DEVELOPING CYBER SECURITY AS A PROFESSION

A REPORT BY THE GLOBAL FORUM ON CYBER EXPERTISE

July 2022

Acknowledgements

The GFCE would like to acknowledge the work of the Project Team on 'Developing cyber security as a profession' of GFCE Working Group D Cyber Security Culture and Skills. The Project Team led work on the survey and the report and included contributions from:

- Paul Blaker, Department for Digital, Culture, Media and Sport (UK)
- Heather MacLean, Public Safety Canada (Canada)
- Basie von Solms, University of Johannesburg (South Africa)
- Anna Moran, Department for Digital, Culture, Media and Sport (UK)
- Richard Harris, MITRE (USA)
- Nthabiseng Pule, Cybersecurity Capacity Centre for Southern Africa (South Africa)
- Danielle Santos, National Initiative for Cybersecurity Education (USA)
- Chris Martin, Department for Digital, Culture, Media and Sport (UK)
- Tereza Horejsova, GFCE Working Group D Chair
- Giouli Lykoura, GFCE Secretariat.

In case of any questions, please contact the GFCE Secretariat at contact@thegfce.org

Disclaimer

Foreword by Tereza Horejsova,
Chair of Working Group on Cyber Security Culture and Skills,
Global Forum for Cyber Expertise

Cyber security has become an increasingly urgent global priority in recent years. There is clearly a serious need to increase the number of trained professionals able to tackle the cyber threats we face. If companies and other organisations are to address cyber risks effectively, they need to have the right people with the right skills.

More and more stakeholders are looking at how we can make cyber security an attractive career choice and how we can develop it as a recognised profession. Professions such as law, medicine, engineering and accountancy all have clear career paths which employers can understand. And, perhaps more importantly, they offer a kind of status that many people would aspire to. Why not cyber security too?

The Global Forum on Cyber Expertise has developed a unique role in bringing together stakeholders from around the world to find solutions to shared challenges. At the end of 2021, the GFCE Working Group on Cyber Security Culture and Skills initiated a global survey on developing cyber security as a profession in order to gather views and ideas from different stakeholders and regions around the world. We wanted to understand how the cyber security profession is viewed and understood, as our Working Group works towards a better understanding of the skills needed in future to be a successful cyber professional, be it in a very technical field or for instance in the policy or education sphere.

I would like to thank everyone who participated and who helped us put together such a valuable snapshot of current thinking. I hope the results presented here will help develop the global debate on cyber security, provide useful insights for policy makers around the world and ultimately, contribute to cyber security being a recognised career choice.

Executive Summary

The Global Forum on Cyber Expertise (GFCE) is a multi-stakeholder community of more than 160 members and partners from all regions of the world, aiming to strengthen cyber capacity and expertise globally. This report was drawn up by the GFCE's Working Group D on Cyber Security Culture and Skills in order to better understand different perspectives on developing cyber security as a profession, including the possible barriers that exist, qualifications and accreditations, and the role of awareness campaigns and regulation. Our survey attracted over 200 responses, broadly balanced across stakeholder groups and global regions, with some clear areas of agreement as well as some different views emerging. The full set of questions in the survey can be found at Annex A of this report.

The vast majority of respondents recognised there is a significant shortfall of cyber security professionals across the globe. Most people thought that the idea of a "cyber security professional" is unclear and that this lack of clarity is a barrier to people pursuing a career in cyber. There is very strong support for public awareness campaigns to encourage people to join the cyber security profession, but views are mixed when it comes to possible regulatory interventions.

More than half of the responses were opposed to the idea of introducing regulation such as a "licence to practise" for cyber security professionals, although support for a "licence to practise" was slightly stronger in responses from people in government and responses from people in developing countries. A majority of responses thought that introducing a "licence to practise" would create barriers to people joining the profession and that this would undermine cyber security in the long term. Responses from people in the private sector were particularly concerned about the risk of creating barriers.

Most people (68%) thought that better recognised qualifications were needed to strengthen cyber security as a profession, although this opinion was stronger in developing countries than in developed countries. The vast majority agreed that qualifications needed to be internationally recognised.

These results demonstrate the need to find a balance between strengthening the professional framework for cyber security while also avoiding introducing barriers to entry. They also bring out the different challenges faced by stakeholders in developing countries. Reflecting on these results, the GFCE community would point to recommendations in five broad areas:

1. Stakeholders should consider **how best to use awareness campaigns** to attract more people to pursue a career in cyber security. These should look at a

full range of tools, including not only advertising but also careers advice services, school curriculum content, awareness raising for teachers and industry-led campaigns and events.

2. Governments should work with industry to consider how to **raise awareness of qualifications**, certifications, degrees and apprenticeship standards, reaching out both to employers and to cyber security professionals.

3. Policy makers should consider **a range of interventions to develop cyber security as a profession** without creating barriers to entry. Comprehensive regulation through a compulsory "licence to practise" might undermine cyber security in the long term by making it harder for people to join the profession. But policy makers can consider other more limited interventions, depending on their own circumstances, such as establishing a voluntary register of qualified practitioners.

4. Stakeholders should take into account the particular **challenges faced by developing countries**. We heard, for example, that the subscription rates for some professional associations can be higher than the average monthly salary for some cyber security professionals in developing countries. Some respondents to the survey also raised the affordability of qualifications. Stakeholders should consider steps to address these kinds of barriers.

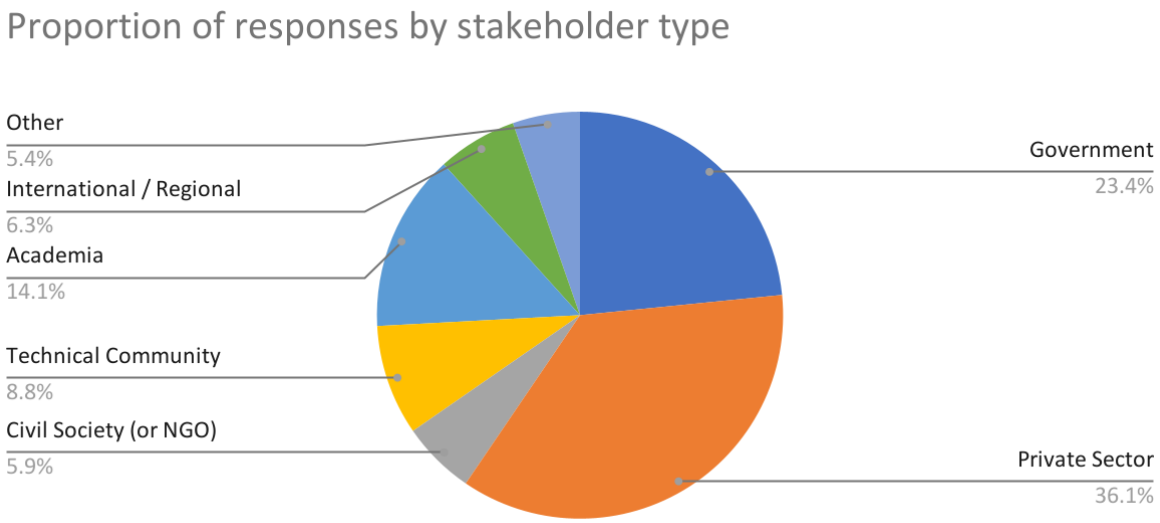
5. **Further research is needed**, particularly in areas such as the role of universities and the need for effective and accessible training programmes. This should take into account views of all stakeholders, including governments, industry, the technical community, education experts and others.

We hope that this report will provide a useful starting point for a wider global debate on how best to develop cyber security as a profession, to attract more people to pursue a career in cyber and to support employers to identify and recruit the right people for their needs. GFCE will continue to address these issues and we encourage others to join us in this effort.

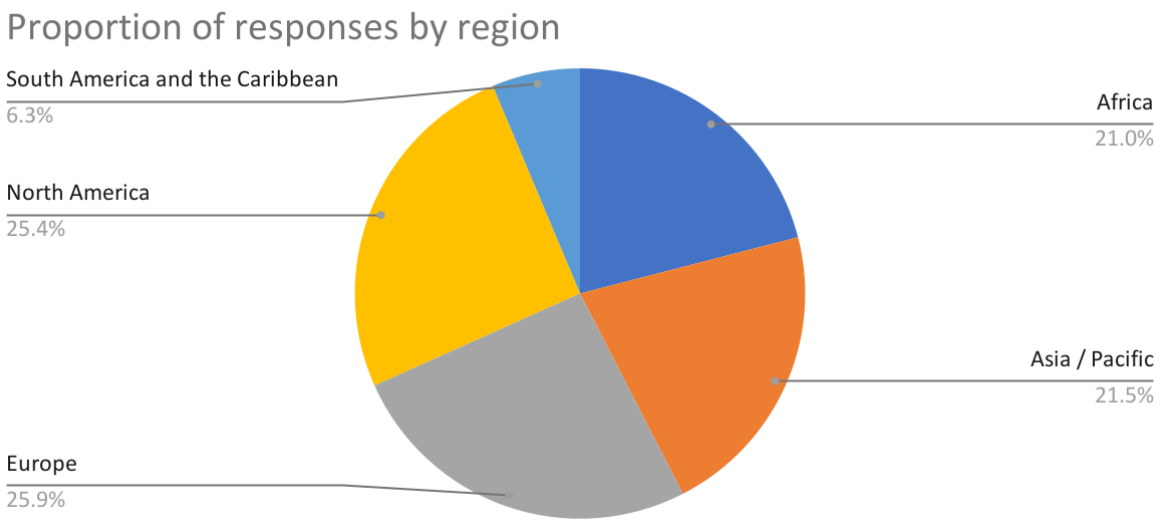
Methodology

The GFCE Working Group D on Cybersecurity Culture and Skills began creating a global survey on developing cyber security as a profession in the summer of 2021. A project team was created including representatives from Canada, South Africa, the United Kingdom and the United States of America. The survey was launched at the GFCE Annual General meeting in November 2022 and ran until 5 February 2022. It was widely shared and promoted by the GFCE community. GFCE also approached regional organisations to encourage more participants.

The survey asked respondents to identify which stakeholder group they were from and the country they were responding from. This data allowed us to assess where there were differences in opinion between stakeholder groups and between more developed, less developed and least developed countries, using OECD classifications.



The sectoral breakdown shows that 36.5% of respondents identified themselves as from the private sector, the largest group. 23.1% said they were from a Governmental organisation, 14.4% from academic, 8.7% from the technological community, 6.3% from international/regional organisations, 5.8% were from the civil society, and 5.3% from other.



The regional breakdown was as follows: Europe (26%), North America (25.5%), Asia/Pacific (21.2%), Africa (20.7%), and South America and the Caribbean (6.7%). 112 participants were from a more developed country, 77 were from a less developed country, and 16 were from a least developed country.

The survey asked 10 quantitative questions, where respondents were asked to rank a statement by one of the following: strongly agree, agree, neither agree nor disagree, disagree, or strongly disagree. It also asked 12 qualitative questions, most of which invited people to comment on the statement in the quantitative question. In presenting the results here we have combined the “strongly agree” and “agree” categories. We have also combined the stakeholder groups into “government”, “private sector” and “other”. The full set of results can be found at Annex A attached to this report.

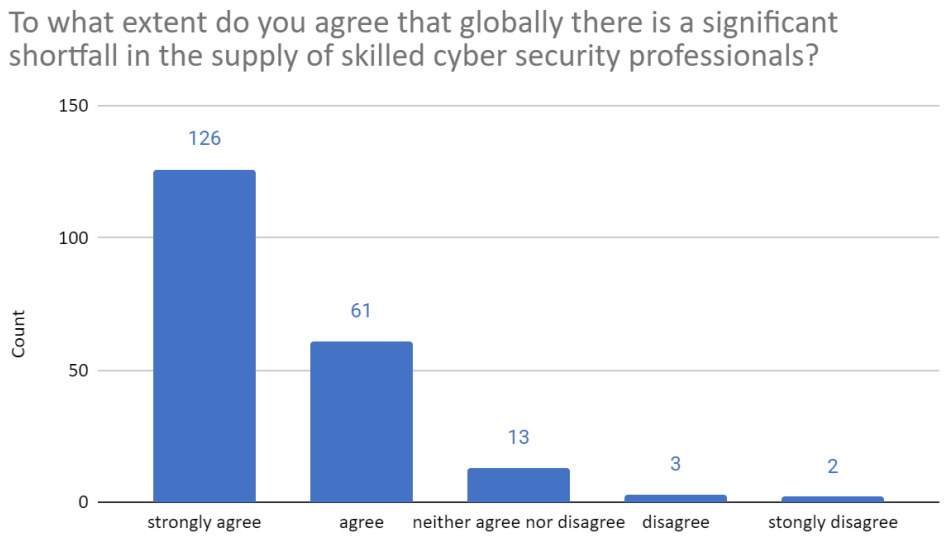
The survey received a total of 208 responses. The number of responses to the qualitative questions ranged from 120 to 46. In order to analyse the responses to the qualitative questions, we coded responses using key words and themes. The analysis of the qualitative questions is not exclusive: that is to say, if a respondent made more than one point in their answer to an qualitative question, each point has been recorded separately.

Key findings

The results of the survey fall into three main categories: (i) attitudes towards cyber as a profession (ii) measures to encourage people to join the profession and (iii) qualifications and certifications. This section looks at each of these categories in turn.

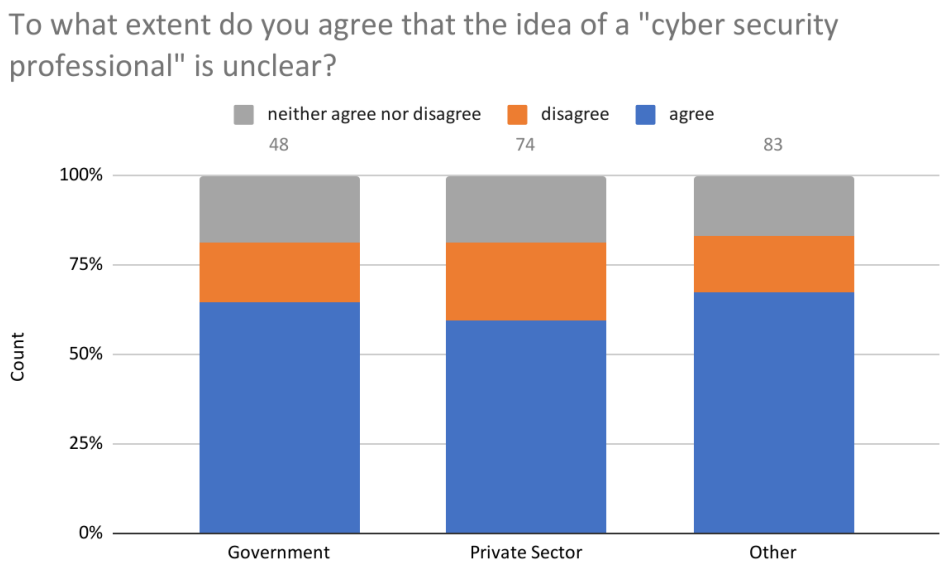
1. Attitudes towards cyber as a profession

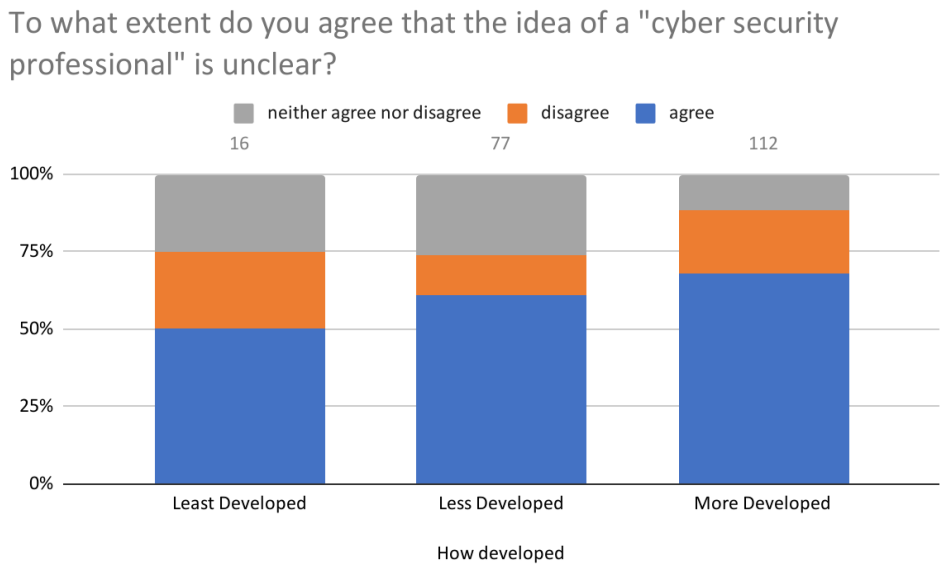
The first major finding was that the vast majority of people believe there is a significant shortfall of cyber security professionals across the globe. Out of 208 respondents, only 2% disagreed. It is interesting to note that all of the respondents who disagreed were from a more developed country.



Qualitative responses noted that employers tend to look for experienced professionals but there is limited workforce readiness at junior levels and the training currently available is not best for preparing young professionals. A number of participants said that recruiters do not know how to hire relevant cyber security professionals.

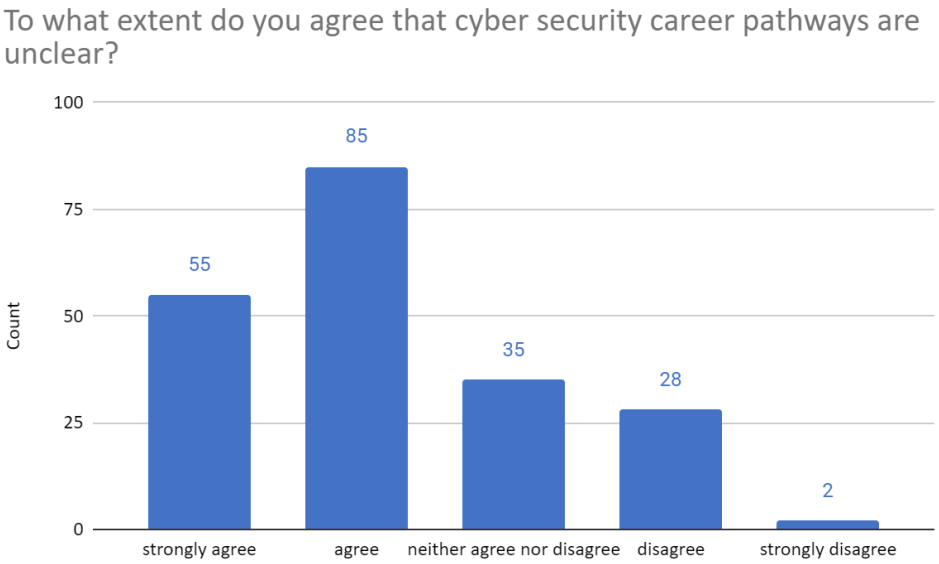
47% of respondents agreed that the idea of a “cyber security professional” is unclear while only 18% disagreed. The proportion of people who thought it was unclear was broadly the same across all stakeholder groups. It was slightly higher among respondents from developed countries.

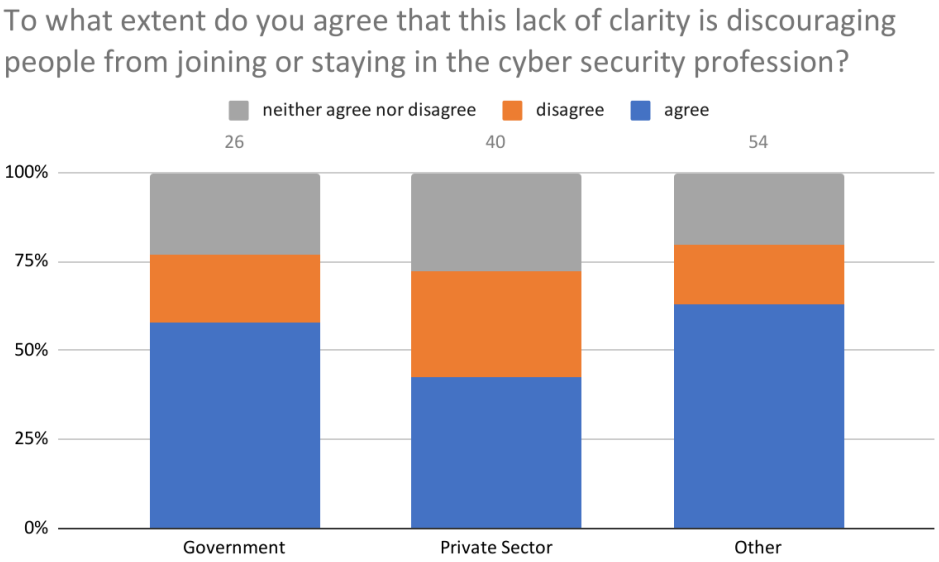




In the qualitative responses, respondents noted that “cyber security” is a very broad term which can involve different fields and that it is sometimes perceived to be part of information technology (IT).

Two thirds of respondents agreed that cyber security career pathways are unclear and of those the majority thought that this lack of clarity was discouraging people from joining or staying in the cyber security profession. This view was stronger in people working in government (60%) and less strong in people working in the private sector (40%).

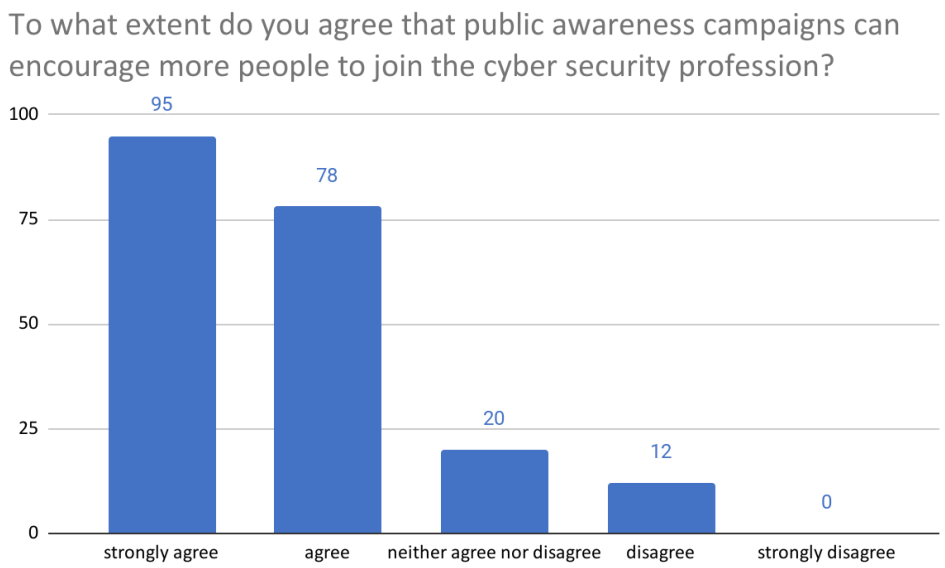




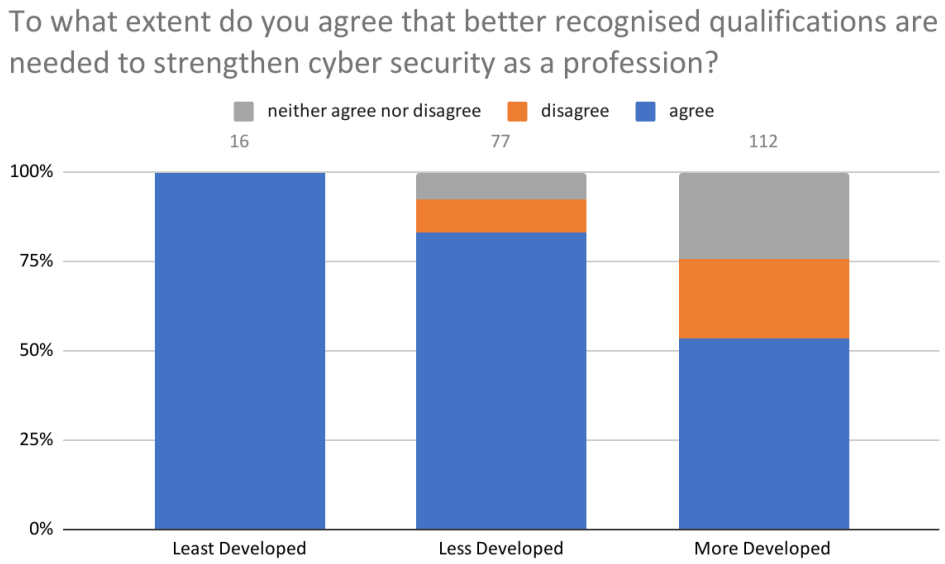
In their qualitative responses, some respondents suggested that the role of cyber professionals was constantly evolving and therefore it was hard to define.The lack of recognised frameworks for standards or certification was also highlighted. It was noted that people lack knowledge of how to become a cybersecurity professional or the opportunities it provides.

2. <u>Measures to encourage people to join the profession</u>

There was very strong agreement that public awareness campaigns can encourage more people to join the cyber security profession. This view was particularly strong among people working in government and people in developing countries. A number of respondents suggested early age awareness and education is needed.

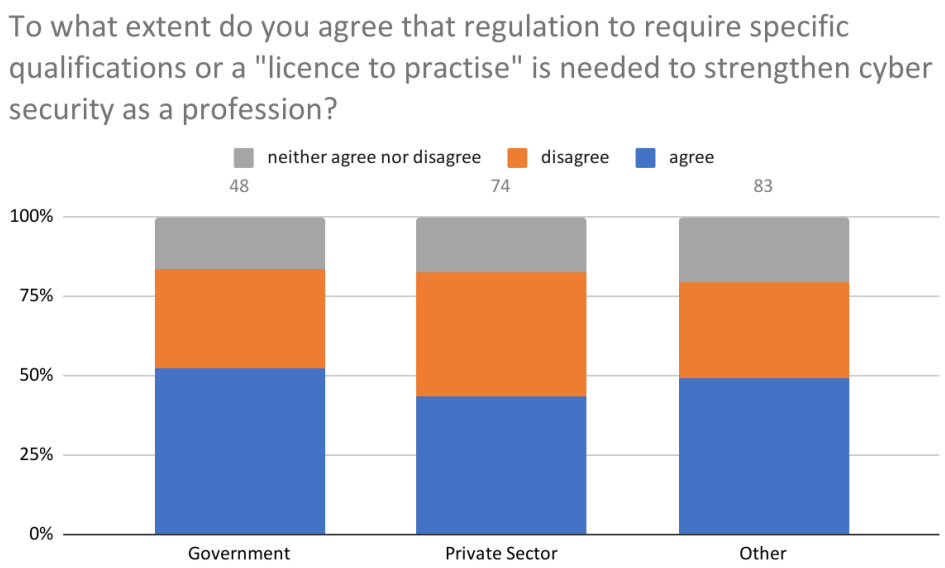


There was consensus that better recognised qualifications are needed, although this was much less strong in developed countries.



In their qualitative responses, several people said that experience was more important than qualifications. Others said there should be clarity about the relationship between specific qualifications and roles. The issue of accessibility and affordability of qualifications was also raised: high fees and charges can be a major barrier to people getting qualifications, particularly in developing countries.

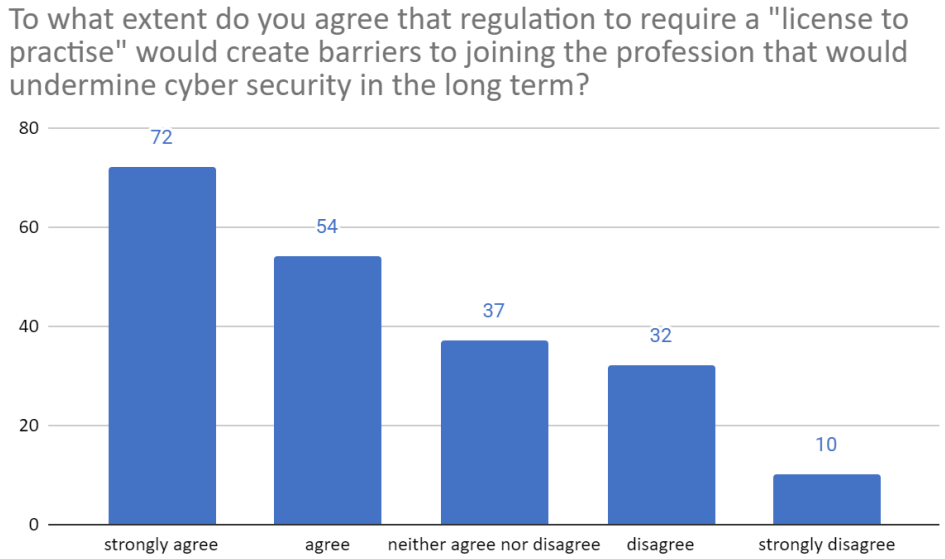
Participants were asked if regulation to require specific qualifications or a “licence to practise” would strengthen the cyber security profession. Almost half of respondents agreed that it would. Support for regulation was slightly higher among those working in governments as opposed to the private sector.

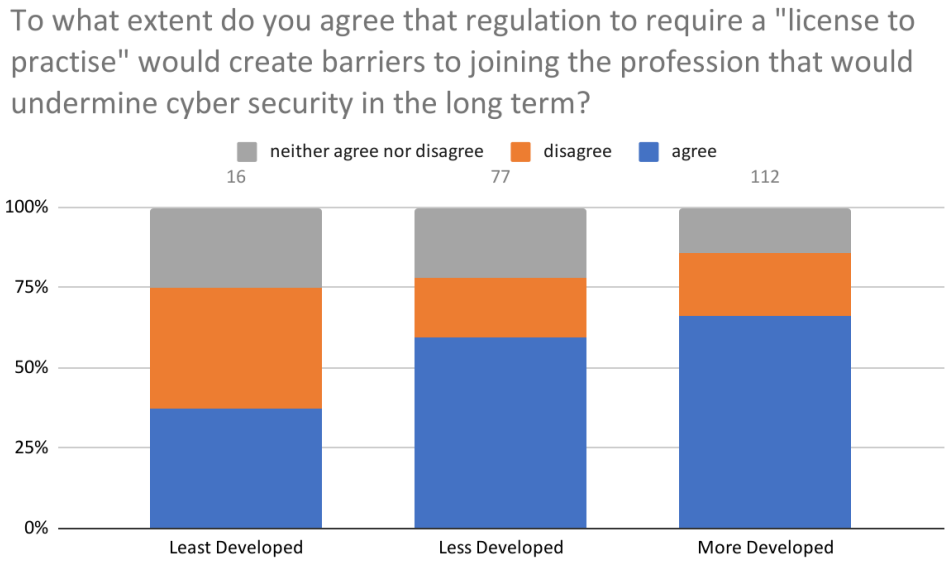


There was also a stark difference of views between developed and developing countries on the issue of regulation. In least developed countries, 88% supported regulation compared to 33% in more developed countries.

Out of the total respondents, 60% of people agreed that regulation requiring a licence to practise would create barriers to joining the profession, and this view is more common among private sector respondents than government employees. This view was most strong in developed countries and particularly strong in the private sector, with 70% of respondents from the private sector agreeing that a licence will create a barrier, and only 14% of respondents from the same sector disagreed

Qualitative responses said that a ‘licence to practise’ would pose a barrier to entry to the profession. A number of respondents said that practical experience was more important, or a licence would not sufficiently address the root cause of the issue. Some respondents remarked that regulation was only needed for certain critical roles and it was commented that regulation in the cyber security profession would be premature.

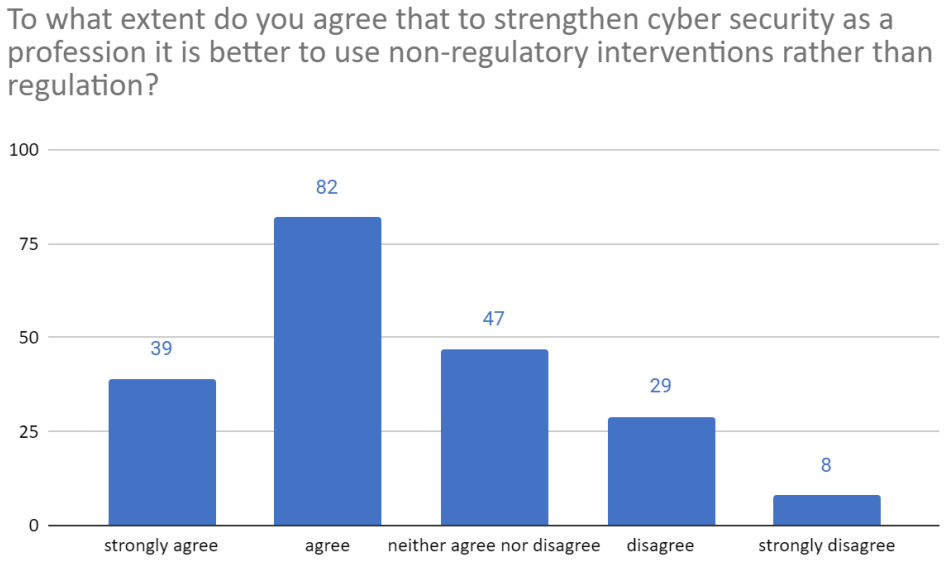




There were a large number of qualitative responses that argued that a “licence to practise” would create barriers. Some respondents also highlighted that the profession was not yet mature enough or that it would depend on how a licence was implemented.

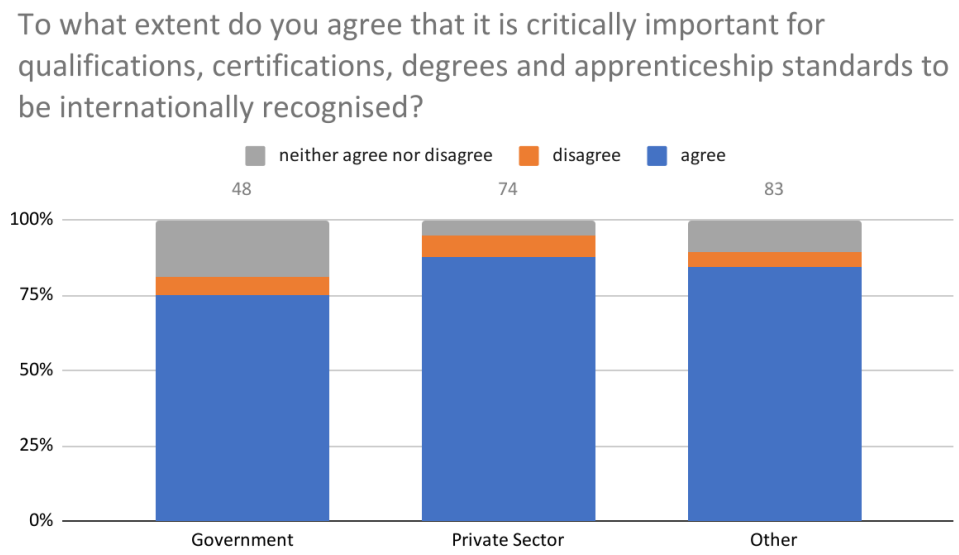
3. Qualifications and certifications

Most people agreed that non-regulatory interventions were better than regulation for strengthening cyber security as a profession.



Many respondents said that non-regulatory measures would encourage more people into the profession and some believed that voluntary certification is the best way to test skills. However, other respondents suggested that non-regulatory measures are already in place in some areas and do not work, or that regulation is needed in order to create a minimum ‘baseline’ of expertise and to keep pace with rapid technological developments. It was also noted that organisations need to be nudged into improving cyber security, as they do not do this on their volition. The importance of predictability through regulation was also raised.

When asked about international recognition of qualification, certifications, degrees and apprenticeship standards, the vast majority agreed that they needed to be internationally recognised. This was more true in the private sector responses (88% agreement) than the government ones (75%).



Qualitative responses to this question noted that international recognition is important because cyber security is a global issue with global standards and this recognition would provide benefits in terms of diversity and mobility.

Conclusions and recommendations

We recognise that a survey of 208 respondents cannot provide a completely accurate picture of global opinion. We also recognise the fact that there were more respondents from developed countries than from less developed countries, and significantly fewer responses from those in least developed countries. Nevertheless, the results show some clear trends and point towards some clear conclusions.

It is evident that respondents felt there is a need for more people to pursue a career in cyber security and that there is a lack of understanding about what is meant by a “cyber professional”. A significant part of the problem is that career pathways and qualifications are unclear and often lack recognition. There is strong support for awareness campaigns to tackle this issue and for better recognised qualifications.

Although there is significant support for greater regulation of the profession, with almost half of respondents supporting a “licence to practise”, there is significant concern that new regulation could create barriers to people taking up a career in cyber. It was also observed that the profession is not yet mature enough for a regulatory approach. There is strong support for non-regulatory interventions and for more internationally recognised qualifications.

While there is a need for global collaboration, the following recommendations, drawn from these findings, need to be considered in and adapted to local contexts. Various stakeholders in different countries will face a multitude of challenges and they will need to develop approaches which are right for their circumstances. Nevertheless, in reflecting on the issues that have been raised, the GFCE points to five broad recommendations:

1. Stakeholders should consider **how best to use awareness campaigns** to attract more people to pursue a career in cyber security. These should look at a full range of tools, including not only advertising but also careers advice services, school curriculum content, awareness raising for teachers and industry-led campaigns and events.

2. Governments should work with industry to consider how to **raise awareness of qualifications**, certifications, degrees and apprenticeship standards, reaching out both to employers and to cyber security professionals.

3. Policy makers should consider **a range of interventions to develop cyber security as a profession** without creating barriers to entry. Comprehensive regulation through a compulsory “licence to practise” might undermine cyber security in the long term by making it harder for people to join the profession. But policy makers can consider other more limited interventions, depending on their

own circumstances, such as establishing a voluntary register of qualified practitioners.

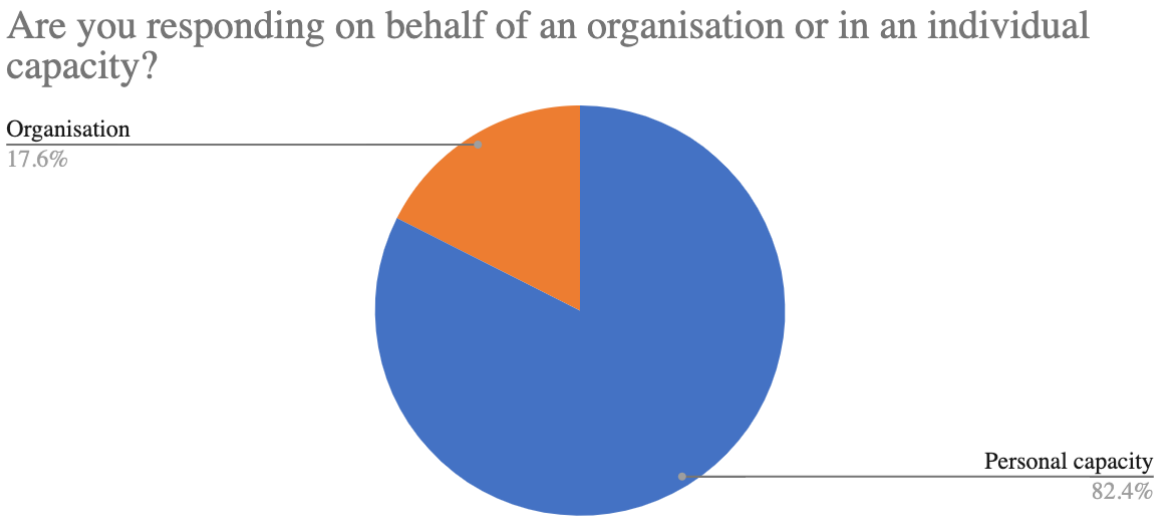
4. Stakeholders should take into account the particular **challenges faced by developing countries**. We heard, for example, that the subscription rates for some professional associations can be higher than the average monthly salary for some cyber security professionals in developing countries. Some respondents to the survey also raised the affordability of qualifications. Stakeholders should consider steps to address these kinds of barriers.

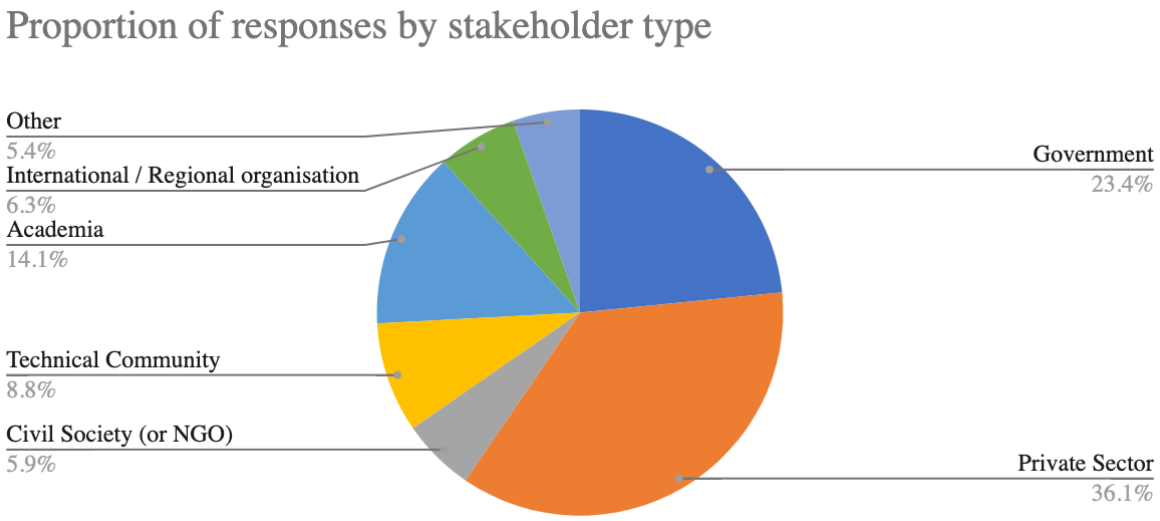
5. **Further research is needed**, particularly in areas such as the role of universities and the need for effective and accessible training programmes. This should take into account views of all stakeholders, including governments, industry, the technical communication, education experts and others.

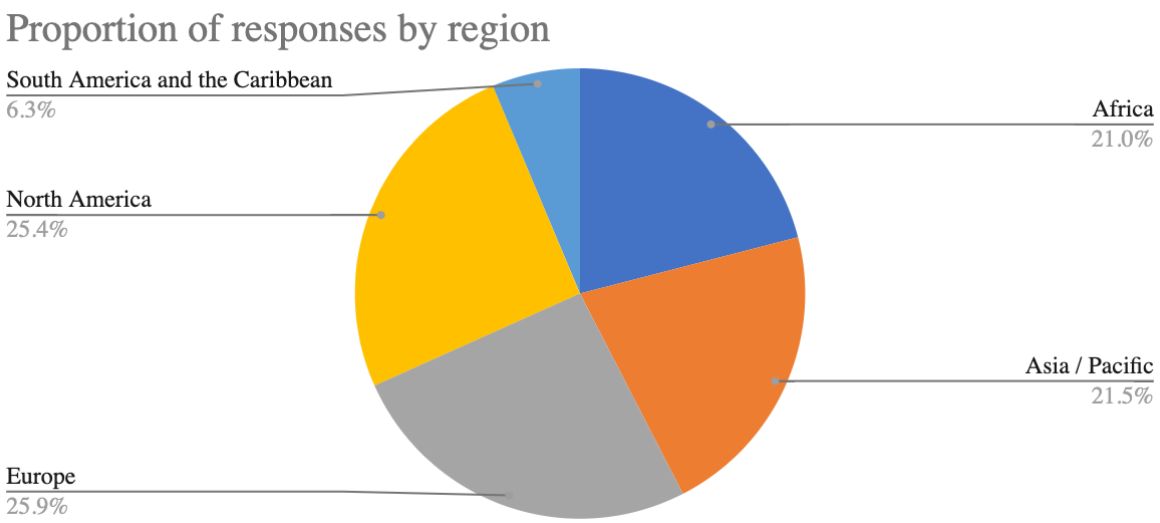
The Project Team, Working Group D, and the whole of the GFCE would like to thank respondents for engaging in this study. Whilst there is evidently grounds for more research, we believe this study has successfully provided an insight into some of the views of those in the cyber sector, whilst also highlighting shared perspectives between sectors and those from countries of varying development.

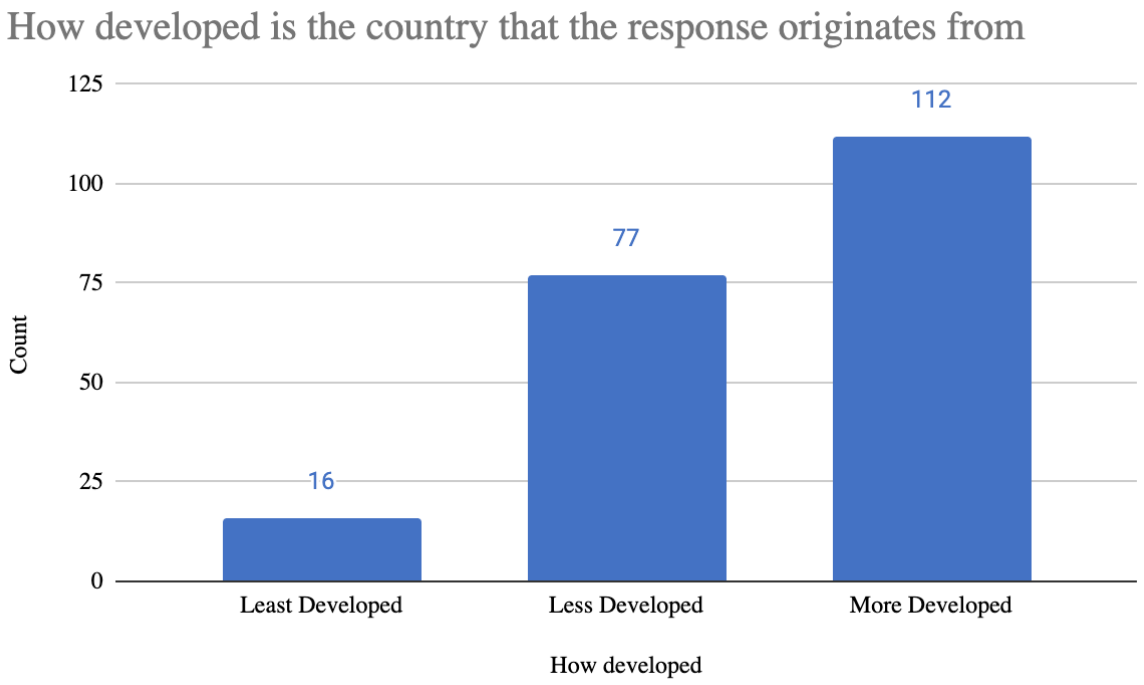
ANNEX A

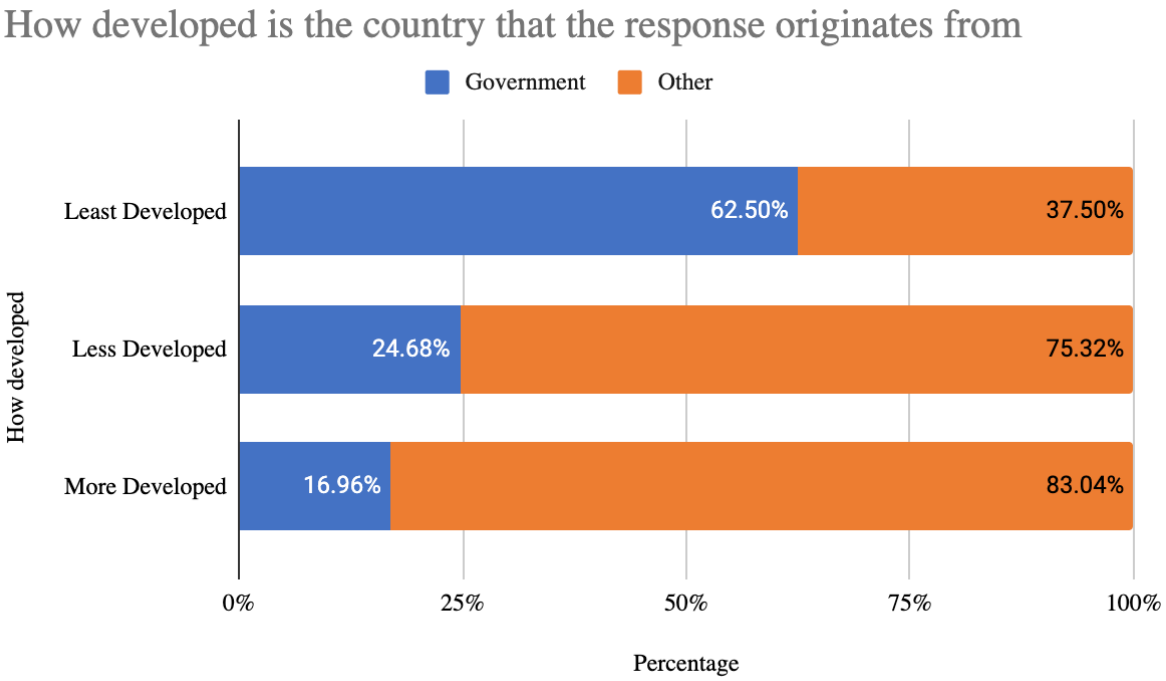
Responses to the survey



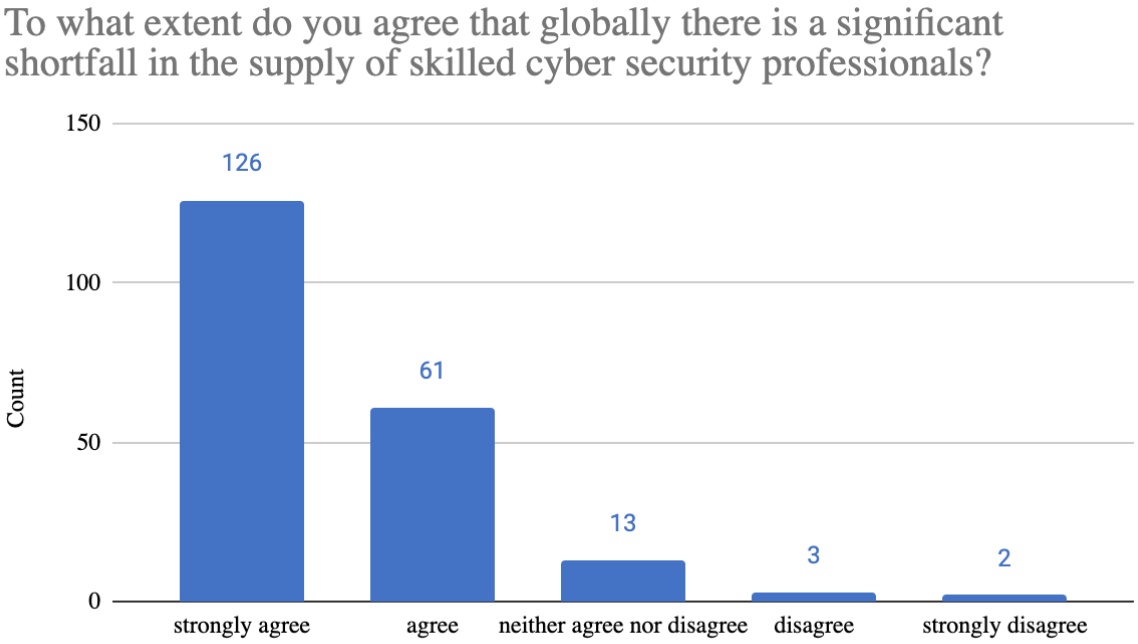



Proportion of responses by region
South America and the Caribbean
6.3%
Africa
21.0%
North America
25.4%
Asia / Pacific
21.5%
Europe
25.9%

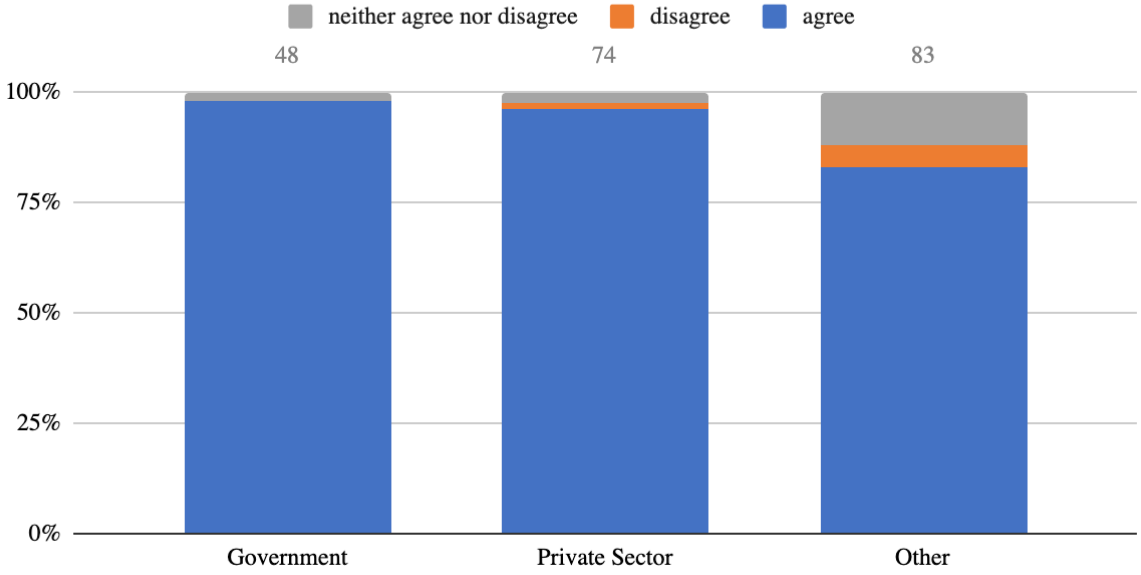

How developed is the country that the response originates from
125
100
75
50
25
0
Count
16
77
112
Least Developed
Less Developed
More Developed
How developed


How developed is the country that the response originates from
Government
Other
Least Developed
Less Developed
More Developed
62.50%
37.50%
24.68%
75.32%
16.96%
83.04%
How developed
0%
25%
50%
75%
100%
Percentage

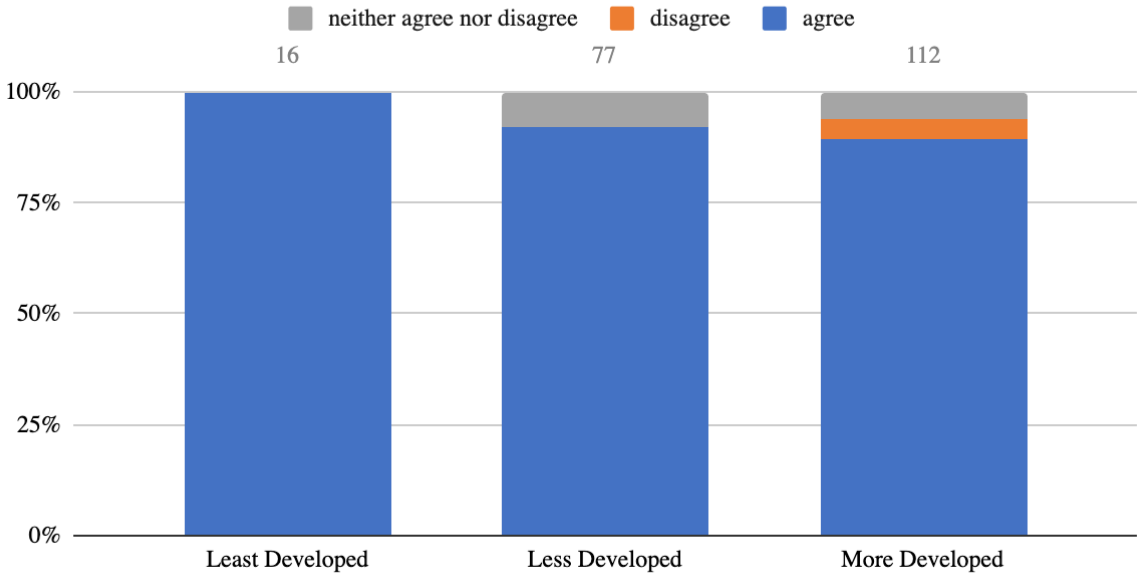
Q4)


To what extent do you agree that globally there is a significant shortfall in the supply of skilled cyber security professionals?
150
100
50
0
Count
126
61
13
3
2
strongly agree
agree
neither agree nor disagree
disagree
strongly disagree

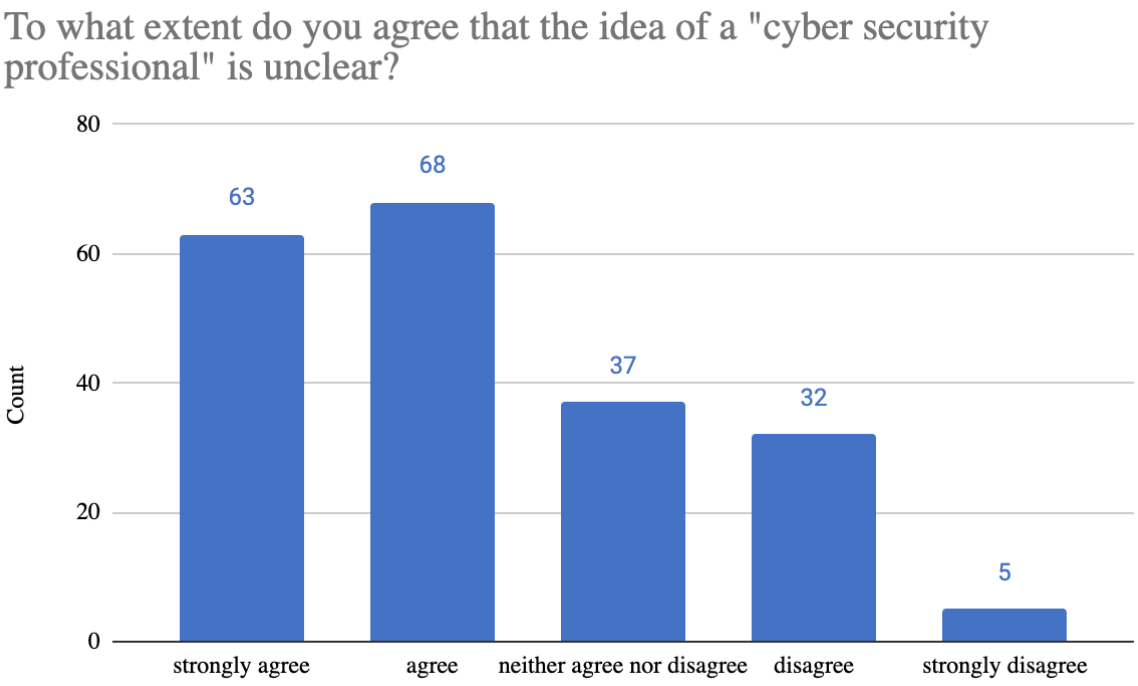
To what extent do you agree that globally there is a significant shortfall in the supply of skilled cyber security professionals?

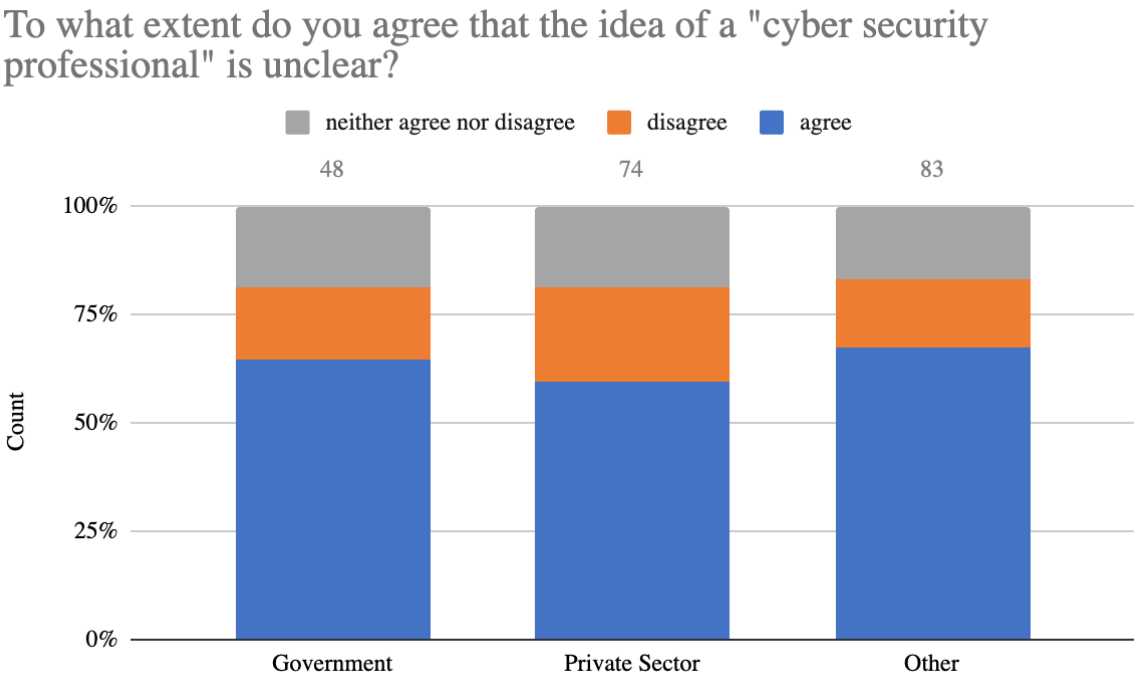


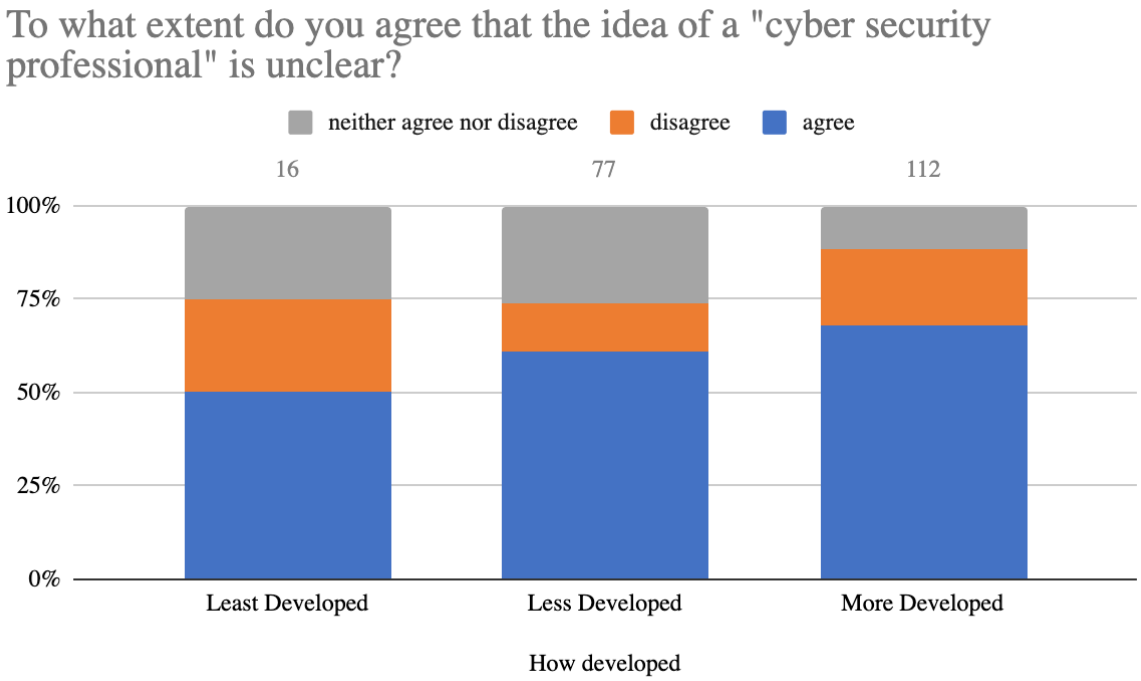
To what extent do you agree that globally there is a significant shortfall in the supply of skilled cyber security professionals?



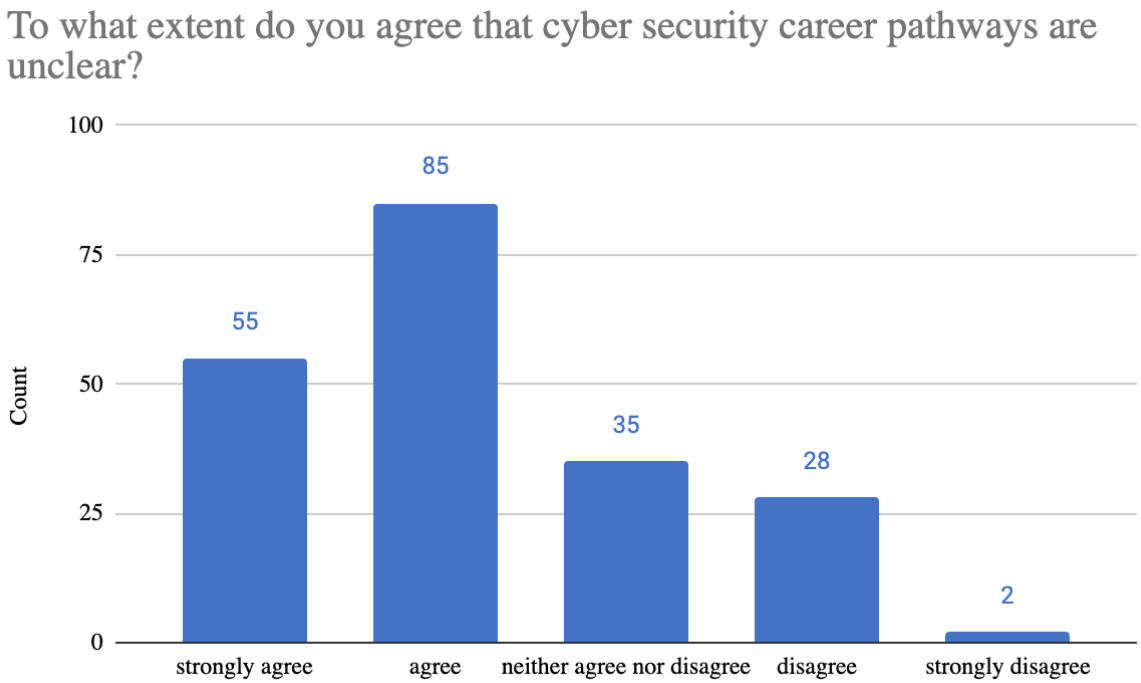
Q5)


To what extent do you agree that the idea of a "cyber security professional" is unclear?
Count
80
60
40
20
0
63
68
37
32
5
strongly agree
agree
neither agree nor disagree
disagree
strongly disagree

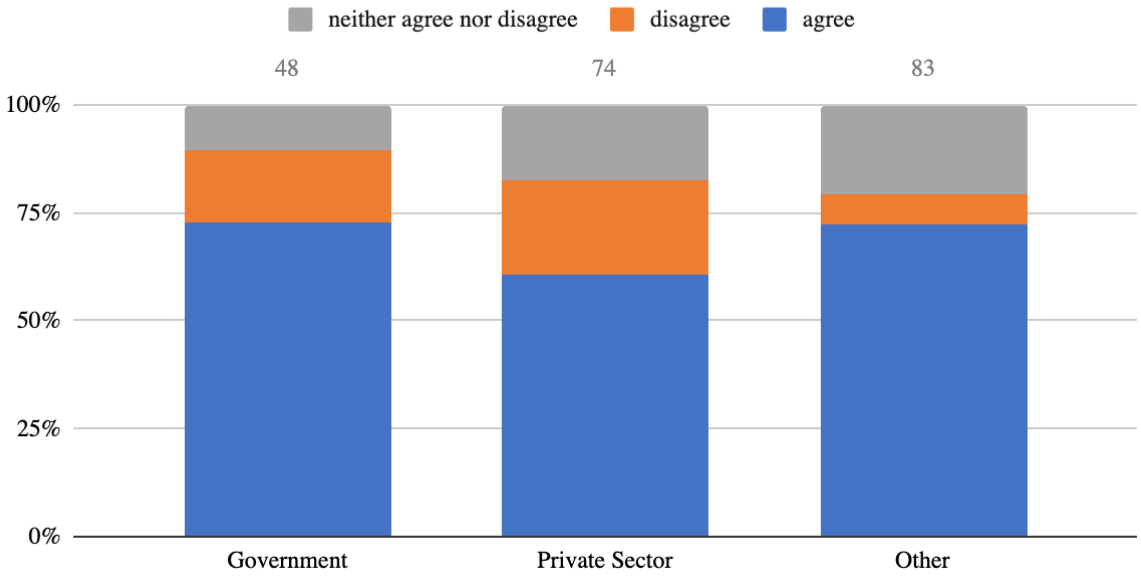

To what extent do you agree that the idea of a "cyber security professional" is unclear?
neither agree nor disagree
disagree
agree
48
74
83
Count
100%
75%
50%
25%
0%
Government
Private Sector
Other


To what extent do you agree that the idea of a "cyber security professional" is unclear?
neither agree nor disagree
disagree
agree
16
77
112
100%
75%
50%
25%
0%
Least Developed
Less Developed
More Developed
How developed

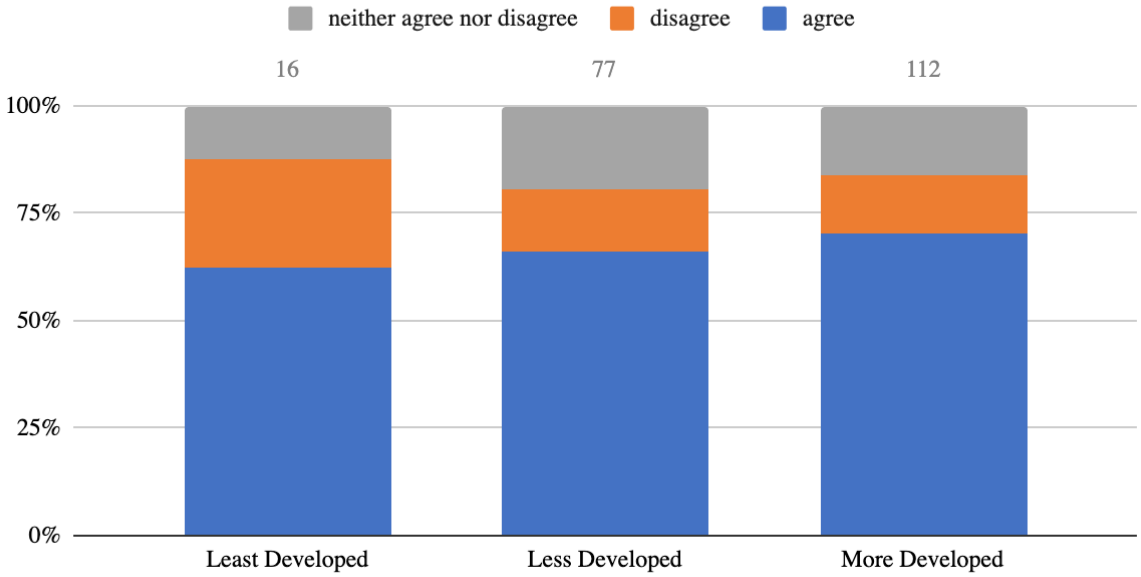
Q6)


To what extent do you agree that cyber security career pathways are unclear?
100
75
50
25
0
Count
55
85
35
28
2
strongly agree
agree
neither agree nor disagree
disagree
strongly disagree

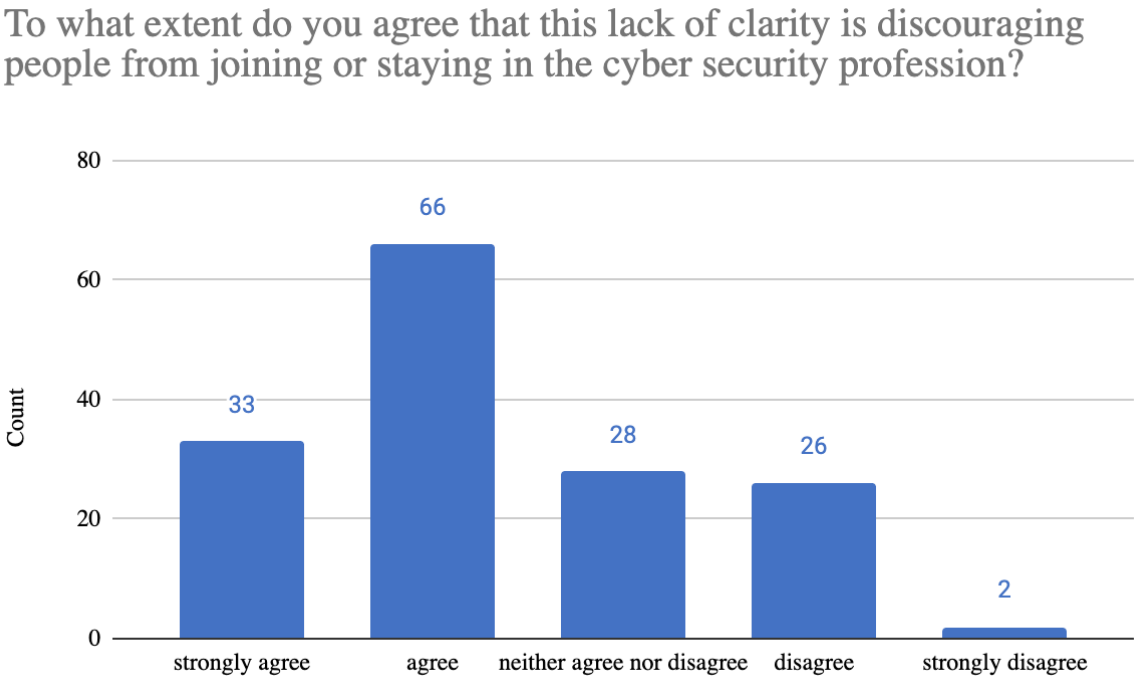
To what extent do you agree that cyber security career pathways are unclear?

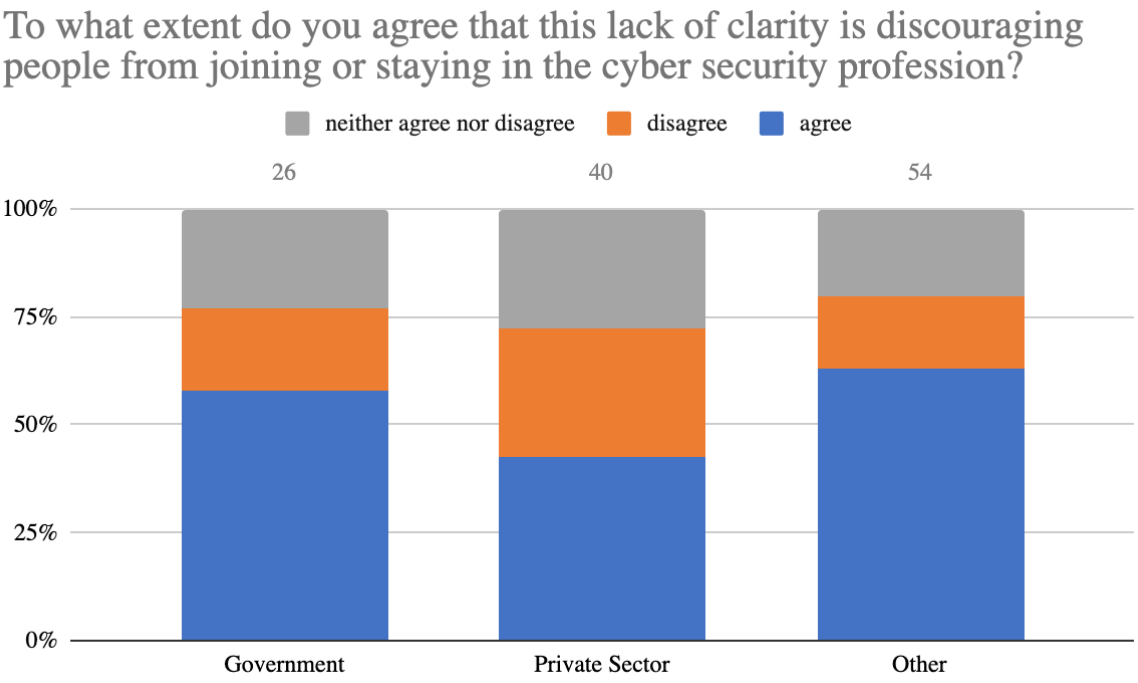


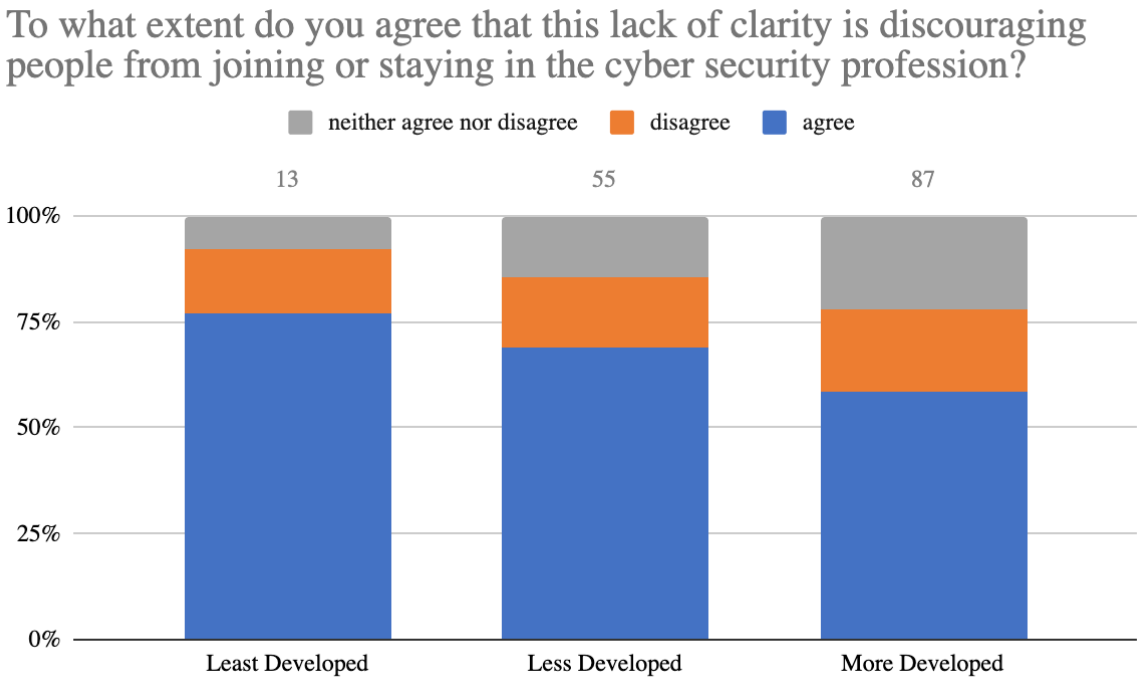
To what extent do you agree that cyber security career pathways are unclear?



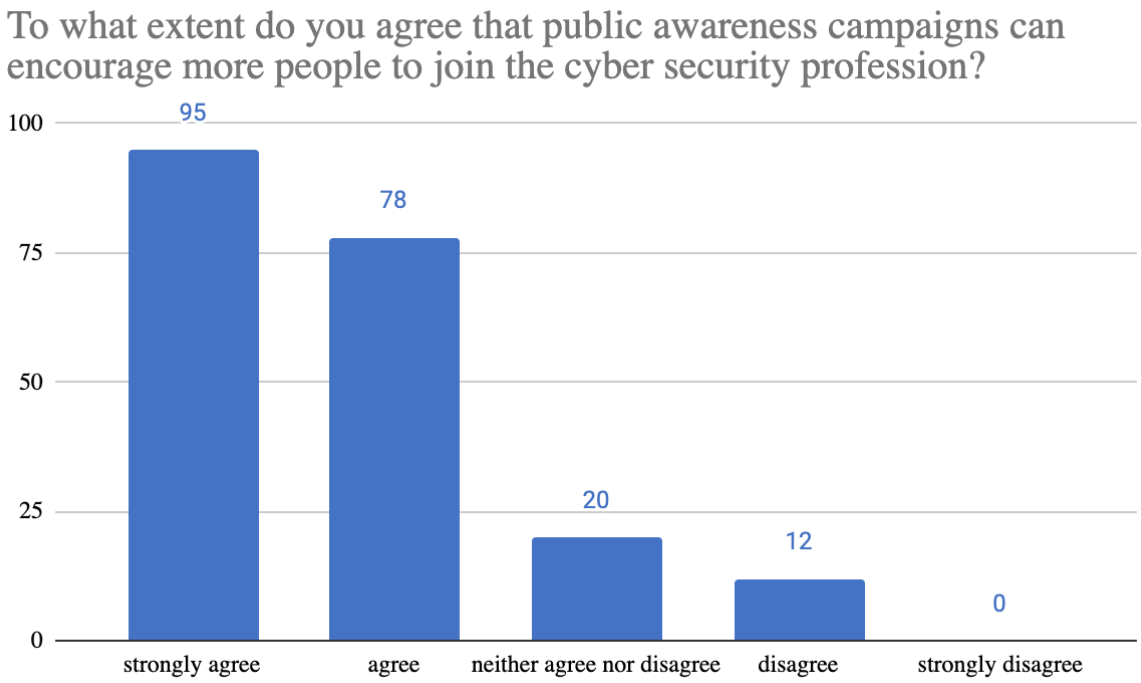
Q6.1)


To what extent do you agree that this lack of clarity is discouraging people from joining or staying in the cyber security profession?
Count
80
60
40
20
0
33
66
28
26
2
strongly agree
agree
neither agree nor disagree
disagree
strongly disagree

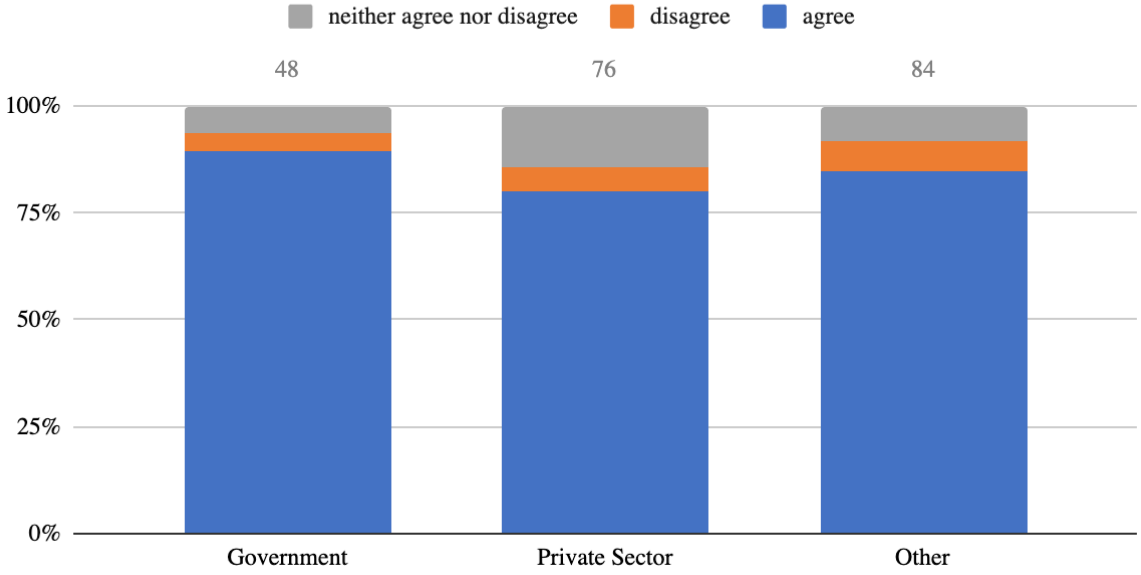

To what extent do you agree that this lack of clarity is discouraging people from joining or staying in the cyber security profession?
neither agree nor disagree
disagree
agree
26
40
54
100%
75%
50%
25%
0%
Government
Private Sector
Other


To what extent do you agree that this lack of clarity is discouraging people from joining or staying in the cyber security profession?
neither agree nor disagree
disagree
agree
13
55
87
100%
75%
50%
25%
0%
Least Developed
Less Developed
More Developed

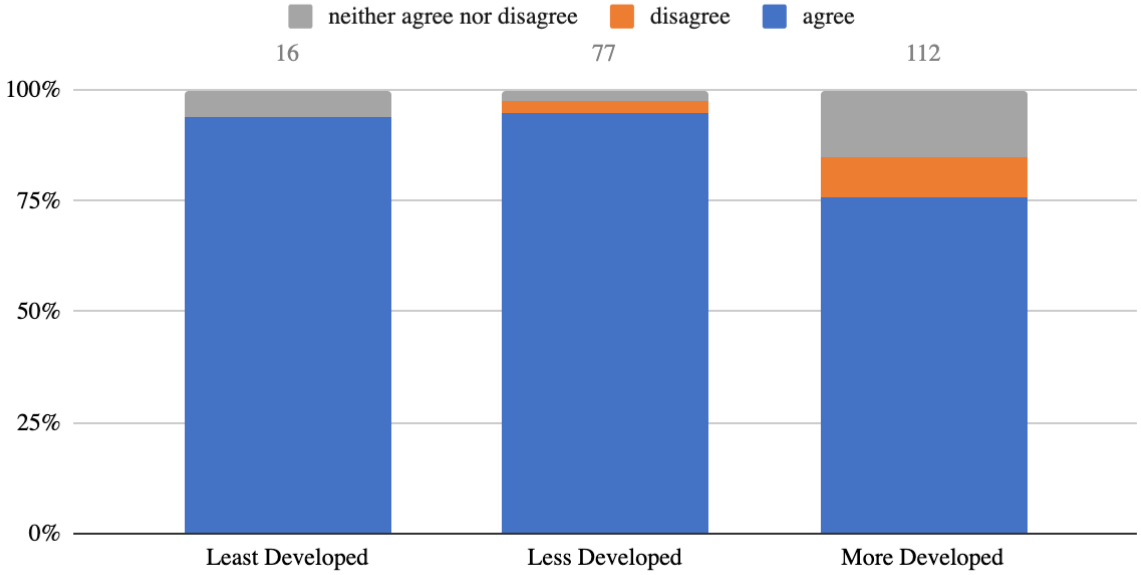
Q7)


To what extent do you agree that public awareness campaigns can encourage more people to join the cyber security profession?
100
75
50
25
0
95
78
20
12
0
strongly agree
agree
neither agree nor disagree
disagree
strongly disagree

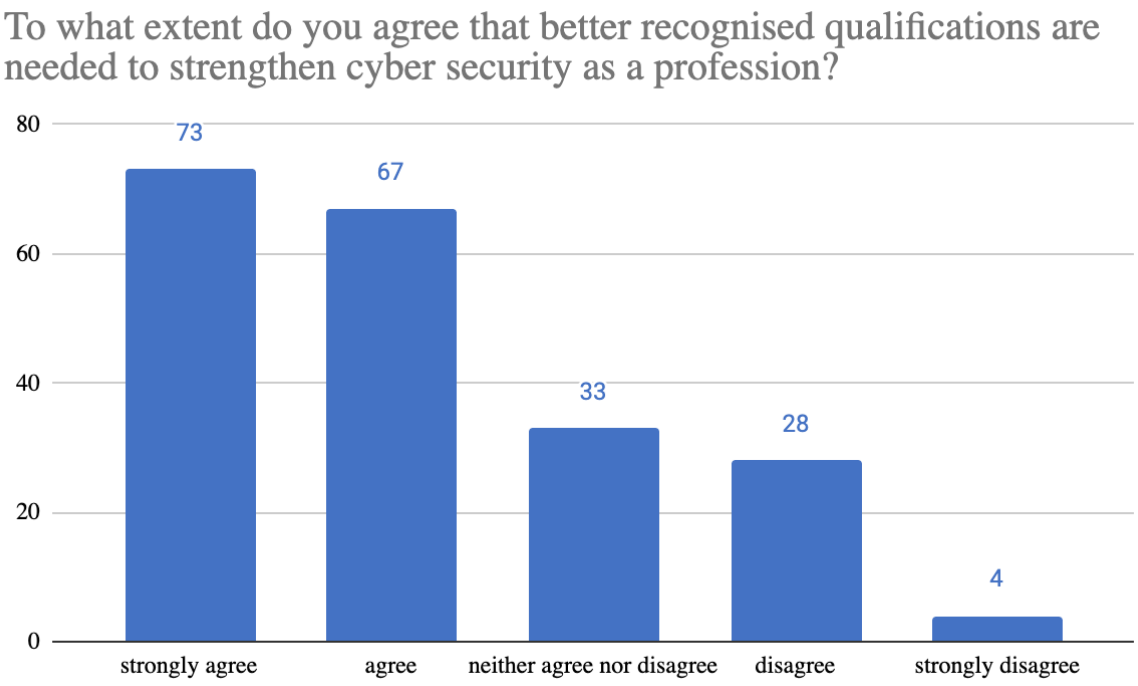
To what extent do you agree that public awareness campaigns can encourage more people to join the cyber security profession?

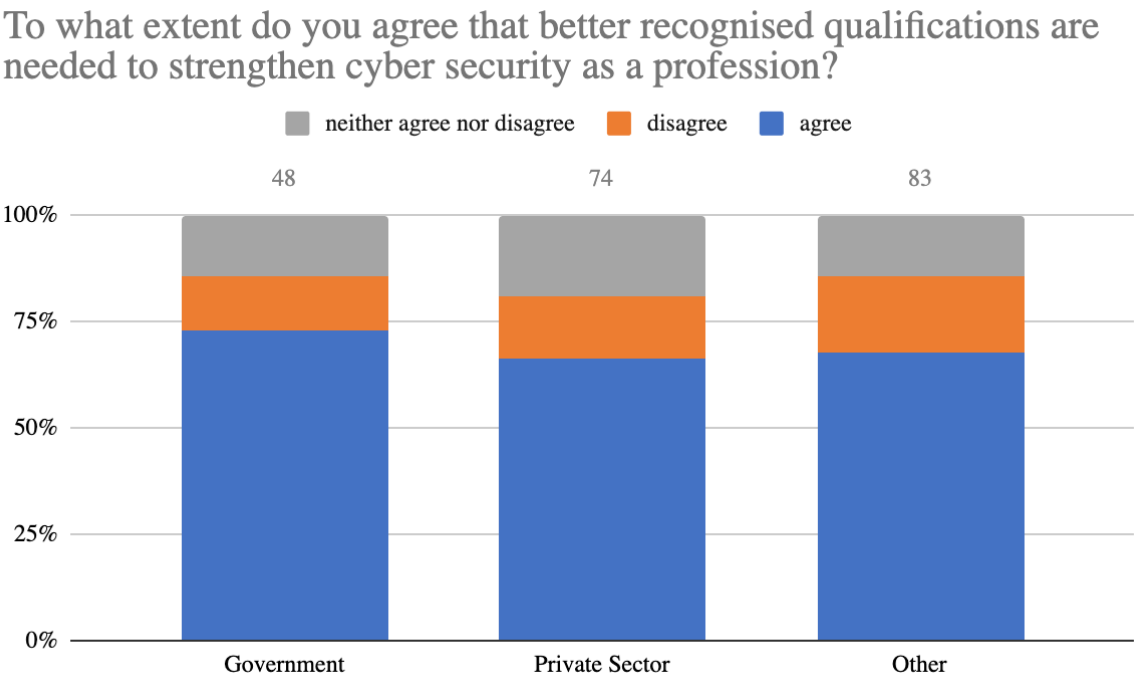


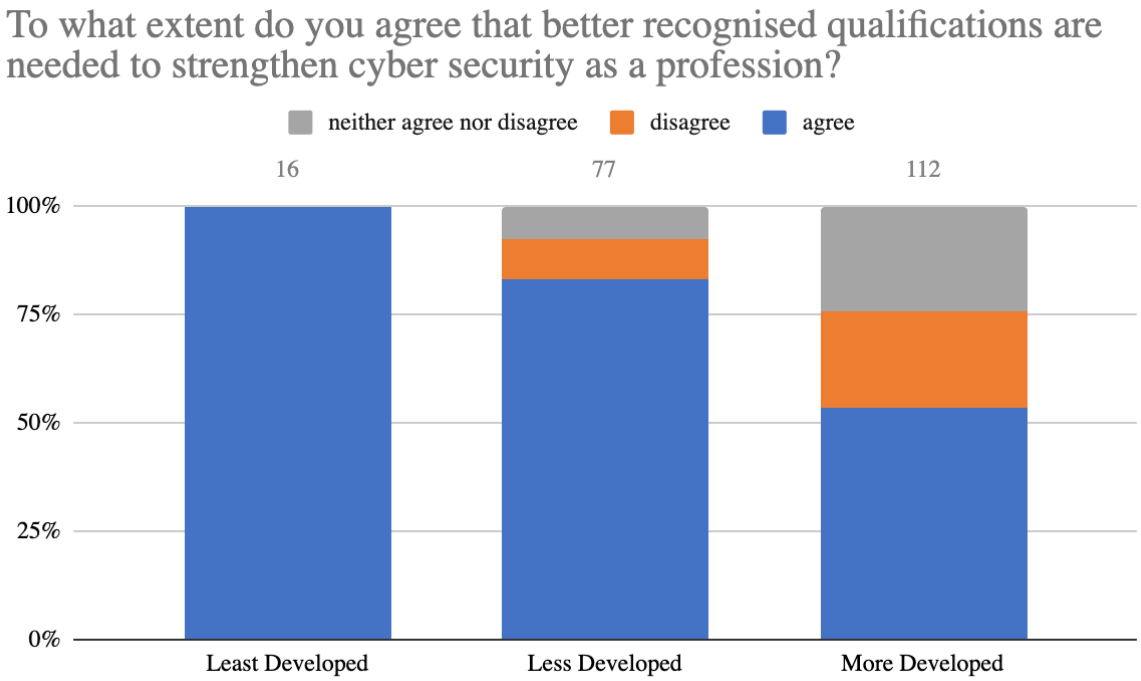
To what extent do you agree that public awareness campaigns can encourage more people to join the cyber security profession?



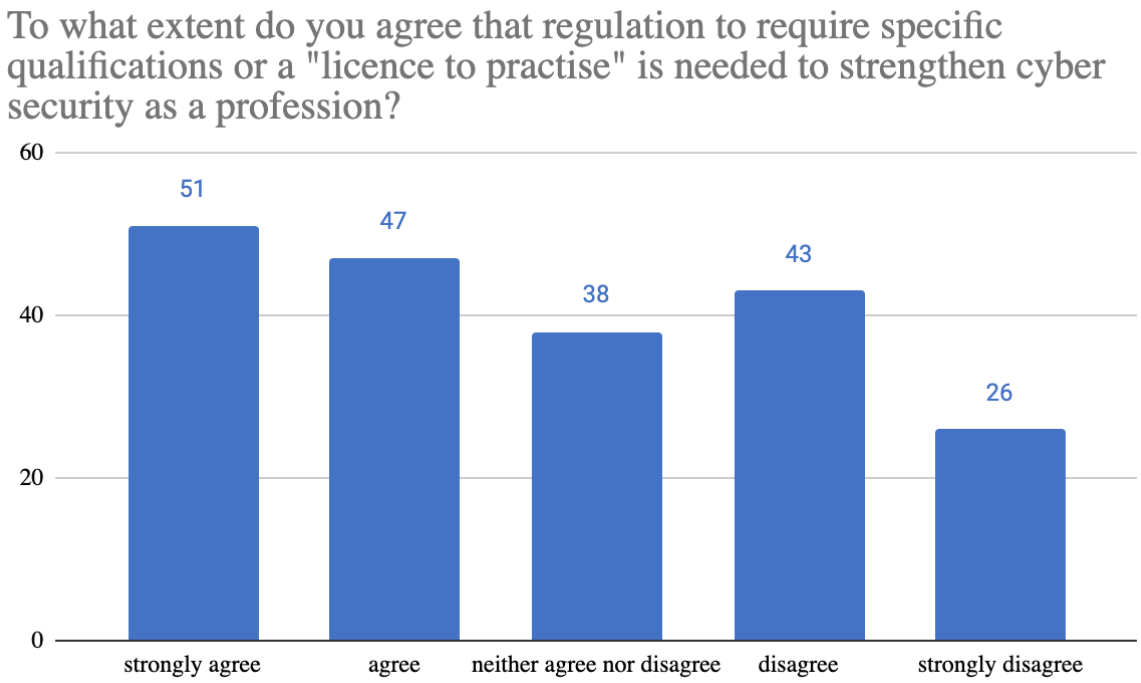
Q8)


To what extent do you agree that better recognised qualifications are needed to strengthen cyber security as a profession?
80
60
40
20
0
73
67
33
28
4
strongly agree
agree
neither agree nor disagree
disagree
strongly disagree

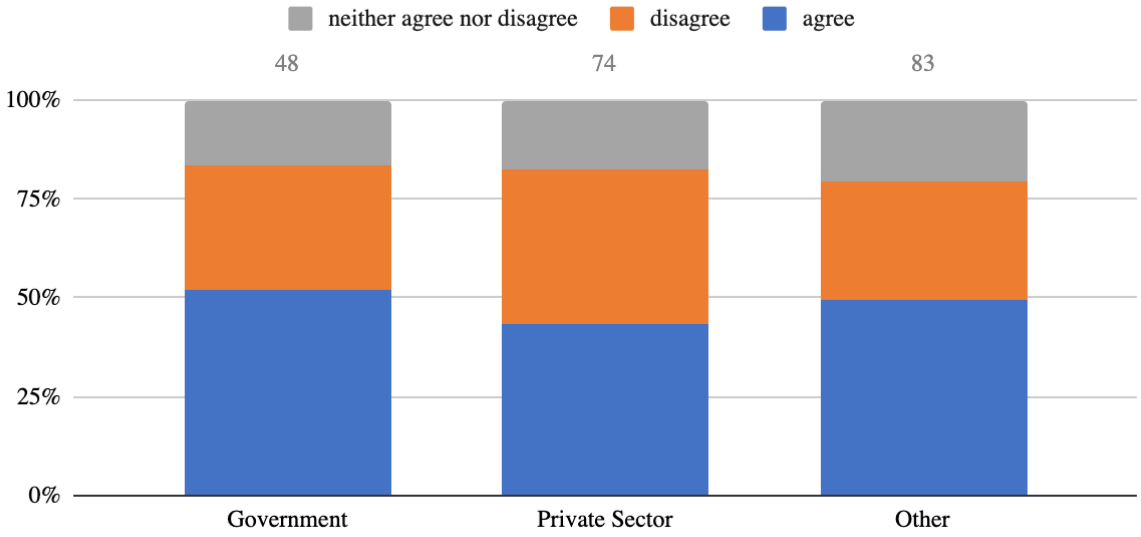

To what extent do you agree that better recognised qualifications are needed to strengthen cyber security as a profession?
neither agree nor disagree
disagree
agree
48
74
83
100%
75%
50%
25%
0%
Government
Private Sector
Other


To what extent do you agree that better recognised qualifications are needed to strengthen cyber security as a profession?
neither agree nor disagree
disagree
agree
16
77
112
100%
75%
50%
25%
0%
Least Developed
Less Developed
More Developed

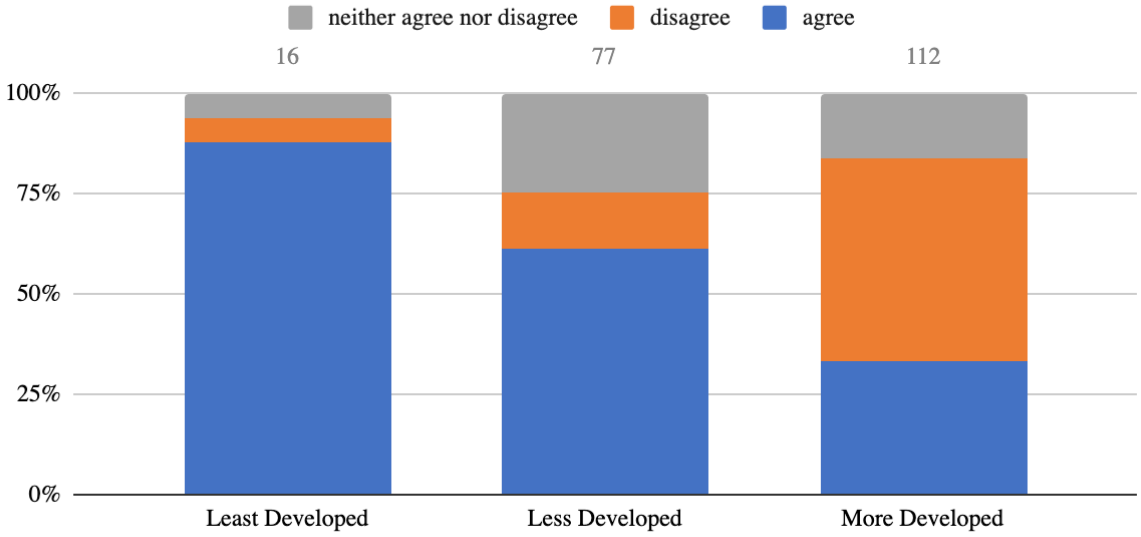
Q9)


To what extent do you agree that regulation to require specific qualifications or a "licence to practise" is needed to strengthen cyber security as a profession?
60
40
20
0
51
47
38
43
26
strongly agree
agree
neither agree nor disagree
disagree
strongly disagree

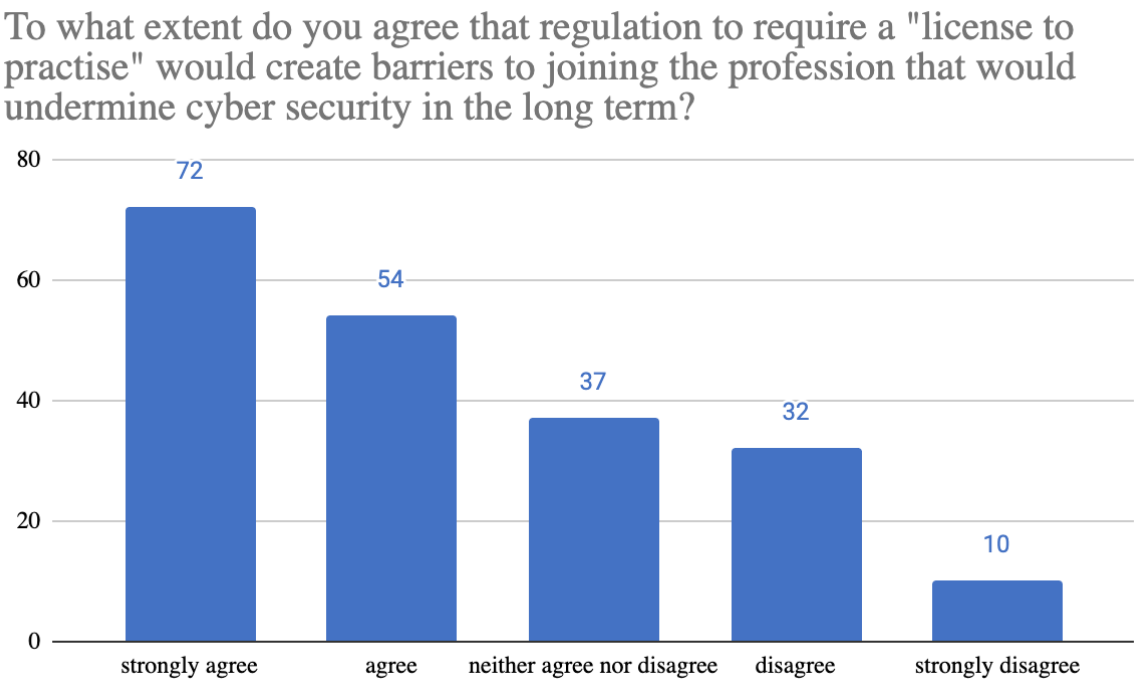
To what extent do you agree that regulation to require specific qualifications or a "licence to practise" is needed to strengthen cyber security as a profession?

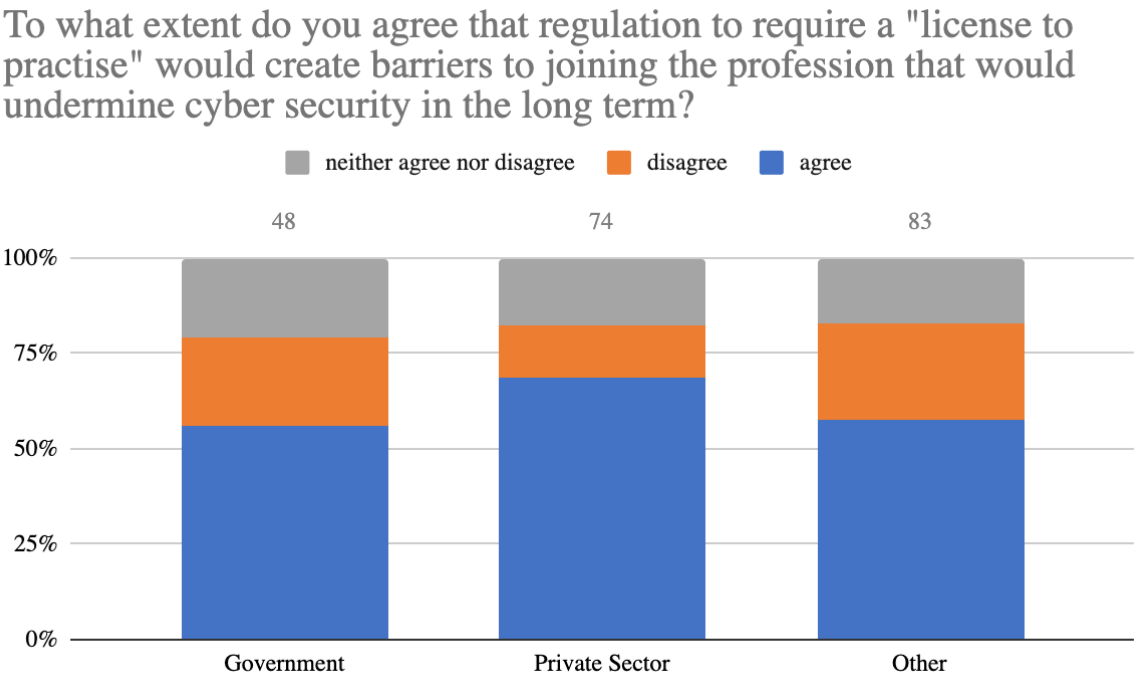


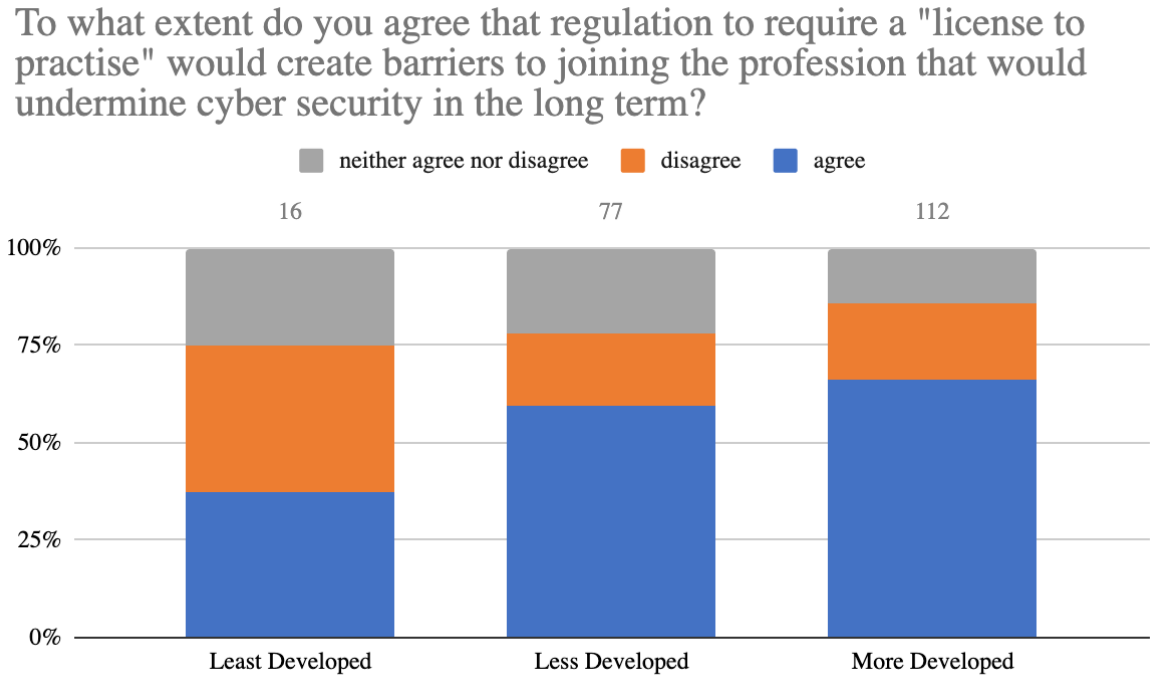
To what extent do you agree that regulation to require specific qualifications or a "licence to practise" is needed to strengthen cyber security as a profession?



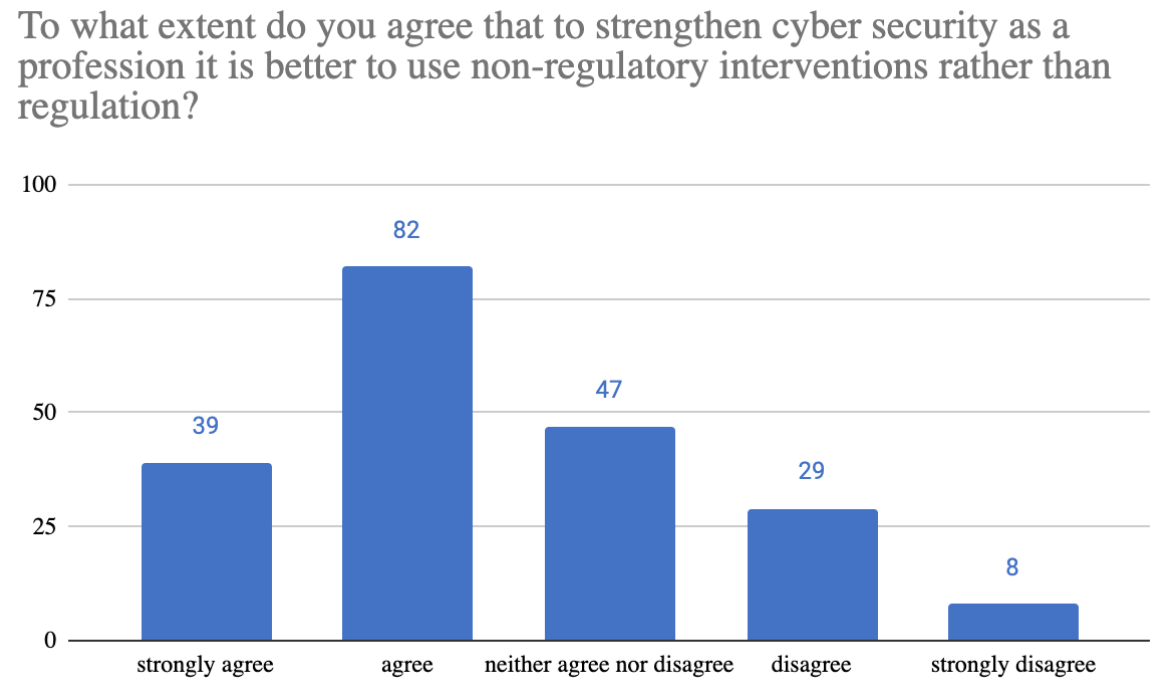
Q10)


To what extent do you agree that regulation to require a "license to practise" would create barriers to joining the profession that would undermine cyber security in the long term?
80
60
40
20
0
72
54
37
32
10
strongly agree
agree
neither agree nor disagree
disagree
strongly disagree

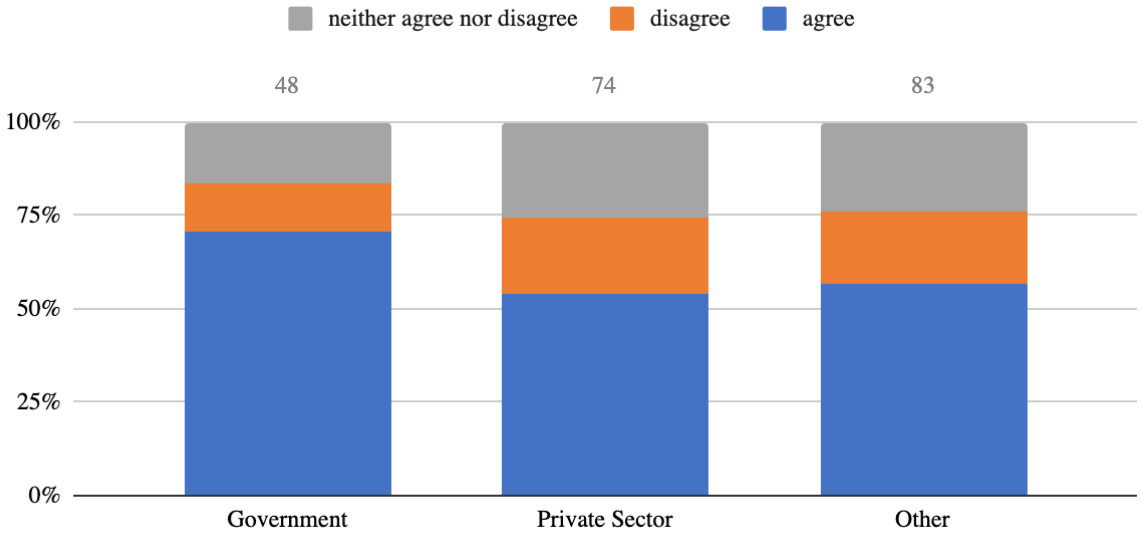

To what extent do you agree that regulation to require a "license to practise" would create barriers to joining the profession that would undermine cyber security in the long term?
neither agree nor disagree
disagree
agree
48
74
83
100%
75%
50%
25%
0%
Government
Private Sector
Other


To what extent do you agree that regulation to require a "license to practise" would create barriers to joining the profession that would undermine cyber security in the long term?
neither agree nor disagree
disagree
agree
16
77
112
100%
75%
50%
25%
0%
Least Developed
Less Developed
More Developed

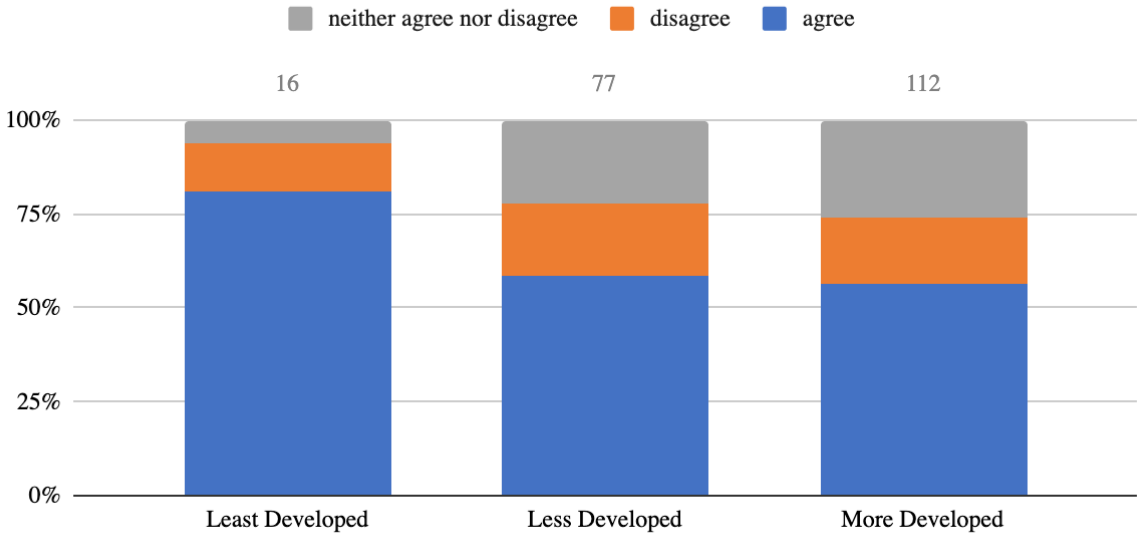
Q11)


To what extent do you agree that to strengthen cyber security as a profession it is better to use non-regulatory interventions rather than regulation?
100
75
50
25
0
39
82
47
29
8
strongly agree
agree
neither agree nor disagree
disagree
strongly disagree

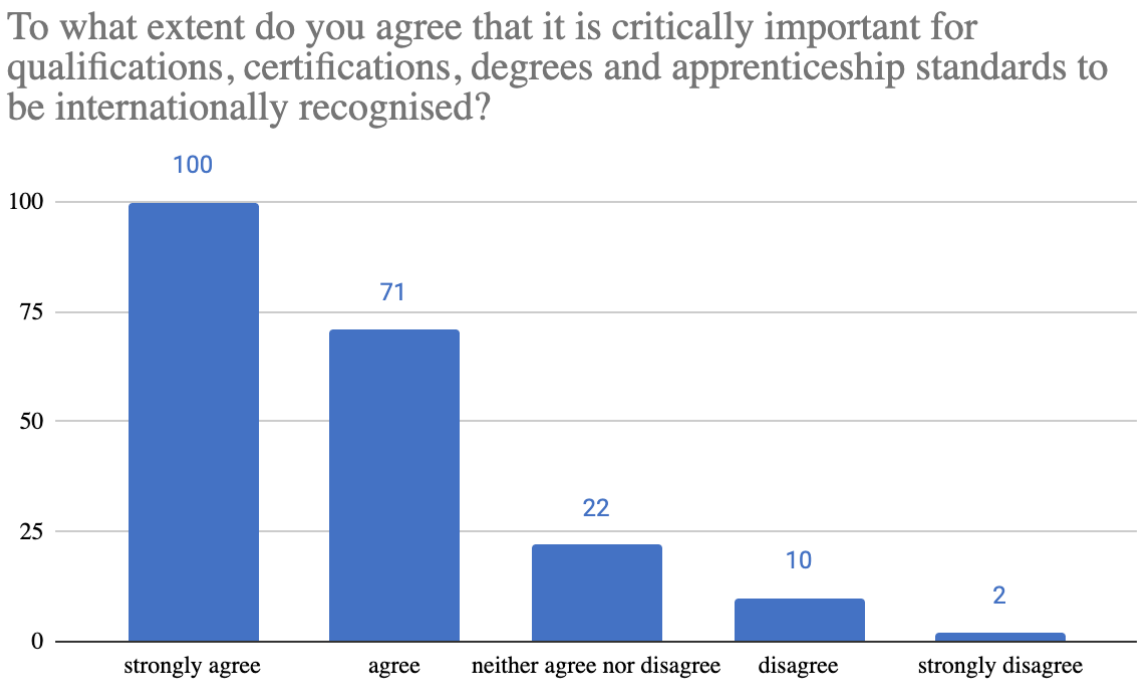
To what extent do you agree that to strengthen cyber security as a profession it is better to use non-regulatory interventions rather than regulation?

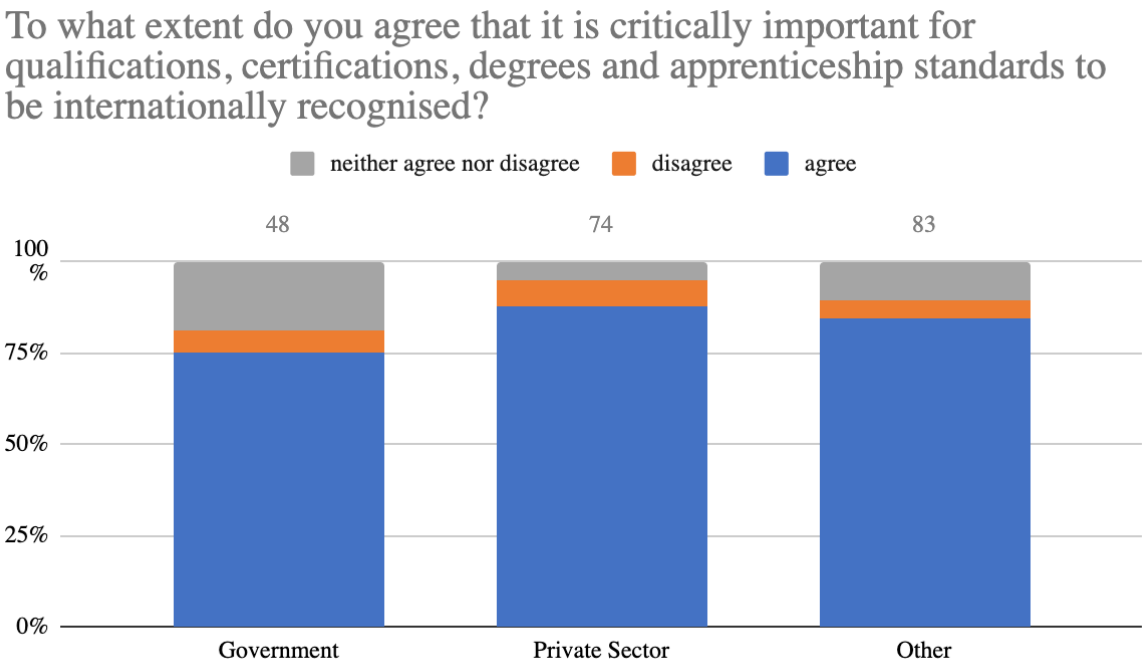


To what extent do you agree that to strengthen cyber security as a profession it is better to use non-regulatory interventions rather than regulation?



Q13)


To what extent do you agree that it is critically important for qualifications, certifications, degrees and apprenticeship standards to be internationally recognised?
100
71
22
10
2
100
75
50
25
0
strongly agree
agree
neither agree nor disagree
disagree
strongly disagree


To what extent do you agree that it is critically important for qualifications, certifications, degrees and apprenticeship standards to be internationally recognised?
neither agree nor disagree
disagree
agree
48
74
83
100 %
75%
50%
25%
0%
Government
Private Sector
Other

To what extent do you agree that it is critically important for qualifications, certifications, degrees and apprenticeship standards to be internationally recognised?