Submitted via e-mail: CDTPengagement@homeoffice.gov.uk

27 October 2022

FSB response to the Call for information on unauthorised access to online accounts and personal data consultation

The Federation of Small Businesses (FSB) welcomes the opportunity to respond to the Home Office's Call for information on unauthorised access to online accounts and personal data consultation.

FSB is a non-profit making, grassroots and non-party political business organisation that represents members in every community across the UK. Set up in 1974, we are the authoritative voice on policy issues affecting the UK's 5.5 million small businesses, micro businesses and the self-employed.

Cybercrime continues to be a prevalent issue and has only been further exacerbated by the increasing number of businesses moving online during the pandemic. Our research shows that one in five of small businesses report that they have been a victim of cybercrime over the prior two years, with 43% suffering three or more incidents during that time.[1] The cost of cybercrime is also significant, with an average business affected suffering a loss of £7,093. With the latest FSB Small Business Index figures revealing that rising costs continue to affect the vast majority of small firms (89%), with nearly two in five seeing cost increases of more than 10%, now more than ever a cyberattack could be extremely damaging for the business.

As more and more businesses continue to move their operations online, and cybercriminals will continue to grow in sophistication, it is imperative businesses are able to stay informed of and on top of existing risks. For example, it is already known that cybercriminals are targeting existing vulnerabilities in businesses and individuals using the cost-of-living crisis by sending phishing emails that include links to fake energy bill rebates in order to encourage recipients to fall for their scams. It is clear that cybercriminals are indiscriminate of their targets, and therefore, joint action is needed by both the Government as well as industry to tackle these.

Concerns and consequences of unauthorised access

Small businesses are particularly sensitive to any disruption due to their lack of financial reserves and resources to be able to withstand it. Therefore, the risk of longer-term business and supply chain disruption as well as reputational damage is much higher than that of a larger business. Unsurprisingly, our research also found that cybercrime was in the top three of the most disruptive single crimes for businesses.[2] A cyber-attack on a small firm is likely to divert already stretched resources from delivering business services, and the aftermath of loss of data and money will be particularly disruptive for small businesses.

[1] FSB Report, Calling Time on Business Crime, 2019, https://www.fsb.org.uk/resource-report/calling-time-on-business-crime.html

[2] *Ibid.*

For small businesses, concerns around unauthorised access to accounts and personal data as well as the consequences are also significant. Our research found that the most frequently reported cybercrimes are phishing, malware and processing of fraudulent payments online, and a small minority reported incidences of theft of money using digital technology, external and internal data theft and business identity theft.[3] These issues not only have financial or reputational consequences for businesses, the psychological and physical fallout for the business and the business owner to manage the recovery process as well as potentially legal and insurance impacts will also be substantial.

In terms of actions that small businesses take to protect themselves against cybercrime, our 2019 findings show that only around two thirds of small firms have installed security software and less than half report using a strict password policy for devices or network, or a secure wireless network.[4] The larger the business, the higher the number of security measures they will have taken on average. In 2019, our research showed that micro-businesses had taken 5.1 security measures on average, compared to an average of 7.6 measures for businesses with more than 20 employees.

Challenges and barriers

Our research shows that only a small minority of small businesses say that they have accessed NCSC’s small business advice and the Government’s Cyber Aware initiatives. We are supportive of such initiatives and believe that they are key in raising awareness amongst small businesses and will help with the understanding of the extent and dangers of cybercrime, as well as appropriate resilience measures that businesses should have in place. It is positive to see in the National Cyber Security Strategy, the recognition for the need of tailored and targeted guidance and tools to be made available for small businesses. Small businesses struggle with the technical jargon that is often used in guidance and communications, which presents a significant challenge to those willing and wishing to implement appropriate measures. This is why relevant information could also be shared with businesses through the regional cyber centres as well as those deemed as trusted advisors such as IT managed services for small businesses.

It is clear that more could be done to encourage small businesses and raise awareness about effective security measures. The publication of recent guidance by NCSC on the different types of 2FA and MFA and removing malicious content was a step in the right direction,[5] particularly through asking businesses to consider the level of risk and potential impact that an attack may have. However, we also believe that it could go further in providing the detail in implementation with step-by-step guide for businesses of different sizes and sectors. We agree that using more than one authentication method is beneficial when logging into accounts, particularly for accounts that hold personal data. We would welcome further advice and initiatives in this area.

Wider regulation issues

The consultation document also states that further regulation or legislation will not be implemented without a clear case. We agree that if it is necessary to implement any new measures as part of the Cyber Duty to Protect programme, that they should complement existing obligations for businesses, as this would help to reduce any disproportionate burden on

[3] FSB report, Calling Time on Business Crime, 2019, https://www.fsb.org.uk/resource-report/calling-time-on-business-crime.html

[4] *Ibid.*

[5] NCSC, NCSC launches package of support to help retailers protect themselves and their customers online, 2022, https://www.ncsc.gov.uk/news/ncsc-launches-package-of-support-to-help-retailers-protect-themselves-and-their-customers-online

small businesses. Our research has found that two thirds of small businesses perceive the domestic regulatory environment more as a burden than benefit to their businesses, impacting their growth and productivity. They also cite a greater financial burden owing for the need of external advice in light of resource constraints.[6] Therefore, further regulation must be kept to an absolute minimum, and consider the ability of small businesses to comply.

Thank you for considering our response to this consultation. If you would like to discuss any of the points further, please contact me via my colleague Kristina Grinkina, Policy Advisor, on Kristina.Grinkina@fsb.org.uk.

Yours sincerely,

Francis West
Policy Champion, Cyber Security
Federation of Small Businesses

[6] FSB report, Escaping the Maze: How small businesses can thrive under the British Columbia regulatory model, 2021, https://www.fsb.org.uk/resource-report/escaping-the-maze.html