hackerone

6 April 2023

SUBMITTED VIA E-MAIL

Cyber Policy Unit
Homeland Security Group
Home Office
5th Floor, Peel Building
2 Marsham Street
London
SW1P 4DF

Re: Review of the Computer Misuse Act 1990: consultation and response to call for information

Dear Rt Hon Tom Tugendhat MBE VR MP:

HackerOne Inc. ("HackerOne") respectfully submits this letter in response to the open consultation on the review of the Computer Misuse Act 1990 ("CMA").[1] We commend the UK Government's commitment to reviewing the 30-year-old legislation with a keen eye toward meeting the future needs of UK law enforcement, citizens, businesses, and security researchers.

HackerOne is the world's most trusted hacker-powered security platform, connecting organizations to the largest community of hackers on the planet to find and safely report security weaknesses across attack surfaces. HackerOne was started by hackers and security leaders who are driven by a passion to make the internet safer. We partner with the global hacker community to surface the most relevant security issues of our customers before they can be exploited by criminals. HackerOne is headquartered in San Francisco with offices in London, and the Netherlands. In the UK, HackerOne works with entities in the public and private sectors such as Costa Coffee, Starling Bank, and the National Cyber Security Centre ("NCSC"). The ethical hacking community in the UK has generally ranked among the largest in the world, often only behind countries with larger population like the USA and India.

As a champion for the security community at large, HackerOne strongly recommends that any CMA update address the restrictions this legislation currently places on legitimate third-party security researchers and the act of finding and reporting vulnerabilities in good faith. The revision of the CMA should make it clear and unquestionable that the operation of a VDP, and the act of reporting a vulnerability through that VDP, is a sanctioned and encouraged practice that does not conflict with the purpose and intent of the CMA. In essence, VDPs should become the de facto channel for security researchers to communicate vulnerabilities and security gaps to organizations. HackerOne encourages the Home Office to incorporate and legitimize VDPs through the CMA

[1] *Review of the Computer Misuse Act 1990: consultation and response to call for information (accessible)*, HOME OFFICE (7 February 2023), *available at* https://www.gov.uk/government/consultations/review-of-the-computer-misuse-act-1990/review-of-the-computer-misuse-act-1990-consultation-and-response-to-call-for-information-accessible#ministerial-foreword.

legislation as the single best channel for responsible reporting of vulnerabilities and security issues to organizations. Our thoughts and arguments are presented below.

A. The Importance of Vulnerability Disclosure Programs

A vulnerability disclosure process, also known as a vulnerability disclosure policy ("VDP"), is an organization's formalized method for receiving vulnerability submissions from the outside world. A VDP is intended to give finders—anyone who stumbles across something amiss (aka "researchers", "hackers", "security researchers")—clear guidelines for reporting potentially unknown or harmful security vulnerabilities to the proper person or team responsible. This practice is defined and outlined in a number of different government and non-government publications, including:

- European Telecommunications Standards Institute's ("ETSI") European Standard ("EN") 303 645 v2.1.1;[2]

- International Organization for Standardization ("ISO") Standard 29147;[3]

- U.S. Department of Justice's ("DOJ") *Framework for a Vulnerability Disclosure Program for Online Systems*;[4] and,

- National Cyber Security Centre, Vulnerability Disclosure Toolkit;[5]

Each of these documents emphasizes the importance of instituting formal VDPs and provides a framework to do so. For example, the NCSC *Toolkit* notes, "Having a clearly signposted reporting process demonstrates that your organisation takes security seriously. By providing a clear process, organisations can receive the information directly so the vulnerability can be addressed, and the risk of compromise reduced. This process also reduces the reputational damage of public disclosure by providing a way to report, and a defined policy of how the organisation will respond."[6]

Generally, there are five key components of a VDP:

- **Promise**: Demonstrate a clear, good faith commitment to customers and other stakeholders potentially impacted by security vulnerabilities;

- **Scope**: Indicate what properties, products, and vulnerability types are covered;

[2] ETSI EN 303 645 at Provision 5.2 (2020-06), *available at* https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf.

[3] ISO/IEC 29147:2018 ("Information technology -- Security techniques -- Vulnerability disclosure"). The standard details the methods a vendor should use to address issues related to vulnerability disclosure.

[4] *A Framework for a Vulnerability Disclosure Program for Online Systems* (v1.0), DOJ (July 2017), *available at* https://www.justice.gov/criminal-ccips/page/file/983996/download.

[5] *Vulnerability Disclosure Toolkit*, NATIONAL CYBER SECURITY CENTRE*, available at* https://www.ncsc.gov.uk/information/vulnerability-disclosure-toolkit.

[6] *Id.* at 3.

- **Safe Harbor**: Assures that reporters of good faith will not be unduly penalised;
- **Process**: The process finders use to report vulnerabilities; and,
- **Preferences**: A living document that sets expectations for preferences and priorities regarding how reports will be evaluated.

A well-established VDP also can be coupled with a bug bounty program ("BBP"), which is an organization's bounty-driven rewards program inviting a select group of hackers (private BBP) or any hacker (public BBP) to find exploits and vulnerabilities in its systems. A BBP is a proactive challenge to identify bugs by actively encouraging the security community to target select assets. When VDPs and BBPs are implemented in a progressive fashion, they are commonly seen as the most resourceful and cost-effective way to identify and ultimately remediate cyber vulnerabilities. However, they are fundamentally two different security exercises, and a VDP is a well-accepted start to engagement with security researchers.

This practice is well defined and outlined in a number of government and non-government publications, and there are strong examples of successful VDPs in place that have benefited both the hosting organizations and security researchers. Some UK Government specific examples include the VDPs for The Ministry of Defense ("MOD")[7] and the UK's NCSC[8]. The safe harbor inclusion for the MOD VDP is an example of language that clarifies protections in place for security researchers:

> "The MOD affirms that it will not seek prosecution of any security researcher who reports any security vulnerability on a MOD service or system, where the researcher has acted in good faith and in accordance with this disclosure policy."

The former Department of Digital, Culture, Media & Sport ("DCMS") has already taken a leading role in normalizing the operation of VDPs as a vital best practice for the protection of the end consumer. DCMS has required, among other things, VDPs for any Internet of Things ("IOT") manufacturer selling smart products to UK consumers[9] and recommends VDPs as part of its non-binding Code of Practice for app store operators and app developers.[10]

While there are many established examples of the benefits of VDPs, the lack of clarity in the current CMA legislation can unintentionally elicit fear that even sanctioned programs may be operating in violation of the CMA, despite the fact they're perfectly legitimate. Safe harbor

[7] *Vulnerability Disclosure Policy,* MINISTRY OF DEFENSE (8 December 2020), *available at* https://www.gov.uk/guidance/report-a-vulnerability-on-an-mod-system.

[8] *Vulnerability Reporting,* UK NATIONAL CYBER SECURITY CENTRE (15 November 2018), *available at* https://www.ncsc.gov.uk/information/vulnerability-reporting.

[9] *Code of Practice for consumer IoT security*, DEPARTMENT FOR DIGITAL, CULTURE, MEDIA & SPORT, available at https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security/code-of-practice-for-consumer-iot-security.

[10] *Code of practice for app store operators and app developers*, DEPARTMENT FOR DIGITAL, CULTURE, MEDIA & SPORT, available at https://www.gov.uk/government/publications/code-of-practice-for-app-store-operators-and-app-developers/code-of-practice-for-app-store-operators-and-app-developers.

components are built-in to encourage researchers to disclose vulnerabilities without hesitation. As stated above, this revision of the CMA should make it clear and unquestionable that the operation of a VDP, and the act of finding and reporting a vulnerability through that VDP, is a sanctioned and encouraged practice that does not conflict with the purpose and intent of the CMA. In essence, VDPs should be further enabled by the revised CMA as a sanctioned channel for security researchers to communicate vulnerabilities and security gaps to organizations.

B. Protecting Good Faith Security Research

Though not specifically referenced in this particular consultation, we continue to strongly recommend that the revised CMA should clarify that independent security research undertaken in good faith for the purpose of finding and having security vulnerabilities fixed is not subject to criminal sanction under the CMA. There are suggestions that the current language in the CMA chills independent security research because it makes no provision for legitimate, good faith testing.[11]

Section 1(1) prohibits all "unauthorised access to computer material". This leaves no room for good faith security testing undertaken to reduce cyber-risk, nor does it acknowledge the role of acts the security researcher has taken to mitigate any negative outcomes. Clarifying that this prohibition is not intended to criminalise good faith security research would align the UK's approach with trends among its peer countries. For example, the United States Department of Justice ("DOJ") clarified its own stance toward good faith security research in relation to the U.S.'s equivalent of the CMA, the Computer Fraud and Abuse Act ("CFAA"). In a May 2022 update to its charging policy under the CFAA, the DOJ stated that the "government should decline prosecution if available evidence shows the defendant's conduct consisted of, and the defendant intended, good-faith security research."[12] They then provide a definition of "good faith security research":

> "good faith security research" means accessing a computer solely for purposes of good-faith testing, investigation, and/or correction of a security flaw or vulnerability, where such activity is carried out in a manner designed to avoid any harm to individuals or the public, and where the information derived from the activity is used primarily to promote the security or safety of the class of devices, machines, or online services to which the accessed computer belongs, or those who use such devices, machines, or online services.[13]

In addition, the Belgian government recently adopted a new legal framework to provide a safe harbor for good faith security research.[14] HackerOne urges the Home Office to similarly establish a safe harbor in the CMA.

[11] *About the Campaign*, CYBERUP CAMPAIGN, *available at* https://www.cyberupcampaign.com/about.

[12] *9-48.000 – Computer Fraud and Abuse Act*, UNITED STATES DEPARTMENT OF JUSTICE, *available at* https://www.justice.gov/jm/jm-9-48000-computer-fraud.

[13] *Id.*

[14] *Vulnerability Reporting to the CCB,* CENTER FOR CYBER SECURITY BELGIUM, https://ccb.belgium.be/en/vulnerability-reporting-ccb. While the new Belgian safe harbor is a step in the right direction, it does have limitations. Namely, the Belgian approach unnecessarily conditions the safe harbor under certain circumstances and imposes flawed restrictions on public disclosure. *See* https://www.hackerone.com/ethical-hacker/what-does-belgiums-new-legal-framework-hacking-mean-me.

C. Establishing an Equitable Statutory Defence

We commend the Home Office for seriously considering the inclusion of a statutory defence to ensure that security researchers are not unnecessarily prohibited from conducting activities that would protect entities and individuals from hostile cyber actors. Recognizing that the Home Office intends to continue to consider how best to do this, we again strongly recommend that the Home Office include a statutory defence in the revised CMA that does not rely on certifications, education, and/or formal training requirements, as that would unfairly disadvantage the self-educated and self-employed component of the independent security research community.

This is not simply a fairness issue but can also help the UK Government with its stated objective of increasing the supply of digitally and tech enabled workers, particularly in the vital cyber security field.[15] The UK Government's own research finds that there remains a significant cyber skills gap in the UK, and, in particular, that there is a "broad sense that cyber security qualifications were no guarantee of aptitude in a workplace."[16] Good faith security research provides opportunities for ethical hackers to develop their skillsets at no cost to them (such as participation in VDPs or BBPs), and even to be compensated for their findings as they learn in the case of BBPs. HackerOne conducts one of the largest annual surveys of the ethical hacking community and the results indicate that ethical hacking is a growing pathway for developing cybersecurity skills. Seventy-nine percent of respondents state that they hack to learn new skills. The survey also shows that ethical hacking can be a stepping-stone to a great cyber security career. Thirty-four percent of respondents stated that they have secured a job based on their ethical hacking experience, while a further 25% indicate that it has helped them secure a promotion or otherwise progress their career. A full 41% of respondents hack ethically as their full-time career.

A statutory defence to the CMA should ensure that all good faith security research is covered and no security researcher is penalised for the particular pathway that was available to them to develop their cyber security skills. We look forward to engaging with the Home Office on this issue as part of the Government's wider work to improve national cyber security.

D. Narrowly Targeting Data Copying Offences

As the Home Office considers whether to create a general offence for possessing or using illegally obtained data, we strongly encourage ensuring that legitimate cybersecurity uses of such data continue to be enabled under the CMA. Cybersecurity professionals may search for or possess stolen information in order to help potential victims know whether their data has been breached. Good faith security researchers may copy a small quantity of data from a computer to demonstrate the existence of a vulnerability for the purpose of disclosing that vulnerability to the computer owner so that it can be addressed, making system more secure. In addition, there is a likelihood that individuals will come into contact with stolen data without knowing that it has been stolen.

[15] *UK Digital Strategy*, DEPARTMENT FOR DIGITAL, CULTURE, MEDIA & SPORT, available at https://www.gov.uk/government/publications/uks-digital-strategy/uk-digital-strategy#s3.

[16] *Cyber security skills in the UK labour market 2022: Findings Report*, DEPARTMENT FOR DIGITAL, CULTURE, MEDIA & SPORT, p. 17, *available at* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1072767/Cyber_security_skills_in_the_UK_labour_market_2022_-_findings_report.pdf.

A potential way to narrow a data copying offense may be to allow prosecution of those using such data to commit fraud or extortion. However, it would not be narrow enough to require the intent that the stolen data would be used for another CMA offence. Without a defence to protect good faith security researchers in the CMA, security research activity could still be swept in under such a data copying offence.

E. Enabling a Safer Internet for All

Again, HackerOne encourages the Home Office to further incorporate and legitimize VDPs through the CMA legislation as a vital channel for responsible reporting of vulnerabilities and security issues to organizations. Additionally, VDPs should be clearly approved as a practice in line with public interest. This commitment to broadly protecting good faith security research, whoever undertakes it, through the practice of coordinated vulnerability disclosure should be clearly stated within the CMA. A revised CMA should explicitly protect independent security research and encourage organizations to establish VDPs to help foster the culture of responsible vulnerability disclosure.

* * *

HackerOne thanks you for considering its comments. Should you have any questions, please contact us at policy-team@hackerone.com.

Sincerely,

Ilona Cohen

Ilona Cohen
Chief Policy Officer
HackerOne