| | | |
|---|---|---|
| **Institution:** University College London | | |
| **Unit of Assessment:** 11 – Computer Science and Informatics | | |
| **Title of case study:** Human-centred security policy | | |
| **Period when the underpinning research was undertaken:** 2003-2020 | | |
| **Details of staff conducting the underpinning research from the submitting unit:** | | |
| **Name(s):**<br>(1) Angela Sasse<br>(2) Simon Parkin<br>(3) Adam Beautement | **Role(s) (e.g. job title):**<br>(1) Professor of Human-Centred Technology<br>(2) Senior Research Associate/Fellow<br>(3) PhD then Research Associate | **Period(s) employed by submitting HEI:**<br>(1) 1990 - 2020<br>(2) 2012 - 2020<br>(3) 2007-2015 |
| **Period when the claimed impact occurred:** 2013 - 2020 | | |
| **Is this case study continued from a case study submitted in 2014?** Y | | |

**1. Summary of the impact** (indicative maximum 100 words)

Professor Sasse and colleagues' influential, user-centric research on cybersecurity has informed security thinking in both government and corporate domains in the UK and globally. This work has shaped revision of official, nation-wide Government guidance from the UK National Cyber Security Centre (NCSC) on how to manage passwords more sustainably without compromising users' security. This user-centric perspective has also informed guidance targeted at smaller organisations such as businesses, charities, and home users. [TEXT REMOVED FOR PUBLICATION].

**2. Underpinning research** (indicative maximum 500 words)

Professor Sasse and Dr. Parkin's research at UCL explored factors that can influence peoples' behaviours around information security controls and policies, and the role that these behaviours play in the continuing productivity of employees.

Research published in 2003, analysing system logs of login attempts for hundreds of users, showed users struggle to manage an increasing number of passwords (**R1**). The research suggested re-considering the "3-strikes" policy commonly applied to password login systems as an immediate way of reducing this demand. They found that not having to change a password reduces the mental load on users and increasing the number of login attempts to 10 reduces the time taken away from, and interference caused with, users' production tasks.

In 2008, Professor Sasse and team developed the compliance budget concept, which explains how friction between information security and business process reduces both security compliance and personal and organizational productivity (**R2**). The user's ability to comply – the "compliance budget" – is limited and needs to be managed like any other finite corporate resource. The compliance budget concept includes ways to improve secure working, including designing less user-costly technologies and improving awareness support.

Through interviews with approximately 100 employees in each of the two large organizations, the research team identified how employees may create user-centric balance of security and productivity when workable institutional support is not provided, as 'shadow security' practices emerge (**R3**); this was also an opportunity for organizations to learn from challenges that employees manage in trying to achieve secure working practice.

Through comparison between existing and emerging technologies, UCL researchers were able to identify how individuals weigh up alternative approaches to security tasks against the context and goals of what they were trying to achieve in a primary task (**R4, R5**). The case study paints a picture of chronic 'authentication fatigue' resulting from current policies and mechanisms, and the negative impact on staff productivity and morale (**R4**). Another methodological approach

developed in the project included informing methods for understanding the role of security technologies in peoples' lives, and the team also assessed emerging biometrics technologies (facial liveness detection) as part of representative everyday tasks (**R5**). This approach also complemented methods developed to inform top-level decisions about the adoption of usable technologies.

Associated research considers these challenges from a psychological perspective, starting from the premise that understanding how people perceive risks is critical to creating effective awareness campaigns (**R6**). Changing behaviour requires more than providing information about risks and reactive behaviours; rather, people must first be able to understand and apply the advice, and secondly, they must be motivated and willing to do so—and the latter requires changes to attitudes and intentions.

**3. References to the research** (indicative maximum of six references)

R1. Brostoff S, and **Sasse, M.A.** 2003. ""Ten strikes and you're out": Increasing the number of login attempts can improve password usability."
R2. **Beautement A**., **Sasse M.A**., and Wonham M. 2008. The compliance budget: managing security behaviour in organisations, Proc. NSPW '08, 47–58. DOI: 10.1145/1595676.1595684
R3. Kirlappos I., **Parkin S.**, and **Sasse, M.A.** 2014. Learning from "Shadow Security": Why understanding non-compliance provides the basis for effective security. Proc. USEC.
R4. **Sasse M.A.**, Steves M, Krol K, Chisnell D. 2014. The Great Authentication Fatigue – And How To Overcome It. Proc. HCI International 2014.
R5. Krol K., **Parkin S.**, **Sasse M.A.** 2016. "I don't like putting my face on the Internet!": An acceptance study of face biometrics as a CAPTCHA replacement. Proc. ISBA 2016.
R6. Beris O, **Beautement A.**, **Sasse M.A.** 2015. Employee rule breakers, excuse makers and security champions: mapping the risk perceptions and emotions that drive security behaviors. Proc. NSPW 2015.

**4. Details of the impact** (indicative maximum 750 words)

This research contributed significantly to the evidence base for two influential pieces of Government and business guidance: firstly, the 2015 GCHQ/NCSC Password Guidance for UK organisations and secondly, the "Awareness is Only the First Step" business whitepaper. These documents superseded previous inferior guidance and offered both business and individual better ways of staying secure. Following on from this policy impact, this research was picked up by iProov and OutThink, two top UK security and IT firms, whose products were not only influenced by Sasse's research but also both appointed her their Chief Scientific Advisor.

**Influence on Government guidance: 2015 GCHQ/NCSC Password Guidance**

Findings from **R1** and **R4** reviewing the '3 strikes' policies have informed the GCHQ/NCSC Password Guidance to UK organisations published in 2015 (**S1, S2**). This led to a change in thinking, putting the users of technology in organisations first, and identifying practical ways to achieve productivity and security at the same time (for instance, directly advocating recommendations from **R1** be put into practice). For instance, a testimonial from the NCSC stated, "The UCL password 'Ten strikes and you're out' and 'Great authentication fatigue' research provided evidence and encouragement for the redevelopment of top-level password guidance which is intended as advice for large and small UK businesses and charities to follow, to more effectively consider the end-user in the management of security in organisations (Specifically, emboldening efforts to move away from a three-attempts 'anchor' that would otherwise prevail)" (**S3**).

In addition, this research (**R1, R2, R3**) have led to increased capacity in sociotechnical security among the 'Five Eyes' international intelligence alliance comprising Australia, Canada, New Zealand, UK and the US, as evidenced by further testimony from NCSC: "The 'Ten strikes and you're out', 'Compliance budget', and 'Shadow security' research (and its inclusion in the 'Awareness is only the first step' whitepaper) fed into the evidence base which the sociotechnical

security team (in CESG and then NCSC) referred to as a starting point when developing a user-centred perspective on security and leading in this direction among the Five Eyes nations" (**S3**).

This approach prevented negative impacts upon users. For instance, Bill Burr (the originator of many of the previous rules about password creation) issued an 'apology' in 2017 for those rules and their impact on users, admitting that his 2003 manual was "barking up the wrong tree." He had advised, for instance, that users change their password every 90 days (**S4**). When the revised password guidance was issued, the head of NCSC pointed to Sasse's analysis of Burr's guidelines, noting that, "That's why we changed the unworkable password guidance, which Professor Sasse calculated was the equivalent of remembering a new 600-digit number every month" (**S5**).

**Influence on business policy with "Awareness is Only the First Step" whitepaper**

Outputs from the compliance budget and shadow security papers (**R2** and **R3**) were used to inform a business whitepaper, "Awareness is Only the First Step", with HP Enterprise (with oversight from CESG) co-authored by Professor Sasse and Dr Simon Parkin (**S6**). As evidenced by NCSC testimony: "UCL research into the 'Compliance budget', and later the 'Shadow security' (and the 'Awareness is only the first step' whitepaper resource which is distributed to enterprises, and incorporates principles from these pieces of research) provided evidence and heuristics upon which the You Shape Security advice collection was based, at least in part (as well as their inclusion as resources for further reading for practitioners)" (**S3**).

The You Shape Security collection (published early 2019) is the main sociotechnical advice collection provided by the NCSC (and prior to that, CESG), among many which involve how UK organisations manage security for their members. The Deputy Director of the National Technical Authority for Information Assurance described how the whitepaper intended to create organisational change across the UK: "At CESG, we advise both organisations and Government on the challenges that their security practitioners face when it comes to security awareness. With this whitepaper we hope to give them a refreshing new way to approach the challenge of involving employees in order to create a more secure organisation, instead of simply implementing a one-size-fits-all approach" (**S7**). The whitepaper has been viewed online 6706 times between August 2017 and December 2020 (**S8**).

This advice has been extensively consulted, as can be seen from the unique pageviews from Jan 1 2018 to Dec 31 2020 for Password Policy, You Shape Security, and then the top 5 password-related blogs:

- Password policy: updating your approach = 48967
- You Shape Security = 5188
- Three random words or think random = 62272
- Passwords, passwords everywhere = 48820
- What does the NCSC think of password managers = 37274
- Let them paste passwords = 26704
- The problems with forcing regular password expiry = 14416

These webpages had an average time of 2 minutes 54 seconds spent on each page (**S8**).

[TEXT REMOVED FOR PUBLICATION]

**5. Sources to corroborate the impact** (indicative maximum of 10 references)

S1. The UK Government guidance, 'Simplifying Your Approach: Password Guidance' document: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/458857/Password_guidance_-_simplifying_your_approach.pdf
S2. NCSC Guidance, Password administration for system owners. https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach.
S3. Testimonial from the Sociotechnical Security Group (StSG) at NCSC

S4. BBC news, “Password guru regrets past advice,” 9 August 2017. https://www.bbc.co.uk/news/technology-40875534.
S5. CBI conference speech, by Chief Executive of the NCSC: https://www.ncsc.gov.uk/speech/ciaran-martins-speech-cbi-cyber-conference
S6. Hewlett Packard Enterprise, Business white paper, “Awareness is only the first step.” https://www.riscs.org.uk/wp-content/uploads/2015/12/Awareness-is-Only-the-First-Step.pdf
S7. HPE press release (with quote from Chris Ensor, Deputy Director at the National Technical Authority for Information Assurance): https://web.archive.org/web/20170913042816/http://m.hp.com/uk/en/news/details.do?id=2274472&articletype=news_release
S8. NCSC pageview data.
[TEXT REMOVED FOR PUBLICATION]