MARKET DATA FROM SECONDARY SOURCES

Femke De Keulenaer, Ipsos European Public Affairs

November 2022

1 DEMAND-SIDE RESEARCH

2 MACRO-ENVIRONMENTAL FACTORS (POLITICAL, ECONOMIC, SOCIAL AND TECHNOLOGY)

Logical blocks/modules of ECSMAF

3 PRIMARY VS SECONDARY RESEARCH

enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

ENISA CYBERSECURITY MARKET ANALYSIS FRAMEWORK (ECSMAF)

APRIL 2022

SECONDARY DATA

DEMAND-SIDE RESEARCH

1

EUROPEAN
PUBLIC
AFFAIRS

Ipsos

Cybersecurity maturity

Cyber security awareness

Cyber security skills

Experienced impact on business

Some examples of surveys conducted by Ipsos

Flash Eurobarometer 496 SMEs and cybercrime (EU-wide random probability telephone survey of 12,863 SMEs, conducted in 2021)

https://europa.eu/eurobarometer/surveys/detail/2280

Understanding the UK cyber security skills labour market (a quantitative survey of 1,030 UK businesses, 127 public sector organisations and 470 charities, conducted in 2018)

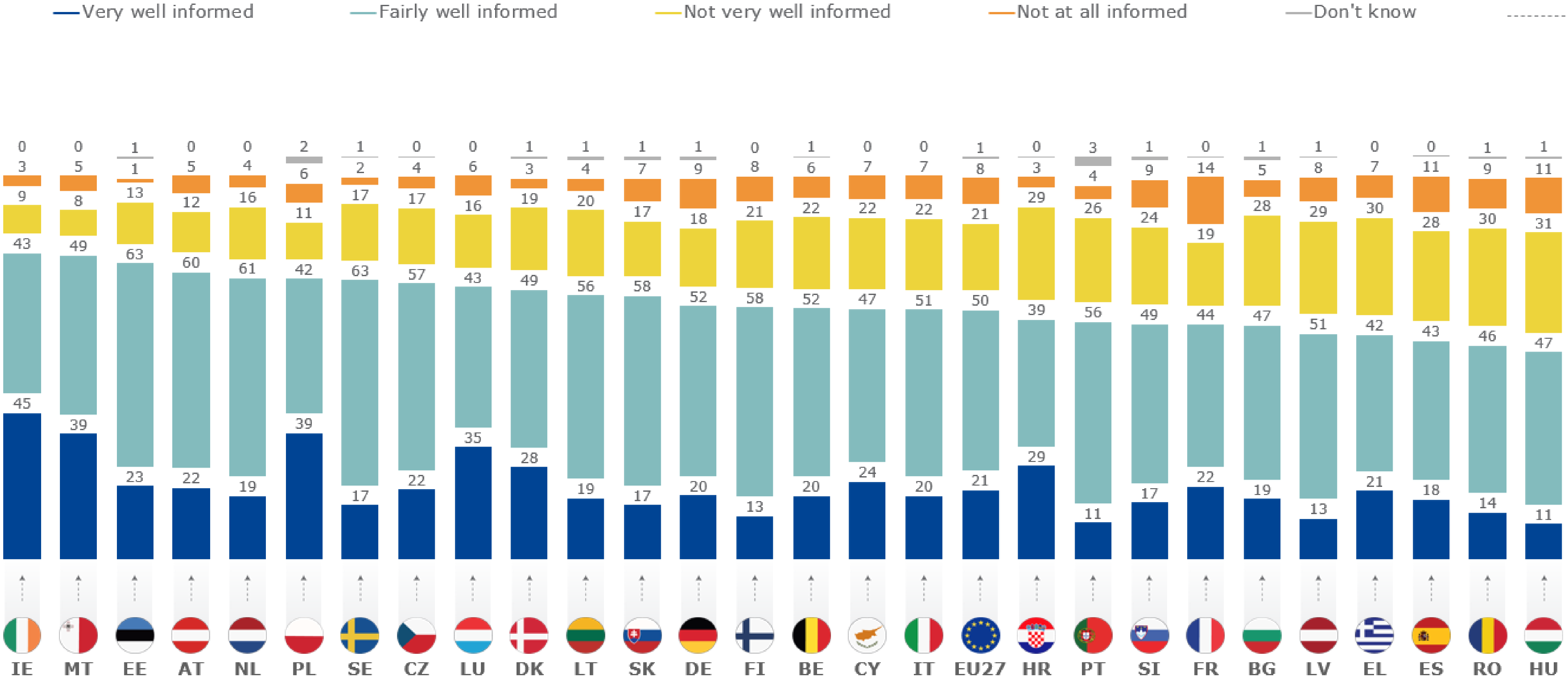
https://www.ipsos.com/en-uk/understanding-uk-cyber-security-skills-labour-market

Cyber Security Breaches Survey 2022 (a random probability telephone survey of 1,243 UK businesses, 424 UK registered charities and 420 education institutions)

https://www.ipsos.com/en-uk/cyber-security-breaches-survey-2022

Flash Eurobarometer 496 - SMEs and cybercrime

How well informed do you feel about the risks of cybercrime?

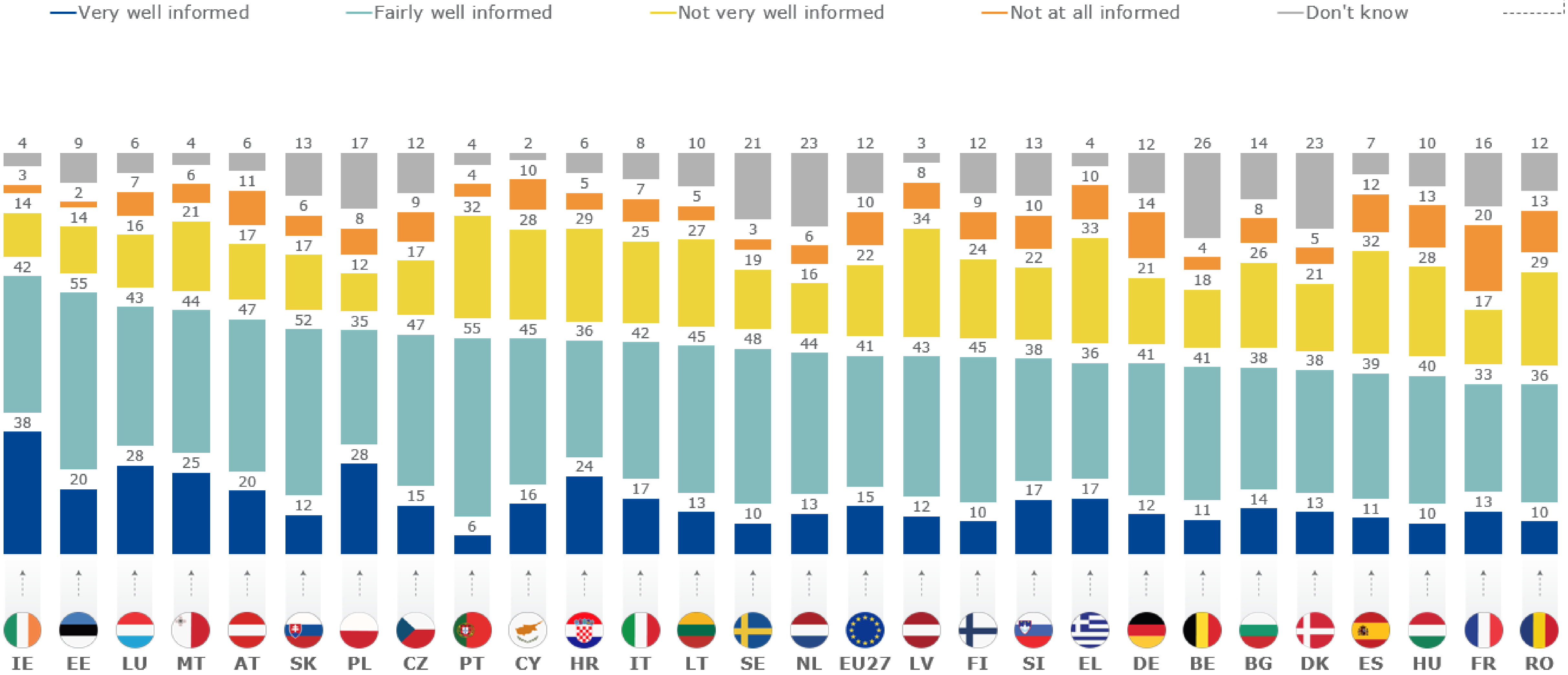


Flash Eurobarometer 496 - SMEs and cybercrime / Fieldwork: 26/11 - 17/12/2021 / Base: n=12 863 - All SMEs (%)

European Commission

Flash Eurobarometer 496 - SMEs and cybercrime

How well informed do you feel your employees are about the risks of cybercrime?

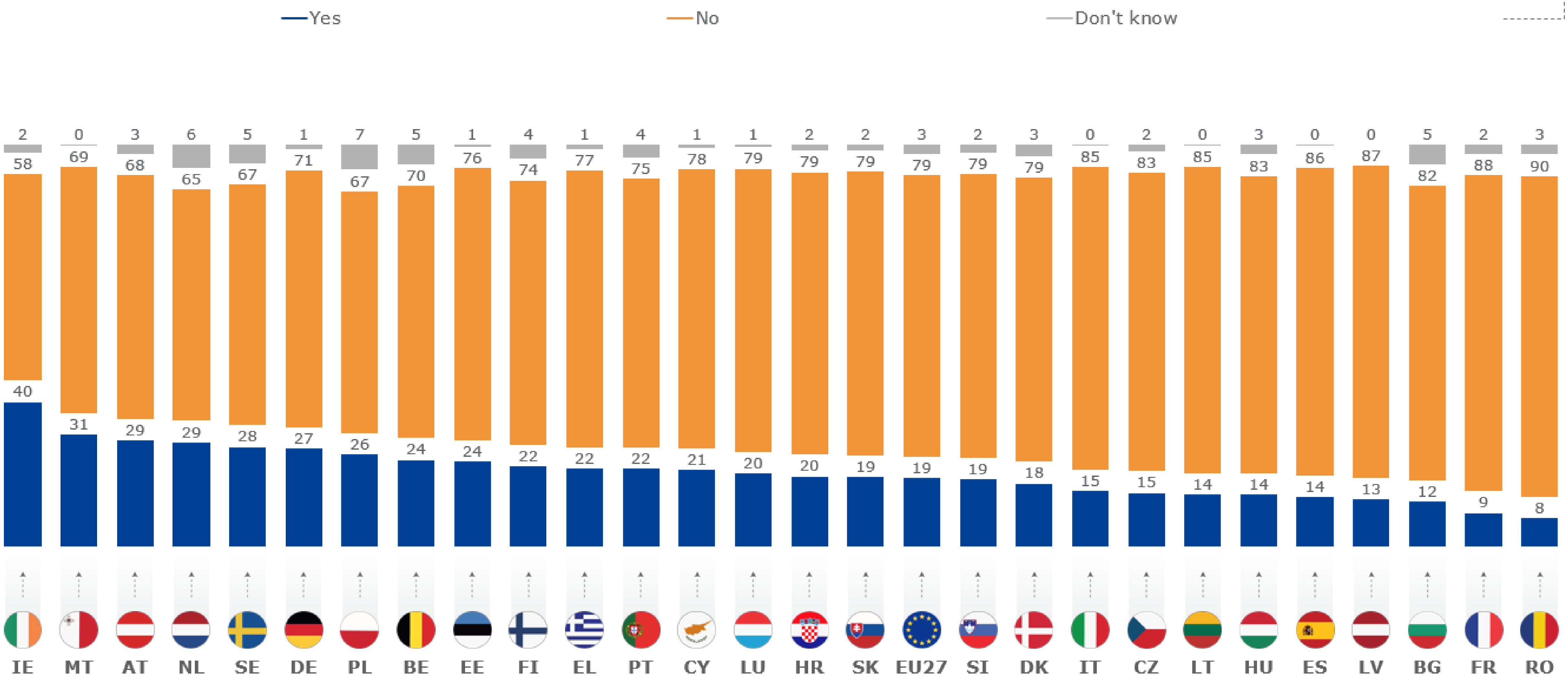


Flash Eurobarometer 496 - SMEs and cybercrime / Fieldwork: 26/11 - 17/12/2021 / Base: n=12 863 - All SMEs (%)

European Commission

Flash Eurobarometer 496 - SMEs and cybercrime

In the last 12 months, has your company provided employees with any training or awareness raising about the risks of cybercrime?



Flash Eurobarometer 496 - SMEs and cybercrime / Fieldwork: 26/11 - 17/12/2021 / Base: n=12 863 - All companies (%)

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

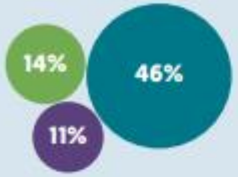
Ipsos

How cyber security is staffed

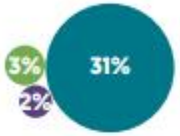
The average cyber security team consists of:

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

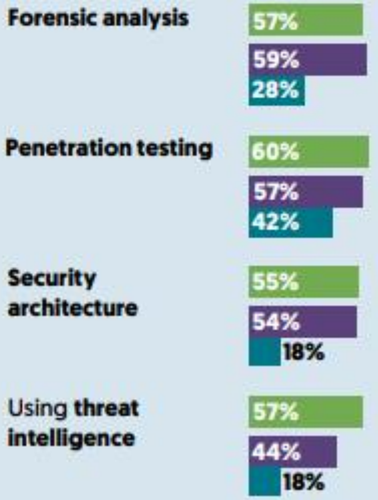
710,000 have a basic technical cyber security skills gap.**

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

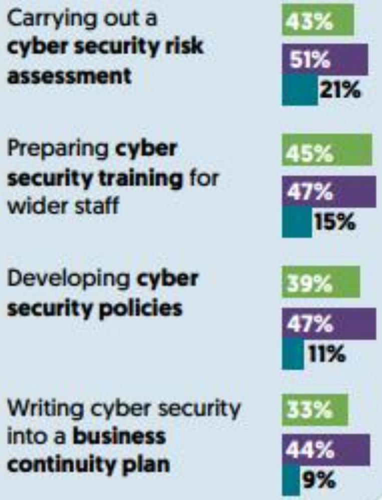
Most notable skills gaps

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:***



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



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.

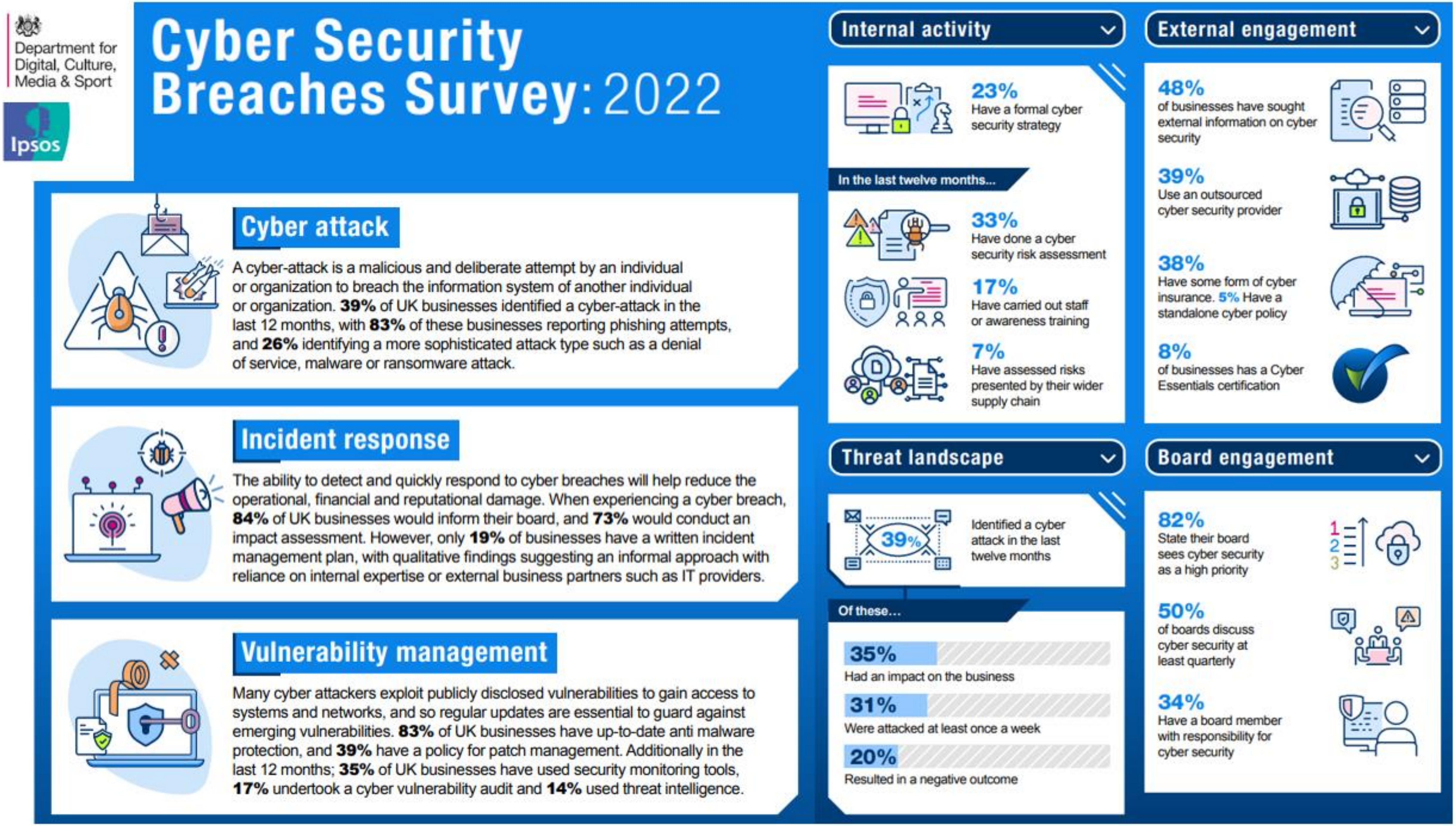
% not confident in dealing with a cyber security breach or attack

51% 47% 18%

% not confident in writing an incident response plan

49% 51% 17%

Ipsos



Department for Digital, Culture, Media & Sport

Ipsos

Cyber Security Breaches Survey: 2022

Cyber attack

A cyber-attack is a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization. **39%** of UK businesses identified a cyber-attack in the last 12 months, with **83%** of these businesses reporting phishing attempts, and **26%** identifying a more sophisticated attack type such as a denial of service, malware or ransomware attack.

Incident response

The ability to detect and quickly respond to cyber breaches will help reduce the operational, financial and reputational damage. When experiencing a cyber breach, **84%** of UK businesses would inform their board, and **73%** would conduct an impact assessment. However, only **19%** of businesses have a written incident management plan, with qualitative findings suggesting an informal approach with reliance on internal expertise or external business partners such as IT providers.

Vulnerability management

Many cyber attackers exploit publicly disclosed vulnerabilities to gain access to systems and networks, and so regular updates are essential to guard against emerging vulnerabilities. **83%** of UK businesses have up-to-date anti malware protection, and **39%** have a policy for patch management. Additionally in the last 12 months; **35%** of UK businesses have used security monitoring tools, **17%** undertook a cyber vulnerability audit and **14%** used threat intelligence.

Internal activity

23% Have a formal cyber security strategy

In the last twelve months...

33% Have done a cyber security risk assessment

17% Have carried out staff or awareness training

7% Have assessed risks presented by their wider supply chain

External engagement

48% of businesses have sought external information on cyber security

39% Use an outsourced cyber security provider

38% Have some form of cyber insurance. **5%** Have a standalone cyber policy

8% of businesses has a Cyber Essentials certification

Threat landscape

39% Identified a cyber attack in the last twelve months

Of these...

35% Had an impact on the business

31% Were attacked at least once a week

20% Resulted in a negative outcome

Board engagement

82% State their board sees cyber security as a high priority

50% of boards discuss cyber security at least quarterly

34% Have a board member with responsibility for cyber security

SECONDARY DATA

MACRO-ENVIRONMENTAL FACTORS

2

EUROPEAN
PUBLIC
AFFAIRS

Ipsos

Political, Economic and Social Factors

Citizens' concerns about data privacy

Safeguarding reputation through investment in cyber security

Support for government policies

Some examples of surveys conducted by Ipsos

2019 CIGI-Ipsos Global Survey on Internet Security and Trust (survey with 25,229 Internet users in 25 economies, via online or face-to-face interviewing, conducted between December 2018 and February 2019)

https://www.ipsos.com/en/2019-cigi-ipsos-global-survey-internet-security-and-trust

Ipsos MORI's annual Captains of Industry Survey (opinion survey among Britain's most senior business leaders)

https://www.ipsos.com/en/reputation-rise-safeguarding-your-brand-reputation-through-investment-cyber-security

Trust in the Internet, survey released by The NEW INSTITUTE in Germany (Online survey with 14,519 Internet users in 20 economies using the Ipsos panel, conducted in November 2021)

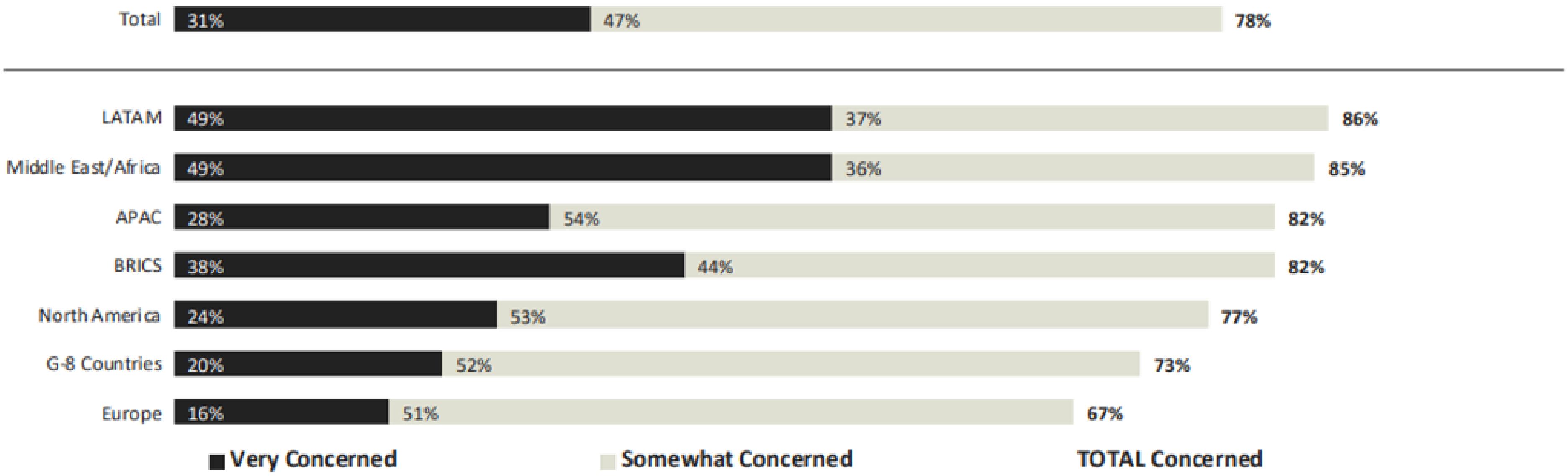
https://www.ipsos.com/sites/default/files/ct/news/documents/2022-11/Trust%20in%20the%20Internet%2C%20Nov%202022.pdf

PRIVACY & SECURITY

CIGI-IPSOS GLOBAL SURVEY INTERNET SECURITY & TRUST

Across all regions, most have at least some degree of concern when it comes to their online privacy, with those living in developing economies being significantly more likely to express at least some level of concern. Europeans are least concerned.

A1. How concerned are you about your online privacy?
Base: 2019 (n=23,854)



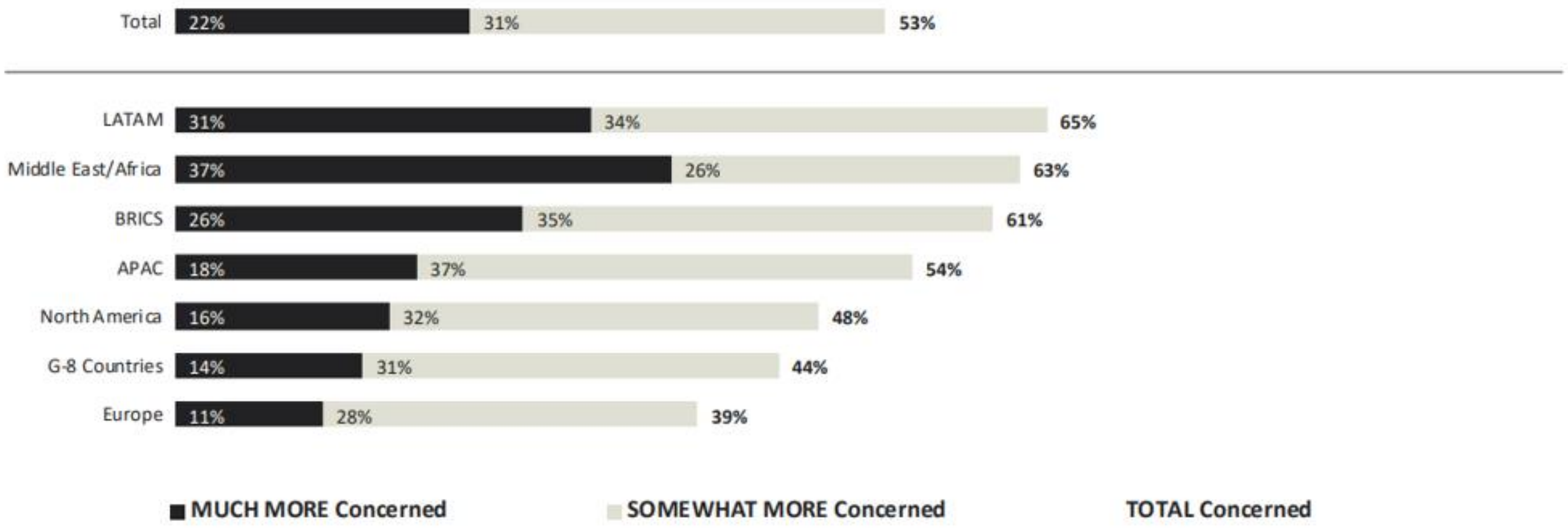
PRIVACY & SECURITY

CIGI-IPSOS GLOBAL SURVEY

INTERNET SECURITY & TRUST

Growing concerns towards online privacy are less pronounced in developed economies. More specifically, less than half in Europe (39%), North America (48%) & the G-8 more generally (44%) say they're more concerned than last year, but a majority in LATAM (65%), The Middle East (63%), BRICS (61%) and APAC (54%) cite a growing concern.

Q1. How concerned are you about your online privacy compared to one year ago?
Base: 2019 (n=23,854)



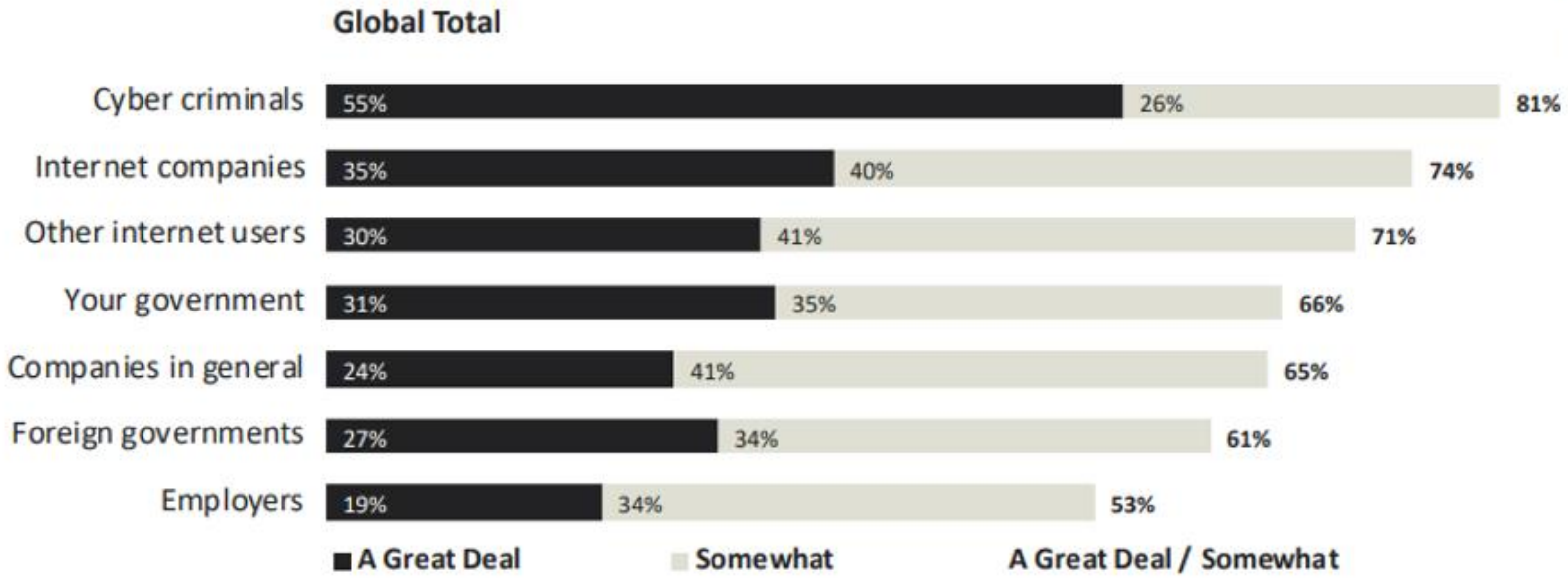
PRIVACY & SECURITY

CIGI-IPSOS GLOBAL SURVEY

INTERNET SECURITY & TRUST

Among those who claim to be at least *somewhat more concerned* about their online privacy, compared to a year ago, cyber criminals are the leading factor that has contributed to their increased levels of concern. However, since 2016, concerns about governments, both domestic and foreign, have grown the most.

Q2. To what extent have the following sources contributed to your being more concerned than last year about your online privacy?
Base: A Great Deal / Somewhat More Concerned About Online Privacy 2016 (n=13,867); 2017 (n=12,468); 2018 (n=12,956); 2019 (n=25,229)



[NET] Contribution

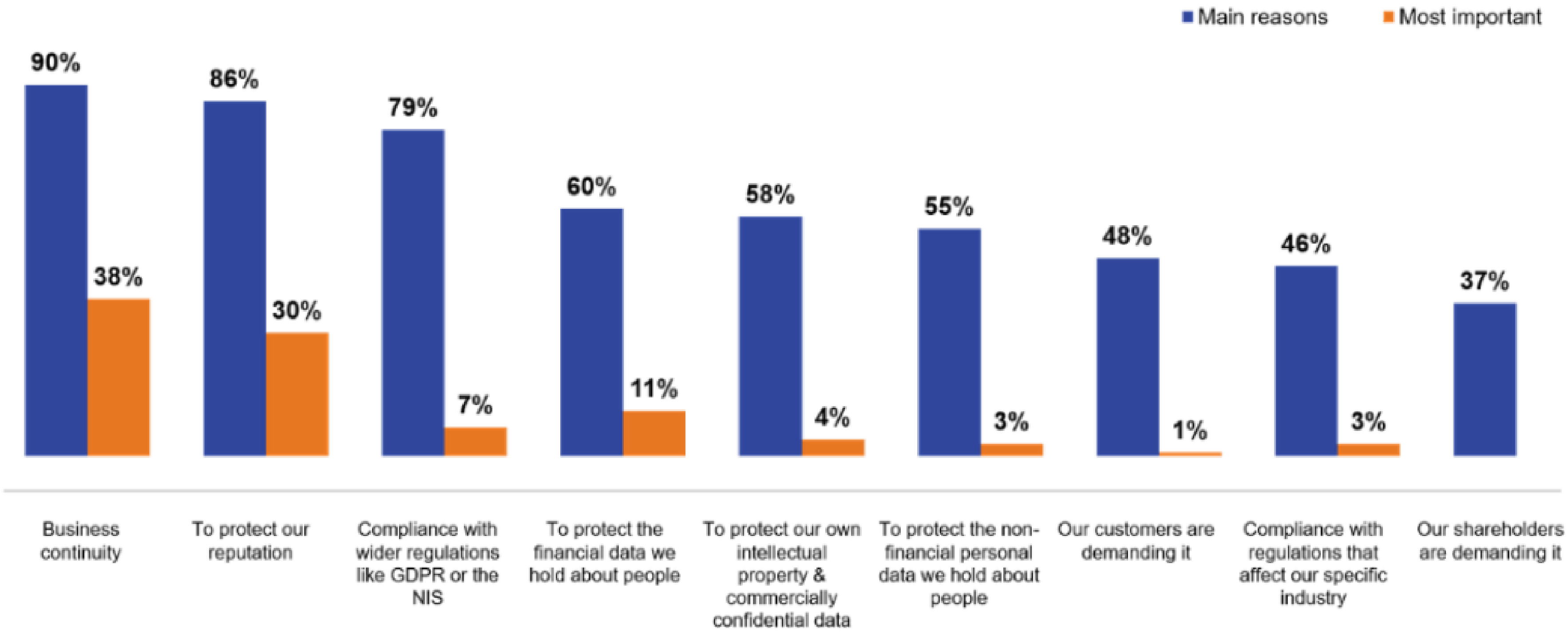
	2018	2017	2016
Cyber criminals	81%	82%	79%
Internet companies	74%	74%	72%
Other internet users	66%	67%	66%
Your government	63%	65%	60%
Companies in general	65%	61%	62%
Foreign governments	58%	61%	50%
Employers	48%	49%	48%

Captains of Industry

Ipsos MORI

2020 Findings

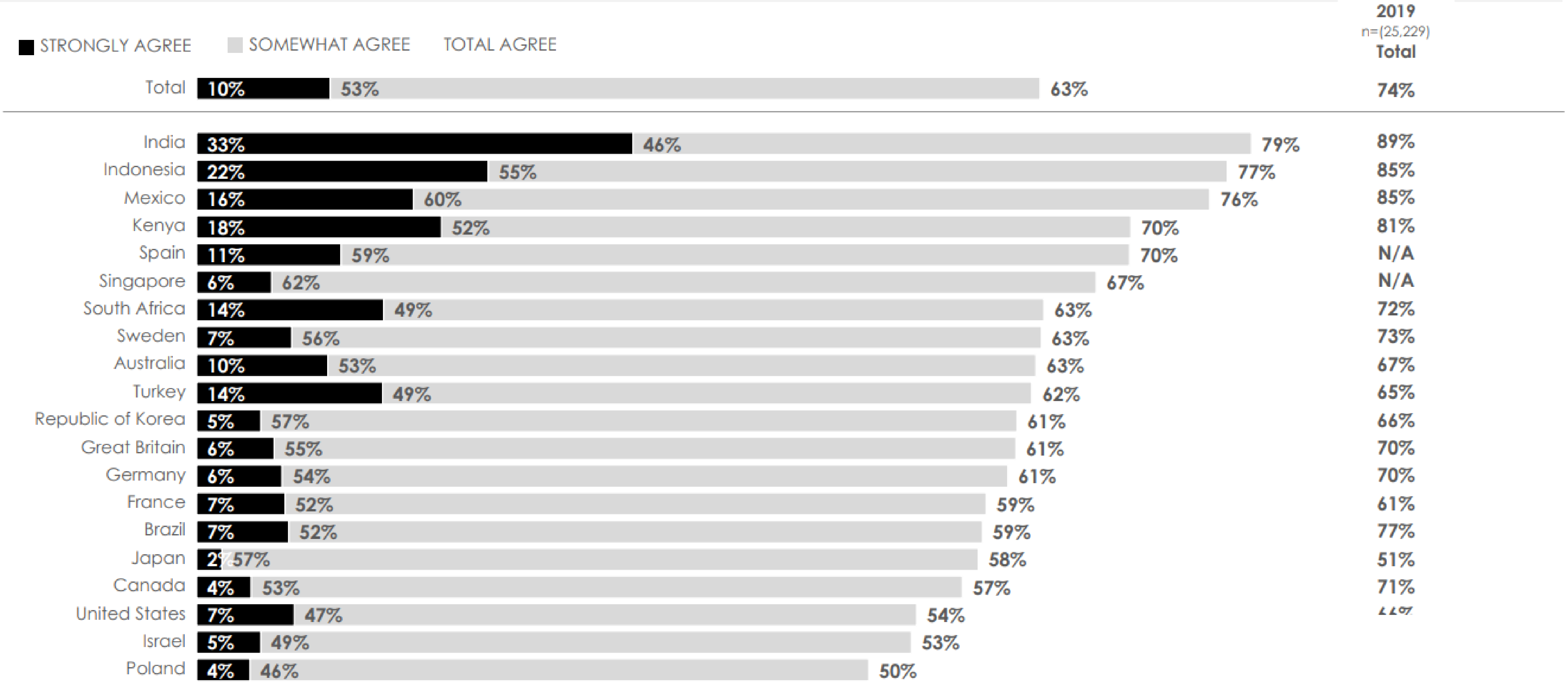
Firstly, please tell me which of the following would you say are the main reasons for your company to invest in cyber security? And which one of these would you say is the most important reason?



Base: British Captains of Industry (102); Interviewed Feb – July 2020

Overall, trust in the internet has declined by 11 points to 63%. A majority of economies experienced a decline from 2019 but the most notable include Poland decreasing by 26 points (50%), Brazil decreasing by 18 points (58%), and Canada decreasing by 14 points (57%).

AGREEMENT WITH STATEMENT: OVERALL, I TRUST THE INTERNET

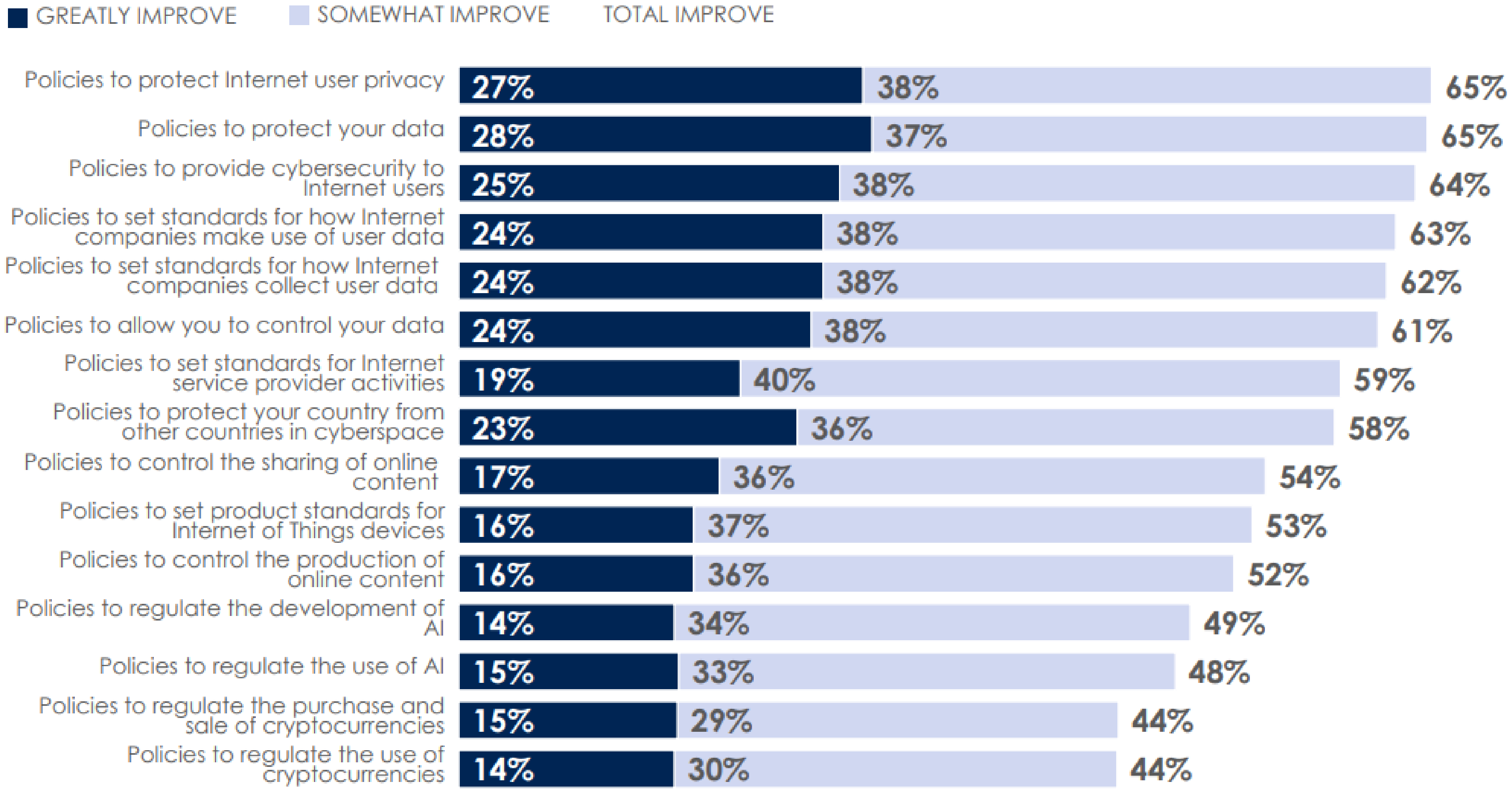


© Ipsos

Base: Total respondents 2020 (n=14519) ; 2019 (n=25,229);
Q2.1 How much do you agree or disagree with the following statements …

A majority agree that most proposed government policies will improve internet trust. Specifically, three in five agree that policies to protect internet user privacy (65%), providing cybersecurity (65%), set standards om how companies make use of user data (64%), set standards for companies collecting user data (62%), and allow you to control your data (61%) would improve trust.

SUPPORT FOR GOVERNMENT POLICIES TO IMPROVE TRUST IN THE INTERNET



Base: Total respondents (n=14519)
Q2.4 To what extent would new government policies in the following areas improve or worsen your trust in the Internet?

THANK YOU!

FEMKE DE KEULENAER
Senior Research Director

✉ **femke.dekeulenaer@ipsos.com**
☎ +32 485 182 350

EUROPEAN
PUBLIC
AFFAIRS

About Ipsos

Founded in 1975, Ipsos is the third largest market and public opinion research company in the World – and currently the only large global research company primarily managed by researchers and focused entirely on research.

Headquartered in Paris, Ipsos maintains locally incorporated offices in 90 countries globally, including 21 of the European Union's 27 Member States, and is at the forefront of developing state-of-the-art tools and methods to provide clients with robust evidence for confident decision making.

The company is structured around a number of services covering a range of sectors and solutions, including:

Public Affairs; Corporate Reputation; Retail and Consumer Intelligence; Retail Performance; Audience Measurement; Customer Experience; Employee Relationship Management; Media Development; Mystery Shopping; Qualitative; Social Intelligence Analytics; and User Experience.

European Public Affairs

Ipsos' European Public Affairs (EPA) team, based in Belgium, specialises in conducting pan-European (and global) public opinion research to the highest standards of methodological rigour for clients ranging from the European institutions and EU political parties/groups, to international organisations (e.g. the United Nations, NATO and the World Bank Group).

As well as undertaking commissioned research, Ipsos Public Affairs is at the forefront of developing and sharing best practice in polling and survey research. Such work is a defining element of our brand, contributing to high response rates from the public, more openness to our communications and heightened credibility for our findings.