Bringing the UK's cyber laws into the 21st century

2023 CyberUp Industry Survey on reform of the UK's Computer Misuse Act 1990

December 2023

Foreword by Flick Drummond MP for Meon Valley

The UK faces unprecedented levels of cybercrime and fraud. As we witness the ever-increasing frequency and sophistication of cyber threats to our computer and personal devices, businesses and critical national infrastructure, it is imperative that we ensure that our legislative frameworks are able to safeguard our nation's cybersecurity. The Computer Misuse Act 1990, the cornerstone of cybercrime legislation in the UK, was put on the statute book when 0.5% of the population had access to the internet. Now 33 years on, the digital world has since changed beyond recognition and the Act requires urgent modernisation. Inaction will continue to be a risk to UK security and prosperity.

In Parliament, I have long advocated for a proactive approach to addressing the challenges posed by cyber threats. The findings presented in this report serve as a clear and urgent signal, exposing the restrictive impact that the Act is having on the very professionals tasked with defending our businesses, citizens, and national security from the ever-evolving landscape of cyber threats. This is because, as it is currently written, the Act inadvertently criminalises a large proportion of vulnerability and threat intelligence research that UK cybersecurity professionals are capable of carrying out to protect the UK.

The cybersecurity professionals and businesses that participated in this report by the CyberUp Campaign unveiled a sobering reality: the Act is not only a significant impediment to the effective pursuit of cyber resilience in the UK; it is creating a ‘chilling effect’ by inflicting substantial financial setbacks on the thriving UK cybersecurity industry. The economic repercussions are felt not only in the loss of potential new jobs and contracts but also in the broader economic fabric of our nation.

The restrictions put in place by the Act put the brakes on what has the potential to be one of the biggest growth areas in the UK’s burgeoning tech sector. This is because companies headquartered in jurisdictions that offer more permissive legislative regimes, such as France, the US and Israel, are able to supply the market with a rich supply of threat intelligence gathered abroad, putting UK businesses at a competitive disadvantage. This week, Germany looks set to begin updating its own cyber laws. The UK cyber industry is at risk of falling behind its international competitors.

The CyberUp Campaign's survey findings serve as an essential contribution to the ongoing discourse on the impact of the Computer Misuse Act. As we navigate the complex terrain of cybersecurity, it is paramount that we strike a balance between strong legal safeguards against cybercrime and enabling professionals to deploy the necessary cybersecurity techniques to fortify our national resilience against cyber threats like ransomware.

The call for a statutory defence, as advocated by the CyberUp Campaign, resonates strongly. A framework that promotes responsible and in good faith research activities aligns with the principles of a robust cybersecurity strategy. The emphasis on implementing precise safeguards is crucial, offering a path forward that ensures the protection of our digital landscape without unduly stifling essential cyber defence initiatives.

A reformed Act will strengthen the essential building blocks needed to be a leading democratic and responsible global cyber power – an ambition the UK Government set out in the Integrated Review and reiterated in the National Cyber Strategy 2022. It will make the UK safer and more secure by allowing cyber security professionals to improve cyber security and detect and prevent crime in the public interest without the threat of prosecution.

The Government has repeatedly emphasised the crucial role of the UK's public-private sector partnership in keeping UK cyberspace safe, as part of a whole-of-society approach. The longer we wait to reform the Computer Misuse Act, the longer the UK's private sector cyber defenders must operate with one hand tied behind their back. A reformed Act is key to delivering effective actions against such threats and several other Government priorities, including tackling disinformation, illicit finance and corruption, and fraud.

As we confront the challenges presented by an increasingly interconnected world, the need for a robust and resilient cybersecurity sector is undeniable. Urgent reform is key and inaction will continue to leave the UK vulnerable. This report adds a valuable perspective to the ongoing dialogue on cybersecurity legislation and serves as a catalyst for necessary reforms. I commend the CyberUp Campaign for their dedication to shedding light on this critical issue, and I hope that this report sparks informed discussions leading to a more secure and prosperous future for the UK.

Why did we conduct this survey?

The CyberUp Campaign conducted a survey to better understand how the UK's Computer Misuse Act 1990 impacts cyber security researchers, professionals, and businesses in the UK.

The aim of this work was to gain insights into the real impact of UK cybercrime legislation on undertaking cyber defensive activities domestically and its effect on the growth and investment of the UK's cyber security sector.

The **survey ran from 19 September to 9 October 2023**, and has been completed by a total of 79 UK cyber security professionals. Different questions had differing response rates.

The majority of respondents worked for organisations or were themselves based in the UK. The average annual turnover of the responding organisations was £519.5 million (or c. 5% of the UK cyber security sector's 2022/23 total annual revenue); the average number of employees was c. 28,000, just short of half the total number of people the Department for Science, Innovation and Technology (DSIT) identified as working in a cyber security related role across the cyber security firms identified.

The CyberUp Campaign believes that the findings of this latest survey make a meaningful contribution to those trying to assess the impact of the Computer Misuse Act on UK cyber security activities as well as to quantify the Act's chilling effect, and economic loss.

What were our main findings ?

The Computer Misuse Act 1990 is having a **meaningful detrimental impact on cyber security professionals' ability to protect UK businesses and citizens from cybercrime and national security threats**. The survey provides further evidence that **continued government inaction threatens the UK's security and prosperity.**

The Act is **posing significant financial and economic setbacks for the UK cyber security industry.** In brief, the chilling effect on the industry can be seen through both activities not being undertaken to improve cyber resilience overall and the direct impact on the sector on jobs and economic loss.

The survey findings also confirm that there is **robust backing for implementing a statutory defence to tackle these challenges**, with a focus on implementing precise safeguards to promote responsible and legal research activities in line with the CyberUp's Campaign **principles-based defence framework** (cyberupcampaign.com).

Impact of the Computer Misuse Act 1990 on Threat Intelligence and Security Vulnerability Researchers:

- **60% of respondents believed that the Computer Misuse Act acts as a barrier to their work** across areas of threat intelligence and security vulnerability research (25 respondents – those identified as threat intelligence, security vulnerability and both combined).
- Reasons included limitations in mapping cyber actors, challenges in obtaining permission, and ambiguity in the Act's definitions.
- **71% of threat intelligence researchers were concerned about inadvertently breaching the Computer Misuse Act** ("always", "frequently" and "occasionally" making up 10 out of 14 respondents).
- Lack of clarity in UK law and the absence of safe harbour provisions for legitimate researchers were cited as concerns.

"We cannot map actors nearly as accurately (...) or as in enough depth to get a true picture of their attack infrastructure and thus cannot defend ourselves or others fully."

Quantifying economic loss:

- **80%** of respondents believed that the UK was at a competitive disadvantage due to the Computer Misuse Act ("strongly agree" and "tend to agree" made up 16 out of 20 respondents).
- **34% found it extremely or very difficult to compete with non-UK firms** (6 out of 18 respondents).
- **30% reported losing contracts or customers to non-UK firms** due to activities deemed illegal under the Act, potentially resulting in significant economic losses (6 out of 20 respondents).
- Approximately **337 UK cyber security firms may have lost around 16,850 full-time equivalent employees** to competitors in more permissive jurisdictions (3 out of 17 respondents stated that they had lost 50 or more employees - around 17%. If this figure was representative of the sector - 17% of all companies is 337 with 16,850 employees being affected).

£3 billion put at risk

30% reported that their organisation had lost contracts or customers because of the CMA. If we extrapolate this result to the UK sector this means that 594 out of 1,979 UK cyber security firms may have experienced an economic loss as a result of the Act, putting at risk up to £3 billion (out of £10.5 billion revenue generated by the entire sector).

Snapshot on the 'chilling effect': an in-depth look at how the CMA is affecting survey respondents:

- Over the last 12 months, respondents to these questions have undertaken between 12 and 5,000+ threat intelligence investigations and engagements per month, or an average of 20 i.e. roughly one per working day of the month.
- Respondents noted that they **decided not to commence or aborted about a third of all threat intelligence investigations due to concerns** about inadvertently breaching the Computer Misuse Act.
- Adding to this the number of times that **r**espondents reported having halted vulnerability research work due to concerns about breaching the Computer Misuse Act (over a third of all vulnerability research activities), it is possible to estimate the Computer Misuse Act's chilling effect in terms of 'prevented benefits'. **With a fit-for-purpose regime, the cyber resilience benefits delivered through UK-based vulnerability research would have been at least three times as significant.**

"A statutory defence seems to be the most practical method for providing legitimate researchers with some certainty that their activities are allowable"

Support for Statutory Defence

100% of respondents support the introduction of a statutory defence for good faith research

61% believe that the sector could see a significant increase in threat intelligence and cyber security activities

This is consistent with other polling figures on this topic. An FoI also revealed that two thirds of respondents to the Home Office Call for Information raised concerned over the current protections in the Act or sought clarifications of those protections.

Sir Patrick Vallance recognised this and called on the government to urgently reform the CMA and recommended the introduction of a statutory public interest defence in the CMA as part of his Digital Technology Regulation Review in March 2023.

Required Safeguards:

- Respondents identified key safeguards needed for the statutory defence, including an actor's competence and the existence of governance processes.
- Some supported pre-notification of unauthorised access to an independent body, while others expressed concerns about bureaucratic obstacles in red teaming and vulnerability discovery.

"Defending the country's critical national infrastructure comes first, but actually being confident that you are always doing the right and legal thing would hugely improve matters. In particular, actually having truly defined what we can and cannot do would be a massive improvement".

Conclusions:

Collectively, these findings suggest that the Computer Misuse Act 1990 has a substantial impact on cyber security professionals, hindering their work and causing economic losses. There is strong support for the introduction of a statutory defence to address these issues, with an emphasis on specific safeguards to ensure responsible and lawful research activities in line with the CyberUp's Campaign principles-based defence framework (cyberupcampaign.com).

About the CyberUp Campaign

The CyberUp Campaign has long been advocating for reform of the UK's outdated Computer Misuse Act 1990, to update and upgrade cybercrime legislation to protect our national security and resilience to digital crime, and to promote the UK's international competitiveness in the rapidly evolving global technology sector. The campaign brings together a broad coalition of supporters across the UK cybersecurity sector and beyond.

For more information about the CyberUp campaign, please see:
www.cyberupcampaign.com or email at **contact@cybercampaign.com**