Department for Digital, Culture Media & Sport

CYBER SECURITY SKILLS GAPS

Research findings on the UK cyber security skills labour market

Key: Charities | All businesses | Large businesses

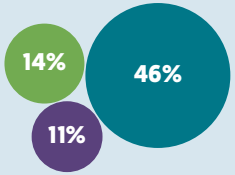
Ipsos

How cyber security is staffed

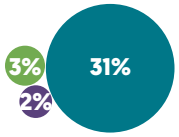
The average cyber security team consists of:

Charities — **2 employees**
All businesses — **2 employees**
Large businesses — **4 employees**

In most organisations, cyber security roles are covered informally



% of organisations where a cyber security role is **formally written into job descriptions**



% of organisations that have **tried to recruit for cyber security roles** in the past 3 years

These survey findings are reflective of businesses and charities across all sectors. They do not focus on external cyber security providers*, who are the high volume recruiters in the market.

"**We are always recruiting; we have induction days every Monday.**" External cyber security provider interview

Measuring cyber security skills gaps

The survey measures skills gaps in terms of whether those in cyber security roles feel confident carrying out specific cyber security tasks.

Of the c1.32million UK businesses, we estimate that around

710,000 have a basic technical cyber security skills gap.**

407,000 have a high-level technical cyber security skills gap.

Most notable skills gaps

There are cyber security skills gaps in basic and high-level technical skills, as well as managerial, planning and organisation skills.

% of organisations **not confident** in performing the following high-level technical tasks:***

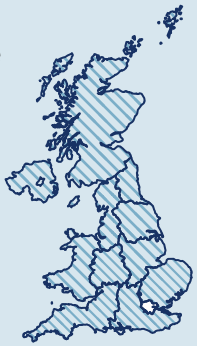
	Charities	All businesses	Large businesses
Forensic analysis	57%	59%	28%
Penetration testing	60%	57%	42%
Security architecture	55%	54%	18%
Using **threat intelligence**	57%	44%	18%

% of organisations **not confident** in performing the following managerial, planning or organisational cyber security tasks:

	Charities	All businesses	Large businesses
Carrying out a **cyber security risk assessment**	43%	51%	21%
Preparing **cyber security training** for wider staff	45%	47%	15%
Developing **cyber security policies**	39%	47%	11%
Writing cyber security into a **business continuity plan**	33%	44%	9%

Where are cyber security skills gaps most pronounced?

- Organisations outside London have more pronounced skills gaps in each of the areas asked about (e.g. 59% not confident in penetration testing outside London, vs. 51% in London).



Incident response

Incident response is an area that many organisations underestimate or do not understand to be important, but where there are notable skills gaps.

% not confident in dealing with a cyber security breach or attack

Charities	All businesses	Large businesses
51%	47%	18%

% not confident in writing an incident response plan

Charities	All businesses	Large businesses
49%	51%	17%

Base: 470 UK charities; 1,030 UK businesses (excluding agriculture, forestry and fishing businesses); 110 large businesses with 250+ staff | Fieldwork dates: 12 June to 6 August 2018 | All data are weighted.
*External providers are those that offer IT or cyber security services to other organisations.
**We define a basic cyber security skills gap as being where organisations are not confident in carrying out one or more basic tasks, including: creating back-ups, controlling admin rights, setting up automatic updates, choosing secure settings, restricting what software can run, detecting and removing malware, secure personal data transfers or storage, and setting up configured firewalls.
***Among those that consider these tasks important for their organisation, and do not outsource them).

Department for Digital, Culture Media & Sport

OUTSOURCING CYBER SECURITY

Research findings on the UK cyber security skills labour market

Key: Charities | All businesses | Large businesses

Ipsos

Outsourcing to external cyber security providers

27% of charities outsource

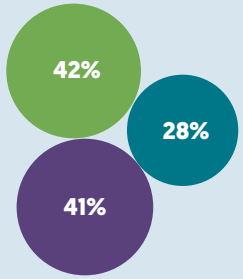
30% of businesses outsource

For businesses, outsourcing is more common in the finance or insurance sectors (49%), and administration or real estate sectors (48%).

Why do organisations outsource?

When asking organisations that outsource their cyber security why they do so, the primary (unprompted) reasons are related to filling cyber security skills gaps:

To access greater expertise



Internal staff lack necessary knowledge or experience

A lack of funds to recruit specialist cyber security staff

Too busy to manage cyber security internally

Qualitative interviews suggest that many organisations consider hiring internal cyber security staff to be too costly or unsustainable, so they outsource.

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

What functions do organisations commonly outsource?

% outsourcing these functions, among organisations that outsource any aspects of cyber security"

The most commonly outsourced aspects of cyber security are:

Less technical aspects are less commonly outsourced:

High-level technical skills are outsourced by 71% of businesses and 80% of charities. The most common are:

Base: 470 UK charities (187 that outsource); 1,030 UK businesses, excluding agriculture, forestry and fishing businesses (427 that outsource); 110 large businesses with 250+ staff (63 that outsource) | Fieldwork dates: 12 June to 6 August 2018 | All data are weighted.

Department for Digital, Culture Media & Sport

DEFINING CYBER SECURITY SKILLS

Research findings on the UK cyber security skills labour market

Key: Charities | All businesses | Large businesses

Ipsos

A definition of cyber security skills

Cyber security skills that all organisations need are a combination of essential and advanced technical expertise and skills, strategic management skills, planning and organisation skills, and complementary soft skills that allow them 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 have, either within their workforce, or externally.

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.

Which cyber security skills are considered most important?

The following cyber security skills are valued the most highly among organisations:
% of organisations considering each of the following cyber security skills categories as essential for their organisation:

Understanding legal or compliance issues

Soft skills, such as communication and team working skills

Understanding how actions on cyber security can affect performance

Basic technical skills*

Incident response skills

High-level technical skills**

Skills gaps in high-level technical skills

Organisations generally considered high-level technical skills to be less important than other areas, potentially lacking understanding of the highly technical nature of cyber security. There are notable skills gaps in these skills. Below is the % of organisations not confident in performing the following high-level technical tasks (among those that consider these tasks important for their organisation, and do not outsource them):

Forensic analysis
57% | 59% | 28%

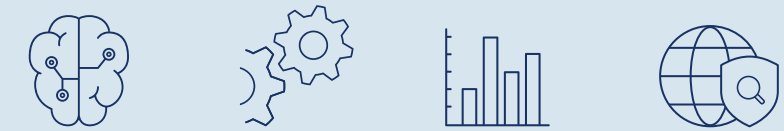
Penetration testing
60% | 57% | 42%

Security architecture
55% | 54% | 18%

Using **threat intelligence**
57% | 44% | 18%

Predicted future cyber security skills needs

Qualitative interviews with external cyber security providers*** highlighted a number of skills areas that they predict will be in greater demand in the future:



Artificial intelligence

Automation

Data analytics

Threat hunting

Base: 470 UK charities; 1,030 UK businesses, excluding agriculture, forestry and fishing businesses; 110 large businesses with 250+ staff | Fieldwork dates: 12 June to 6 August 2018 | All data are weighted.
*Basic technical skills defined in the survey as including areas like: setting up firewalls, choosing secure settings for devices or software, controlling who has access, setting up anti-virus protection, and keeping software up to date.
**High-level technical skills defined in the survey as including areas like: security engineering, penetration testing, using threat intelligence tools, forensic analysis, interpreting malicious code, or using tools to monitor user activity.
***External cyber security providers are those that offer IT or cyber security services to other organisations