hackerone

March 19, 2022

SUBMITTED VIA E-MAIL

Re: Open Consultation on Embedding Standards and Pathways Across the Cyber Profession by 2025

Dear Minister Lopez:

HackerOne Inc. ("HackerOne") submits this letter in response to the Open Consultation on Embedding Standards and Pathways Across the Cyber Profession by 2025 ("Open Consultation") issued by the Department for Digital, Culture, Media & Sport's ("Department"). We also attached an appendix with answers to many of the Department's specific questions in the Open Consultation.

HackerOne is the market leading hacker-powered security platform, helping organisations find and fix critical vulnerabilities before they can be exploited. HackerOne is headquartered in San Francisco, California with offices in London and the Netherlands. HackerOne is proud to work with the National Cyber Security Centre ("NCSC") on its vulnerability disclosure policies ("VDP"), as well as with over 40,000 UK-based security researchers who, through their individual contributions, collectively make the internet safer.

As the champion of a global community of security researchers, HackerOne does not support establishing requirements for a formal nation-wide UK certification pathway for individuals in the cybersecurity field. Our community of over one million security researchers provide real world evidence that possessing a formal certification is unrelated to a security professional's ability to positively contribute to the industry. Furthermore, the act of requiring a certification for security talent would be an unnecessary barrier to entry for new and even current UK security talent.

As a part of our representation of the HackerOne community, we release an annual Hacker Report as a collection of responses and inputs from the community. To support the claim that formal qualifications do not define security capabilities, out of our community only "37% of hackers have studied computer science at a post graduate level and 20% hold post graduate qualifications in computer science" (HackerOne, 2021). Despite many Hacker Report respondents not maintaining a technical or advanced degree in security, their ability to help secure the internet has not been hampered; over 200,000 vulnerabilities submitted in the last 12 months to organisations across the globe would confirm that.

It is our belief that instead of legislating a cumbersome certification process and registration, the security community in the UK would instead benefit from increased opportunity and access to

Department for Digital, Culture, Media, and Sport. (2022, 01 19). Retrieved from https://www.gov.uk/government/consultations/embedding-standards-and-pathways-across-the-cyber-profession-by-2025/embedding-standards-and-pathways-across-the-cyber-profession-by-2025#fn:8

HackerOne. (2021). *The 2021 Hacker Report.*

affordable security training. Often, formal certification bodies are not capable of keeping up with advancements in the industry, so instead the emphasis on security training should be built on real world security experience, with participation in Vulnerability Disclosure Programs and Bug Bounty programs as one example. Programs like these provide low barrier avenues for individuals to get hands-on experience in security and participation should be a critical component of any voluntary certification process implemented. Within our own security research community, "47% of the community actively participates in VDPs. Furthermore, 51% of those who hack VDPs do so out of a sense of responsibility, [and] 79% do it to learn..." (HackerOne, 2021), this is a clear indication of the value of hands-on learning for security professionals and contributors. When it comes to Bug Bounty participation, which operates in a similar fashion to a VDP, "85% of [the security community] are also doing it to learn and expand their skill sets and 62% do it to advance their careers." (HackerOne, 2021) Security professionals are already using these channels to improve their hands-on capabilities and it would be in the best interest of any voluntary certification program implemented to emphasise learning through these channels.

In summary, we believe that legislating a requirement for cyber talent of the UK to attain a single designated cybersecurity certification path would have the adverse impact of what the Department is hoping to achieve with this proposal. Instead, it would have the overwhelming potential to cripple the diversity of the security community in the UK. To prevent that from happening, we encourage the Department to consider a voluntary certification path available to all UK security talent.

*   *   *

We appreciate the opportunity to provide these comments in response to the Department's Open Consultation. Please do not hesitate to contact us for further information or if we may otherwise be of assistance.

Sincerely,

Kayla Underkoffler

Kayla Underkoffler
Senior Security Technologist
HackerOne

APPENDIX

HACKERONE ANSWERS TO SELECT CALL FOR VIEWS QUESTIONS

Below are our responses to certain questions within the Call for Views.

Question 1. *To what extent do you agree or disagree, ranging from fully agree to fully disagree, that the market is best placed to define and embed professional standards?*

- [✓ Fully agree]
- Mostly agree
- Neither agree nor disagree
- Mostly disagree
- Fully disagree
- Do not know

Question 2. *To what extent do you agree or disagree, ranging from fully agree to fully disagree, that government intervention is required to support this approach?*

- Fully agree
- Mostly agree
- Neither agree nor disagree
- [✓ Mostly disagree]
- Fully disagree
- Do not know

Question 2a. *[If mostly or fully disagree] Please expand on the reasons for this response. [Open-ended question]*

It is important for the government to prioritise paths and certifications that are most critical for the success of the field, but this should be done through guidance, not legislation.

Question 3. *To what extent do you agree or disagree, ranging from fully agree to fully disagree, with the proposal that the UK Cyber Security Council should be formally recognised (via* *legislation) as the standard setting body for the cyber profession with a view to it overseeing the regulation of the profession under a legislative scheme?*

- Fully agree
- Mostly agree
- Neither agree nor disagree
- [✓ Mostly disagree]
- Fully disagree
- Do not know

Question 3a*. [If mostly or fully disagree] Please expand on the reasons for this response? [Open-ended question]*

Officially making the UK Cyber Security Council responsible for providing guidance around the certifications most recommended would be a better fit.

Question 4*. To what extent do you agree or disagree, ranging from fully agree to fully disagree, that regulating by activity should be explored in future plans?*

- Fully agree
- Mostly agree
- Neither agree nor disagree
- Mostly disagree
- [✓ Fully disagree]
- Do not know

Question 5*. To what extent do you agree or disagree, ranging from fully agree to fully disagree, that under-qualified professionals should be prohibited from carrying out activities related to a specialism until they are qualified to do so?*

- Fully agree
- Mostly agree
- Neither agree nor disagree
- Mostly disagree

- [✓ Fully disagree]
- Do not know

Question 6*. To what extent do you agree or disagree, ranging from fully agree to fully disagree, that role definitions across cyber security functions are inconsistently defined and require consolidation?*

- Fully agree
- [✓ Mostly agree]
- Neither agree nor disagree
- Mostly disagree
- Fully disagree
- Do not know

Question *7. Do you think there are any additional considerations that need to be examined to ensure that the proposed measures to regulate professional job titles do not provide unnecessary barriers to entry for candidates entering or wishing to progress in a cyber security career?*

- [✓ Yes]
- No
- Do not know

Question ***7a.*** *[If yes] what additional measures should be considered? [Open-ended question]*

Cost. Both in time to acquire certifications and enter the workforce and in financial capital needed to purchase access to certifications. Time needed for ongoing training and recertifications. Ensuring open access to training for all.

Question 8*. To what extent do you agree or disagree, ranging from fully agree to fully disagree, that the profession should regulate the use of professional job titles?*

- Fully agree
- Mostly agree
- Neither agree nor disagree

- Mostly disagree
- [✓ Fully disagree]
- Do not know

Question 9*. To what extent do you agree or disagree, ranging from fully agree to fully disagree, that individuals should have to meet particular competency standards set by the UK Cyber Security Council in order to utilise a specific job title?*

- Fully agree
- Mostly agree
- Neither agree nor disagree
- Mostly disagree
- [✓ Fully disagree]
- Do not know

Question 10*. To what extent do you agree or disagree, ranging from fully agree to fully disagree, that statutory regulation on the use of title will not significantly exacerbate the existing skills shortage across cyber security roles in the UK?*

- Fully agree
- Mostly agree
- Neither agree nor disagree
- Mostly disagree
- [✓ Fully disagree]
- Do not know

Question 20*. To what extent do you agree or disagree, ranging from fully agree to fully disagree, that there should be a centrally-held Register of Practitioners for the cyber profession?*

- Fully agree
- Mostly agree
- Neither agree nor disagree
- Mostly disagree

- [✓ Fully disagree]
- Do not know

Question 22*. To what extent do you agree or disagree, ranging from fully agree to fully disagree, that employers should not be legally required to employ practitioners whose titles have been recognised through the UK Cyber Security Council?*

- [✓ Fully agree]
- Mostly agree
- Neither agree nor disagree
- Mostly disagree
- Fully disagree
- Do not know

Question 23*. Do you consider there to be any perceived risks or overlaps with existing legislative arrangements, particularly in devolved nations?*

- [✓ Yes]
- No
- Do not know

Question 23a*. [If yes] In what areas do you think there would be perceived risks or overlaps with existing legislative arrangements?*

This has a potential chilling effect on information sharing and sharing of security talent from other nations. Namely in vulnerability disclosure.

Question 24*. To what extent would it be helpful or unhelpful, ranging from very helpful to very unhelpful, to explore introducing public procurement routes to embed competency requirements for the market, as it relates to cyber professionals?*

- [✓ Very helpful]
- Slightly helpful
- Neither helpful nor unhelpful

- Slightly unhelpful
- Very unhelpful
- Do not know

Question 26. *Should the government and/or the UK Cyber Security Council continue to explore the creation of a further voluntary certification scheme that is aligned to existing programmes?*

- [✓ Yes]
- No
- Do not know

Question 27. *To what extent do you think it would be helpful or unhelpful, ranging from very helpful to very unhelpful, for Cyber Essentials and CCP to align their requirements with any future professional standards that may be set by the UK Cyber Security Council?*

- Very helpful
- [✓ Slightly helpful]
- Neither helpful nor unhelpful
- Slightly unhelpful
- Very unhelpful
- Do not know

Question 28. *In addition to the proposals mentioned in the document above, what more could be done to further support cyber security professionals and the policy ambition to embed standards and pathways within the profession?*

Increase in accessible and affordable security training for all persons interested in cybersecurity, with a critical emphasis on hands on learning (i.e., Vulnerability Disclosure Program (VDP), Bug Bounty programs, Hacktivity, Capture the Flag programs (CTF))

Question 29. *Do you consider there to be additional considerations required to ensure that these proposed measures will not provide unnecessary additional barriers to entry for candidates to enter and progress a career in cyber security?*

- [✓ Yes]

- No
- Do not know

Question 29a*. [If yes] what additional measures could be considered?*

Emphasising the importance that all the certifications and training programs would be voluntary and accessible and affordable to all who are interested in learning more about security and increasing their security talent.