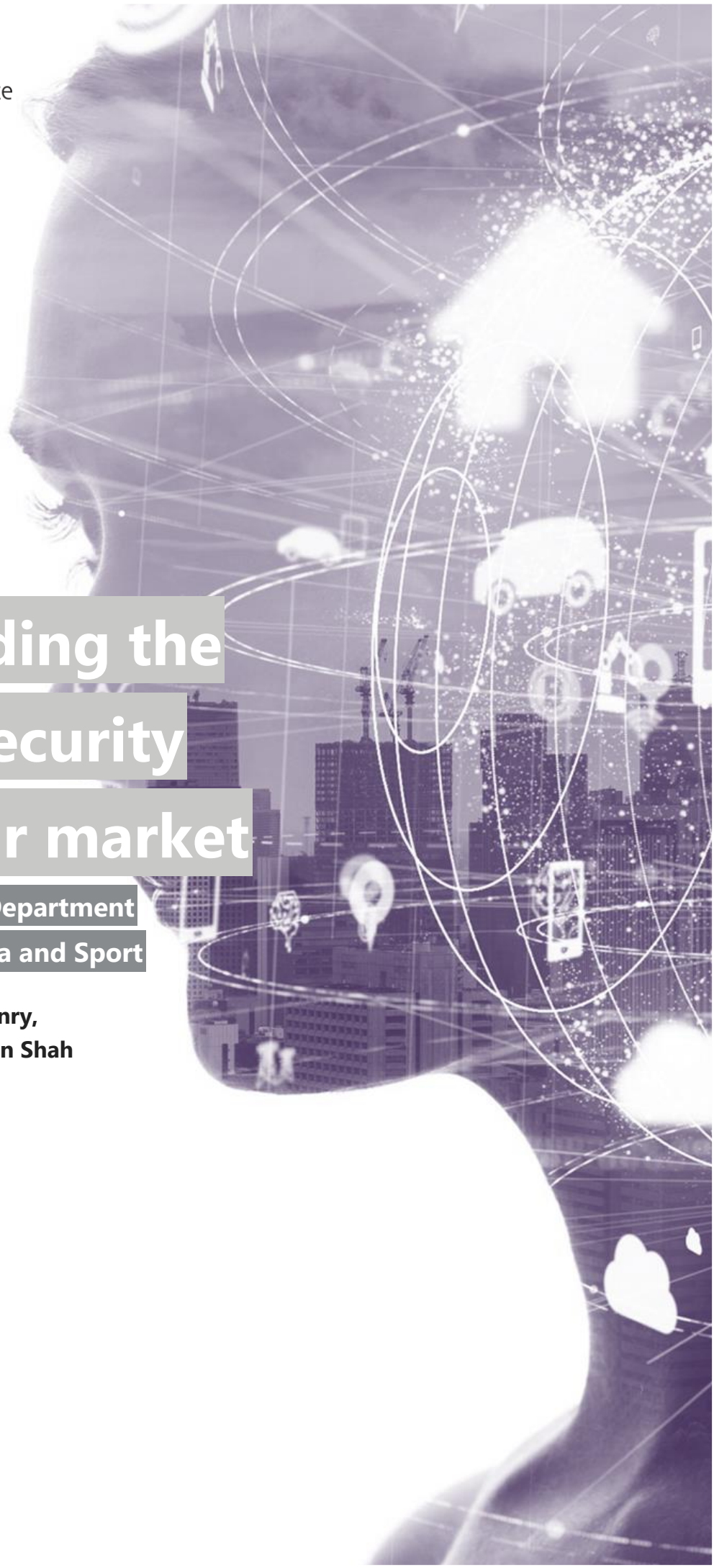
Ipsos MORI
Social Research Institute



December 2018

Understanding the UK cyber security skills labour market

Research report for the Department for Digital, Culture, Media and Sport

Daniel Pedley, Darragh McHenry, Helen Motha and Jayesh Navin Shah

Department for Digital, Culture, Media & Sport

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

Summary

This summary covers a programme of research on the current state of the UK cyber security skills labour market. The Department for Digital, Culture, Media and Sport (DCMS) commissioned the work as part of the UK Government's National Cyber Security Strategy 2016 to 2021. The research involved:

- a literature review and 12 interviews with industry experts from the private and public sectors, and academia, to understand existing evidence and expert opinion
- a quantitative survey of 1,030 businesses, 127 public sector organisations and 470 charities, from 12 June to 6 August 2018[1]
- qualitative interviews with 32 organisations across the private, public and charitable sectors, as well as those providing cyber security products and services for others, from July to August 2018.

A definition of cyber security skills

We define cyber security skills as the combination of essential and advanced technical expertise and skills, strategic management skills, planning and organisation skills, and complementary soft skills that allow organisations to:

- *understand the current and potential future cyber risks they face*
- *create and effectively spread awareness of cyber risks, good practice, and the rules or policies to be followed, upwards and downwards across the organisation*
- *implement the technical controls and carry out the technical tasks required to protect the organisation, based on an accurate understanding of the level of threat they face*
- *meet the organisation's obligations with regards to cyber security, such as legal obligations around data protection*
- *investigate and respond effectively to current and potential future cyber attacks, in line with the requirements of the organisation.*

This is the core set of knowledge and skills that organisations need to either have within their workforce, or seek externally (for example, if they outsource their cyber security or take on external consultants). Those working in the wider cyber security industry – developing cyber security products or services, or carrying out fundamental research – may require additional skills, such as the technical expertise and skills needed to research and develop new technologies, products or services.

Our definition builds on the Cyber Security Body of Knowledge, or CyBOK (Rashid et al., 2017), which already indicates that cyber security is an extremely diverse field, requiring strong technical skills. Based on the existing literature and industry expert views, we have split these broadly into basic and high-level technical skills:

- We consider basic technical cyber security skills to be the ones that are needed to implement the minimum technical controls laid out in the Government-endorsed Cyber Essentials scheme. This covers: secure internet connections, secure devices and software, controlling user access to data and devices, protection from viruses and other malware, and keeping devices and software up-to-date.[2]

- Many organisations require access to high-level technical skills, that can implement cyber security beyond the minimum standard. Our findings cover the following broad high-level technical skills areas: security architecture,

[1] This excludes sole traders, agriculture, forestry and fishing businesses, and parish councils, which were all outside the scope of the survey. Data are weighted to be representative of the respective populations of businesses, charities and public sector organisations.
[2] See https://www.cyberessentials.ncsc.gov.uk/.

 © Department for Digital, Culture, Media and Sport 2018

penetration testing, threat intelligence, forensic analysis, interpreting malicious code, and user monitoring. This is the collection of areas commonly mentioned in existing literature and in the industry expert interviews.

For individuals working in cyber security roles, implementing technical controls or carrying out technical tasks would require a sufficient understanding of one or more of the specific cyber security Knowledge Areas listed in CyBOK. However, our findings indicate that private and charitable sector organisations often lack an understanding of the technical skills they need to manage their cyber security. Consequently, they may undervalue such skills. An implication is that organisations may need more education or guidance on the value of technical cyber security skills.

Nevertheless, performing a cyber security role is not simply about technical know-how. For a start, CyBOK shows that the knowledge underpinning many cyber security roles is not simply IT knowledge, but encompasses maths, wider security elements, and also knowledge of the human factors that can lead to cyber security breaches. And whereas knowledge limited to IT products can become outdated, working in a cyber security role often requires keeping up-to-date with the latest technological trends and developments.

Our research also validates the importance of other, complementary skillsets in the effective implementation of cyber security. This includes the ability to plan ahead and manage current and potential future risks – a necessary skillset both for senior managers and for those working directly in cyber security. Soft skills, such as communication skills, are also important complementary skills, and this was a common theme across all strands of the research.

The current cyber security skills labour market

We find that the current cyber security labour market is relatively immature. The qualitative interviews suggest that there is not a large crop of candidates who have previously worked in professional roles in cyber security. Across the private sector, seven in ten of the individuals (68%) working in cyber security roles within a business have absorbed this role into an existing non-cyber security job. The next most common situation (for 22% of individuals) is to have been recruited, but from a previous non-cyber security job.

The size of cyber security teams across the private and charitable sectors is relatively small, with the average business and charity having around two people working in cyber security roles. This compares to an average team size of five people across public sector organisations. As might be expected, this reflects organisation size, with larger organisations tending to employ more people in cyber security roles.

Within such teams, the cyber security role is often not badged as such. In fact, there is a large informal cyber security sector, where the individuals working in these roles often lack the technical expertise, skills or experience to fully understand or carry out their work. Just 11 per cent of businesses and 14 per cent of charities have cyber security written formally into the job descriptions of one or more staff. And we find that cyber security teams are often run in very different ways, from different departments such as finance, IT or operations.

Our findings suggest that there is currently no widely accepted definition of a cyber security professional. For example, there was no single gold-standard cyber security qualification, or even an accepted minimum qualification to work in the role, that emerged across interviews. In fact, outside of those we spoke to in firms providing cyber security products or services, there was not a great deal of awareness of any cyber-specific qualifications. Overall, our survey records that four per cent of businesses and six per cent of charities have individuals with or working towards cyber security qualifications, such as the Certified Information Systems Security Professional (CISSP) accreditation.

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

An important caveat for all these findings is that they do not specifically reflect firms in the cyber security industry itself (the ones working on cyber security technological developments, products or services) – they represent those working in cyber security roles within other industries. However, qualitative interviews with the organisations providing cyber security products or services to others suggest that they too are dealing with a newly formed labour market. Participants from these organisations indicated a heavy focus on recruiting graduates and apprentices, at the start of their careers.

The extent and nature of current skills gaps

We primarily measure skills gaps in terms of how confident those responsible for cyber security feel in carrying out certain technical and non-technical cyber security tasks. We ask about confidence in performing these tasks only in organisations where they are not outsourced, so where the skills gap is not already filled by an external cyber security provider.

The majority of individuals across all types of organisations (private, public and charitable) are either very or fairly confident in performing the basic technical tasks noted earlier in our categorisation of basic technical cyber security skills. Nevertheless, the proportions vary considerably depending on the task. While nine in ten businesses (90%) are confident about being able to back up files, far fewer are confident at being able to detect and remove malware (67%), store or transfer personal data in a secure way (65%) or set up configured firewalls (59%). We identify more than half (54%) of all businesses as having a basic cyber security skills gap, as they are not confident in carrying out one or more of the basic tasks asked about. Of the c.1.32 million businesses in the UK, this accounts for approximately 710,000 businesses.

There are also sizable skills gaps when it comes to the high-level technical skills covered in our earlier categorisation (such as penetration testing, forensic analysis, and user monitoring). The survey takes into account that not all organisations require these high-level skills. We only ask about confidence in undertaking these tasks in cases where organisations tell us it is important for them to have these skills in-house. Here, we find that skills gaps are greatest for the areas of security architecture (where 21% of all businesses are not confident), penetration testing (22%) and forensic analysis (23%). And across all the six high-level technical tasks asked about, we find that approximately 407,000 businesses (31%) have a high-level technical skills gap (lacking confidence to do one or more of these high-level tasks in-house).

In the qualitative interviews with those providing cyber security products or services to others, we also gained insights into the current and upcoming skills needs within the cyber security industry. The additional specialist skills areas they noted as having gaps were: cloud security, end-point security, identity and access management, and threat hunting. Looking ahead to the future, they saw the emergence of artificial intelligence and automation as importance skills areas to develop within the next three to five years.

Another major skills gap is in incident response. In total, 460,000 businesses (35%) have an incident response skills gap, and are not confident in their ability to deal with a cyber security breach or attack. Once again, we assume that those that outsource incident response do not have a skills gap in this area, as they are filling this skills need externally.

How are organisations attempting to address skills gaps?

Our research explores recruitment, training and outsourcing (hiring consultants, or external organisations to provide cyber security products and services) as different ways in which organisations try to fill their cyber security skills gaps.

Recruitment

Among the firms who specifically operate in the cyber security industry (developing or delivering cyber security technologies, products or services), the qualitative evidence suggests recruitment of career starters is continuous. It was much more challenging to recruit individuals with existing skills and experience. Participants told us there was not a large

 © Department for Digital, Culture, Media and Sport 2018

pool of individuals with both specific technical qualifications and experience, and that such individuals had high salary demands. This often priced medium organisations, charities, and public sector organisations out of the market. Those working on public sector contracts also faced an additional barrier around security clearance, which prevented them employing foreign nationals.

Outside the firms within the cyber security industry, or the typically-larger firms that have more sophisticated cyber security needs, recruitment into cyber security roles is very rare. Just two per cent of businesses, three per cent of charities and 13 per cent of public sector organisations tried to recruit anyone in such roles within the last three years. Our findings suggest several reasons for this, including a lack of understanding of the cyber security skills that organisations actually need, a preference for generalist IT staff over specialist cyber security staff, and a perceived lack of budget or work to justify a cyber security role.

Where recruitment was taking place, organisations tended to stick to tried-and-tested recruitment methods. We spoke to those that used recruitment agencies, recruitment websites, sector-specific magazines, and LinkedIn. These were typically not specialist IT or cyber security recruitment channels, even among the firms working in the cyber security industry.

Training

We found that some organisations had tried to overcome their external recruitment challenges by focusing on internal recruitment (shifting staff from other teams into cyber security roles), and upskilling or reskilling existing cyber security staff. They felt these individuals would have a better idea of the practical implications of cyber security for their own organisation, and be better at spreading good practice to wider staff, given their existing institutional knowledge.

However, across the wider business population, investment in cyber security training over the last 12 months appears rare:

- Just 14 per cent of businesses have undertaken a formal analysis of their cyber security training needs in this period.
- Around one in four businesses (23%) have had staff in cyber security roles undergo cyber security training in the past year, and one in nine (11%) have taken wider, non-specialist staff through training.

In our qualitative interviews, there were various barriers to providing training. This included, but was not limited to, the cost of training. In addition, some barriers were about awareness – no single training product was considered to be the baseline or gold standard for cyber security – and attitudes – some saw cyber security simply as a common-sense issue, and did not see the value added through formal training.

Our research also suggests that the current training products available to organisations are often not fit for purpose. Only one in five (19%) of the businesses providing training for those in cyber security roles say that it met their needs completely. And a similar proportion (22%) of the businesses providing cyber security training for wider staff say that it met their needs.

Outsourcing

Outsourcing is a common solution for addressing cyber security skills gaps, typically more so than recruitment. Three in ten businesses (30%) and a similar proportion of charities (27%) outsource one or more aspects of their cyber security. Two-thirds (65%) of public sector organisations outsource. Moreover, the survey suggests that the primary reason for outsourcing among private, public and charitable sector organisations is not about cost or efficiency savings, but about filling cyber security skills gaps.

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

Among those outsourcing high-level technical tasks, the most common aspects that are outsourced include: interpreting malicious code, security architecture and forensic analysis. These mirror the aforementioned areas where the organisations who do not outsource are most likely to have high-level technical skills gaps.

While outsourcing may be a convenient way for many organisations to fill their in-house cyber security skills gaps, the research highlights that organisations still need the skills in-house to effectively find and manage the right external cyber security providers. We find that, in organisations where the in-house staff dealing with external cyber security providers were not experts, they largely chose external providers based on cost, and not necessarily on quality. Some of these participants also felt they did not have the knowledge to effectively monitor the performance of their chosen providers.

Conclusions and recommendations

This research highlights the complexity and diversity of cyber security skills. It reinforces the view that cyber security cannot be pigeonholed as an IT issue. It requires a much broader set of technical expertise and skills, complemented by the right soft skills to do the job effectively.

We have evidenced the large group of organisations where staff cover cyber security in an informal way, and where there is a basic technical cyber security skills gap. We have also uncovered high-level technical skills gaps in areas such as security architecture, penetration testing, forensic analysis and incident response.

Organisations are trying to address these gaps through a mix of recruitment, training and outsourcing, but face barriers in each of these areas. This suggests that there is more to be done to help fill the cyber security skills gap, and we make recommendations in the following areas:

- adopting our proposed definition of cyber security skills, if considered useful by the industry at large, to help organisations better understand their skills needs, and individuals better understand their job roles
- outlining standard career pathways and relevant qualifications, to help further professionalise the industry
- promoting existing Government guidance on cyber security, and developing new Government and industry-supplied guidance, to encourage more organisations to better understand and address their skills gaps
- focusing on potential future skills needs as well as current skills needs.

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

Contents

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

1 Introduction

The UK Government Department for Digital, Culture, Media and Sport (DCMS) commissioned Ipsos MORI and the Institute of Criminal Justice Studies (ICJS) at the University of Portsmouth to carry out quantitative and qualitative research to better understand the current state of the UK cyber security skills labour market. The work forms part of the UK Government's National Cyber Security Strategy 2016 to 2021. The £1.9 billion investment taking place under this strategy aims, alongside other objectives, to ensure the UK has a sustainable supply of home-grown cyber professionals to meet the growing demands of an increasingly digital economy, in the public and private sectors, and in defence. This research is intended to inform DCMS's strategic vision and programmes of activity on cyber security skills development.

The Government defines cyber security in the Strategy as: the protection of information systems (hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures.

The research aims to address the following overarching questions:

- What is a cyber security skill?
- How does the market understand the term "cyber security professional"?
- Where are the current skills and skills gaps across organisations and in the market?
- What cyber security skills needs are organisations attempting to meet through training and recruitment?
- What are the recommendations for the Government and industry?

1.1 Summary of the methodology

The methodology consisted of four strands, as outlined here. The first two strands fed into the development of the quantitative survey, and the results from the survey fed into the follow-up qualitative interviews.

1. Professor Mark Button and Dr Victoria Wang from ICJS carried out a rapid evidence review of 32 existing evidence sources (surveys and white papers, globally and in the UK). We include a full list of references in the separately-published technical report. Ipsos MORI carried out the remaining strands.
2. We carried out 12 in-depth interviews with industry experts representing a range of trade associations, multinational businesses, cyber security specialists, training providers, recruitment agencies, academics and Government. These took place in March and April 2018.
3. We conducted a quantitative survey of 1,030 businesses, 127 public sector organisations and 470 charities from 12 June to 6 August 2018. Survey data are weighted to be representative of these respective audiences. The business sample excludes agriculture, forestry and fishing businesses. The public sector sample excludes parish councils and central Government Departments.[3]
4. We carried out 32 further in-depth interviews, including 27 with a mix of organisations that took part in the survey and 5 with external cyber security providers that were not in the survey, across July and August 2018. External

[3] We considered organisations with no IT capacity or online presence as ineligible, which led us to exclude small number of specific sectors (agriculture, forestry and fishing). We would typically have screened such organisations out of the survey, so we excluded them from the sample instead. This matches the approach taken in DCMS's Cyber Security Breaches Survey series. We excluded parish councils, which also tend to have little or no IT capacity. If included, the volume of parish councils means that the public sector sample would have been dominated just by these. Finally, in agreement with DCMS, we ensured that central Government Departments were not on the sample, as we anticipated they would not be able to take part, or share sensitive information.

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

providers are those that offer cyber security services or cover cyber security as part of their IT service for other organisations.

The separately-published technical report provides more detail on the methodology, including sampling, data collection, response rates and weighting.[4]

1.2 Differences from previous research on this topic

This research is the first of its kind that DCMS has carried out, so there was no established methodology for measuring cyber security skills and skills gaps. Our primary research takes a different approach to other studies published in recent years in this area, such as the ISC2 Cybersecurity Workforce Study (formerly known as the Global Information Security Workforce Studies, or GISWS, last published in 2018 under Frost & Sullivan), the Centre for Strategic and International Studies (CSIS, 2016) survey, and the annual ISACA surveys (last published in 2018).

We included all these existing studies in our rapid evidence review. Where relevant to the UK context, we pull out findings from these and other reviewed papers

- Our primary research is UK-specific and has a large sample size. This means we can break down findings for UK organisations by size, sector and region (in the small number of instances where there are regional differences to comment on). The aforementioned previous studies have not been able to be so granular, or have reported findings for Europe as a whole, rather than the UK.

  Our survey results are sampled and weighted to be representative of organisations of all sizes and sectors. This includes micro and small businesses, and low-income charities, that may be less aware of their cyber security skills needs, and make up the vast majority of all businesses and charities in the UK. The aforementioned earlier surveys in this area have been carried out online with a self-selecting sample, skewed towards the largest and most engaged organisations. These studies are important, as they have good coverage of the organisations with the most sophisticated cyber security skills needs. However, they are not representative, and typically omit micro, small and medium businesses, and the charitable sector, where there are more basic cyber security skills needs.

  As a trade-off, this means that the quantitative survey element includes fewer large organisations with more sophisticated cyber security skills needs – this would be the case for any representative business survey. Our sampling approach nonetheless boosted the number of medium and large businesses, and we carried out additional qualitative interviews with external cyber security providers. Therefore, we are still able to explore high-level technical skills gaps, particularly in the qualitative research, but it is not possible to quantify these in great detail for specific disciplines.

- This research measures skills gaps – the number of organisations lacking particular cyber security skills – in a particular way. As we cannot objectively test whether organisations are capable of carrying out specific cyber security tasks involving specialist skills, we instead ask about their confidence at being able to carry out a range of these tasks (see Chapter 4 for full details).

  We also attempted to estimate skills shortages – the shortfall in the number of skilled individuals working in or applying for cyber security roles – by quantifying the proportion of organisations that had hard-to-fill vacancies in such roles. However, the survey results covered in Chapter 5 show that, in a representative survey including micro and small businesses, very few organisations have tried to recruit for these roles. This means that we can report on cyber security skills gaps, but not on cyber security skills-shortage vacancies. We recommend that quantifying cyber

[4] See https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market.

security skills-shortage vacancies in the UK is the subject of future research, focusing on the high-volume recruiting organisations in the labour market – organisations specialising in cyber security technological development, products or services, as well as very large (for example, FTSE 350) businesses – and not on all sizes and sectors.

- The research participants were the individuals who had the most knowledge or responsibility when it came to cyber security in their organisation. We allowed organisations to self-define who best fit this description. This is different to all the aforementioned studies, which have specifically targeted hiring managers, in charge of recruiting people to cyber security roles. We cognitively tested our survey questionnaire with both groups. We found that hiring managers, responsible for recruitment but not for cyber security, did not know enough about the topic, so would not be able to answer questions about skills gaps among these staff. Moreover, many organisations were simply not hiring for these roles, so would not have been able to take part in the survey on this basis.

  As a result of this approach, we often talked to individuals who informally covered cyber security for their organisation, or without it being badged as a cyber security role. These individuals tended to have more basic cyber security skills needs, so gave less insight into the technical high-level skills gaps in the cyber security skills labour market. This is an important finding itself, discussed in Chapter 3, showing that there is a large informal cyber security sector. The individuals covering this area often lack basic cyber security skills, while the organisations they work for do not always understand their own cyber security needs, and the cyber security job role.

1.3 Interpretation of findings

Rounding of survey results

Where figures in charts do not add to 100% this is due to rounding of percentages or averages, or because the questions allow more than one response.

Statistical significance

The survey results are subject to margins of error, which vary with the size of the sample and the percentage figure concerned. We only highlight subgroup differences by size, sector, region, income band (for charities) or any other variable where these differences are statistically significant (at the 95% level of confidence).

Subgroup analysis

For businesses, analysis by size splits the population into micro businesses (1 to 9 employees), small businesses (10 to 49 employees), medium businesses (50 to 249 employees) and large businesses (250 employees or more). For charities, we consider size in terms of annual income band. This analysis splits charities into low-income (under £100,000), middle-income (£100,000 to under £500,000) and high-income (£500,000 or more) groups. There are too few public sector organisations sampled to split out results by size.

Due to the relatively small sample sizes for certain business sectors, these have been grouped with other similar sectors for more robust analysis. The groupings follow the same ones used in DCMS's Cyber Security Breaches Survey series.[5] Business sector groupings referred to across this report, and their respective SIC 2007 sectors, are:

- administration or real estate (SIC L or N)
- construction (SIC F)
- education (including academies) (SIC P)

[5] See https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2018.

 © Department for Digital, Culture, Media and Sport 2018

- entertainment, service or membership organisations (SIC R or S)
- finance or insurance (SIC K)
- food or hospitality (SIC I)
- health, social care or social work (including NHS organisations) (SIC Q)
- information or communication (SIC J)
- professional, scientific or technical (SIC M)
- retail or wholesale (including vehicle sales and repairs) (SIC G)
- transport or storage (SIC H)
- utilities or production (including manufacturing) (SIC B, C, D or E).

Typically, we compare each sector to the average private business. The education sector and health, social care or social work sectors include a mix of private and public sector organisations. We therefore compare these sectors to a merged sample of private and public sector organisations, specially weighted to represent a merged population profile.

Regional differences are reported in as granular a way as possible. We also combined regions in the analysis into the North of England (this does not include Scotland), Midlands and South of England (excluding London), as well as looking at England as a whole versus the rest of the UK, to be able to pull out more statistically robust differences. The relative lack of regional differences in this report indicates that – outside of differences between London and the rest of the UK – there is generally little consistent regional variation in the findings.

Interpreting qualitative data

The qualitative survey findings offer more nuanced insights and case studies into how organisations address their cyber security skills needs, and why they take certain approaches. The findings reported here represent common themes emerging across multiple interviews. Where we pull out an example or insight from one organisation, this is to illustrate findings that emerged more broadly across multiple interviews. As with any qualitative findings, these examples are not intended to be statistically representative of the wider population of businesses, public sector organisations and charities, and should be treated accordingly.

1.4 Acknowledgements

Ipsos MORI would like to thank all the industry experts, businesses, public sector organisations, charities, external cyber security providers, and the individual research participants who took part in the survey and interviews. We would also like to thank the DCMS colleagues who worked on the study.

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

2 What are cyber security skills?

In this chapter, we discuss a possible definition of cyber security skills. Fundamentally, to clarify what we are defining, we consider cyber security skills to be, primarily, the core set of knowledge and skills that organisations need to have, either within their workforce, or externally – for example, if they outsource their cyber security or take on external consultants – in order to successfully implement cyber security across their organisation.

Cyber security skills are also needed to carry out fundamental cyber security research, and to develop new technologies, products and services for other organisations. These were not major themes in our primary research (reflecting who we spoke to) but we acknowledge that they must also be an important part of any definition of cyber security skills.

Our definition takes as a starting point the existing literature and frameworks that define cyber security as a discipline, or field of study. However, as another fundamental principle, we consider the definition of cyber security skills to be wider than the definition of cyber security as a discipline. This is in the same way that, for instance, the skills needed to work as a lawyer are broader than knowledge of law – even though this knowledge underpins the role. This is why we explore the relative importance of non-technical skills, as well as technical knowledge of cyber security, for people working in cyber security roles. We also break down basic technical skills that can be considered relevant for all organisations, and the advanced professional technical skills that certain organisations with more sophisticated needs are looking for.

Existing evidence

- The UK parliament Joint Committee on the National Security Strategy (JCNSS, 2018) suggests dividing cyber security skills into three broad tiers, including: elite skills required by a small number of employees doing specific tasks, such as penetration testing, moderate skills required by those whose job has evolved to include a cyber security role, and basic cyber hygiene, for which all employees are responsible. It highlights the need to consider cyber security skills at an organisational level, not just among specialists, but also within management boards and across wider staff.
- Rashid et al. (2017) lay out the Cyber Security Body of Knowledge (CyBOK). These are five categories of knowledge, divided further into 19 specialist Knowledge Areas, which define cyber security as a discipline. Those working in cyber security roles will be implementing the learnings from one or more of these Knowledge Areas, and will need to have the skills to do this This is an especially important framework developed in consultation with UK organisations and beyond, and is a starting point for understanding the breadth and complexity of cyber security skills. We cover it further within this chapter.
- In the US, the National Initiative for Cybersecurity Education (NICE) framework (Newhouse et al., 2017) adds a further category to the mix – oversight and governance – which includes understanding of legal issues, management skills, planning skills, and the ability to train wider staff and raise their awareness of cyber security. This highlights the importance of non-technical skills and soft skills for those working in cyber security roles, and is why we have also explored these types of skills in our primary research.

2.1 Cyber security as a wide-ranging discipline

CyBOK is a starting point for understanding the breadth of knowledge areas that cyber security encompasses, formalising it as a discipline, similar to law or engineering. The following list includes the five broad CyBOK categories of knowledge and the specific Knowledge Areas that fall within these.

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

1. human, organisational and regulatory aspects	▪ risk, management and governance ▪ law and regulation ▪ human factors ▪ privacy and online rights.
2. attacks and defences	▪ malware and attack technologies ▪ adversarial behaviours ▪ security operations and incident management ▪ forensics.
3. systems security	▪ cryptography ▪ operating systems and virtualisation security ▪ distributed systems security ▪ authentication, authorisation and accountability.
4. software and platform security	▪ software security ▪ web and mobile security ▪ secure software design and development.
5. infrastructure security	▪ network security ▪ hardware security ▪ cyber-physical systems security ▪ physical layer security.

The content of the 19 Knowledge Areas is currently under development, and due for publication at the end of 2019.[6]

The CyBOK knowledge areas illustrate that cyber security is an extremely diverse field, and that strong technical skills – sometimes taking many years to obtain – are required to be a practitioner in many of these areas.

2.2 Technical cyber security skills

Basic versus high-level technical skills

The extent to which organisations require different technical skills to be cyber-secure varies. The qualitative interviews suggest that there are broadly two tiers of technical requirements: basic technical requirements and highly technical requirements.

- Basic technical requirements – smaller businesses and low-income charities often felt that their level of cyber risk was not high enough to require anything more than basic controls. While this was their subjective assessment, it was clear that each organisation had varying levels of need. Some were making conscious decisions for their cyber security to reach an adequate level. On the other hand, some of those responsible for cyber security in smaller organisations clearly lacked an understanding of the basics, and failed to articulate the kinds of technical skills needed for the role.

  Our research finds that there is no agreed definition of what basic skills are in the context of cyber security. The JCNSS (2018) report suggests they are the minimum skills that all organisations need for good cyber hygiene.

[6] See https://www.cybok.org/.

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

"The word 'cyber' indicates something other-worldly to me. I don't really know what cyber is. Is it the internet? Is it websites? Is it social media?"

Small business

One definition for basic technical cyber security skills could be adapted from the Government-endorsed Cyber Essentials scheme – we use this in our quantitative survey. The scheme lays out the minimum basic technical controls that all organisations should have to be cyber secure. These include: secure internet connections, secure devices and software, controlling who has access to the organisation's data and devices, protection from viruses and other malware, and keeping devices and software up-to-date.[7] Smaller businesses and charities often did not have the skills internally to fully cover each of these areas.

- Highly technical requirements – certain organisations – typically larger ones or those in the public sector – had more sophisticated cyber security. They therefore had a greater need for specialist in-house staff, or external experts from external cyber security providers, who could carry out advanced technical tasks for them. The types of advanced professional roles mentioned were wide-ranging, and included: security architecture, security engineering, intrusion detection, forensic analysis, network management, penetration testing (or ethical hacking), and systems administration. They again reflected the range of sub-disciplines found in the CyBOK framework.

"Well as long as we've got the anti-virus, anti-malware and encryption, and it's fully documented, then that is as sufficient as we need."

Medium business

This mirrors the recommendations of the JCNSS (2018) report to have a tiered approach. The distinction between basic and high-level skills is also very similar to the categorisation of digital skills in previous Ecorys UK/DCMS (2016) research. This split digital skills into three areas, with two of these being relevant for organisations (rather than for the general public): basic digital skills that set a minimum standard across all sectors, and advanced digital skills for IT professionals. It suggests that any framework for cyber skills can be similarly structured, in terms of basic and high-level technical skills.

When it comes to dissecting high-level technical skills, the literature review, industry expert interviews and interviews with large organisations highlighted the following areas:

- the skills to design secure networks, systems and application architectures
- the skills to carry out penetration testing
- the ability to use cyber threat intelligence tools or platforms
- the skills to carry out a forensic analysis of a cyber security breach
- the skills to interpret malicious code (for example, the results shown after running anti-virus software)
- the ability to use tools to monitor user activity.

This does not make it essential for organisations with more sophisticated cyber security needs to cover all these areas – our findings again suggest that different organisations will have different needs and focuses.

The difference between cyber security skills and IT skills

The CyBOK Knowledge Areas show that IT and computer science knowledge contribute to cyber security – several Knowledge Areas are computing based, to do with operating systems and networks – but that the discipline is also

[7] Cyber Essentials is a Government-endorsed accreditation scheme for organisations to demonstrate that they meet a minimum cyber security standard. As part of this, organisations need to implement basic technical controls in five areas. See: https://www.cyberessentials.ncsc.gov.uk/.

 © Department for Digital, Culture, Media and Sport 2018

broader than IT. Some Knowledge Areas, such as cryptography, have a foundation in maths. Others focus on knowledge of human factors, or having the organisational knowledge to assess risk levels.

It is also important to note that IT functions are not all related to cyber security. They do not necessarily encompass the security element. This is another reason why cyber security skills are distinct from, and broader than, IT skills.

The qualitative interviews also show that cyber security skills are broader than IT skills. In particular, awareness of risks, developments and trends in cyber security was an important theme. For example, those in cyber security roles said they needed to be aware of the specific risks facing their organisation, and as part of this, many felt part of their job was about keeping up to date with the latest cyber threats.

And awareness applies not just to those in cyber security roles, but to wider staff. For example, one public sector organisation wanted all their staff to be aware of the latest phishing threats. Another medium business said that all staff had a role to play in maintaining basic cyber hygiene, for instance by not leaving laptops unattended. In addition, several participants said it was incumbent on all staff to be aware of their organisation's data security requirements and policies. This focus on basic cyber hygiene across all staff mirrored the suggestions from the JCNSS (2018) report.

Implementing cyber security across an organisation can also encompass management and leadership traits that are not necessarily IT-focused, such as project management, providing business continuity, creating good cyber security policies, carrying out risk assessments, and managing the human factors that can lead to cyber security breaches. Part of the job of those in cyber security roles also included managing external cyber security providers (who ran the organisation's cyber security services for them, or managed it as part of a wider IT service) and looking at the security of third-party suppliers, so required people in these roles to be able to work effectively with these organisations.

"Cyber security skills are all about looking at the big picture, looking at risk."
Large business

"It's a bit like describing the difference between an accountant and an auditor … Cyber security skills are about making sure we are protected, and the organisation is not exposed because of our systems. IT skills are about the techy bits of keeping us working."
High-income charity

Some participants noted that effective management and leadership from those in cyber security roles requires them to also have a broader understanding of the organisations they work in – their business strategy, insurance coverage, and legal and compliance issues related to the kind of data they handle. For example, one residential home charity felt that anyone in a cyber security role in their organisation would need to understand how data protection regulations affect the care sector, and the kinds of sensitive customer data that their staff handle.

These themes again reflect the CyBOK knowledge category covering the human, organisational and regulatory aspects of cyber security. Together, these findings make clear that cyber security skills also cover understanding cyber risks and legal obligations, and being able to manage these appropriately.

Related to this, several organisations specifically mentioned that knowledge of the General Data Protection Regulation (GDPR) and its implications for cyber security was important for them. The fact that this arose in interviews is also likely to be linked to the timing of this research, taking place a few months after the implementation of GDPR. This meant that, in many organisations, it was something they had discussed very recently and at a management board level.

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

"Until recently, we have been quite backwards with our approach to governance and risk. We only recently implemented risk registers across the organisation. That includes GDPR compliance which we are taking very, very seriously now."
High-income charity

Of course, cyber security and GDPR are distinct, though related, topics. The qualitative findings suggest that GDPR has helped to highlight the importance of cyber security risk management. However, it has not necessarily given organisations a better understanding of their technical skills needs, and the interviews suggest that many still need to address their technical cyber security skills gaps, beyond simply addressing GDPR requirements.

IT product obsolescence

Another major reason that cyber security skills cannot solely be defined in terms of specific IT skills is that the latter quickly become out of date. This came up in multiple interviews. One public sector organisation noted that IT skills are often product-based, with people trained on particular programmes. As software evolves, some programmes cease to be secure or compatible, so become obsolete. They gave the example of previous colleagues in the past being trained on a particular type of imaging software (to clone laptops), which had become more exposed to security flaws over time.

2.3 Soft and intangible skills

The following section explores the importance placed on soft skills by organisations. One caveat to note is that, in smaller businesses and charities where cyber security was dealt with relatively informally, participants often struggled to think about the technical requirements of the role. This meant that they had a tendency to focus on soft skills simply because they could not consider the technical skills. Another cautionary point within this is that, among those outsourcing their cyber security, good communication was often the primary metric by which they judged their external cyber security provider – because they did not have a grasp of the technical aspects of the work. All this is not to say that soft skills are unimportant, but more that they may have underestimated the need for technical skills alongside soft skills.

We also should not discount the fact that soft skills were a consistently important topic of discussion not just in interviews with small organisations, but also with industry experts, large private and public sector organisations with sophisticated cyber security operations, and external cyber security providers offering services to other businesses. The importance of soft skills complementing the necessary technical skills was a universal theme in this research.

The interviews suggest that effective implementation of cyber security also requires soft skills, such as common sense, pragmatism and communication skills. In particular, good communication was commonly raised when talking both to industry experts and to organisations. Anecdotally, many participants said they had come across individuals in cyber security roles who had the expertise to carry out technical tasks, but were less able to communicate well with senior managers or wider staff – so less able to change cultures or behaviour. These anecdotes were based on a mix of people applying for roles in participants' current organisations, from their past experience in other jobs, and from their general sense of those working in the industry. As such, several participants considered good communication to be instrumental in effecting change within their organisation. This was both upwards communication, in terms of communicating cyber risks to senior managers, and downwards communication, educating wider staff on cyber security.

At the same time, communication skills were also very important for external cyber security providers themselves, when recruiting for entry-level roles. This was a major skills area that they focused on developing as part of their graduate training programmes. They wanted to develop staff to be effective consultants for their clients, and good communication, as well as the ability to listen and present well, were considered essential for this.

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

The qualitative interviews also highlighted a number of intangible qualities that those with more sophisticated cyber security needs – typically larger organisations and external providers – looked for when recruiting people to more technically advanced cyber security roles. This included attention to detail, an investigative nature, an ability to spot patterns, a willingness to check their own work, and a self-initiative to learn new things. External cyber security providers also mentioned creativity and problem-solving skills. Beyond simply having advanced professional IT skills, these external providers said that they were ideally looking for someone with a deeper understanding of IT – someone that understood how different systems were linked together and might be exploited.

"Cyber security is about understanding how technology can be exploited by hackers, understanding how software works, and how networks are joined together."
External cyber security provider

2.4 A broad categorisation and definition of cyber security skills

By bringing together all of the strands of this research, it is clear that the implementation of cyber security necessitates strong technical skills. The level and nature of these will vary across organisations depending on their needs – while all organisations need a minimum level of basic hygiene, not all organisations need to have more advanced technical cyber security skills. It is also evident that these technical skills cannot be defined solely in terms of IT knowledge and capabilities. Wider technical skills to do with risk management, understanding new security developments and trends, and understanding legal obligations, as well as other complementary non-technical skills, are also important. From the literature review (incorporating, in particular, CyBOK) and the primary research, we have drawn up six broad skills areas:

1. understanding an organisation's legal and compliance issues which could affect cyber security
2. understanding how the implementation of cyber security affects business performance, and therefore how to most effectively implement it with the engagement of senior managers and wider staff
3. the technical skills to implement basic technical controls, which could include the five sets of technical controls covered in the Cyber Essentials guidance
4. where necessary in organisations with more sophisticated cyber security requirements, high-level technical skills, which are likely to be tailored to the organisation's needs
5. incident response skills, which could include things like writing an incident response plan, incident management and recovery from cyber security breaches
6. soft skills, particularly upwards and downwards communication skills and the ability to train or educate wider staff.

Another key aspect to consider is that cyber security skills are needed not only among those in cyber security roles, but among wider non-specialist staff. The qualitative interviews highlight that management and leadership skills related to cyber security matter for board-level staff. Wider staff also require an awareness of cyber security, a basic understanding of how their actions impact on cyber security, and an ability to work collaboratively with those in cyber security roles to help identify and deal with cyber attacks – all areas highlighted as important in interviews with industry experts and organisations. This includes anything as basic as all staff understanding how to spot and deal with phishing emails, through to board members understanding how well cyber security is staffed in their organisation.

In addition to what we found in our primary research, we also acknowledge further feedback from stakeholders involved in this research that cyber security can also involve:

- investigation of the causes and perpetrators of cyber attacks, and bringing offenders to justice
- the research and development of new technologies, products or services, to address cyber security needs based on emerging technologies such as quantum computing, and to deal with new cyber threats in the future.

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

These activities does not typically fall under the remit of private and charitable sector organisations, but are important elements nonetheless, requiring specific technical expertise and skills.

Our suggested definition of cyber security skills

With all this in mind, we propose the following definition (in italics):

We define cyber security skills as the combination of essential and advanced technical expertise and skills, strategic management skills, planning and organisation skills, and complementary soft skills that allow organisations to:

- *understand the current and potential future cyber risks they face*
- *create and effectively spread awareness of cyber risks, good practice, and the rules or policies to be followed, upwards and downwards across the organisation*
- *implement the technical controls and carry out the technical tasks required to protect the organisation, based on an accurate understanding of the level of threat they face*
- *meet the organisation's obligations with regards to cyber security, such as legal obligations around data protection*
- *investigate and respond effectively to current and potential future cyber attacks, in line with the requirements of the organisation.*

This defines the core set of knowledge and skills that organisations need to either have within their workforce, or seek externally (for example, if they outsource their cyber security or take on external consultants). Those working in the wider cyber security industry – developing cyber security products or services, or carrying out fundamental research – may require additional skills, such as the technical expertise and skills needed to research and develop new technologies, products or services.

While this definition is intended to be succinct, we believe it covers a very wide range of cases. For example, designing, building and maintaining secure networks and systems comes under the implementation of appropriate technical controls. Drawing up and implementing effective cyber security policies comes under effectively spreading the rules or policies to be followed, upwards and downwards across the organisation. The forensic investigation of cyber attacks and legal pursuit of perpetrators falls under the final point about investigating and responding effectively to cyber attacks.

For individuals working in cyber security roles, implementing appropriate technical controls or carrying out the needed technical tasks would require a sufficient understanding of one or more the specific cyber security Knowledge Areas listed in CyBOK, such as software security, cryptography, or forensics.

The definition also acknowledges that there are specialist technical skills areas that are not relevant for all organisations, but are an important aspect of the cyber security industry (and are sought-after skills in the cyber security skills labour market). This covers the individuals within the industry who use high-level technical expertise and skills to carry out fundamental cyber security research, and to develop new technologies, products and services for other organisations.

2.5 What cyber security skills are considered more or less important?

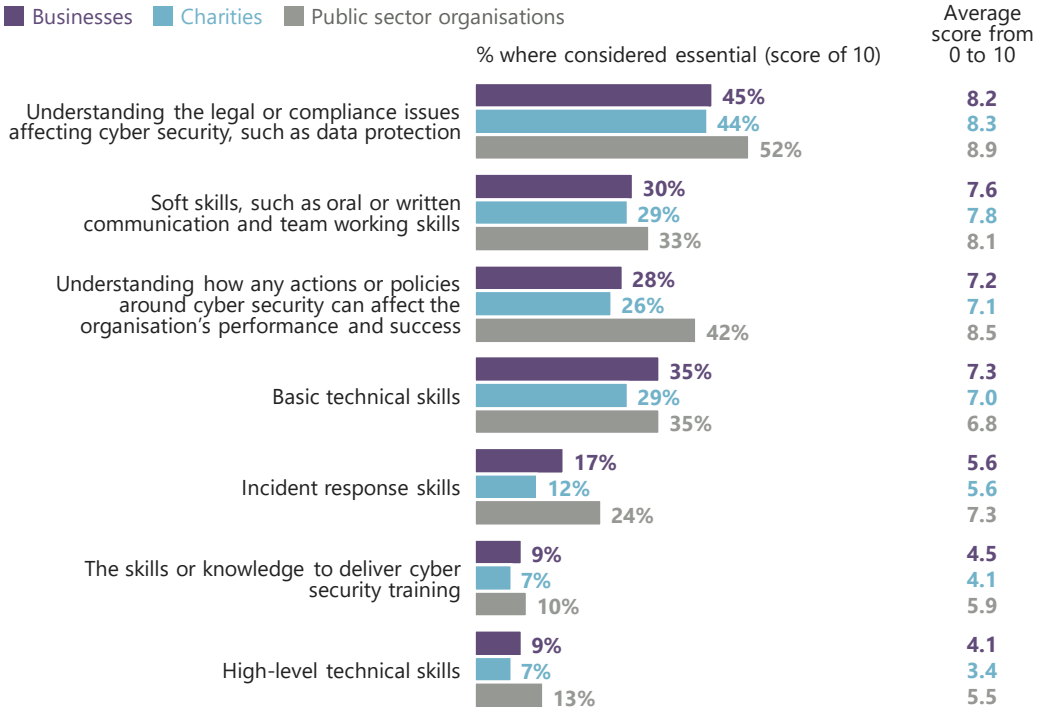
The quantitative survey takes the broad skills categories outlined in the previous section and asks organisations to rate them in terms of importance. A score of 0 means something is not at all important for those working in cyber security roles in the organisation to possess, while 10 means it is essential for them to have this skill. We define "basic technical skills" in the survey as having the abilities to implement the five technical controls covered in Cyber Essentials (which the question wording lays out in full). We define "high-level technical skills" in the survey as incorporating areas like the ones

 © Department for Digital, Culture, Media and Sport 2018

mentioned in Section 2.2 (designing secure networks and systems, penetration testing, threat intelligence, forensic analysis, interpreting malicious code and monitoring user activity).

As Figure 2.1 shows, across all types of organisations, soft skills and broader strategic management skills rate relatively highly, as do basic technical skills. In terms of the average response, soft skills are typically considered at least as important as basic technical skills. Again, this does not mean that organisations are making an informed decision to prioritise soft skills over technical skills. In reality, what this once more indicates is that organisations often lack an understanding of the technical skills they require to manage their cyber security, and consequently may undervalue such skills relative to the more easily understood soft skills. An implication is that organisations may need more education or guidance on the value of technical cyber security skills – to understand that successful cyber security involves more than just common sense. Furthermore, this analysis excludes external cyber security providers, where we would expect high-level technical skills and incident response skills to be considered more important.

Figure 2.1: Perceived importance of various skills areas for those working in cyber security roles



Bases: 1,030 businesses; 470 charities; 127 public sector organisations

Public sector organisations are more likely than those in the private or charitable sector to rate the following as important:

- understanding the business impact of actions or policies on cyber security
- high-level technical skills
- incident response skills
- training skills.

Businesses and charities are more closely matched. This suggests that in the public sector, there is a greater understanding of what the organisation needs from those in cyber security roles. In businesses and charities, this may be less well understood – it is not that businesses and charities have less need for technical skills, but rather that they do not know what kinds of technical skills the job requires.

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

There are also differences within businesses and charities. In particular, micro and small businesses, and low-income charities, are less likely than the average business and charity respectively to consider several of these skills areas as being important. For example, around a third of micro (35%) and small businesses (33%) consider basic technical skills to be essential, compared to over two-fifths of medium (45%) and large businesses (44%). This again could be explained by the findings from qualitative interviews with smaller businesses and charities – as aforementioned, they tended to have less of a grasp overall of the kinds of technical skills that were needed to cover cyber security.

There are a wide range of differing priorities by business sector (again, focusing on wider sectors of the economy – not firms working specifically in cyber security):

- Understanding of legal and compliance issues is considered far more important than average for businesses in the finance or insurance sectors (65%, vs. 45% on average), education sector (60%), and health, social care or social work sectors (59%). This may reflect that these are all highly-regulated industries.
- Soft skills are more likely than average to be considered as essential in the food or hospitality sector (49%, vs. 30% for the average business) and education sector (51%).
- Basic technical skills are more likely than average to be considered essential in information or communication firms (51%, vs. 35% on average) and education firms (47%).
- Incident response skills are more likely than average to be considered essential in finance or insurance firms (29%, vs. 17% on average) and education firms (27%).
- Training skills are more likely than average to be considered as essential in the construction sector (18%, vs. 9% for the average business).

Across these sector differences, it is clear that finance or insurance firms and education firms are more likely than others to emphasise the importance of the technical aspects of cyber security. This may reflect a higher engagement with cyber security generally in these sectors – something which has been previously established in the DCMS Cyber Security Breaches Surveys.

There are relatively few definitive regional differences. One significant difference that does emerge is that businesses in London are more likely than the average business to see incident response skills as essential for those working in cyber security roles (28% vs. 17%).

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

3 Who works in cyber security roles?

This chapter talks about the people covering cyber security across organisations – their pathway into this cyber security role, how much priority the role is given and how formalised it is, their seniority, and any relevant qualifications they hold. As context upfront, we also cover the typical size of cyber teams within organisations.

For this research, we allowed participants to self-define who the person most responsible for cyber security in their organisation was. Therefore, we are not talking exclusively about those who work in specialist high-skilled cyber security roles. Our approach raises important findings, such as the extent to which those working in cyber security roles are doing so informally.

The quantitative survey also included a question on the number of women working in cyber security roles. While the data generated are representative of businesses, they do not necessarily reflect true gender diversity among those working professionally in the cyber security sector. For example, they do not account for gender diversity within firms specifically working on cyber security technology development, or supplying cyber security products or services, which are the high-volume recruiters in the labour market. This was also not a core objective for this research. Therefore, we have not reported these findings, as they risk misleading readers on the extent to which gender diversity is a problem. We return to the issue of gender diversity in recruitment in Chapter 5.

Existing evidence

- The Inspired Careers website (a UK Government-supported recruitment website specialising in cyber security roles) illustrates the complexity of the cyber security jobs market. It identifies 87 specific job roles falling under five grades, from trainee, to practitioner, senior practitioner, principal, and lead.[8]
- Equally complex frameworks exist abroad. The NICE framework (Newhouse et al., 2017) for the US cyber workforce lists seven categories, covering a mix of technical and non-technical roles: security provision, maintenance, oversight and governance, protection and defence, analysis, operations and investigation.
- Both the 2017 GISWS (Frost & Sullivan) and Information Assurance Advisory Council (IAAC, 2017) suggest that it is common for individuals to progress into cyber security roles from outside the cyber or IT industry, from areas as diverse as human resources or physical security.
- Gender diversity has previously been established as a problem in cyber security, and in IT more broadly. The 2018 (ISC2) Cybersecurity Workforce Study finds that women comprise just 24% of the global cyber security workforce.

3.1 Size of cyber teams

It is highly common for businesses and charities to have just one individual managing or running cyber security in-house (the case in 49% of businesses and 40% of charities – including those that outsource aspects of their cyber security). This is much more atypical in public sector organisations, where 12 per cent have just one individual working in this area. The average business and the average charity tend to have around two people working in cyber security roles, whereas the average public sector organisation has around five people.

[8] See https://www.inspiredcareers.org/browse-careers/cyber-security/.

As might be expected, this varies by business and charity size. For medium businesses, there are an average of three people in the team, and for large businesses, there are an average of five, similar to public sector organisations. High-income charities have an average of three people in cyber security roles.

At a sector level, organisations in the finance or insurance sectors are more likely than average to have more than one person working in this area (65%, vs. 49% on average).

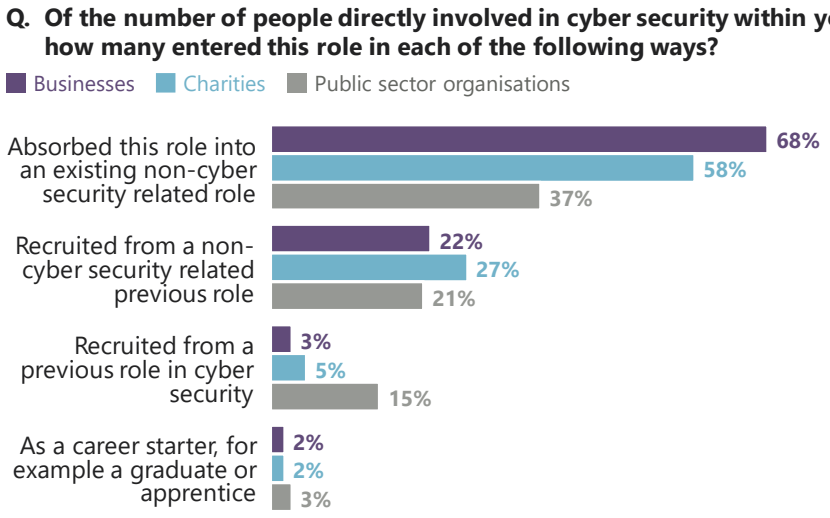
Businesses in the East Midlands stand out from other regions as having larger cyber security skills capability. Two-thirds (67%, vs. 49% on average) have more than one person on the team. Beyond this, there is no significant geographic variation.

3.2 Career pathways into cyber security roles

As Figure 3.1 demonstrates, the vast majority of those working in cyber security roles across businesses, charities and the public sector have absorbed this into their existing non-cyber security jobs.[9] These figures reflect those performing the role on their own or leading a team of people, as well as the people working under them within the team. This suggests that most organisations avoid having to recruit someone new to be responsible for their cyber security, and instead reposition internal staff to take this responsibility.

The second most common entry into a cyber security role is to be recruited from a previous non-cyber security job. This reflects qualitative findings from the industry expert and organisation interviews, where various participants pointed out that this is an immature labour market, where there is not a large crop of candidates who have previously worked in professional cyber security roles. It also highlights that career routes into cyber security roles can be very varied, often without defined career pathways.

Figure 3.1: Percentages of those in cyber security roles within organisations (excluding external cyber security providers) who enter the role through particular routes



Bases: 1,030 businesses; 470 charities; 127 public sector organisations

As an important caveat, these findings do not include those working specifically in cyber security firms (working on cyber security technology development, or supplying cyber security products or services), which are the high-volume recruiters in this labour market. Figure 3.1 is instead representative of those employed in operational cyber security roles across

[9] We have calculated these findings by first summing up the total number of team members that have entered their cyber security role via each route, and dividing this by the total number of people working in cyber security roles (as covered in Section 3.5). The figures are based on weighted data.

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

other organisations. The qualitative interviews with external cyber security providers suggest that these organisations focus their recruitment activities especially on graduates and apprentices at the start of their careers, so are likely to be the top employers for career starters in the cyber security industry. The external providers we spoke to were typically very large multinational organisations, and had split their businesses into different service lines based on specialist skillsets. For example, one participant was part of a specialist ethical hacking team.

3.3 How formalised are cyber security roles?

Integration into job descriptions

Overwhelmingly, cyber security roles within organisations – outside of external cyber security providers – are not badged as "cyber" roles. In the private and charitable sectors, the vast majority of organisations have individuals working in these roles informally rather than professionally. Just 11 per cent of businesses and 14 per cent of charities have cyber security written formally into the job descriptions of one or more staff.

The cyber security role is typically more formalised in the public sector, but it is still a minority of public sector organisations overall (39%) that have cyber security written into job descriptions.

Figure 3.2: Whether the cyber security role is included in job descriptions

Bases: 1,030 businesses; 470 charities; 127 public sector organisations

Having a formal cyber security role is linked to the size of the organisation. It is more common than average in medium (25%, vs. 11% on average) and large businesses (46%), and in high-income charities (38%, vs. 14% on average) – although it is still a minority of organisations even within these subgroups.

These results vary slightly across individual business sectors, although the role is still typically informal across all sectors. There are more people working formally in the role in information or communication businesses (18%, vs. 11% on average), and in the health, social care or social work sectors (19%) than in other businesses. By contrast, utilities or production firms (which includes manufacturing businesses) are among the least likely to have someone working formally in this role (6%).

Why are these roles not always badged as "cyber" roles?

The qualitative interviews help to explain why so many individuals move into cyber security roles on an informal basis, and therefore why they are not always badged as "cyber" roles. Participants across the private, charitable and public sectors typically did not have a job that was 100 per cent to do with cyber security. When moving into cyber security roles, people often maintained their previous jobs alongside taking on the cyber security brief. This is reflected in the variety of job titles we came across, including, for example: IT manager, information security manager, security manager, systems architect, head of finance and administration, technical director, operations manager and systems manager. With a few exceptions, these job titles typically did not have cyber security, or even security, in them.

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

"We have quite a few roles which have cyber security elements within them."
High-income charity

Instead, the qualitative research finds that there were typically three types of people who had absorbed cyber security roles into wider non-cyber security roles. These ranged from those with good technical skills (such as IT skills) to a total lack of technical skills.

- Those with good technical IT skills – several participants were performing the cyber security role as part of a wider IT maintenance job. For instance, we spoke to various heads of IT, service desk managers and IT managers. They generally considered cyber security to be an important part of their job, but did not always consider themselves to be cyber security specialists or to have high-level cyber security skills. Some of these organisations still accessed these high-level skills by using external cyber security providers. However, in other cases it was evident that the cyber security role had simply fallen to a single IT manager, because they had technical IT skills, and they were just expected to pick up cyber security skills on the job.

  There was one standout exception to this. One team in a public sector organisation had specifically called themselves the "information services" team. This was to avoid being associated simply with IT issues, and instead to help portray themselves as having a broader information governance role. This team did in fact have three people working in specialist high-skilled cyber security roles, under a team leader who worked as a systems architect.

- Those with basic to no technical skills – some felt that cyber security was a small part of their overall job, which was in a completely different area outside of IT, such as finance or general management. The cyber security role was considered tangential to their wider brief, rather than being seen as part of that brief, as it was with the IT professionals who had absorbed the role into their work. Some had moved into this role informally, as they were the same people that had been tasked with implementing GDPR in their respective organisations. In some cases, this meant that they did not dedicate much of their time to cyber security, relative to their other work priorities. In other cases, it meant that they limited their role to simply dealing with an external cyber security provider, and not taking any further actions beyond this.

  As might be expected, these individuals typically had less developed technical skills for the cyber security role – at best, they had basic IT skills, but lacked any knowledge of the higher-level technical skills that might be needed for the role. Nevertheless, those working in senior finance roles in large organisations were often more of a special case. These senior individuals were not technical IT experts themselves, but had an IT manager or team reporting directly to them, so still had access to these technical IT skills within the organisation.

- Those working informally, in a largely undefined role – finally, there were also smaller organisations that felt they did not have the budget to recruit someone to focus full-time on IT or cyber security. In these organisations, it had often fallen to one of the directors or a business owner to take direct responsibility for cyber security, because no one else would otherwise be doing this role. Again, as might be expected, these individuals also typically lacked technical skills, and also sometimes did not know what kinds of technical skills were needed for cyber security.

"In this company, we would just see cyber security as part of the general IT role … I think the Network Officer would have just picked up cyber security skills working in that environment."
Medium business

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

"I definitely think I've got an idea, a very basic idea, but I wouldn't feel comfortable being the sole responsible person for identifying all possible threats."

Large business (participant is the Head of Finance)

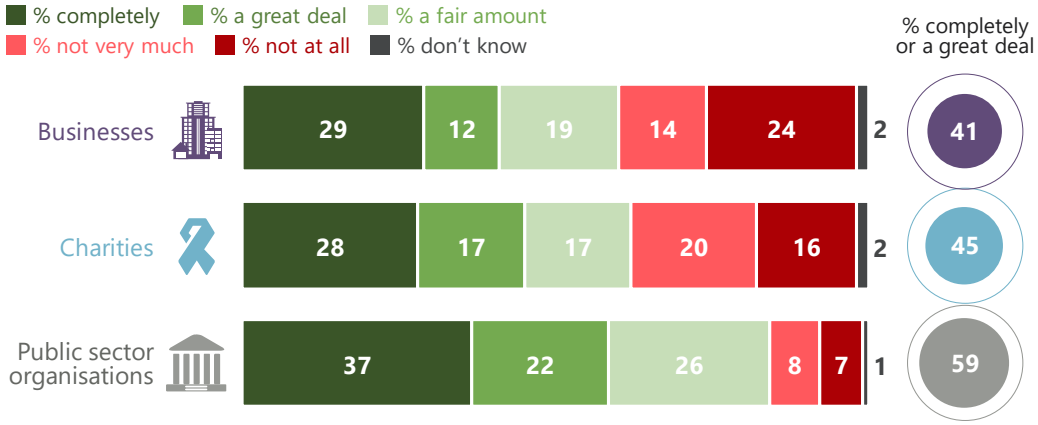
Is the cyber security role covered during absences?

One of the industry expert interviews raised the issue that organisations may be more exposed to cyber risks if there is only one individual working in cyber security, and there is no one else to cover this work in their absence. This could be whenever they are ill or take holiday. It could also mean that organisations inadvertently lose cyber security skills when those performing cyber security roles leave the organisation, and no one else takes on this role.

The survey results suggest a significant minority of organisations are exposed to this kind of risk, and that this is greater in businesses and charities than in the public sector. As Figure 3.3 shows, the majority of those responsible for cyber security in public sector organisations think that this role could be covered during absences, a great deal or completely (59%). This falls to a minority in businesses (41%) and charities (45%).

Figure 3.3: Extent to which the cyber security role could be covered when the lead individual is absent

Q. If you were away for an extended period of time … to what extent, if at all, would others in your organisation have the right skills or knowledge to cover your role with regards to cyber security?



Bases: 1,030 businesses; 470 charities; 127 public sector organisations

Micro businesses tend to be more vulnerable to this risk than larger ones. Two-fifths (38%) say the role could be covered completely or a great deal during absences, rising to half of all small businesses (51%), and around three-fifths of medium (57%) and large businesses (63%).

At the industry sector level, businesses in the finance or insurance sectors stand out as being more likely than others to say they could cover the cyber security role during absences (57% a great deal or completely, vs. 41% on average).

Businesses in London are also more likely than others to say they could completely cover the cyber security role if the main individual responsible is absent (47%, vs. 29% on average).

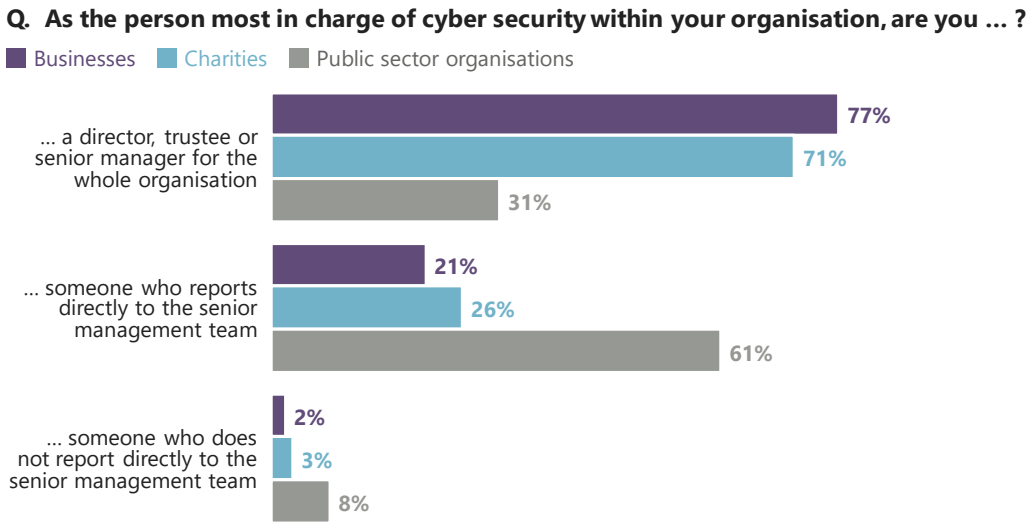
The individuals who have cyber security formally written into their job descriptions are also more likely than others to say their work could be covered in absences (53% say it could be covered a great deal or completely, vs. 39% of those doing the role informally). This again suggests that there is a strong divide between the organisations where cyber security roles are professionalised – where there are clearer chains of command and delegation of responsibilities – and the organisations where cyber security is handled in an informal way.

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

3.4 Seniority of those in charge of cyber security

As Figure 3.4 shows, the vast majority of businesses (77%) and charities (71%), have someone responsible for cyber security who is on the senior management team or board. This contrasts with public sector organisations, which tend to have individuals in these roles who do not sit on the board, but report into it (61%). Public sector organisations are also the most likely to have individuals in charge of cyber security who do not directly report to the board.

Figure 3.4: Seniority of the individuals most in charge of cyber security



Bases: 1,030 businesses; 470 charities; 127 public sector organisations

This might reflect the relative size of public sector organisations. They tend to be bigger than the average business or charity, meaning they necessarily have to have cyber security roles performed by more junior staff in the hierarchy. Large businesses more closely reflect the profile of public sector organisations in this regard, with those in charge of cyber security being on boards in 43 per cent of large businesses and reporting up to boards in 50 per cent of large businesses.

3.5 Qualifications of those in cyber security roles

Reflecting the fact that cyber security is most often managed on an informal basis across organisations, the results show, as expected, the vast majority of individuals working in cyber security roles do not have formal qualifications, and are not working towards them either. Overall, four per cent of businesses, six per cent of charities and 19 per cent of public sector organisations have individuals with or working towards relevant qualifications. The presence of qualifications is similarly rare across all business sectors. Again, this reflects our methodology, where we asked to speak to the individual most responsible for cyber security within each organisation. The findings highlight that in most cases, organisations do not employ cyber security professionals (i.e. outside of more generalist IT professionals or other, non-IT staff).

The prevalence of qualified staff in cyber security roles is higher than average in medium (19%, vs. 4% on average) and large businesses (32%). It is also higher than average, but to a lesser extent, in high-income charities (14%, vs. 6% on average).

Regionally, qualified staff are in higher numbers in businesses in the West Midlands (14%, vs. 4% on average).

The qualitative interviews with organisations can help to explain this state of affairs. Organisations often preferred experience over qualifications when recruiting. Some also discussed their feeling that cyber security qualifications were, at present, a poor indicator of all the non-technical skills required in cyber security roles. Others felt that they were priced out

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

of the market for qualified candidates, who could demand a higher salary, even though these organisations would have ideally preferred to have qualified staff. This is something we discuss again in more detail in Chapter 5.

Types of qualifications held

The survey included follow-up questions for those with qualifications, asking what these were. There are too few organisations answering this question to consider answers as statistically valid. However, the indicative answers suggest that most qualifications – among those in in-house cyber security roles (outside of external cyber security providers or firms developing cyber security technology) – tend to be either generalist IT qualifications, or technical cyber security qualifications achieved outside of the higher education system.

Perceptions of cyber apprenticeships

The indicative survey data on types of qualifications held also suggest that the prevalence of cyber apprenticeships across the private, public and charitable sectors is relatively low, with only a handful of respondents saying they took on cyber apprentices (and we did not ask organisations to define the level of the apprenticeship in the survey). As aforementioned, one important caveat is that these findings aim to represent people working in cyber security roles across all sectors, and not specifically within cyber security firms (working on cyber security technology development, or supplying cyber security products or services). These firms are the high-volume recruiters in this labour market.

In the qualitative interviews with external cyber security providers, apprenticeships appeared to be a common recruitment method, alongside graduate schemes. All the external providers we spoke to had taken on apprentices and considered cyber or IT apprenticeships to be a standard career path into the industry.

Some participants, both external providers and other organisations taking on apprentices, nonetheless suggested it was challenging for smaller teams to offer cyber apprenticeships, because existing team members often did not have the relevant cyber security skills or time to be able to train and supervise apprentices. This was more of a problem for cyber apprenticeships than for general IT apprenticeships, where existing staff were more likely to have relevant skills and knowledge to impart. As might be expected, it was also a more acute issue outside of external cyber security providers. The typical business that did not have existing technical cyber security skills within their organisation could not train an apprentice, so felt they had no choice but to look for staff with pre-existing technical skills instead.

The types of apprenticeships offered also differed between external cyber security providers and other organisations. Some external providers said they preferred cyber apprenticeships to more generalist IT apprenticeships, because they want apprentices to have a deeper understanding of this specialist area. By contrast, IT apprenticeships were more common among other organisations, reflecting that cyber security was often managed as part of a wider IT role.

3.6 Is there an agreed definition of a "cyber security professional"?

Altogether, the research suggests that there is currently no single definition of a cyber security professional. For a start, many of those identifying as working in cyber security roles have picked up these tasks informally, while maintaining their existing jobs in unrelated areas. In other cases, where it was more formalised, it was still often run from different departments such as finance, IT or operations. And even those working in specialist technical roles could not necessarily cover the absences of colleagues working in other, specialist areas.

Even within external cyber security providers, there are a range of job roles within the cyber area. As well as people with high-level technical skills, some of these businesses also employed staff in sales and client liaison roles. This meant that they were not using technical skills day-to-day, but were more focused on client relationship management, and needed soft skills alongside technical knowledge of their products and offering, to be able to discuss and understand the client's

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

needs. While these are not traditional cyber security roles, they do add to the complexity around defining roles in the industry. Furthermore, the relatively senior staff in these organisations who we interviewed also said their own roles were on balance not technical, but more focused on project management.

This is not to say that there could not be a definition or framework in place, to better help formalise cyber security roles. This is something we return to in the conclusions and recommendations, acknowledging the existing work that DCMS and the National Cyber Security Centre (NCSC) are already doing to develop a Cyber Certified Professional status. This is a new certification, aiming to set a benchmark standard for UK cyber security professionals.[10]

[10] See https://www.ncsc.gov.uk/scheme/certified-professional.

 © Department for Digital, Culture, Media and Sport 2018

4 Current skills and skills gaps

This chapter looks at the current spread of cyber security skills across the UK private, public and charitable sectors. There are no totally objective measures of many of the skills discussed here. When attempting to measure specific skills gaps, we are not able to objectively test whether an organisation has the skills among its workforce to manage or carry out certain cyber security tasks. We instead focus on the next closest measure – individuals' perceptions of the skills within their workforce. In the survey, we measure this in terms of how confident those responsible for cyber security would feel in carrying out certain tasks, and how well they feel they or their team understand particular knowledge areas.

Existing evidence

- There is a global cyber security skills shortage. The 2017 GISWS (Frost & Sullivan) finds that two-thirds (66%) of global organisations surveyed do not feel they have enough cyber security staff to meet the challenges they face. Half (49%) of these say this is because of difficulty finding qualified candidates. Europe and North America are in line with the average, while skills shortages are lower in the Asia-Pacific region (61%).
- This includes the UK, where this skills gap is partly fuelled by the rapid increase in demand for cyber security skills over the past five years. The former Tech Partnership (2017) found on average, there were just under 7,000 cyber security positions advertised in the UK across 2015/16, an increase of 103% on the level five years earlier.
- The Tech Partnership review of job adverts in 2015/16 identified that the top three most demanded skills areas were information security (41%), firewalls (26%) and network security (17%).
- The CSIS (2016) survey of IT decision makers found that intrusion detection, attack mitigation, software development and effective communication were the cyber security skill sets most lacking in the UK. The latter again highlights the importance of non-technical skills.

4.1 Basic technical skills and knowledge

Confidence in carrying out basic technical tasks

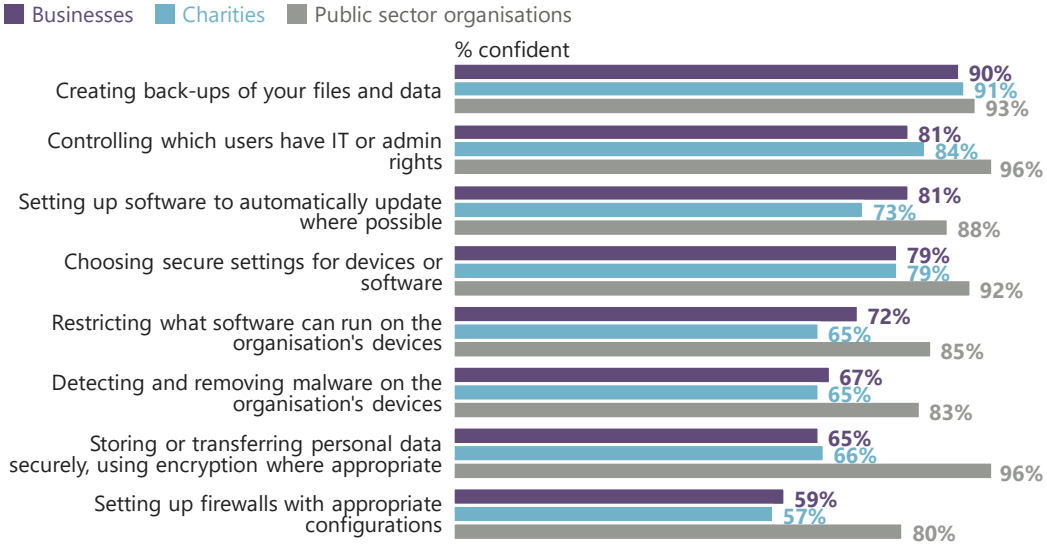
The survey asks the individuals responsible for cyber security across the private, public and charitable sectors how confident they would feel implementing basic technical controls to secure their organisation from cyber attacks. Five of these controls come from the Cyber Essentials scheme, as noted in Chapter 2. We also cover two other basic aspects of cyber security beyond this: storing or transferring personal data securely, which is a requirement of all organisations under GDPR, and backing up files and data. These questions exclude the organisations that say they outsource these functions to an external provider, so would not need to do them internally.

The summarised results, in Figure 4.1, show that the majority of individuals across all types of organisations are at least fairly confident in performing these basic tasks. Across these tasks, the greatest skills gap is in setting up firewalls with appropriate configurations (59% in the private sector and 57% in charities are confident in this area).

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

Figure 4.1: Overall confidence in performing basic cyber security tasks

Q. How confident, if at all, would you feel about the teams or any of the other individuals directly involved in cyber security being able to do each of the following technical tasks in your work?

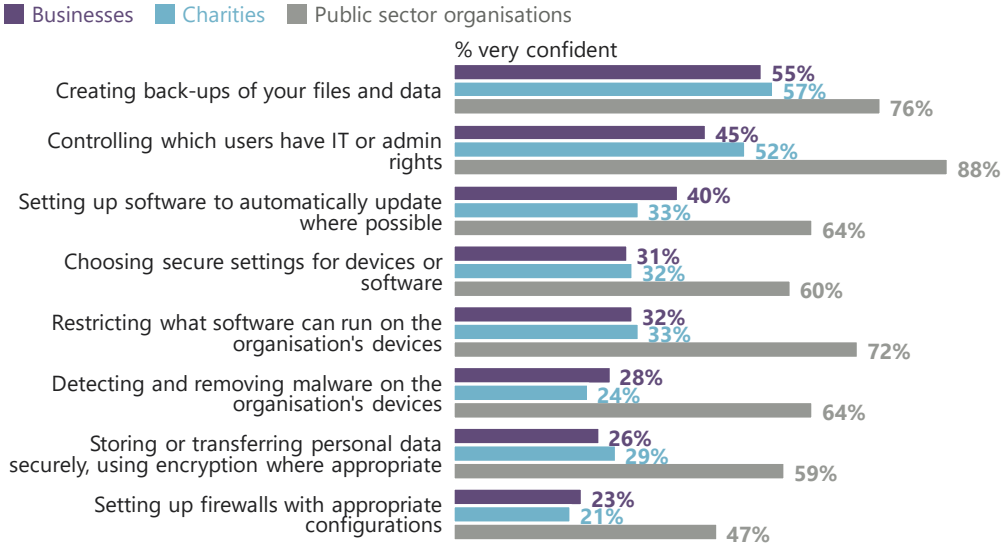


Bases (among those not outsourcing each activity): c.700 businesses; c.300 charities; c.70 public sector organisations

There is, however, a considerable disparity between those responsible within public sector organisations and others. This becomes even more stark when looking solely at the individuals who feel very confident, as Figure 4.2 does.

Figure 4.2: Proportion very confident in performing basic cyber security tasks

Q. How confident, if at all, would you feel about the teams or any of the other individuals directly involved in cyber security being able to do each of the following technical tasks in your work?



Bases (among those not outsourcing each activity): c.700 businesses; c.300 charities; c.70 public sector organisations

A combined basic technical skills indicator

It is possible to combine the eight basic technical tasks listed in Figures 4.1 and 4.2, and come up with a single indicator of the basic technical skills gap across organisations. We have calculated this as the percentage of organisations that are not

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

very confident or not at all confident in carrying out one or more of these eight basic tasks. On this basis, more than half (54%) of all businesses and the same proportion (54%) of charities have a basic technical cyber security skills gap. For public sector organisations 18 per cent have a basic technical skills gap. These figures are representative of their respective populations, so we can extrapolate them to indicate the total number of firms that have these basic technical skills gaps:

- Of the c.1.32 million businesses in the UK, approximately 710,000 have a basic technical cyber security skills gap.
- Of the c.199,000 registered charities, approximately 107,000 have this gap.
- Of the c.12,400 public sector organisations, approximately 2,200 have this gap.[11]

Knowledge of basic technical terms

As part of the Cyber Essentials checklist, organisations should understand the difference between personal and boundary firewalls, and what a sandboxed application is. Only 44 per cent of those in charge of cyber security in the private sector and 36 per cent in charities say they understand the distinction between the two different types of firewalls very or fairly well. And only a quarter (24%) each in the private or charitable sector say they understand what a sandboxed application is very or fairly well.

In businesses where individuals in cyber security roles say they are confident in setting up firewalls with appropriate configurations, a higher proportion than average (56%, vs. 44% on average) say they understand the difference between personal and boundary firewalls. This difference is expected, but it still means that there is potentially a false sense of confidence among the 42 per cent who feel confident in setting up firewalls, but say they do not understand the different types of firewalls.

The different types of firewalls are much better understood in the public sector (76% very or fairly well). However, even in the public sector, only half (51%) of those in cyber security roles feel say they understand what a sandboxed application is.

4.2 High-level technical skills

The survey also asks those who consider various high-skill technical tasks to be important whether they feel confident doing these tasks in-house.[12] The six high-level technical skills areas, in Figure 4.3, once again come from our categorisation of cyber skills in Chapter 2. They emerged as the areas of broad importance in the literature review and industry expert interviews. Once again, our findings here exclude the organisations that say they outsource these high-level functions to an external provider, so would not need to do them internally.

As Figure 4.3 shows, the greatest skills gaps for these high-level technical tasks are in the areas of security engineering, penetration testing and forensic analysis. Once again, across all these areas, skills gaps are higher in the private and charitable sectors than in the public sector. With that said, two areas where these high-level skills are lacking in the public sector, relative to other areas, are penetration testing (53% confident) and forensic analysis (55% confident). One area where charities have a greater skills gap than businesses is in threat intelligence (38% confident, vs. 53% in businesses).

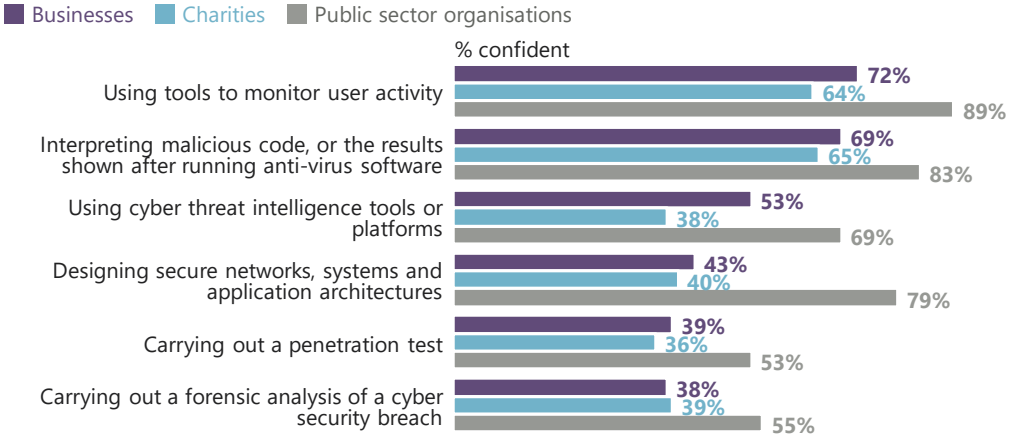
[11] The business and public sector population data are taken from BEIS business population estimates in 2017. These are the latest estimates as of the publication of this report. See https://www.gov.uk/government/statistics/business-population-estimates-2017. The charity estimates are taken from the combined total populations across the three charity registers for England and Wales, Northern Ireland and Scotland. For all the extrapolated figures presented here and across the report, we have rounded to either the nearest 100, or to three significant figures. These figures are of course subject to margins of error, as with all the results from the survey. The margin of error for businesses in this case is ±4.2 percentage points. This means that the true figure could be between approximately 660,000 and 765,000 businesses.

[12] The survey asked organisations how important it was for them to possess high-level technical skills to carry out the kinds of tasks in Figure 4.3. This was on a scale of 0 to 10, where 10 was essential. This follow-up question about confidence in performing these tasks was only asked to those giving an answer of 5 or more.

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

Figure 4.3: Overall confidence in performing high-level cyber security tasks

Q. How confident, if at all, would you feel about the teams or any of the other individuals directly involved in cyber security being able to do each of the following technical tasks in your work?

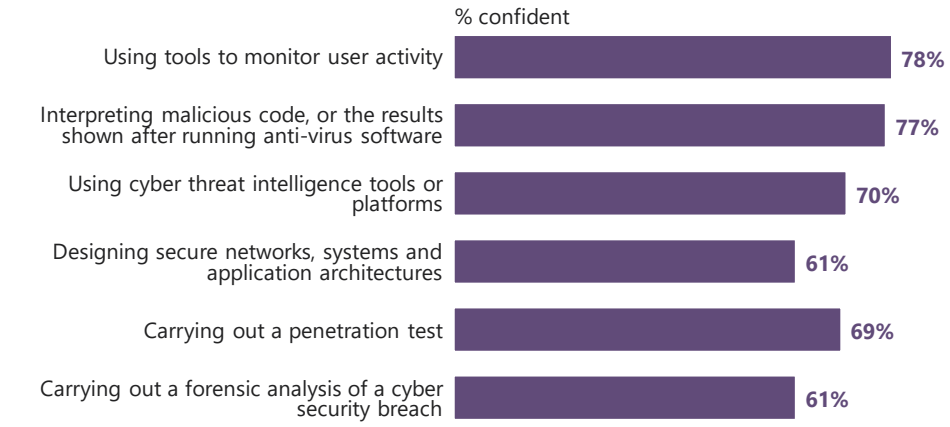


Bases (among those not outsourcing each activity): c.400 businesses; c.150 charities; c.60 public sector organisations

As covered in Chapter 2, nine per cent of businesses consider these kinds of high-level technical skills to be "essential" skills for those working on cyber security in their organisations. Among these businesses, as might be expected, the individuals responsible for cyber security are far more likely to have skills in these areas than in other businesses. However, as Figure 4.4 shows, there are still around three to four in ten of these organisations – the ones where these tasks are considered essential – where those working in cyber security roles are not very or fairly confident at performing them. The biggest skills gap here is again for security engineering and forensic analysis, but less so for penetration testing. This gives an idea of which skills gaps are most acute among those that have very sophisticated cyber security needs.

Figure 4.4: Overall confidence in performing high-level cyber security tasks, in businesses that consider these skills to be essential

Q. How confident, if at all, would you feel about the teams or any of the other individuals directly involved in cyber security being able to do each of the following technical tasks in your work?



Bases: c.90 businesses that consider high-level skills to be essential and do not outsource these activities

Extrapolating high-level technical skills gaps across the business population

Once again, we can extrapolate these figures to indicate the total number of private sector firms that have skills gaps in each of these more advanced technical areas of cyber security. We take this to be the number of businesses that are not

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

very confident or not at all confident in carrying out these advanced cyber security tasks. For this analysis, we have rebased proportions to be out of all businesses. So businesses that outsource these tasks are considered not to have a skills gap in this area. Businesses that do not consider these tasks to be important for their organisations (a score of 0 to 4 in Figure 2.1) are also, for the purposes of this analysis, considered not to have a skills gap in this area. On this basis, approximately:

- 302,000 businesses (23%) have a skills gap in forensic analysis
- 289,000 businesses (22%) have a skills gap in penetration testing
- 276,000 businesses (21%) have a skills gap in security architecture
- 223,000 businesses (17%) have a skills gap in threat intelligence
- 145,000 businesses (11%) have a skills gap in interpreting malicious code
- 131,000 businesses (10%) have a skills gap in user activity monitoring.

A combined high-level technical skills indicator

We have combined these six high-level technical skills areas (from Figures 4.3) and once again come up with a single indicator of the high-level technical skills gap across organisations. This is the percentage of organisations that are not very confident or not at all confident in carrying out one or more of these six advanced tasks. On this basis:

- 407,000 businesses (31%) have a high-level technical skills gap[13]
- 43,700 charities (22%) have this skills gap
- 3,300 public sector organisations (27%) have this skills gap.

While this gap is lower among charities than among businesses, this does not necessarily mean that charities have more of these advanced skills in-house. In fact, it suggests that charities are less likely to consider themselves as needing these high-level skills at all. This is based on charities' own perceptions of what skill they need, and the findings may hint that they are simply less aware of what they need to do on cyber security than the typical private sector business.

Qualitative views on high-level technical skills gaps

The qualitative research provides further insight into the specific disciplines that currently lack candidates with sufficient skills. The following disciplines in particular were mentioned several times by large organisations and external cyber security providers:

- cloud security
- end-point security
- identity and access management
- penetration testing (sometimes referred to as ethical hacking)
- security architecture
- threat hunting (i.e. actively searching networks for advanced cyber threats).

A common theme from both the industry expert interviews and the follow-up interviews with organisations was that the labour market for many specialist high-level skills was immature. Participants said that there are not many people available to work in specialist areas because it takes many years for people to get relevant experience, and because further and

[13] Again, these figures are subject to margins of error. In this case, the margin of error for businesses is ±3.9 percentage points. This means that the true figure could be between approximately 356,000 and 462,000 businesses.

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

higher education courses have not focused on these specific areas. By contrast, the labour market has lots of people with more generalist IT skills.

External cyber security providers highlighted that the technical skills needed to manage their clients' cyber security are constantly changing. This reflected that people who have high-level technical skills often have these for particular security products – products which can change over time, or become obsolete. The implication was that there would always be skills gaps and shortages in these high-level technical skills. One provider had addressed this by investing in reskilling existing staff on an ongoing basis, so that their skillsets stayed up to date – an approach we discuss more in Chapter 6.

As a result of both labour market immaturity and the issue of product obsolescence, external providers said they needed to think ahead about what skills would be needed the next three to five years, when making decisions now on training and recruitment, and not just focus on current skills needs. The anticipated future cyber security skills that came up in the external provider interviews were around artificial intelligence, automation and data analytics, as well as threat hunting.

One external provider considered knowledge of artificial intelligence and automation to be particularly important to invest in for future cyber security staff. They said that in the future, it is likely that the more basic aspects of a security analyst's role will be automated. This would mean that the role either becomes unnecessary, or becomes focused on more complex security analysis, leaving machines to do the more basic tasks. A long-term implication, they said, would be the need to employ more mathematicians.

"The software manufacturers are making their products more inter-operative, which then reduces some of the skills required to knit them all together. So the future of cyber is going to want more mathematicians than programmers."
External cyber security provider

The same provider also noted the current emerging role of threat hunter, and how this would be more prominent in the future. They felt that cyber security in the largest and most sophisticated organisations is moving from being reactive to proactive. So instead of simply dealing with cyber threats after identifying them, organisations would invest more in threat hunters that actively seek out cyber threats by scouring the dark web.

4.3 What types of organisations have greater technical skills gaps?

Differences by size

Technical skills gaps tend to be correlated with the size of an organisation. Among businesses, those working in cyber security roles in micro organisations tend to be less confident than average in dealing with each of the basic and high-level tasks asked about in the survey. For instance, looking at the overall basic technical skills indicator (grouping together all the tasks in Figure 4.1), almost six in ten micro firms (57%) and four in ten small firms (41%) say they do not have the skills to carry out at least one of these basic technical tasks, compared to two in ten medium businesses (22%) and three in ten large businesses (30%).

Across charities, basic technical skills gaps are also more prevalent in low-income charities than in high-income ones. On the overall basic technical skills indicator, six in ten low-income charities (61%) have a skills gap, compared to three in ten high-income charities (31%).

Those working in medium and large businesses tend to be equally confident, although there are some important areas where confidence is lower in large businesses than in medium ones:

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

- choosing secure device or software settings (98% confident in medium businesses, vs. 90% in large businesses)
- creating back-ups (97% vs. 89%)
- setting up software to automatically update (97% vs. 86%)
- restricting what can run on internal devices (91% vs. 78%).

It is unclear what is behind this, but it may be that in larger organisations, some of these basic tasks become harder to manage with higher volumes of staff.

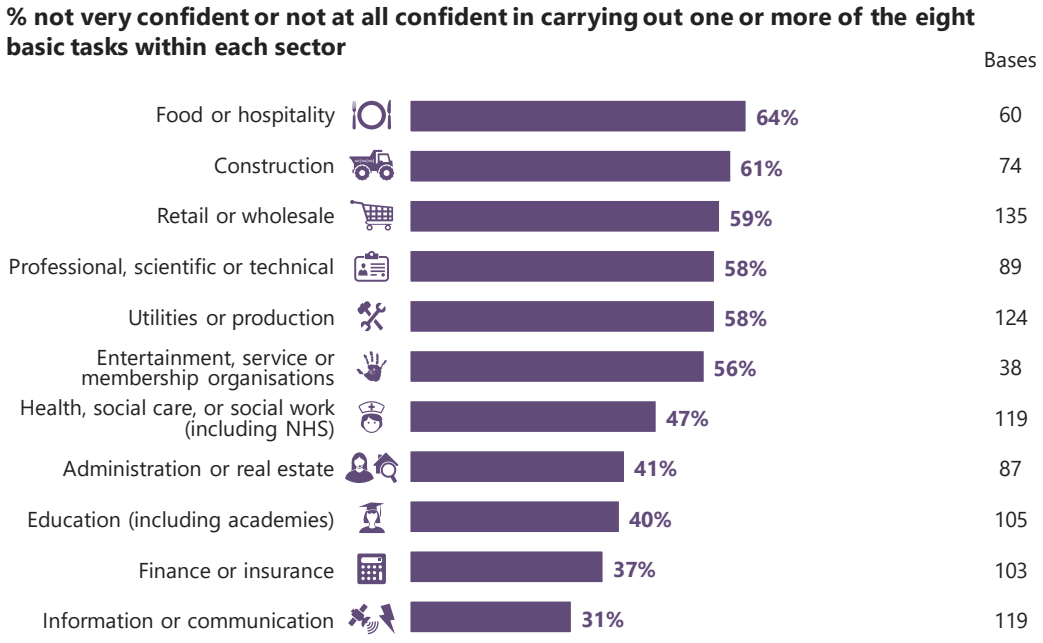
Team sizes also make a difference. In businesses where multiple people work in cyber security roles, there are less likely to be skills gaps for penetration testing (48% confident, vs. 29% in businesses with a single person covering cyber security) and forensic analysis (47% confident, vs. 28% in businesses with a single person). This suggests that businesses are employing specialists to cover these roles specifically, or that larger teams simply have more capacity to carry out these tasks.

For all the technical tasks included in the survey, there also tend to be bigger skills gaps when individuals are working in the role informally – where cyber security is not written into their job description.

Sector differences

Looking at our combined basic technical skills indicator, we can see in Figure 4.5 that there is a clear split in sectors. Basic technical skills gaps tend to be more prevalent in the following sectors: food or hospitality, construction, retail or wholesale, professional scientific or technical firms, utilities or production (including manufacturing firms), and entertainment, service or membership organisations. Information or communications firms, and finance or insurance firms, are especially well covered in terms of basic technical skills, relative to others.

Figure 4.5: Basic technical skills gap by sector



Bases are noted on the chart.
Too few transport or storage firms to analyse as a separate subgroup (effective base size under 30).

More specifically, individuals responsible for cyber security in the professional, scientific or technical sector are less likely than average to feel confident in carrying out various basic tasks, including:

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

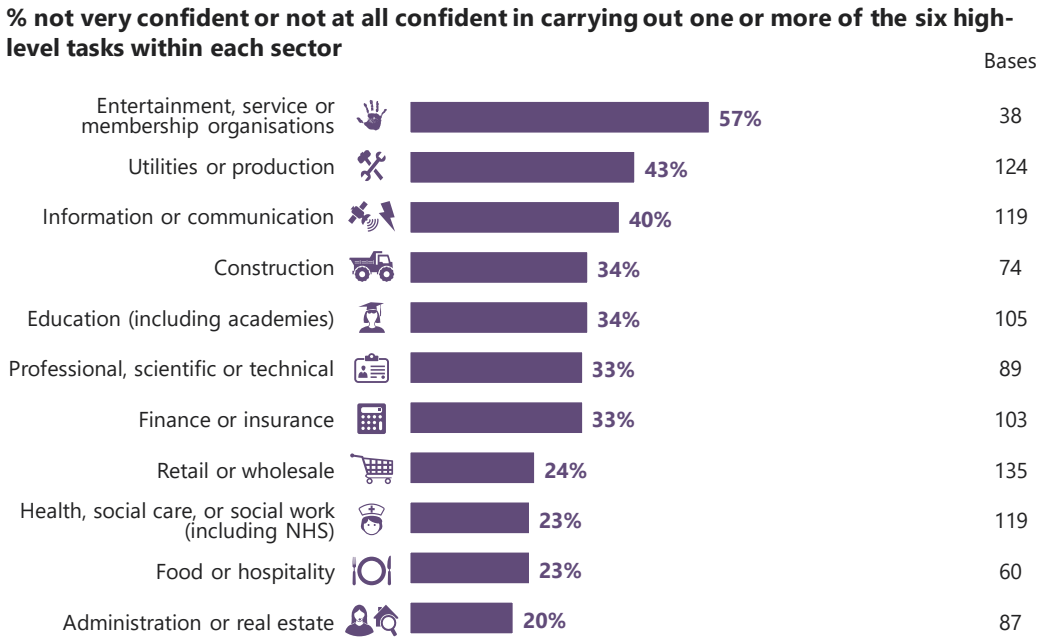
- storing or transferring personal data securely (44% not confident, vs. 30% on average)
- restricting what can run on internal devices (39% vs. 25%)
- choosing secure device or software settings (33% vs. 19%)
- controlling who has admin or access rights (25% vs. 14%).

The reasons behind this specific set of sector differences are unclear. DCMS's Cyber Security Breaches Survey series typically finds professional, scientific or technical businesses to be more engaged with cyber security than others. However, these differences (as with all the others we comment on in this report) are statistically significant.

When it comes to high-level technical skills, utilities or production firms, and information or communication firms stand out as being among the most likely to face a skills gap. On this indicator, there is a difference between information or communication businesses and finance or insurance businesses, suggesting that, while both types of businesses tend to be highly engaged in cyber security and cover the basics relatively well, information or communication firms have a bigger unfulfilled need for advanced technical skills in-house to manage their cyber security.

While entertainment, service or membership organisations come at the top of Figure 4.6, it is worth noting the very small sample size for this particular sector. This means that the margins of error around the survey findings for this sector are especially high, and this finding should be treated with caution.

Figure 4.6: High-level technical skills gap by sector



Bases are noted on the chart.
Too few transport or storage firms to analyse as a separate subgroup (effective base size under 30).

Geographic differences

Businesses in London express lower skills gaps than those in other regions in relation to nearly all of the technical tasks asked about in the survey. This includes, as an example of the size of these differences:

- storing or transferring personal data securely (80% confident in London, vs. 65% on average)
- setting up firewalls with appropriate configurations (73% confident, vs. 59% on average)
- carrying out a penetration test (54% confident, vs. 38% on average).

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

When looking at the combined basic technical skills indicator (again grouping together all the tasks in Figure 4.1), around four in ten firms in London (42%) say they do not have the skills to carry out at least one of these basic technical tasks, compared to over five in ten firms outside London (55%).

The London differences reflect the anecdotal findings from the industry expert interviews. Various experts mentioned that London and Cheltenham were big hubs for cyber security skills in the UK. It also mirrors previous research from the former Tech Partnership (2017), which tracked jobs in cyber security skills and found that around six in ten were based in London or the South East of England. Altogether, these findings suggest that candidates for cyber security roles cluster in London, where there is a relatively high demand for skills. Businesses outside London may not understand their cyber security skills needs as well (as Chapter 2 suggested), and even those that do have a harder time filling these gaps, potentially due to the best candidates being drawn to London.

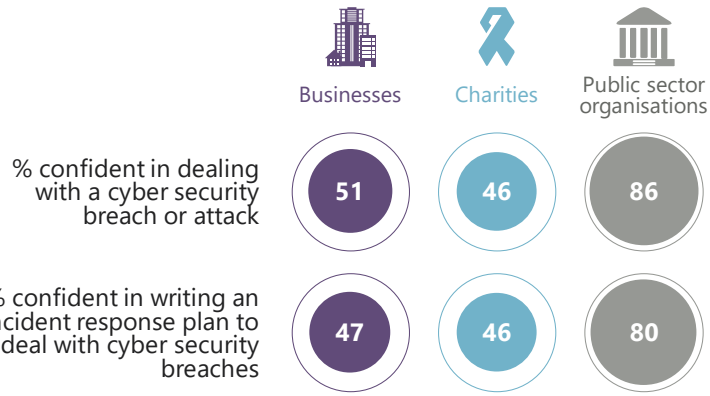
The qualitative interviews with organisations also suggest challenges filling cyber security skills gaps for organisations outside of any big city, and not just London. For example, one borough council in the Midlands mentioned that there were few IT jobs in its local area, which meant most IT professionals had moved away to nearby big cities.

4.4 Incident response

Figure 4.7 shows that those working in cyber security roles in the public sector feel far more confident dealing with cyber security breach or attack than those in the private and charitable sectors (where around half or more do not feel very or fairly confident). Just 15 per cent in the private sector, 14 per cent in the charitable sector and 35% in the public sector feel very confident in this. Again, this excludes organisations that say they outsource incident response.

Across each type of organisation, similar proportions feel confident that they could write an incident response plan – also shown in Figure 4.5. These two sets of results suggest that, across all organisations, one of the biggest skills gaps is in incident response and it is greater than the need for any specific technical skills.

Figure 4.7: Overall confidence in dealing with a cyber security breach or attack



Bases (among those not outsourcing each activity): c.500 businesses; c.200 charities; c.60 public sector organisations

The relatively large skills gap in incident response partly reflects that, compared to other skills areas, many organisations do not seem to consider incident response skills as particularly important. As Chapter 2 discusses, just 17 per cent of businesses consider these to be "essential" skills for those working in cyber security roles in their organisation. Within these businesses, seven in ten (69%) are confident that the individuals responsible for cyber security have the skills needed to deal with a breach or attack. However, this still leaves three in ten businesses (31%) where the people in these roles are not confident in doing this.

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

Once again, this is perceived to be a much bigger skills gap for micro (49% confident) and small businesses (60% confident) than for medium (79% confident) and large ones (80% confident). Similarly, in charities this is a bigger gap for low-income (41% confident) and middle-income charities (49% confident) than for high-income ones (84% confident).

These size differences are linked to whether organisations have someone formally working in a cyber security role, and the size of the team. As Chapter 3 discusses, smaller organisations are less likely to have formalised their cyber security, and tend to have just one person covering this area. In businesses where someone is formally working in this role, seven in ten (69%, vs. 51% on average) are confident that these individuals have the skills to deal with a breach or attack. Businesses with multiple people working in cyber security roles typically have a lower skills gap on this issue than when there is just one person (59% vs. 45% confident).

The business sectors where staff are among the least likely to be confident in dealing with an incident are the food or hospitality sector (39% confident) and construction sector (41% confident). The sectors where this skills gap is lowest are the administration or real estate sectors (76% confident, vs. 51% overall), finance or insurance (71% confident) and information or communication (68% confident).

We discuss the incident response capabilities of senior management teams separately in Section 4.4.

Extrapolating incident response skills gaps

Once more, we can extrapolate the survey data to indicate the total number of organisations that have an incident response skills gap. We calculate this as the number of businesses that are not very confident or not at all confident in dealing with a cyber security breach. We have again rebased this proportion to be out of all firms, so the ones that outsource incident response are considered not to have a skills gap in this area. On this basis, approximately:

- 460,000 businesses (35%) have an incident response skills gap
- 77,400 charities (39%) have this skills gap
- 700 public sector organisations (6%) have this skills gap.

4.5 Management and communication skills of those working in cyber security roles

As we note in Chapter 2, organisations place a particularly high value on broader management, planning and communication skills. They typically rank these as highly or higher than basic technical skills in terms of importance.

Upwards and downwards communication and training skills

The qualitative interviews with both industry experts and organisations uncovered, anecdotally, a sense that people working in technical cyber security roles can be too focused on the technical elements. This means they often end up lacking soft skills, such as communication skills needed to educate other staff members. Interviews with organisations that outsource cyber security also hinted that communication is often an aspect that their external cyber security providers can improve on. Poor communication was a commonly recalled aspect of bad experiences with providers. We return to this topic in Chapter 7.

Chapter 2 notes that communication is both upwards, to senior managers, and downwards, to wider staff. The survey explores both types, as Figure 4.8 illustrates.

While the vast majority of individuals in cyber security roles across all types of organisations are confident in providing guidance on passwords and in communicating cyber risks to more senior colleagues, they are far less confident in preparing training materials for wider staff. Even within public sector organisations, where three-quarters (75%) are

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

confident overall in preparing training, just 18 per cent are very confident in this (vs. 10% in the private sector and 12% in charities). This may reflect that these individuals do not consider training to be a core cyber security skill, and part of their cyber security role – although these figures include the individuals identified by the organisation as being most responsible for that organisation's cyber security.

Figure 4.8: Overall confidence in communicating cyber security risks and guidance

Q. How confident, if at all, would you feel about you or any of the other individuals directly involved in cyber security being able to do each of the following communication tasks in your work?

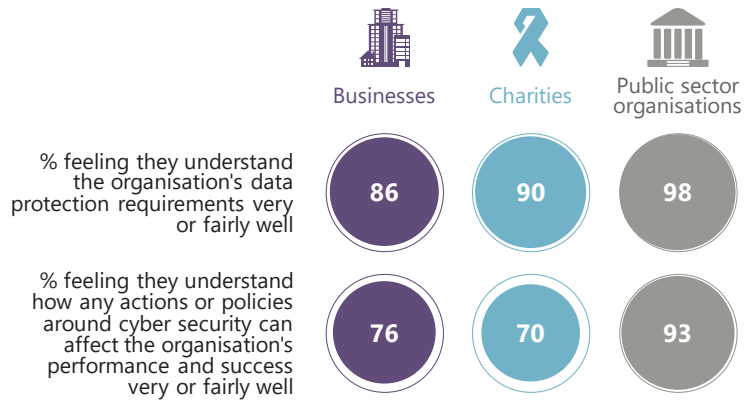
Bases (asked of random selection of total sample): c.350 businesses; c.200 charities; c.90 public sector organisations

The ability to communicate risks and good practice across the organisation is more likely to be missing in businesses that outsource cyber security. Businesses that outsource are more likely than others to have an internal skills gap in communicating risks effectively to senior managers (61% confident, vs. 70% on average) and in preparing training materials (57% not confident, vs. 47% on average). This mirrors some aspects of the external cyber security provider-client relationship that we discuss more in Chapter 7. In the qualitative interviews, some businesses felt that they did not have good communication from their external provider. It is probable that businesses in cases like this there is also less discussion of cyber security within the business.

Strategic management and planning ability

Across all types of organisations, there is a high level of perceived understanding of the organisations data protection requirements, and of how actions on cyber security impact on wider business objectives. This is shown in Figure 4.9.

Figure 4.9: Self-reported understanding of compliance requirements and wider impact of cyber security

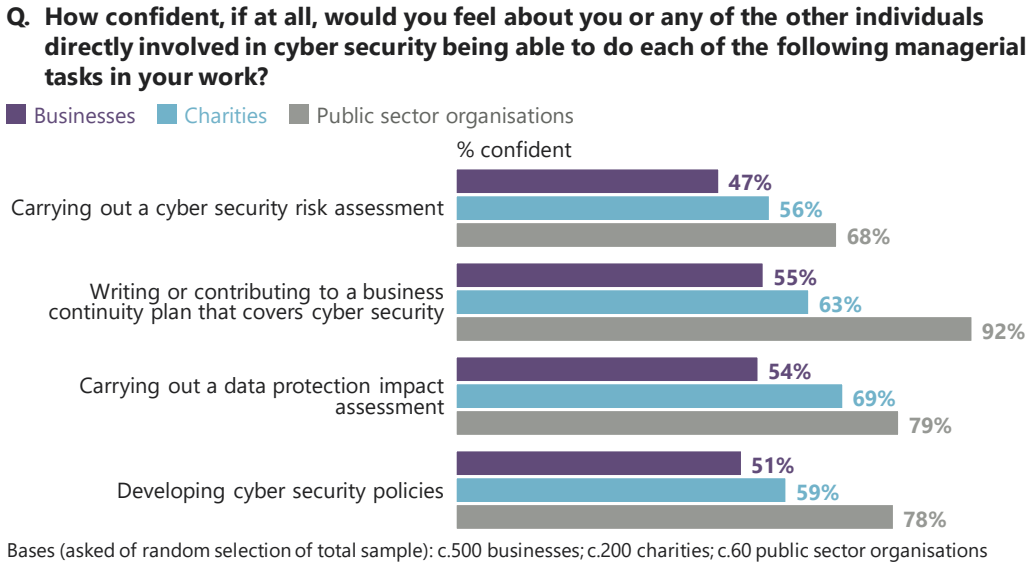


Bases (asked of random selection of total sample): c.500 businesses; c.200 charities; c.60 public sector organisations

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

At the same time, those working in cyber security roles are not necessarily confident in documenting these things. The survey covers how confident they would be at writing risk or impact assessments, business continuity plans and cyber security policies. This is an area where businesses typically have greater skills gaps than charities, and both fall behind the public sector, which Figure 4.10 shows. In the private sector, around half feel confident in doing each of these things.

Figure 4.10: Overall confidence in documenting cyber risks and planning how the organisation responds



Bases (asked of random selection of total sample): c.500 businesses; c.200 charities; c.60 public sector organisations

Once again, confidence on each of these aspects tends to be highest in the information or communication sectors, and finance or insurance sectors. There are specific instances of lower-than-average confidence in certain sectors: in construction around data protection impact assessments (65% not confident, vs. 43% on average), and in retail or wholesale businesses in relation to developing cyber security policies (60% not confident, vs. 47% on average).

4.6 Cyber security skills at the board level

As we outline in Chapter 2, cyber security skills matter not only for those working directly in cyber security roles, but also for senior managers and wider staff. Figure 4.11 shows how much those at the board level are felt to understand cyber risks, and their obligations towards cyber security and data protection. The responses here represent the perceptions of those directly responsible for cyber security, rather than the senior managers themselves.

It is clear that the vast majority of senior managers are felt to understand their organisation's data protection requirements well. This relatively high score across all types of organisations may reflect that the survey took place around one to three months after the implementation of GDPR. In this period, we would expect a heightened awareness of data protection.

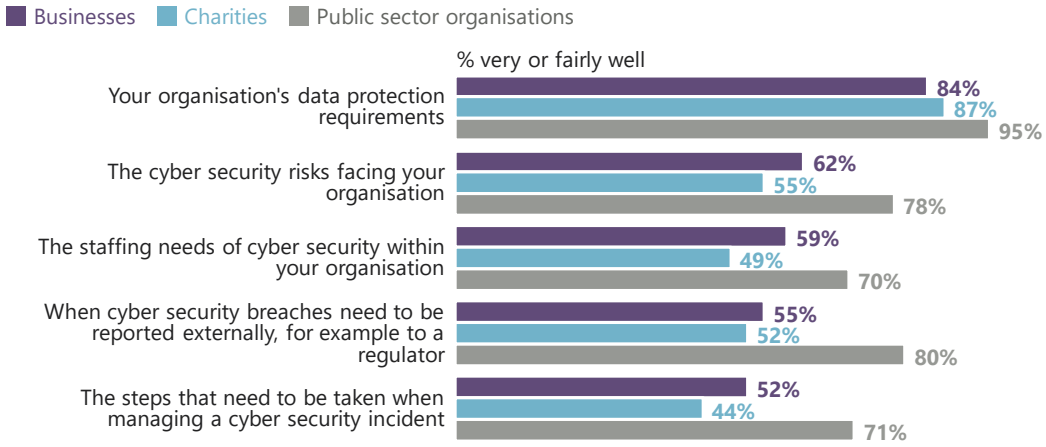
At the same time, in the private and charity sector especially, there is typically less understanding around when cyber security breaches need to be reported to the regulator (when they involve personal data). This is even though this kind of reporting is a new requirement of GDPR.

There is also relatively low understanding in businesses and charities of the cyber risks facing their organisations, how to respond to cyber security incidents, and the staff needed to cover cyber Incident response in particular appears to be one of the least well understood aspects among senior managers. For example, senior managers in fewer than half (44%) of all charities are felt to understand how to respond to a cyber security incident well.

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

Figure 4.11: Perceived understanding of cyber security and data protection among senior managers

Q. How well, if at all, would you say your organisation's directors, trustees or senior managers, including council members, understand each of the following?



Bases: 1,030 businesses; 470 charities; 127 public sector organisations

Among charities, understanding is closely associated with income. Senior managers and trustees in high-income charities are more likely than those in the average charity to be felt to understand each of these aspects of cyber security.

In businesses, there are also differences by size, but these are less clear-cut. Senior managers in micro businesses are typically among the least likely to be felt to understand each of these aspects. But senior managers in large businesses are felt to be less understanding of several aspects than those in medium businesses. This includes:

- the cyber risks facing the business (65% felt to understand this well in large firms, vs. 81% in medium firms)
- the business's data protection requirements (84% vs. 94%)
- the staffing needs of cyber security within the organisation (58% vs. 71%)
- the steps to take for incident response (52% vs. 68%).

This suggests that it is tougher to engage directly with senior management on cyber security in large organisations than in medium ones. This is possibly because in these larger organisations, the individuals in cyber security roles may have less direct contact with board-level senior managers, making it harder to get the message across. This highlights the importance of ongoing Government efforts to make everyone – including board members – aware of their responsibilities when it comes to cyber security, through existing efforts such as the board toolkit[14] under continual development. It also suggests more work is needed in this area.

Senior managers in utilities or production firms are felt to have a lower-than-average understanding of the cyber risks facing their business (24% are felt to understand this not at all well, vs. 14% on average). Senior managers in construction firms also fall below average (48% are felt to understand this not very well or not at all well, vs. 34% on average). The sectors in which senior managers are perceived to understand this better than average are finance or insurance (92% well, vs. 62% on average), information or communication (78% well), administration or real estate (77% well) and education (75% well). These same sector differences are also present in relation to senior managers' understanding of incident response and of when to report cyber security breaches.

[14] See https://www.ncsc.gov.uk/guidance/board-toolkit-five-questions-your-boards-agenda.

The challenges engaging senior management in cyber security

In the qualitative interviews, those in cyber security roles had mixed experiences trying to engage senior managers in cyber security. In some cases, while senior managers considered cyber security important, it was not seen as a strategic priority on the same scale as other issues like budgets and financial management. One public sector school noted that the school's senior management would always be more focused on teaching, finances and building renovation than on cyber security, because the former issues would always be higher strategic priorities for them.

Those responsible for cyber security also pointed out that staffing and training needs were dynamic, constantly evolving in line with the evolving cyber threat – the job has become more demanding over time.

"I do feel that the rate of attack has increased disproportionately to our ability to respond. Although we're in a better place than we were five years ago, the world is a more threatening place than it was five years ago, and we're playing catch up."
Middle-income charity

When it came to decisions around staffing, outsourcing and training, the involvement of senior managers in cyber security was often felt to be fairly superficial, with cost overriding other factors. For example, some participants highlighted that their senior managers would not necessarily know the difference between a technically-proficient external cyber security provider and one that was not, or the difference between good and bad training, and would focus on what cost the least. This may be an area where the Government could provide further guidance.

At the same time, a common theme was that senior management teams had become more engaged with cyber security as part of the wider GDPR agenda. Since it was a legal requirement to be GDPR-compliant, GDPR was discussed at board level. Organisations where senior managers had not invested in cyber security training had nonetheless invested in GDPR training or seminars in some cases. This potentially represents an opportunity to improve board-level engagement with cyber security, by injecting more cyber security content into GDPR guidance and training, or potentially finding other ways to make it the same kind of strategic priority as GDPR.

4.7 Cyber security skills among wider staff

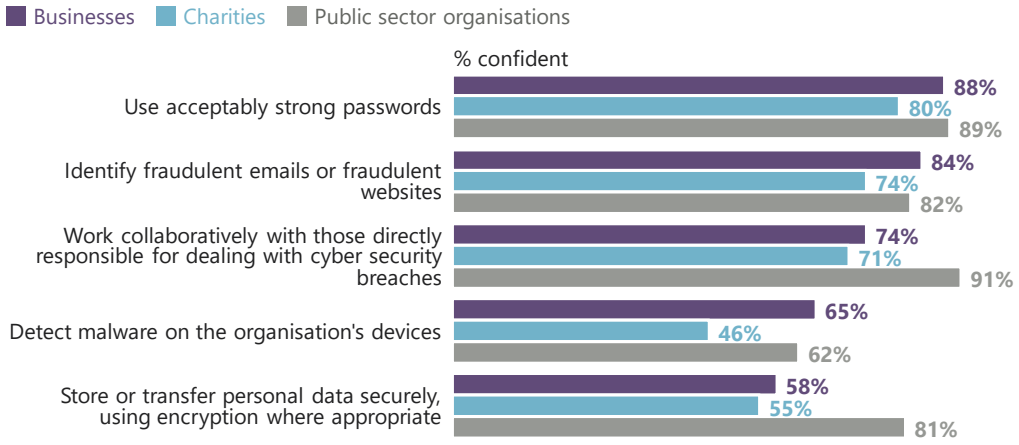
Figure 4.12 shows how well wider non-specialist staff understand important aspects of cyber security across different types of organisations. On these measures, public and private sector organisations are generally more in line with each other. This is with the exception of two areas where again the public sector scores more highly than the private sector: the ability of wider staff to store and transfer personal data securely, and their ability to work collaboratively with those in cyber security roles.

Private and public sector organisations also score more highly than charitable organisations in three other areas: the ability of wider staff or volunteers to use strong passwords, detect malware or identify fraudulent emails. This suggests that charities have a more challenging job when it comes to getting their staff to follow good practice with cyber security.

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

Figure 4.12: Perceived understanding of cyber security among wider non-specialist staff

Q. How confident, if at all, would you feel in your organisation's core staff or volunteers or council members as a whole being able to do each of the following?



Bases: 1,030 businesses; 470 charities; 127 public sector organisations

Cyber security training is associated with good practice by wider staff. Figure 4.13 shows the difference between businesses that have carried out any kind of cyber security training with non-specialist staff, and those that have not.

Figure 4.13: Perceived understanding of cyber security among wider non-specialist staff, in businesses that have carried out cyber security training with these staff

Q. How confident, if at all, would you feel in your organisation's core staff or volunteers or council members as a whole being able to do each of the following?

Bases: 193 businesses that have carried out training; 837 that have not

Once again, across all the aspects of good practice noted in Figure 4.12, results are typically more positive for the information and communications sectors, and finance or insurance sectors. These are the two sectors that frequently emerge in the survey as having fewer cyber security skills gaps. This again mirrors findings from DCMS's Cyber Security Breaches Surveys, which also show these sectors to be among the most engaged when it comes to cyber security. For both sector groups, this possibly reflects the relatively high digitisation of these sectors, and the associated high cyber risk. With finance and insurance, the Cyber Security Breaches Surveys have also highlighted the strong focus on regulation and compliance in this sector, which increases the focus on cyber security.

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

5 Recruitment

This chapter covers the kinds of organisations that have looked for staff to fill cyber security roles in recent years. We also look at the different approaches to recruitment, and the kinds of candidates that organisations are looking for. The chapter also covers diversity, and how this factors into recruitment approaches.

The quantitative survey included various questions looking at recruitment methods and the extent of hard-to-fill vacancies for these roles. However, the sample sizes for organisations that have attempted to recruit were too low to produce statistically valid responses. We instead address these issues with insights from the qualitative fieldwork, wherever possible.

Existing evidence

- A Recruitment and Employment Confederation (2017) survey found that 81% of UK recruitment agencies surveyed thought the demand for cyber security staff would increase in the next year.
- Reece and Stahl (2015) conducted qualitative research with individuals in cyber security roles. This found that UK employers are often less interested in degrees than in professional cyber security certifications when seeking out candidates for cyber security roles.
- Similarly, the CSIS (2016) survey of IT decision-makers (in the UK and elsewhere) found that technical degrees tend to be less valued than experience and professional certifications for cyber security roles.
- A feature article by Cobb (2018) notes that women are more likely than men to only apply for vacancies when they meet all the requirements. At the same time, hiring managers will typically describe vacant positions in terms of the ideal candidate, which may put women off applying.

5.1 Recruitment activity

The survey finds that, within the last three years, recruitment activity for cyber security roles across organisations has been very rare. Just two per cent of businesses tried to recruit anyone in this period. Similarly, three per cent of charities have attempted to do so. Public sector organisations are more likely to have done so (13%). These figures are similar regardless of whether the organisation outsources cyber security to an external provider, or attempts to manage it in-house.

Recruitment activity is higher than average among large businesses (31%, vs. 2% on average), and to a lesser extent among businesses in the education sector (11%). Outside of these variations, there is little difference by business sector or geographic region.

Recruitment is also somewhat higher among businesses where cyber security is a formal part of individuals' job descriptions. One in nine of these businesses (11%, vs. 2% on average) have attempted to recruit in the past three years.

Once again, it is important to consider these figures in context:

- They do not reflect recruitment activity specifically among cyber security firms (working on cyber security technology development, or supplying cyber security products or service). In the qualitative interviews, these providers noted that they are constantly recruiting, through a mix of graduate schemes, apprenticeships and other vacancies. One large provider noted that they have inductions for new joiners every week, reflecting that their organisation was growing and regularly had unfilled positions.

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

- Furthermore, many organisations opt to outsource their cyber security, which will be explored later in the report. As a result, it is likely they would have less of a requirement to recruit staff in-house if they were already accessing these skills from a provider.

- As we discuss in Chapter 3, not all organisations have a clear idea of their cyber skills needs. Therefore, the lack of recruitment activity also reflects this lack of understanding of needs, and of what cyber security roles entail.

Ultimately, the quantitative survey results show that recruitment into cyber security roles is largely restricted, at present, to the firms specifically in the cyber security industry, as well as large businesses and, to a lesser extent, the public sector. In other types of organisations, the prevailing approach seems to be to assign cyber security responsibilities to existing staff, be they IT staff or non-IT specialists.

5.2 Barriers to recruitment

Again, the qualitative interviews give several insights into why organisations outside of external cyber security providers often do not turn to recruitment to address their cyber security skills gaps. One overriding reason was that some of the organisations we interviewed were not aware of their skills needs. A compounding factor was when these organisations had generalist IT staff who were not specialists in cyber security. They felt that these staff would have picked up enough cyber security skills and knowledge on the job, removing the need to have specialists in cyber security roles.

"If my IT colleagues tell me that we are secure, then I've got to believe them because I don't know otherwise."
Large business

Many were recruiting for broader IT roles, and expected these staff to have knowledge of cyber security. In these cases, recruiting more generalist IT staff seemed like better value, as organisations saw this as filling their cyber security skills needs as well as their broader IT needs.

Even where organisations recognised cyber security skills gaps, there were other practical barriers to recruiting cyber specialists. Some felt they did not have the budget to spend on a full-time staff member, or would not have enough work for them to justify the role. Some also felt they would not know how to put together a job description for such a role. Often, these organisations thought a better solution to filling their skills gaps was by outsourcing to an external provider.

"I feel that cyber is covered within the network team. It would be great to have another pair of hands to be solely on security, but budget will not allow that."
Public sector organisation

Challenges when recruiting for specialist high-skilled cyber security roles

The qualitative interviews highlight that recruiting staff with pre-existing specialist skills and experience in particular disciplines is very difficult. The larger organisations with more sophisticated cyber security set-ups, and the external cyber security providers we spoke to, both raised a number of challenges around this.

Firstly, many thought that with this labour market being relatively immature, there simply was not a large pool of individuals with both specific technical qualifications and experience. External cyber security providers had minimum experience requirements for these non-entry level roles, and some said that they typically found these individuals by poaching them from competitors – as there was no other route to access experienced people.

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

The small talent pool also meant that these individuals had high salary demands, which priced out medium organisations, as well as charities and public sector organisations, which all had salary constraints linked to their funding. One public sector organisation also noted that public sector pay bands were based on seniority rather than skillsets. This meant that they were forced to cap the salary of junior cyber security staff at the same level as junior IT staff, even though the former could command higher salaries elsewhere due to their premium skills.

Some organisations and external providers said that high salary demands were becoming a bigger issue as new employers entered the market. Alongside the traditional IT service providers that also offered cyber security services, they noted that there are now large established consultancies who have started to grow their cyber business. There are also lots of sole traders or small consultants offering services directly to organisations, and small organisations working with teams of freelance subcontractors. Both of these were seen to be taking skills out of the labour market.

"Given that a good member of my staff was recruited away for a big raise and less responsibility … I would say that any good cyber security people are being sucked up for a fairly astronomical price. The kind of price that we can offer is not attractive to people who are specialists."
Public sector organisation

Participants considered pay to be the main driver when trying to recruit high-skilled candidates with existing higher-level qualifications (such as Masters degrees). However, they also said that candidates valued the opportunity to get experience, further training and do a range of interesting work. Several of the external providers we spoke to went directly to universities to speak to undergraduates and graduates, to encourage them to apply to work in their organisations.

Public sector organisations, as well as one of the external cyber security providers that worked on public sector contracts, also raised the issue of security clearance. The external provider noted that there were sometimes good candidates from abroad, or with dual nationality, who could not get security clearance to work on Government contracts or subcontracts, meaning the business could not take them on. This was also an issue if they wanted to hire people with a criminal record or with a history of substance abuse, for example.

5.3 Approaches to recruitment

Where recruitment was taking place, the qualitative interviews show organisations using a range of recruitment methods to fill cyber security roles. Across those we spoke to, this included recruiting via recruitment agencies (who also helped with headhunting), posting vacancies on their own websites and on recruitment websites, adverts in sector-specific magazines, and recruiting via LinkedIn. Recruitment websites and recruitment agencies were not necessarily specialist IT or cyber security recruitment channels, even across the external cyber security providers. Several participants mentioned Indeed.co.uk. With recruitment agencies, organisations tended to go through the same agency they used for their entire business, as they had an existing relationship and good experiences with them.

As aforementioned, several participants noted that they had faced challenges trying to recruit high-skilled candidates from outside the organisation, due to the premium salaries these candidates commanded. Some had tried to overcome this by instead focusing on internal recruitment and reskilling. Where organisations were taking this approach, they felt internally-recruited individuals would be more likely to stay loyal to the organisation. They also felt that these individuals' existing institutional knowledge was an asset – they would have a better idea of the practical implications of cyber security for their own organisation, and be better at spreading good practice to wider staff, having come from a similar role. Some participants also felt that the intangible qualities needed for specialist cyber security roles, such as being able to investigate problems and issues, were easier to discover or develop internally.

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

Case study: getting the right people through internal recruitment

The head of the team dealing with cyber security in a Government regulator had previously attempted to recruit externally with mixed results. They had bad experiences recruiting people with intermediate IT skills – not specialist skills in cyber security disciplines, but things like IT Higher National Diplomas. They felt these individuals often brought bad habits with them, having trained on outdated programmes.

The team head changed their recruitment approach to look for people to transition internally, from a core staff (non-IT) role to being part of the cyber security team. They had recruited one person internally who was very experienced with Microsoft Office and writing macros, but had no IT background. Like others recruited to the team internally, they sent this person on an accredited external training course, and also gave them practical on-the-job experience writing in SQL, to learn the required skills for their new role. This person is now in charge of back-ups, data integrity, and quality assurance, working with end users from their old team.

At the same time, in cases where organisations had a more urgent need to fill cyber security skills gaps, and wanted someone in the role more quickly, they could not afford to have entry-level staff, and take the time to train them up. This was often the case when they did not have the technical skills themselves to be able to train new joiners. In these cases, technical skills and experience became one of the main factors in recruitment decisions.

"Certainly, a requirement of the job is a very good understanding of cyber security, networking, securing severs and anti-virus."
Medium business

Again, this raised challenges in some organisations around being priced out of the labour market. They discussed ideally wanting candidates with both good technical and non-technical skills, but there was a sense that this combination was rare – lots of technically-competent people in the labour market lacked good soft skills around client-management – and therefore these kinds of candidates were more commonly snapped up by the largest employers who could afford to pay a premium salary.

"Ideally, we would be looking for someone with good technical skills such as knowledge of software systems, but they would need to have very good communication skills because of the wide diversity of people that work with us. But we know to get that package could be difficult."
Medium business

Generalists vs. specialists

There were mixed thoughts in the qualitative interviews about whether it was better to recruit generalist IT staff or specialist staff to fill cyber security roles. We discuss earlier in this chapter that specialist high-level cyber security skills tended to command a premium salary, so many organisations had no choice but to recruit generalist IT staff to fill these roles. As many organisations had small teams working on cyber security, they also needed individuals to carry out a diverse range of tasks, so did not necessarily want a specialist, with skills in one area, in these jobs.

"Do I go out and recruit someone with cyber security skills now? No, we rely more on generalists. We have a small team and we kind of need everyone to do everything pretty well."
Public sector organisation

On the other hand, one organisation spoke about the risks of recruiting generalist IT staff in cyber security roles, based on their previous bad experiences of this. In particular, they were cautious about recruiting candidates with general computer

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

science degrees or Higher National Diplomas, compared to recruiting candidates without an existing IT background. They felt these mid-tier candidates sat above entry-level candidates in the labour market, but below those with specialist skills or high-level qualifications (such as Masters degrees). As such, in their opinion, these recruits tended to join in order to get accredited high-level training, and then left the organisation as soon as they were accredited. They also thought these candidates tended to have picked up bad habits from their previous jobs, having worked with outdated programmes.

Formal qualifications vs. experience

Views on the value of formal qualifications in cyber security were also mixed. As might be expected, those that covered cyber security formally, and wanted to employ cyber security professionals, placed greater emphasis on formal qualifications – some demanded qualifications as part of their essential recruitment criteria. However, there was no single gold-standard qualification, or even an accepted industry-wide minimum qualification, that emerged across interviews. In fact, outside of the external cyber security provider interviews, there was not a great deal of awareness of any cyber-specific qualifications.

There was also a common feeling that specialist qualifications in this industry could tie candidates down to specific fields, or even sometimes make them less employable. Organisations were often sceptical about the practical value of accredited cyber security courses currently available (the ones which resulted in a qualification or certification), and how well these matched their own business needs. This was often why they put more emphasis on recruiting entry-level candidates without cyber security industry qualifications and, where they had the time, budget and capabilities to do so, training them on the job or by sending them on accredited courses while working.

"We find that people with certain qualifications tend to attach a certain price tag to that qualification, whereas we feel we can develop practical skills better here, for less money."
External cyber security provider

"I actively avoid people who chase accreditations, because they tend to be people that just chase them for the sake of it."
External cyber security provider

Many thought that qualifications alone were not enough, and ideally wanted candidates with experience in the role. Experience helped to demonstrate some of the intangible qualities and soft skills they thought were important, such as communication skills, client-handling and the ability to work collaboratively.

"I'd like to think I'd got someone degree qualified and they'd been in a similar role for a couple of years. But perhaps the degree wouldn't be necessary if I could see that someone had been working at a recognisable company or a company a similar size to us."
Medium business

One external provider said they felt that the cyber security skills labour market was moving away from a focus on specific qualifications and focusing more on experience, as the labour market matured. This also reflected a common theme from the interviews, that candidates with formal qualifications but no experience were considered ill-equipped for the working environment. The finding reinforces the complexity of various fields in cyber security, and how it can often take many years of experience before organisations consider individuals to be truly capable in a specific field.

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

"There are not enough people coming out of university with usable skills … graduates are not ready for the level of work required. What they're doing at university does not translate well."
External cyber security provider

5.4 Diversity in cyber security

When we probed participants specifically on the issue of diversity, they typically acknowledged it was a problem in the industry. The gender issue is relatively well covered in existing literature with, for example, ISC2 (2018) estimating that women make up only 24 per cent of the global cyber security workforce. Our research finds that diversity issues are perhaps broader than just gender, and may include gender, ethnicity and neurodiversity (which was specifically mentioned, and refers to those with neurological conditions, such as Asperger's).

Some external cyber security providers – the high-volume employers in this labour market – had adopted a small number of initiatives to improve diversity within their organisation. Examples included senior management-level diversity training, and changing job descriptions to only include essential requirements rather than desirable ones. The latter changes were both to encourage people with Asperger's to apply, as they were felt to take job descriptions more literally, and to encourage more female candidates to reply. This reflects our literature review findings around female candidates potentially being more likely than men to be put off applications if they did not fit all the desirable criteria (Cobb, 2018).

However, all the organisations we spoke to felt that they alone could not make much impact on the diversity problem. Some noted that gender diversity in particular was a supply-side issue that could only be resolved in education institutions. Some of the large external cyber security providers said that they only recruited from specific prestigious universities, and that the candidates from these institutions were largely white males. While we were not able to explore this further in a limited number of external provider interviews, this feedback suggests that these organisations could further their own workforce diversity by reaching out to a wider range of universities.

"In five years of working here, we've had 200 applicants across two cyber security roles and only one of those applicants has been female. That really is an issue of supply … In one of the colleges we recruit from, the course had 82 people on it, and just one of them was female."
High-income charity

For some, they had too urgent a need to fill cyber security roles, so did not feel they had the time to be able to consider diversity, over and above simply filling vacancies.

"The pool of people we can recruit from is quite shallow, so while I would honestly like a diverse staff here … we can't be that patient, or put in the time and money to seek them out."
Public sector organisation

Finally, as previously noted, security clearance requirements sometimes prevented external providers from taking on non-UK nationals, which potentially inhibited the ethnic diversity of their workforce.

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

6 Training and upskilling

This chapter explores cyber security training, both for the people who work directly in cyber security roles, and for wider staff who are not specialists in the area. It covers the process of seeking out training materials, the kinds of training delivered, and the perceived effectiveness of training.

Existing evidence

- Reece and Stahl (2015) note that there is no universally-accepted formalised training framework for cyber security. Cyber security professionals have typically joined the industry mid-career, and often lack formally-taught accreditations
- The Information Assurance Advisory Council (2017) find that in the UK, training has previously been ill-defined, and lacking a unified, coherent narrative about how to enter the cyber security industry.
- A Silensec (2017) white paper argues that that is a lack of investment in training from organisations, due to the cost and disruption caused by taking employees away from their day-to-day roles.

6.1 Which organisations are looking into cyber security training?

Formally analysing training needs

Just over one in ten businesses (14%) and one in five charities (20%) have undertaken a formal analysis of their cyber security training needs in the last 12 months. Public sector organisations are more likely to have done so with around one-third (34%) saying they have.

Medium (39%, vs. 14% on average) and large businesses (48%) are more likely than others to have assessed their cyber security training needs, as are middle-income charities (32%, vs. 20% on average) and high-income charities (39%). Differences by size may not simply be about willingness and engagement in this instance, but also about capability – larger organisations are more likely to have the capabilities among HR or cyber security staff to carry out training needs assessments.

Businesses in the finance or insurance sectors are more likely than others to have conducted this formal analysis (43%), as are educational organisations (25%).

How many organisations have actively sought out training?

As Figure 6.1 shows, a minority of organisations have sought out cyber security training materials over the past year (regardless of whether or not they have analysed training needs). This is both training for specialists, working in cyber security roles, and training for wider non-specialist staff. For both sets of staff, public sector organisations are much more likely to seek out relevant training than businesses or charities.

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

Figure 6.1: Whether sought out cyber security training in the last 12 months

Q. In the last 12 months, has anyone in your organisation sought out any formal cyber security training materials or courses for …

Bases: 1,030 businesses; 470 charities; 127 public sector organisations

Large businesses are more likely than others to have sought out training, both for cyber security specialists (52%, vs. 11% on average) and non-specialist staff (30%, vs. 4% on average). The same is true for medium business, to a lesser degree (32% have sought training for those in cyber security roles and 13% have done so for wider staff). Similarly, high-income charities are more likely to have sought training specifically for people in cyber security roles (45%, vs. 23% on average).

Once again the finance or insurance sectors and education sector stand out. In the finance or insurance sectors, 22 per cent have sought training for cyber security employees (vs. 11% on average), and 16 per cent have done so for wider staff (vs. 4% on average). Educational organisations are also more likely than others to have sought training specifically for those in cyber security roles (23%).

Businesses that have staff with cyber security formally written into their job descriptions are more likely than average to have sought out cyber security training for these staff (27% have done so, vs. 11% of all businesses).

There are no statistically significant differences across geographic regions.

Impact of GDPR

The qualitative interviews suggest that, with the introduction of GDPR, a new range of training courses and products related to GDPR awareness and implementation now exists. When asked about seeking out cyber security training in these interviews, several participants discussed their GDPR-related training, suggesting that they saw the two topics of GDPR and cyber security as interlinked. In fact, GDPR currently seemed to be a more significant strategic priority for some of the participating organisations than cyber security on its own terms.

Some organisations that had not sought out or undertaken any specific cyber security-focused training mentioned that they had nonetheless sent staff on GDPR training, and that some of the content of this training included cyber security. This included several mentions of the GDPR information and guidance materials available on the Information Commissioner's Office (ICO) website. This suggests that there may been an opportunity for organisations to extend basic cyber hygiene by placing more of this type of content within wider GDPR training. Again, these findings must be couched in the timing of this research, which took place a few months after the implementation of GDPR.

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

"GDPR is the law and we had to take notice. We couldn't just say, we're protected because we've got anti-virus."

Medium business

6.2 Barriers to finding cyber security training

The quantitative survey asks organisations that sought out cyber security training whether they faced any barriers when looking for training. The barriers included in the survey are each given a score from 0 to 10. Here, 10 means that this barrier completely stopped an organisation from finding training and 0 means it was not a barrier at all.

Figure 6.2 shows the results for training sought out for those in cyber security roles. Among businesses, the cost of training is rated as the most common barrier for finding training for this group. Charities and public sector organisations instead rate the lack of tailored training as the biggest barrier. For all types of organisations, these two barriers are more substantive than the others asked about, including time taken to find training, or the format of training. It is worth noting that, on the whole, none of these barriers appears particularly problematic, with an average score of under 5 for each one.

Figure 6.2: Barriers to finding training for those in cyber security roles

Bases: 225 businesses; 133 charities; 51 public sector organisations

Figure 6.3 shows the perceived barriers when seeking cyber security training for wider staff. There are too few charities that have sought training for wider staff for statistically meaningful analysis at this question.

Here, for businesses and public sector organisations, the lack of tailored training is, relative to other barriers, a bigger issue. Once again, the average score for all barriers is under 5, suggesting there is no standout barrier to seeking training across these organisations.

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

Figure 6.3: Barriers to finding training for non-specialist staff

Q. How much, if at all, did each of the following hinder your organisation's attempt to find training that met the needs of other staff, volunteers or council members?

Bases: 110 businesses; 47 public sector organisations
Too few charities to analyse as a separate group (under 30 effective sample size).

Qualitative insights on barriers to training and poaching of trained staff

In the qualitative interviews, other broad reasons emerged for not seeking out cyber security training, both for specialists and non-specialist staff. Ultimately, organisations only sought and took up training if they felt it the benefits of the training would outweigh the costs, and some were unclear on the benefits. Firstly, some of those working informally on cyber security thought they could fulfil their short term needs by teaching themselves, using online tutorials or forums, as and when specific needs arose. Secondly, some of these staff felt that cyber security was simply an awareness and common-sense issue, and did not see the value added through formal training – which reflects the findings from the latest (2018) Cyber Security Breaches Survey as well. Finally, some saw cyber security as an emerging but not immediate issue that needed tackling, so saw training as a low priority.

We also explored concerns around specialist staff leaving the organisation after receiving training. This appeared to be more of a concern in public sector organisations and in the external cyber security providers we interviewed. This partly reflects the fact that these two types of organisations were the most likely to offer specialist, accredited training to their cyber security staff. It also reflects specific concerns in public sector organisations that they could not compete with the pay offered in the private sector for those with high-level technical cyber security skills.

In external cyber security provider interviews, this was typically treated as an industry-wide problem, and not one that stopped them from providing training. However, some of these providers did note that competition for their staff extended beyond the industry, as they also had competition from large banks and other financial technology (FinTech) businesses poaching trained cyber security staff.

"In the public sector, we do not pay as much as the private sector, so we might lose [specialist staff]. There is a risk that you are paying for these courses and they are going to jump ship."
Public sector organisation

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

6.3 Training undertaken

As Figure 6.4 shows, in around one in four businesses (23%) and one-third of charities (33%), staff in cyber security roles have undergone cyber security training in the past year. Those in public sector organisations are again more likely to have done so (51%). All types of organisations are, by comparison, less likely to have invested in such training for wider staff.

Figure 6.4: Whether undertaken cyber security training in the last 12 months

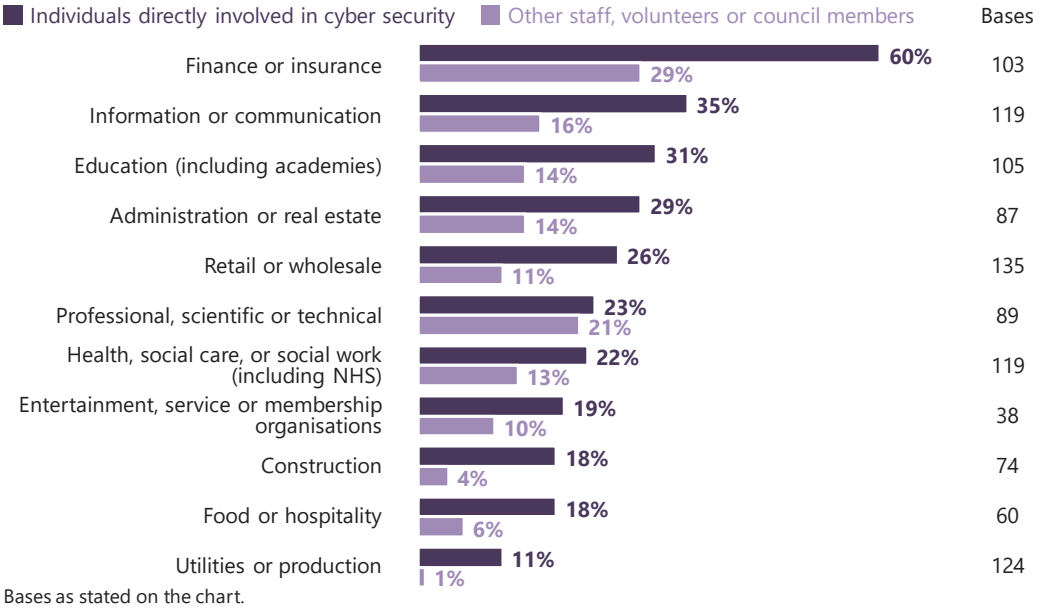
Q. Regardless of whether you sought out training or not, did … undertake cyber security training in any of the following ways in the last 12 months?

Bases: 1,030 businesses; 470 charities; 127 public sector organisations

Figure 6.5 shows that there is wide variation in training activity across sectors. Businesses in the financial or insurance sectors are more likely to have undertaken training compared to other sectors (60% for staff in cyber security roles and 29% for wider, non-specialist staff). Training of wider staff is particularly uncommon in the construction, food or hospitality, and utilities or production sectors.

Figure 6.5: Whether undertaken training for cyber security staff by sector

Q. Regardless of whether you sought out training did this group undertake training related to cyber security in the last 12 months?



Bases as stated on the chart.
Too few transport or storage firms to analyse as a separate subgroup.

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

Format of training

As Figure 6.6 shows, businesses and public sector organisations most commonly use webinars as the format for delivering cyber security training for those working in cyber security roles. By contrast, for charities, there is a more even split in the format, between webinars, face-to-face training or attending conferences.

When it comes to wider staff, there is a much greater focus across all organisations on face-to-face training. Webinars are still a common format, especially for businesses

Large businesses are more likely than average to deliver training to those in cyber security roles via webinars (accounting for 81% of large business that undertook such training, vs. 60% across all businesses).

Figure 6.6: Format of training undertaken

Bases (all among those who have undertaken cyber security training for cyber security staff/wider staff): 378/193 businesses; 203/102 charities; 67/50 public sector organisations

Qualitative evidence on the types of training undertaken and products used

In the qualitative interviews, we asked participants about the types of cyber security training products they had used. Responses were very varied, highlighting that there is no single training product considered to be the baseline or gold standard for cyber security. The methods used for training cyber security specialists varied from online webinars and YouTube videos covering specific software, through to mentions of a handful of accredited courses, such as ISO 27001 Certified ISMS courses or Certified Information Systems Security Professional (CISSP) courses.

Among the external cyber security providers interviewed, there was a mix of both internal training, designed and delivered within the organisation, and external training. The external training was typically purchased in order for staff to gain external accreditations. All these organisations also took on cyber apprentices, and expected junior staff to pick up cyber security skills on the job from more senior staff.

Nevertheless, these external providers considered off-the-job internal training to be very important – they felt it was more cost-effective to retrain existing staff with new cyber security skills to ensure they adapted to changing needs, software and technologies, rather than to recruit new staff to fill emerging skills gaps. Some of these organisations also offered

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

these internally-developed training courses to other organisations, as one of their product lines, giving them an additional incentive to develop bespoke training. One external provider mentioned that they had around 30 bespoke internal training courses for cyber security specialists, while another had an academy style system where staff could book their own training modules to reskill themselves if their existing skills and product knowledge had gone out of date.

For wider staff, training was typically more about general awareness raising. As aforementioned in this chapter, participants also commonly discussed GDPR training in the context of cyber security training for wider staff, and there were a range of external GDPR courses and webinars that they had used, both from the ICO and other external providers or consultants. For example, one small business mentioned free GDPR training offered by the Law Society, their trade body, which covered awareness of basic cyber hygiene, on topics like malware.

Having the skills and capacity to deliver cyber security training was a key challenge, and often organisations felt unable to do this. Participants considered external webinars to be a particularly cost-effective way of getting around this challenge. Across several interviews, participants also discussed one-off training sessions being delivered by their external cyber security or IT providers.

"We haven't accessed much in the way of formal training. We tend to do it off our own back, but we use online training courses from external providers."
Medium business

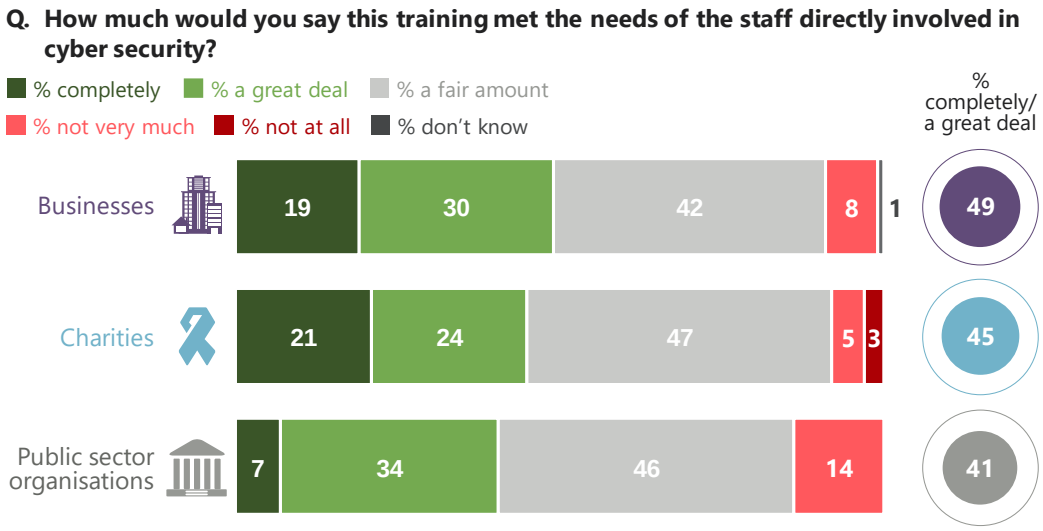
In very large organisations, as well as in the public sector, cyber security training for wider staff was often arranged centrally, either through a parent company or another public body. This meant that the organisations receiving the training sometimes had little control over content. One public sector organisation said that this kind of training was particularly susceptible to becoming out of date. Their current all-staff webinar training – which staff had to do every year – had no mention of ransomware, despite this becoming a growing issue for all staff to be aware of. This participant was also worried about the impact of this kind of training being low, because staff would expect it to be the same each year.

Extent to which training meets needs

Views are mixed on the extent to which cyber security training meets the needs of these employees. Figure 6.7 illustrates the picture for training delivered to staff in cyber roles. Among those accessing this training, half of all businesses (49%) feel that the training met their needs either completely or a great deal. However, only one in five (19%) say it met their needs completely. A similar pattern is evident among charities (45% either completely or a great deal, and 21% completely). Only seven per cent in public sector organisations feel that such training met their needs completely – less than in businesses and charities.

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

Figure 6.7: Effectiveness of training for those in cyber security roles

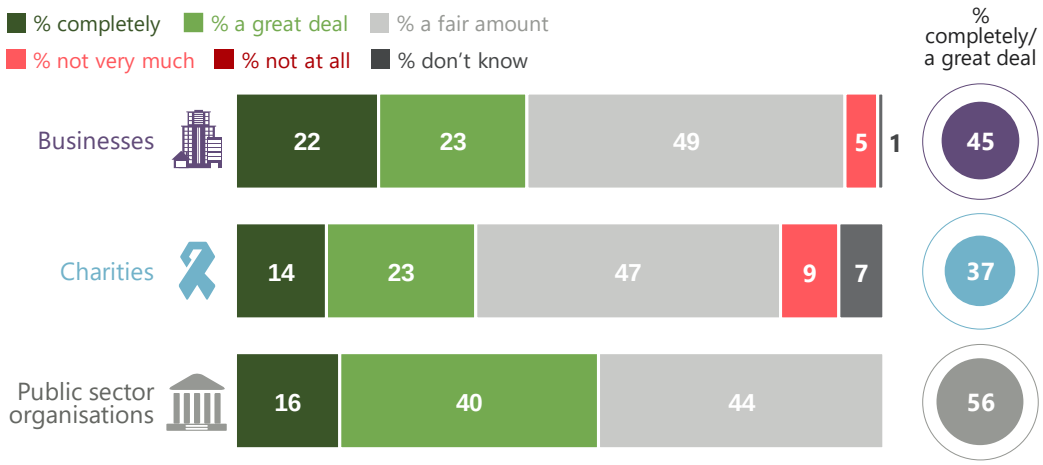


Bases (among organisations that provided training for staff in cyber security roles): 378 businesses; 203 charities; 67 public sector organisations

As Figure 6.8 shows, fewer than half of all the businesses offering cyber security training to wider staff (45%) feel that this training meets their needs, either completely or a great deal. Again, only around one in five (22%) say it met their needs completely. Among charities, views are somewhat less positive (37% of charities say it met their needs either completely or a great deal, and 14% say completely).

By contrast, for the public sector, the picture is more positive on this indicator (56% of public sector organisations say this training met their needs completely or a great deal). This suggests that public sector organisations perceive their own weakness to be more on the training of specialists than on non-specialists when it comes to cyber security.

Figure 6.8: Effectiveness of training for employees not involved in cyber security



Bases (among organisations that provided training for wider staff): 193 businesses; 102 charities; 50 public sector organisations

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

7 Outsourcing cyber security

This chapter looks at the organisations that outsource any aspects of their cyber security – what they outsource, and their reasons for doing so. We also explore the dealings that organisations have with their external cyber security providers who run cyber security services for others, or cover it as part of their IT management service for others). This includes whether they feel they have the necessary skills to work with them and assess their performance, and what makes for a good working relationship with providers.

Existing evidence

- Cisco offers cyber security services to other organisations. In a 2015 white paper on the global cyber security skills gap, they suggest that outsourcing can help organisations alleviate their internal cyber security skills gaps.
- The CSIS (2016) survey of IT decision-makers (in the UK and elsewhere) found large businesses saying they would respond to in-house cyber security skills gaps by expanding their outsourcing of cyber security. The surveyed firms suggested that it was most straightforward to outsource automated processes such as threat detection.

7.1 What aspects of cyber security do organisations outsource?

Three in ten businesses (30%) and a similar proportion of charities (27%) outsource one or more aspects of their cyber security. Public sector organisations are more likely to outsource, with two-thirds (65%) doing so.

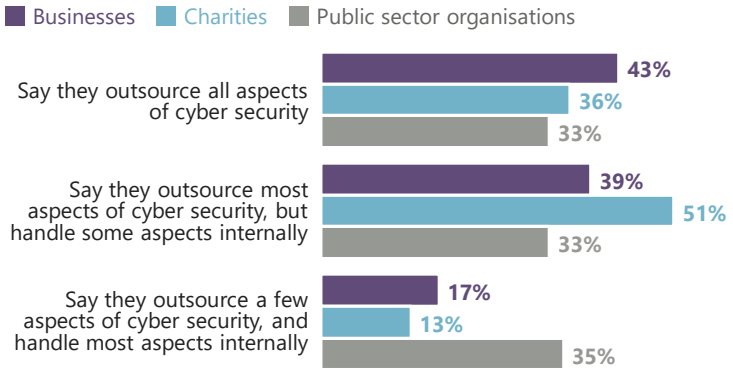
Medium businesses (58%, vs. 30% on average) and large businesses (59%) are more likely than others to outsource. Similarly, high-income charities are also more likely than others to outsource (64%, vs. 27% overall).

Outsourcing is more prevalent among businesses in the finance or insurance industries (49%, vs. 30% on average) and administration or real estate sectors (48%). On the other, food or hospitality businesses are less likely than average to outsource (19%), as are those working in information or communication (23%). The information and communication sector grouping includes IT consultancy, maintenance and other IT services, so it might be expected that more of these kinds of firms would keep cyber security roles in-house.

Figure 7.1 shows that, among organisations that outsource cyber security, most still handle at least some aspects in-house. And while public sector organisations are more likely to outsource some cyber security activities overall, the scope of what they outsource is often narrower, with more aspects typically handled in-house than in businesses and charities.

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

Figure 7.1: Extent to which organisations outsource cyber security



Bases (among organisations that outsource): 427 businesses; 187 charities; 78 public sector organisations

Outsourcing of specific functions

Figure 7.2 shows the specific functions that different organisations outsource. Across all organisations, two of the most commonly outsourced aspects of cyber security are incident response and firewall set-up. Public sector organisations and charities are also highly likely to outsource high-level functions, more so than businesses.[15] Businesses are more likely than other organisations to ask external providers to detect and remove malware.

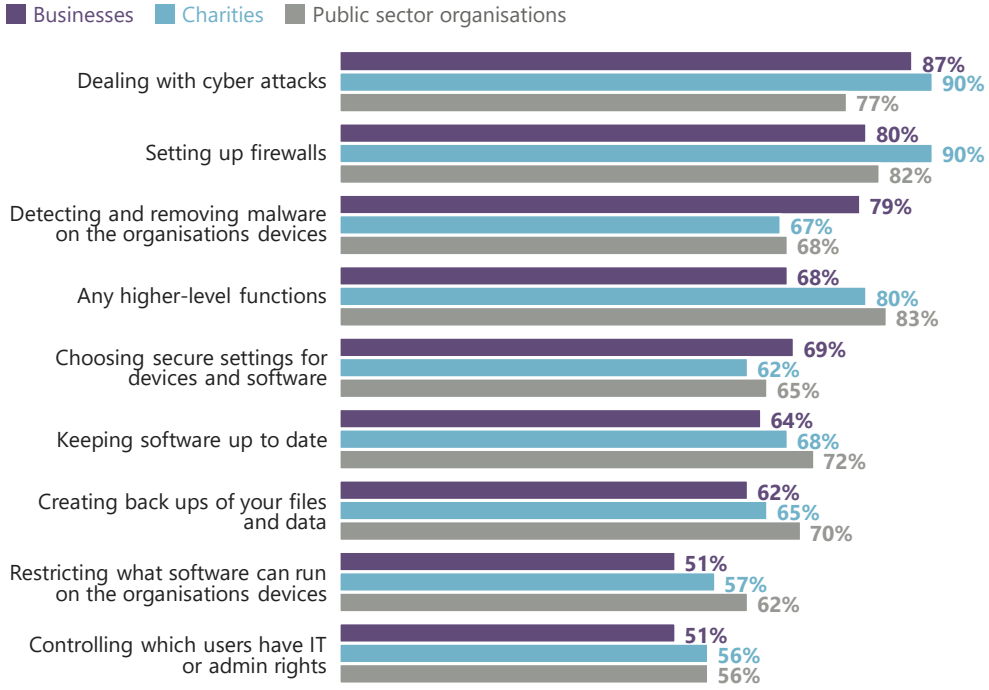
Large businesses are more likely than others to outsource high-level functions than average (83%, vs. 68% on average). However, they are less likely than other businesses to outsource incident response (65%, vs. 87% overall).

[15] The specific examples of high-level functions we gave in the survey included: security engineering, penetration testing, using threat intelligence tools, forensic analysis, interpreting malicious code, and using tools to monitor user activity. These match the high-level skills areas we covered in Chapter 2.

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

Figure 7.2: Specific cyber security functions that organisations outsource

Q. Which of the following aspects of your cyber security are covered by your outsourced provider or providers?

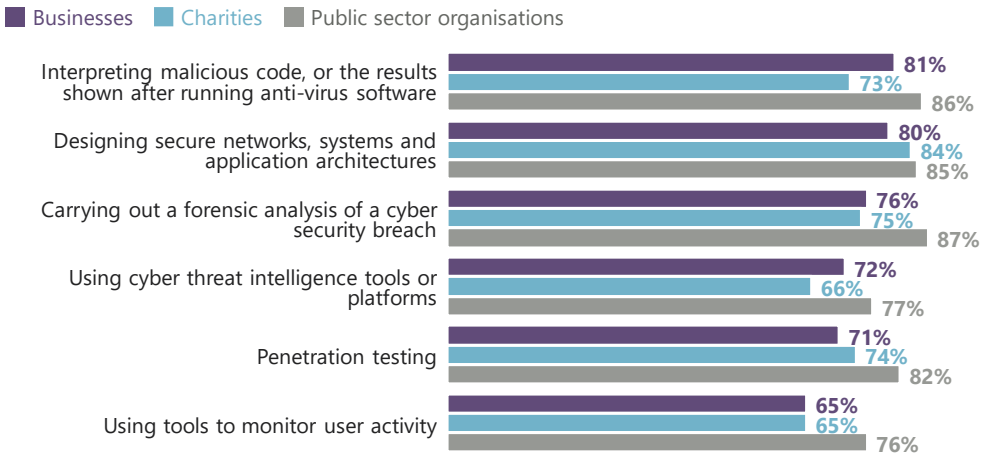


Bases (among organisations that outsource): 427 businesses; 187 charities; 78 public sector organisations

Figure 7.3 breaks down the specific high-level functions outsourced, among those that do outsource these kinds of activities. This shows that the most common high-level needs among businesses and public sector organisations that outsource are around interpreting malicious code, security architecture and forensic analysis. Security architecture also rates top among charities that outsource high-level functions.

Figure 7.3: Breakdown of the high-level cyber security functions that organisations outsource

Q. Which of the following specific higher-level functions are covered by your outsourced provider or providers?



Bases (among organisations that outsource high-level functions): 325 businesses; 150 charities; 65 public sector organisations

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

7.2 Reasons behind outsourcing decisions

The primary reasons for outsourcing are related to filling cyber security skills gaps, rather than cost or efficiency savings. Among those that outsource, over four in ten businesses say, unprompted, that they do so to access greater expertise (46%), and a similar proportion say they do because their internal staff do not have the necessary skills or knowledge (41%). These are the top two reasons charities give as well (42% give each of these as a reason).

Public sector organisations are less likely than others to cite access to greater expertise as a reason (27% do so), although it is still one of the top reasons mentioned. Compared with businesses, public sector organisations are more likely to mention the arrangement being part of a wider IT contract (13%, vs. 6% of businesses) and compliance reasons (8%, vs. 2% of businesses). It is important to note that this is still a relatively small proportion of all public sector organisations.

With that said, it is evident from the qualitative interviews that cost is also a fundamental factor in decisions to outsource – not to make efficiency savings, but because the cost of filling the cyber security skills gap in-house is often too high. Several organisations explained that it would cost too much to recruit additional staff to deal with cyber security (as covered in Chapter 5). Smaller organisations in particular felt that their low-level cyber security requirements did not justify recruiting someone for a full-time role, as they believed there would not be enough work for them.

"Outsourcing suited us from a budgetary point-of-view, as we didn't need a full-time person to look after everything."
Medium business

Some outsourcing arrangements had come about after organisations started using new digital tools or platforms, so had new cyber security requirements. Others wanted to enhance their existing cyber security with a view to getting an accreditation. For example, one high-income housing and mental health charity migrated their data to a cloud service and then decided to let the cloud service provider manage their cyber security. Another high-income youth charity had an information audit, which ended up recommending that they hire an IT provider. And one large business wanted to achieve ISO 27001 information security accreditation, so brought in an external cyber security provider to help with this.

7.3 Choosing providers

The qualitative interviews suggest there is a wide range of ways that organisations go about choosing providers. Public sector organisations, large businesses and large charities typically had a more systematic process than smaller organisations. They discussed inviting several providers to tender for the contract and formally assessing their bids. At the other end, especially in organisations where those in cyber security roles were not experts, or thought cyber security was not a priority, the decision came down almost exclusively to cost, as they had no other way of measuring value for money.

"It was really price more than anything. They were a lot cheaper than the others."
High-income charity

Plenty of micro or small businesses relied on very informal networks to help them find a provider without investing much time or money in the search. Some individuals in cyber security roles had business contacts, or even friends and family, working in IT roles that they drew upon. Some relied on peer networks – for example, one care home manager who took charge of cyber security in their organisation said they were aware of several care homes using the same provider because of good word-of-mouth. In our interviews with external cyber security providers, they themselves reaffirmed that word-of-mouth through informal networks was a key way for them to win new business.

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

Case study: choosing an external cyber security provider systematically

An information security manager in a large retail business had developed a points-based questionnaire to help the business choose between external cyber security providers in a systematic way. The questionnaire covered aspects such as: the robustness and quality of the provider's systems, their reputation, and their ability to communicate the value of their service. Once they gave a score to a wide range of providers, the business managed to narrow down the selection to five candidates that met these minimum requirements. After this, cost became their deciding factor.

The manager felt that it made the firm's decision-making process more transparent for the senior management team. It meant that they could have a suitable trade-off between cost and quality.

Reasons for switching and selecting a new provider

Other than cost, good or poor communication from external cyber security providers was an important theme in qualitative interviews. There were instances where participant organisations were in the process of ending their contract with their existing provider and switching to a new one because of poor communication and account management from existing provider. For example, there were instances of account managers going on maternity or annual leave, this not being communicated to the organisation and no replacement being put in place.

These soft aspects of service were ranked very highly. However, it is once again important to note that this could reflect a lack of technical knowledge on the part of the organisation choosing a provider. This might explain why they focused more on the soft aspects of service delivery rather than the technical aspects. At the same time, this theme emerged across larger businesses and charities, and not simply among smaller organisations (where low technical knowledge might be more expected).

7.4 Dealing with external cyber security providers

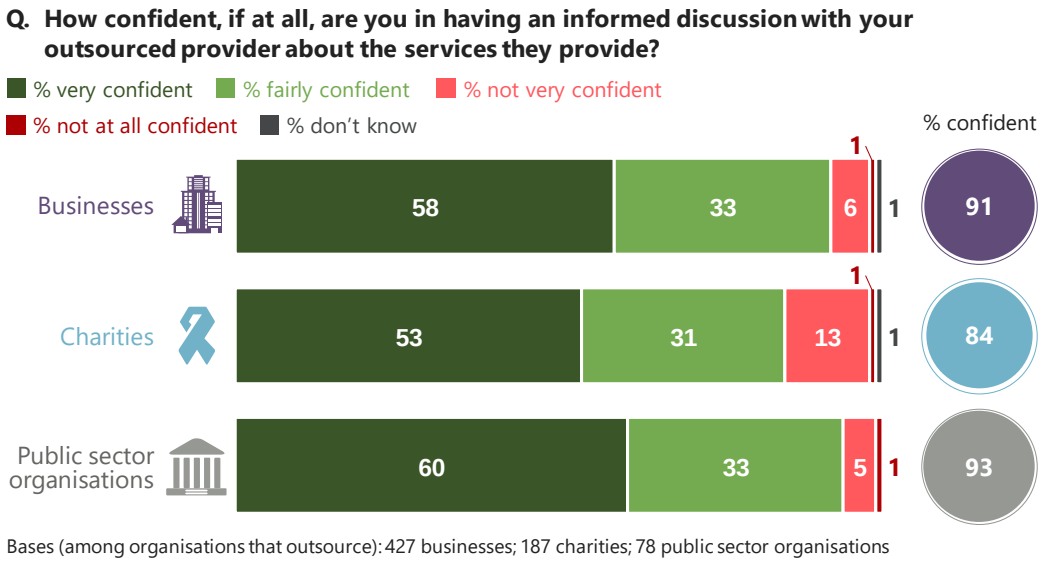
Confidence in dealing with providers

The vast majority of those in cyber security roles in businesses, charities and the public sector are confident in having an informed discussion with their external cyber security provider about the services they provide. Nine in ten businesses (91%) and public sector organisations (93%), and just over eight in ten charities (84%) are either very or fairly confident, as Figure 7.4 shows.

Medium and large businesses are more confident than average (97% for medium businesses, and 97% for large businesses, vs. 91% overall).

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

Figure 7.4: Confidence in dealing with external cyber security providers



Bases (among organisations that outsource): 427 businesses; 187 charities; 78 public sector organisations

The qualitative interviews suggest that, in cases where the individual in charge of cyber security within the organisation lacked expertise, they knew this prevented them from monitoring and scrutinising the performance of their external cyber security provider. They sometimes felt that they had no option but to trust their provider, and defer to their judgement.

Case study: the need for in-house expertise to deal with external providers

One participant from a charity care home suggested it would be helpful to have an in-house expert that they could call on to help them manage the relationship with their external IT provider, which also covered their cyber security. They had back-of-mind concerns about the impartiality of their IT service provider. They also thought the provider's communication could improve, as it had led to some general IT mishaps in the past, with the provider then charging them again for the second callout.

However, the participant thought it was not realistic to employ someone themselves, due to lack of funds and the irregular nature of the work. They thought a solution might be to have an expert working across a consortium of care homes that could be called on as-and-when needed, for example to accompany the participant to meetings with their external cyber security provider.

Relationships with external cyber security providers

The qualitative interviews highlight that large businesses and public sector organisations typically had a more structured approach than others when working with their external cyber security provider. This involved regular meetings and calls, and a reporting schedule. They assessed performance through specific criteria, such as the number of low-level viruses that impacted the organisation per year, or the results from penetration testing.

"I asses them on how many low-level viruses get through on a yearly basis, and if it has gone above a certain level then I would consider changing."
Public sector organisation

Smaller businesses and charities, and the participants that tended to have less technical expertise in cyber security, often approached the relationship more informally. Some would only ever talk to their provider after a cyber security breach or attack. They judged the provider's performance much more on intuition or on good communication, as aforementioned.

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

There was also a sense from these participants that, if they had not heard about any problems or issues from the provider, they were perceived to be doing a good-enough job.

Case study: an informal relationship with the external provider

A small insurance company that sold cyber insurance (as well as other types of business insurance) had a fairly substantial outsourcing requirement. Their provider was a two-person operation. For many years one of the directors had been based at the insurance business's office for regular face-to-face contact. In fact, both directors had previously been employed by the insurance company before choosing to set up their own business, so the working relationship between the two companies was very informal.

The company had a high level of trust in the external provider, based on this informal relationship. The meant that their performance was not formally assessed. Communications about cyber security were ad hoc, usually as face-to-face catch-ups in the office.

Once again, a common theme across all organisations, large and small, was the importance of good communication and approachability (which, of course, is complementary to the more fundamental need for relevant technical expertise). The qualitative interviews show a mixed picture of how providers are seen to be doing on communication. Some participants felt that, while their provider was very technically proficient, they were much less satisfied with their communication, account management and reporting skills. Nevertheless, these concerns were generally not a strong enough reason for breaking off an existing relationship with an external provider, aside from the exceptions covered earlier in this chapter.

"They lack awareness of critical business systems and have poor communication levels with us. I don't feel that they understand the urgency around some of the projects that they do for us."
Large business

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

8 Conclusions and recommendations

Cyber security skills must include technical skills, but are much broader than IT skills.

There is currently no agreed definition of a cyber security skill or of a cyber security professional. This has led to organisations having vastly differing expectations of people in cyber security roles, depending on how they have entered these roles and their pre-existing skills and knowledge around cyber security. Some organisations view these roles solely through the prism of IT, ignoring the other important technical and non-technical aspects. Others consider them as an offshoot of their GDPR obligations, and may not appreciate the need for specialist technical skills. We find that people working in cyber security roles need a range of skillsets to perform the role properly:

- Technical skills are essential for those working in cyber security roles. The level and nature of technical skills required will differ across organisations. Many organisations require advanced specialist skills beyond what their generalist IT staff can provide – the CyBOK framework (Rashid et al., 2017) lays out the breadth and depth of these specialist areas in detail. A first step is for organisations to understand their technical skills needs. Right now, many organisations are unaware of their technical skills gaps, particularly around incident response, often because senior managers have a poor understanding of the technical requirements for the role.

- Beyond technical skills, organisations also need someone to strategically plan and manage their approach to cyber security. This person needs to understand the technological trends and developments in cyber security, the specific cyber risks and compliance issues facing the organisation they serve, and they need to appreciate how cyber security measures can affect business performance. They need to be able to develop appropriate policies and rules for everyone in the organisation to follow.

- People in cyber security roles also need the right soft skills to effectively deploy their technical skills. Particularly important are good communication and client handling abilities, which were recurring themes across our research. This is an area where the labour market generally needs to improve. Our qualitative research finds that it is a particular frustration for those seeking out candidates with specialist IT skills when they lack these sorts of soft skills.

Our proposed definition of cyber security skills covers all these elements. Defining cyber security skills will help organisations to better understand the breadth of skills they need, either in-house or through external cyber security providers (who run cyber security services for others, or cover it as part of their IT management service for others), to make themselves cyber secure. It will potentially help those who want to work in the industry to better understand what skills and knowledge they need to build, beyond specialist IT skills. It can also help in any further research revisiting the cyber security skills gap, to ensure that it is measured in a comprehensive way.

Recommendation 1: The Government should consider adopting our proposed definition of cyber security skills (as drafted in Chapter 2), if considered useful by the industry at large.

There is no clear framework for people looking to become cyber security professionals.

People enter cyber security roles in multiple ways, often evolving from IT roles to cover cyber security, or coming to the role from an entirely unrelated area. These roles are currently not well-outlined, with job titles and job descriptions typically not reflecting the work these individuals do to support cyber security. Even those working for external cyber security providers work across a range of disciplines and service lines, some with a more technical focus than others.

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

Organisations also lack awareness of the qualifications and accreditations available for cyber security professionals. There is no clear baseline standard or gold-standard qualification. At the same time, generalist IT qualifications are also insufficient. This is both because cyber security skills are broader than IT skills, and also because some specialist cyber security roles are highly technical, and cannot be covered by generalists.

We acknowledge that, as there are a variety of specialist cyber security roles requiring different knowledge and different technical skills, no single qualification will be a perfect fit for every type of role. However, IT professionals moving into cyber security roles in their organisations need a to be able to follow a defined career pathway or framework to give them a clearer understanding of how to obtain the right skills for their new role. This framework ideally needs to cover the two tiers of technical cyber security skills. This might take inspiration from the existing NICE framework from the US (Newhouse et al., 2017), the CyBOK Knowledge Areas, and the Institute of Information Security Professionals (IISP) skills framework.

Recommendation 2: The Government should work with external cyber security providers to create an outline of cyber security skills career pathways and the kinds of skill and qualifications that might be required for each role, and at different levels.

Recommendation 3: The Government should continue its work to support and develop the Cyber Certified Professional Scheme, to further professionalise this industry.[16]

There is a large informal sector attempting to cover cyber security, often without support.

Overwhelmingly, cyber security roles within organisations – outside of external cyber security providers – are not badged as "cyber security" roles. In the private and charitable sectors, the vast majority of individuals working in these roles do so informally rather than professionally. These individuals are lacking basic cyber security skills, meaning they are not confident in carrying out the tasks that are necessary to get their organisation up to the basic Cyber Essentials standard. Moreover, the work they do carry out will often not be covered in their absence – across all businesses, six in ten of those working in the lead cyber security role feel their work would not be covered a great deal by others.

Setting to one side those that have more advanced technical skills needs, we estimate that around 710,000 businesses have a basic technical skills gap. As might be expected, this is more prevalent in micro and small businesses, and in small charities than in larger organisations. The areas that face the largest such gaps are in: setting up configured firewalls, storing or transferring personal data securely, and detecting and removing malware on their organisation's devices.

We know the NCSC already provides guidance on these relatively basic issues, with examples being the Small Business Guide[17] and advice on implementing the minimum technical controls from Cyber Essentials[18]. The NCSC is also developing a cyber security awareness guide for non-specialist staff, which will help to raise understanding of cyber threats, and how to stay safe online, and an Exercise in a Box tool, which will help all organisations to gage their baseline level of resilience when dealing with cyber attacks. Evidently, this existing guidance, and guidance under development, can be taken up by a much wider range of organisations to fill their basic skills gaps.

Some of these organisations will fill their skills gap by outsourcing their cyber security. Where this is not happening, these organisations are left exposed to cyber risks – and many will not feel they can afford to recruit new staff to manage their cyber security. There may be a way to better share skills across experts and non-experts, to help bridge these fundamental skills gaps. This could be through a mentoring or partnering scheme, where organisations could low-cost consultancy time from certified cyber security experts (either external organisations or freelancers). This might, for example, be useful for

[16] See https://www.ncsc.gov.uk/articles/about-certified-professional-scheme.

[17] See https://www.ncsc.gov.uk/smallbusiness.

[18] See https://www.cyberessentials.ncsc.gov.uk/advice/.

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

new businesses at the set-up stage, or at specific moments when businesses need guidance, such as when considering new cyber security products or choosing an external cyber security provider.

Recommendation 4: The Government should continue to raise awareness of the guidance targeted at non-cyber security professionals, about the minimum steps they should take to keep their organisation cyber secure.

Recommendation 5: Either the Government or industry bodies (such as trade associations) should look into the best way of linking experts and non-experts working in cyber security roles. One example could be a partnering scheme, allowing senior managers in small businesses and charities to seek help informally from cyber security professionals.

There are gaps in high-level skills and in incident response.

Organisations with more sophisticated cyber security needs also have skills gaps. In total, we estimate that 407,000 businesses have a high-level technical cyber security skills gap. We find this to be most acute in the areas of forensic analysis, penetration testing and security architecture – these are the tasks that those in cyber security roles tend to be least confident in carrying out, even when they consider them important for their organisation. The qualitative research also highlights skills shortages in the labour market when it comes to cloud security, end-point security, identity and access management, penetration testing, security architecture and threat hunting – these are areas where there are not enough people in the labour market to fill vacancies.

External cyber security providers and large organisations also need to anticipate future skills needs – linked to technological trends and developments – for the next three to five years, when recruiting for today's entry-level roles. Here, the areas that arose in interviews were around artificial intelligence, automation and data analytics, as well as threat hunting (again). It is notable that some of these areas have more of a maths focus, rather than a computer science one.

Recommendation 6: External cyber security providers and large organisations with relatively sophisticated cyber security needs should build cyber security into workforce planning, so that current and future high-level cyber security skills gaps can be proactively addressed.

Recommendation 7: Universities and external cyber security providers should encourage a wider range of graduates in science, technology, engineering and maths (STEM), to consider careers in cyber security – so that there are a greater range of candidates from non-programming backgrounds, but with the specialist skills and knowledge to work in wider areas such as artificial intelligence.

Recommendation 8: The Government and industry-led initiatives should continue to improve awareness among young peoples of career options in cyber security, focusing particularly on up-and-coming skills areas such as artificial intelligence, data analytics and threat hunting. This might be through existing initiatives such as CyberFirst, Cyber Discovery and other industry-related websites and initiatives.

There are also a large number of businesses – 460,000 in our estimation – that feel they lack the overall skills needed to respond to a cyber security incident. This is a cyber security skills area that is particularly overlooked, relative to the other areas covered in this research. Only under a fifth of businesses consider incident response skills to be essential, meaning that a large proportion of the 460,000 may not recognise this as a skills gap.

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

Recommendation 9: Senior managers in the private, charitable and public sectors should review the job descriptions of those working in cyber security roles, and ensure they assign responsibility for incident response.

Cyber security skills gaps are not just with those in cyber security roles, but also exist for wider staff.

We find that cyber security skills gaps are an issue to tackle on management boards, as well as across wider non-specialist staff. This links to the fact that cyber security is not just about technical controls, but also about good management and planning. It also relies on wider staff to be able to follow rules and policies, and be aware of their wider responsibilities around cyber security.

A substantive minority – almost half – of those working in cyber security roles in the private and charitable sectors (outside of external cyber security providers) think that their senior managers do not have a good understanding of how to manage a cyber security incident, when to report cyber security breaches, and the staffing needs of cyber security within their organisation. These organisations also reported that senior managers often lacked the expertise to make informed decisions about external cyber security providers. When it comes to wider core staff, again a sizable minority of those in cyber security roles are sceptical of their core staff's ability to store and transfer personal data securely.

Where wider non-specialist staff have received cyber security training, those in cyber security roles tend to be more confident in these staff being able to get the basics right, such as using strong words or identifying phishing emails. And yet, organisations are more likely to invest in cyber security training for those in cyber security roles than for wider staff. Only 11 per cent of businesses have provided cyber security training for wider staff in the past year.

Recommendation 10: The Government should continue to promote its board toolkit (which is being continually developed) to help improve cyber security skills and knowledge among senior managers.[19]

Recommendation 11: Where feasible, organisations should invest in cyber security awareness training for non-specialist staff.

Technical skills gaps tend to be higher outside the finance or insurance sectors, and the information and communications sectors, as well as outside of London.

Those working in cyber security roles in the information or communication sectors, and finance or insurance sectors are typically more confident at dealing with basic technical cyber tasks than those in the rest of the private sector. More broadly, public sector organisations were more confident than businesses and charities in being able to carry out these technical tasks – even when compared just to large businesses and high-income charities. There are no specific business sectors that perform consistently weaker than others in our survey, although it is worth highlighting that those working in cyber security roles in the food or hospitality, and construction sectors are among the least likely to be confident in dealing with an attack or breach. Food or hospitality businesses are also among the least likely to outsource any part of their cyber security, also leaving them open to cyber risks.

We found relatively few consistent geographic differences in this research. One exception to this is the difference between firms in London versus everywhere else. Those working in cyber security roles in London tend to be more confident in carrying out technical cyber tasks. One of the reasons behind this might be that cyber security professionals tend to

[19] See https://www.ncsc.gov.uk/guidance/board-toolkit-five-questions-your-boards-agenda.

cluster in London, where there are more job opportunities for them. This leaves other parts of the country facing a bigger cyber security skills gap.

Recruitment is not a feasible way for all organisations to fill cyber security skills gaps.

This research finds that recruiting new staff from outside an organisation is challenging for various reasons. Many organisations did not fully understand their own cyber security skills needs, so would not be capable of putting together a job description to suit their needs. This also supports Recommendation 2, which will help to more clearly define different levels and roles within cyber security.

Furthermore, organisations did not always consider recruitment to be the best approach to fill cyber security skills gaps. Many organisations feel they cannot justify paying someone to work exclusively in a cyber security role, as they would not have enough work for them. Some do not see the value a cyber specialist would bring over an IT generalist, and therefore try to split the cyber security role with a wider IT position to get better value for money. And when looking to fill high-level technical skills gaps, organisations often cannot afford the premium salaries that those with such advanced skills tend to command. This helps to explain why, outside of external cyber security providers, recruitment into cyber security roles happens very rarely.

Instead, outsourcing cyber security is a more common solution. However, the process of selecting an external cyber security provider is often not very systematic. And when working with external providers, many organisations do not feel they have enough technical knowledge to know whether their provider is doing a good job or not. Overall, this is perhaps a lesser issue, as we do not have any evidence to suggest the external providers in these cases are doing a bad job.

Recommendation 12: The Government should investigate whether additional guidance would be helpful for businesses and charities when it comes to recruiting someone for a cyber security role, or choosing an external cyber security provider. This could be, for example, a checklist to help understand what level of cover is being provided, and what aspects of cyber security would still need covering in-house.

Cyber security skills need to be continually refreshed.

Cyber security, and the technologies, policies and fundamental knowledge underpinning the field, are constantly evolving. In this process, current cyber security skills need to adapt to change. This means that reskilling and continuing professional development is very important for those in cyber security roles. This might also apply to wider staff, as all-staff training is also susceptible to getting out of date.

Only around half of all businesses offering training to those in cyber security roles think that this training met the organisation's needs completely or a great deal. This proportion is slightly lower when it comes to training for wider staff. Moreover, very few organisations – just 14 per cent of businesses – have conducted a cyber security training needs analysis. This suggests that the state of cyber security training and awareness-raising could be broadly improved, and that a first step is for organisations to have a better idea of their needs.

While organisations do not think there are substantive barriers to finding good cyber security training, the cost of training is the biggest issue that puts some organisations off. There are also question marks over the effectiveness of training products, and whether they are as relevant as they could be. The qualitative feedback suggests that, again, better knowledge sharing across organisations may be part of the solution here – sharing training that works, and has relevant content for specific sectors.

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

Recommendation 13: The Government and industry should look into providing guidance on how to carry out a cyber security training needs analysis. Organisations should then be encouraged to implement this, and review their cyber security training to make sure it is up-to-date, if they have not already done so.

Recommendation 14: Industry bodies (such as trade associations) should investigate the feasibility of developing standardised cyber security training materials that can be shared across organisations in similar size bands or sectors. This could involve joint working between industry bodies, businesses and training provides to develop effective training products.

Recommendation 15: The Government should commission further quantitative or qualitative research to review cyber security training provision across organisations and see how it might be improved.

More work can be done to measure skills shortages in specific advanced cyber security roles

This research has aimed to provide a set of findings that represent and reflect organisations of all sizes and sectors. This approach has highlighted the following:

- There are a large set of organisations – the majority, dominated by micro and small businesses, and low-income charities – that approach cyber security informally, and do not feel they need more advanced technical skills.
- The recruitment activity in the cyber security skills labour market is overwhelmingly concentrated within large businesses, large public sector organisations and, most of all, organisations specifically working within the cyber security industry (encompassing external cyber security providers, organisations researching and developing the technologies underpinning cyber security, and public sector organisations focused on national cyber security).

As a result, we have not been able to cover the formal side of cyber security in great detail in this research. In particular, we have not been able to measure formal cyber security skills shortages – the shortfall in the number of skilled individuals working in or applying for formal cyber security positions. Therefore, while we have specific and quantifiable insights about the types of high-level skills that organisations lack the most, we cannot say how many new labour market entrants are needed to fill skills shortages in different cyber specialisms. This may be an area for further work, focusing on organisations specialising in cyber security technological development, organisations providing cyber security products or services, as well as very large (for example, FTSE 350) businesses.

Recommendation 16: The Government should commission further quantitative research to measure skills shortages in specific cyber specialisms, and estimate the number of cyber security skills-shortage vacancies in the UK. This work would not be representative of all organisations, but would instead attempt to get high coverage from the largest private sector organisations and the largest organisations operating specifically within the cyber security industry.

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

References

Centre for Strategic and International Studies (2016) Hacking the Skills Shortage, McAfee (https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hacking-skills-shortage.pdf)

Cisco (2015) Mitigating the Cyber Skills Shortage (https://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-talent.pdf)

Cobb (2018) "Plugging the skills gap: the vital role that women should play in cyber-security", Computer Fraud & Security, 2018(1), pp.5–8 (https://www.sciencedirect.com/science/article/pii/S1361372318300046)

Ecorys UK (2016) Digital skills for the UK economy, Department for Digital, Culture, Media and Sport (https://www.gov.uk/government/publications/digital-skills-for-the-uk-economy)

Global Information Security Workforce Study (2017) Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk (https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf)

Information Assurance Advisory Council (2017) The profession: understanding careers and professionalism in cyber security (http://www.iaac.org.uk/wp-content/uploads/2018/02/2017-03-06-IAAC-cyber-profession-FINAL-Feb18-amend-1.pdf)

Ipsos MORI (2018) Cyber Security Breaches Survey 2018: Main report, Department for Digital, Culture, Media and Sport (https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2018)

ISACA (2018) State of Cybersecurity 2018 (https://cybersecurity.isaca.org/state-of-cybersecurity)

ISC2 (2018) Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens: Cybersecurity Workforce Study 2018 (https://www.isc2.org/Research/Workforce-Study)

Joint Committee on the National Security Strategy (2018) Cyber Security Skills and the UK's Critical National Infrastructure (https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec/706/70602.htm)

Newhouse, Keith, Scribner and Witte (2017) National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. U.S. Department of Commerce (https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework)

Rashid, Danezis, Chivers, Lupu, and Martin (2017) Scope for the Cyber Security Body of Knowledge (https://www.cybok.org/media/downloads/CyBOKScopeV2.pdf)

Recruitment and Employment Confederation (2017) Demand for cyber security staff to surge next year (https://www.rec.uk.com/news-and-policy/press-releases/demand-for-cyber-security-staff-to-surge-next-year-rec)

Reece and Stahl (2015) "The professionalisation of information security: Perspectives of UK practitioners", Computers & Security, 48, pp.182-195

Silensec (2017) Addressing the Cyber Security Skills Gap (https://www.silensec.com/downloads-menu/whitepapers/item/29-addressing-the-cyber-security-skills-gap)

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

Tech Partnership (2017) Factsheet: Cyber Security Specialists in the UK
(https://www.tpdegrees.com/globalassets/pdfs/research-2017/factsheet_cybersecurityspecialists_feb17.pdf)

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

18-008461-01 | Version 1 | Public | This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms. © Department for Digital, Culture, Media and Sport 2018

For more information

3 Thomas More Square
London
E1W 1YW

t: +44 (0)20 3059 5000

www.ipsos-mori.com
http://twitter.com/IpsosMORI

About Ipsos MORI's Social Research Institute

The Social Research Institute works closely with national governments, local public services and the not-for-profit sector. Its c.200 research staff focus on public service and policy issues. Each has expertise in a particular part of the public sector, ensuring we have a detailed understanding of specific sectors and policy challenges. This, combined with our methods and communications expertise, helps ensure that our research makes a difference for decision makers and communities.