationships with other professionals. In part this is because, as many interviewees noted, other professionals tended not to be interested – or comparatively less interested – in security, while security managers were not as influential or visible as other management; building relationships then takes on an extra significance.

5.6 Indeed, over two thirds (68%) believed that a nominated board member with responsibility for security improves security effectiveness but only if the Board member is able and engaged and of course if the individual has a respectable professional rapport with the head of security. Procurement was mentioned frequently in this context too. Nevertheless, it is telling that approaching three fifths of respondents (58%) believed security personnel are not effective at selling the benefits of security (those who were not influential in budget discussions especially thought so).

5.7 Related to this, and another key skill area was being able to argue the business case, not least because, as some interviewees highlighted, it is becoming an increasingly challenging commercial environment. Indeed, only 14% believed that clients are good at allocating the right amount of budget to the level of risks they face, and 63% believed that clients are slow to adapt to changing security requirements. So while most, 73%, believed that security budgets are usually based on the previous year with a percentage change, skills in articulating the Return on Investment in ways that a business can relate too was deemed crucial.

5.8 In this way though security was seen to be at a disadvantage with many security leads lacking business acumen. Interestingly it was not thought many security personnel aspired to be CEOs. Even if they did it was felt many could face difficulties in integrating with the wider business culture and suffer from not being comparatively as able at speaking the language of business; that often they were not strategically placed; and because many security leaders were in second careers lacked this ambition.

5.9 There are though perhaps two factors which pose cause for optimism. The first is that nearly a half of respondents (48%) believed that

Enterprise Security Risk Management (ESRM) – which includes an emphasis on working with business units to identify risk and mitigation measures in business terms - is the future of good security. And second, there was optimism younger security professionals might balk this trend.

5.10 Interviewees identified a range of tactics that helped secure the appropriate budget. Relating the investment in security in terms of the benefits to the business was key; presenting the dangers of not investing (without scaremongering) was legitimate not least when it had the potential to impact on effective business operations; using data and metrics to support evidence based arguments was highlighted; selling the benefits of investing and drawbacks of not investing in terms of other corporate professionals not meeting objectives was also mentioned (so not investing became their problem); and justifying the spend in physical security to improve cyber security (which was widely viewed as having a high profile and was seen as a bigger risk) had much to commend it.

5.11 There was a nod to the possibility that security professionals may have underplayed their position in being recognised as a trusted partner. When asked in interviews whether there was an incentive to perform badly – thereby increasing business risks leading to increased investment - most thought this was a theoretical possibility, but rarely a real world one. Many pointed to their personal ambitions to do a good job and be recognised for it and the good intentions and worthy ethics of fellow professionals.

5.12 We looked at factors considered to be important to organisations purchasing security, and interestingly both 'in-house' and 'contract' security managers gave similar answers. Interestingly both thought there was emphasis on: understanding and responding to the client's identified needs (92%); the expertise of the supplier (88%); and the supplier having a good reputation (86%). In other words that the skills of the supplier are important. Offering the lowest price was considered the least important factor of those explored although still somewhat common (44%). Perhaps a contributory reason is that what is agreed in the contract is rarely a 'very close' match (13%) to what happens in practice; a good working rapport is key and organisations are more committed to spending in security when suppliers can be trusted.

5.13 While the roles of buyers and suppliers are different, they do both play prominent roles in security management. So we explored whether security managers in each had interchangeable roles. The results were illuminating, in that more felt a good security manager working for a security supplier would generally adapt well to being an in-house corporate security manager (60%) than the reverse (45%). Insights from the interviews suggested that in-house security professionals were seen as having less developed sales skills, while contractors had

a more demanding job that lacked experience of Board engagement (amongst other things).

5.14 Looking at factors that influence the budget has revealed a myriad of issues and influences. Further work might explore the different practices evident in different sectors, in different sizes of business, in different organisational structures, take a closer account of the role of security and its relationship to broader operations, consider in more detail the status and relationships of the security lead to other professional heads, and compare the levels of influence across professional groups, they may all reveal new insights. It is probably illusory to seek to identify the optimal or best level of influence for security but developing models or 'ideal types' based on context would be a worthy step. Nor should judgements about what good looks like be treated simplistically. For example, only 14% believed that a reduction in spend was an indication that security is ineffective; there can be good reasons for it.

5.15 In all, this work has underlined the importance to security professionals in being able to influence the budget, and the barriers in being able to do so effectively. There are certainly challenges ahead, a striking finding, perhaps the most striking, is that when it comes to influencing the budget, our sample believe that a majority of security professionals do not have the level of influence that may be desirable. And security is worse as a result.

Appendix 1. Methodology and Sample

The approach

The study involved a review of available sources on the role of security managers and influence on the budget. These were used to give context 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 influencing the budget; 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: factors that influence the security budget; factors that influence how effective security is; whether there are similarities between 'in-house' and 'contracted' security managers; and factors that are important when purchasing security.

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 10th February to 25th March 2022.

A total of 338 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 conversations about the issues covered in this report. This included during our series of

webinars on security.[43] 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 33 professionals.

[43] 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 1: Sector that respondents provide security in (respondents could tick all that apply) (n=337)

Sector	N	%
Public Admin, Other Services, Government	84	25
Property	77	23
Retail	76	23
Health	74	22
Leisure & the Night Time Economy	62	18
Transport	54	16
Education	54	16
Finance	52	15
Manufacturing	47	14
Production	40	12
Energy	37	11
Post & Telecommunications	29	9
Hotel & Catering	28	8
ICT	25	7
Mining, Quarrying & Utilities	21	6
Wholesale	20	6
Motor Trades	15	4
Agriculture	7	2

Table 2: Country where the respondent conducts the majority of their work (where they are based) (n=334)

Country	N	%
UK	208	62.3
Ireland	24	7.2
USA	19	5.7
Nigeria	10	3.0
Kenya	8	2.4
Canada	7	2.1
India	6	1.8
Australia	4	1.2

Netherlands	4	1.2
South Africa	4	1.2
Germany	3	0.9
Switzerland	3	0.9
United Arab Emirates	3	0.9
Afghanistan	2	0.6
Belgium	2	0.6
China	2	0.6
Italy	2	0.6
Serbia	2	0.6
Brazil	1	0.3
Cyprus	1	0.3
Egypt	1	0.3
Finland	1	0.3
Ghana	1	0.3
Guyana	1	0.3
Iceland	1	0.3
Jamaica	1	0.3
Madagascar	1	0.3
Malaysia	1	0.3
New Zealand	1	0.3
Peru	1	0.3
Portugal	1	0.3
Saudi Arabia	1	0.3
Singapore	1	0.3
Sri Lanka	1	0.3
Sweden	1	0.3
Tunisia	1	0.3
Ukraine	1	0.3
Yemen	1	0.3
Zambia	1	0.3

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 19 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 ADS, ASIS International (UK Chapter), the British Security Industry Association, IFPO UK, IPSA, The SASIG, and the Security Institute, 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/

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

