Institution: University of Northumbria at Newcastle		
Unit of Assessment: 4 (Psychology, Psychiatry and Neuroscience)		
Title of case study: Improving human-centred cybersecurity		
Period when the underpinning research was undertaken: 2013 – 2019		
Details of staff conducting the underpinning research from the submitting unit:		
Name(s):	**Role(s) (e.g. job title):**	**Period(s) employed by submitting HEI:**
Pam Briggs	Professor	1992 – present
Lynne Coventry	Professor	2009 – present
Lisa Thomas	Senior Lecturer	2011 – present
Period when the claimed impact occurred: 2014 – 2020		
Is this case study continued from a case study submitted in 2014? N		

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

Cybercrime costs the UK economy approximately GBP27,000,000,000 every year, with many cyberattacks attributed to human error. Research on human-centred cybersecurity at Northumbria University established new theoretical frameworks and developed practical approaches for reducing vulnerability to cyberattacks. With regards to policy, Northumbria's work shaped UK Government campaigns led by the National Cyber Security Centre (including the national Cyber Aware campaign [text removed for publication]), as well as the Government's approach to securing the 'Internet of Things', influencing new funding streams worth GBP32,000,000. Cybersecurity was also improved through novel training and practice. Using Northumbria's research, ThinkCyber redesigned their main cybersecurity awareness training product and developed a new product, generating economic impact. Research was also used by one of the largest private hospitals in Europe to improve behaviours of more than 5,000 members of staff. The Northumbria team also developed and delivered new training for older adults, a group particularly vulnerable to cybercrime.

2. Underpinning research (indicative maximum 500 words)

Human behaviour, including non-compliance with company policy, is a key area of cybersecurity vulnerability for many organisations. Northumbria University specialises in human-centred cybersecurity research and is known for its innovative work in changing cybersecurity attitudes and behaviours. In acknowledgement of this work, Northumbria has been recognised as an Academic Centre of Excellence in Cybersecurity by the National Cyber Security Centre (NCSC). NCSC is a branch of the Government Communications Headquarters, responsible for improving the security of the UK's online activity through technological improvements and advice to citizens and organisations.

Northumbria research that underpins the impact includes the EPSRC project CHAISE (Choice Architecture for Information Security Decisions under Uncertainty, 2013-2016). This was one of the four inaugural projects funded as part of the UK's Research Institute in Sociotechnical Cybersecurity (RISCS). The Northumbria team provided the behavioural science input and generated new knowledge about how to generate, design, and assess behavioural 'nudges' (through changing of interface menus, colour coding of icons, and flagging of warning elements in phishing emails) that can reduce cybersecurity vulnerability in the workplace [**R1**]. The project also used new gamified methods to detect workplace vulnerabilities and reveal the tensions between corporate approaches to cybersecurity compliance and the attitudes and behaviours of employees [**R2**].

Additionally, the researchers used protection-motivation theory (PMT), which seeks to understand the cognitive processes of threat appraisal and coping appraisal ('Am I vulnerable to threat?', 'Do I know what to do?', 'Do I believe this will be effective?') [**R3**, **R4**]. PMT can predict security intentions and adaptive or maladaptive behaviours implemented as a response to the threat [**R3**]. Northumbria research demonstrated that a simple message about protective actions was more influential than a 'fear appeal' in improving security behaviour [**R3**, **R4**].

Most online activities require a secure digital identity to gain access to goods, services, and information (e.g. email or online banking). Passwords, PINS, and biometrics are among the most

commonly used means to authenticate 'digital identity' but these are not always usable or acceptable to the public. This kind of 'digital identity' was the focus of the EPSRC funded IMPRINTS project (Identity Management: Public Responses to Identity Technologies and Services, 2011-2014). The Northumbria team was the first to use an inclusive, citizen-led, and value sensitive approach to identify factors affecting consumer acceptance of digital identity and authentication mechanisms. This included an examination of those elements that are widely disliked and impede take up, and elements that are liked and so facilitate use. The researchers assessed six diverse citizen groups: young people, older adults, refugees, minority ethnic women, people with disabilities, and mental health service users. Trust and acceptance factors were found to differ widely across these communities and across technologies. The research underlined key factors and motivators likely to encourage engagement with new identity technologies, while highlighting that a critical issue is to get the basics of governance right in order to ensure that diverse communities adopt new systems [**R5**]. This project was selected as a 'Big Idea for the Future' by RCUK and shortlisted for the Novay Digital Identity Award in 2013.

The IMPRINTS initiative highlighted some of the specific cybersecurity challenges faced by older adults, a demographic that is increasingly a target for cyber-attacks. Picking up this work, the EPSRC funded cSALSA project (Cybersecurity Across the Lifespan, ongoing since 2017) focused on mitigating age-related vulnerabilities. The Northumbria team had demonstrated the kinds of difficulties older adults and other marginalised communities experienced when trying to authenticate their identity using passwords, PINS, biometrics, and other novel methods [**R5**]. In this new project, the team documented the specific security challenges experienced by older adults and showed the kinds of communication strategies that would be most effective and influential in changing older adult behaviour. The important role of radio, commercial support, and community resources were highlighted, as well as the drawbacks of over-reliance on social information sources [**R6**]. This work has influenced policy and campaign strategies in UK Government.

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

R1. Nicholson*, J., **Lynne Coventry**, and **Pam Briggs** (**2017**) 'Can we fight social engineering attacks by social means? Assessing social salience as a means to improve phish detection' *Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)* https://www.usenix.org/system/files/conference/soups2017/soups2017-nicholson.pdf Papers submitted undergo three rounds of peer review with c.20% acceptance.

R2. Nicholson*, J., **Lynne Coventry**, and **Pam Briggs** (**2018**) 'Introducing the cybersurvival task: assessing and addressing staff beliefs about effective cyber protection' *Proceedings of the Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)* https://www.usenix.org/system/files/conference/soups2018/soups2018-nicholson.pdf Papers submitted undergo three rounds of peer review with c.20% acceptance.

R3. Van Bavel**, R., Rodríguez-Priego**, N., Vila**, J., and **Pam Briggs** (**2019**) 'Using protection motivation theory in the design of nudges to improve online security behaviour' *International Journal of Human-Computer Studies* **123**: 29-39 https://doi.org/10.1016/j.ijhcs.2018.11.003

R4. Blythe*, J. M. and **Lynne Coventry** (**2018**) 'Costly but effective: Comparing the factors that influence employee anti-malware behaviours' *Computers in Human Behavior* **87**: 87-97 https://doi.org/10.1016/j.chb.2018.05.023

R5. **Pam Briggs** and **Lisa Thomas** (**2015**) 'An inclusive, value sensitive design perspective on future identity technologies' ACM Transactions on Computer-Human Interaction **22**(5): 1-28 https://doi.org/10.1145/2778972

R6. Nicholson*, J., **Lynne Coventry**, and **Pam Briggs** (**2019**) 'If it's important it will be a headline: Cybersecurity information seeking in older adults' *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*: 1-11 https://doi.org/10.1145/3290605.3300579

* Internal Northumbria co-authors: J. Nicholson from UoA11 (Computer Science and Informatics), J. M. Blythe (Northumbria PhD student, supervised by Lynne Coventry)
** External co-authors: R. van Bavel and N. Rodríguez-Priego (Joint Research Centre, European

Commission), J. Vila (University of Valencia, Spain)

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

This research has influenced UK and European organisations, enabling them to improve approaches to cybersecurity through innovative training initiatives, policies, and practice.

4.1 Reducing vulnerability to cyberattacks through improved training

Following a presentation of Northumbria research to the national Research Institute in the Science of Cybersecurity (RISCS) in 2018, Professor Pam Briggs was approached by digital training company ThinkCyber to share research findings, particularly around how PMT can be used to design prompts for appropriate behaviour [**R1**-**R3**]. This work influenced the company's approach to training: *'little and often, easy to access, simple and actionable, context driven/real-time'* [**E1**, p2]. The company blogged the influence of this work on its thinking [**E1**, p5] and incorporated Northumbria's findings into its digital cyber awareness training product Redflags [**E1**, p2]. Redflags won 'Best Professional Training or Certification Programme' at the 2020 SC Awards Europe (cybersecurity magazine) [**E1**, p7] and the company has since been added to the CyberTech100 list of the best global cybersecurity companies. ThinkCyber also asked Briggs to collaborate in developing other new products, submitting a joint InnovateUK grant 'Reimagining Cyber Security Awareness Training', which was awarded in November 2018. This enabled Northumbria's team to work with ThinkCyber's clients Camden Council, Deloitte, and Axelos, running workshops to identify problems and suggest design solutions, integrating the 'value-sensitive design' approach [**R5**] from earlier research [**E1**, p2]. Tim Ward, CEO of ThinkCyber, confirmed that *'Two particular ideas from this [work with Northumbria] – Security Bulletins and Real-time tips have evolved into key parts of our product.* [text removed for publication]*'* [**E1**, p2].

[text removed for publication]

The team has also worked directly with older people in the North East of England, through peer-to-peer training to improve e-safety. This work was undertaken in collaboration with the University of the Third Age and the Old Low Light Heritage Centre. Beginning in 2017, the team ran workshops focused on six themes and trained 242 older adults with the result that *'participants improved their online behaviours, in particular with regards to creating better passwords and being more vigilant online'* [**E3**]. Following these, as part of a 'CyberGuardians' project commissioned via EPSRC's Not-Equal Network Plus, Northumbria trained 14 cyber security ambassadors aged in their 50s, 60s, and 70s on how to interact with technology securely. As of September 2020, these ambassadors had cascaded key harm prevention information into their communities, helping approximately 820 people with become more cyber secure [**E3**, p3].

4.2 Impact on public policy and practice

Northumbria's team has made a substantial contribution to the thinking of UK and European bodies working on the human elements of cybersecurity, as few psychologists have been involved in this field from the outset. Paul Waller, Head of Research, NCSC Capability, noted: *'Professors Briggs' and Coventry's sustained public insistence on relating sociotechnical security problems back to psychological theory has percolated the community and our thinking'* [**E4**, p1]. The policy and practice community has benefitted through three types of policy impact: impact on new funding streams, impact on major campaigns to improve cyber security activity by the public, and impact on policy guidance.

Funding Streams: In early 2014, Briggs and Coventry were asked by the then UK Government Behavioural Insights Team to deliver a UK Government Office for Science report on 'Using behavioural insights to improve the public's use of cyber security best practice' [**E5**]. The report, published on 8 May 2014, highlighted the lack of reliable behavioural data on internet users' understanding and use of cybersecurity measures. The report led to an EPSRC 'Human Dimensions of Cybersecurity Workshop' on 22 September 2014 (attended by Briggs) and a subsequent GBP5,000,000 EPSRC call on 'Human Dimensions of Cybersecurity', launched in

2016. Also in 2014, Coventry was asked to contribute a behavioural science/security perspective to the Blackett Review on the 'Internet of Things [IoT]: Making the most of the second digital revolution', which addressed issues of trust and public acceptance [**E6**, p38]. The research agenda outlined in that report led directly to the establishment of the GBP14,000,000 National Centre of Excellence for IoT Systems Cybersecurity (PETRAS), with the GBP13,800,000 PETRAS 2 announced in 2019. PETRAS consists of 16 institutions (including Northumbria University) and ensures that the IoT technologies are safely and securely applied in consumer and business contexts [**E6**, p41]**.**

Public campaigns: 'Cyber Aware' is the UK Government's national campaign on cyber security and recent iterations have been influenced by Northumbria research. 'Cyber Aware' is led by NCSC and delivered in partnership with the Cabinet Office, Home Office, and the Department for Digital, Culture, Media & Sport (DCMS). The campaign has been running for six years, but was relaunched in April 2020 in the light of increasing online activity during the COVID-19 pandemic and received a major marketing push in December 2020 headed up by Penny Mordaunt, the Paymaster General, and Lindy Cameron, Chief Executive of the NCSC. This new approach to the Cyber Aware campaign focused on ideas of positive framing, coping strategies, and realistic action – making cyber security approachable for everyone – that come from the work of Briggs and Coventry [**E4**, p3]. Other NCSC campaigns influenced by this work include 'You Shape Security' and 'People are the Strongest Link' [**E4**, p3].

[text removed for publication]

Policy guidance: Policy has been influenced in Europe, with Briggs' research using PMT used to assess the effectiveness of a range of cybersecurity nudges [**R3**]. This generated three European Commission technical reports for the Joint Research Centre, which provide evidence-based support to European policymaking. These reports covered effective privacy and security 'nudges' in warning messages and banners, with Briggs' contributions explicitly acknowledged [**E7**, p4, p54 and p100 of the compiled document]. The digital identity research also fed into an EU policy guidance document 'Cybersecurity in the European Digital Single Market' which stated *'the importance of sub-topics such as digital identity and the notion of "trust" emerged as central cross-cutting themes which aided the development of the opinion'* [**E8**, p53]. Briggs is cited as a contributor [**E8**, p84].

In the UK, the DCMS used the Blackett IoT report to create the Government guidance 'Secure by Design: Improving the cyber security of consumer Internet of Things' [**E9**]. Coventry was invited onto the panel to create this document and the report referenced cSALSA [**R6**] as the source of findings that helps government *'to design more effective cyber security advice and educational materials that are tailored for different audiences'* [**E9**, p27]. The digital identity research [**R5**] led to an invitation for Briggs to join the All Party Parliamentary Group on Digital Identity. The findings from the IMPRINTS project then informed the House of Commons Science and Technology Committee Report on 'Current and Future Uses of Biometric Data and Technologies', where the challenge in establishing trust – especially around biometrics – was noted from IMPRINTS [**E10**, p29, p43].

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

Ref.	Source of corroboration	Link to claimed impact
E1	Compilation of ThinkCyber materials: testimonial - Tim Ward (CEO and Co-founder of the ThinkCyber), information about RedFlags product, blog about using protection-motivation theory, and SC 2020 award	Corroborates Northumbria's input into award-winning cybersecurity awareness training, economic impact, and deployment of research in marketing (blog)
E2	[text removed for publication]	[text removed for publication]

E3	Compilation of a testimonial from Mike Martin (former Northumbria Regional Committee Member of the University of the Third Age (U3A)), and U3A CyberGuardians project report	Corroborates improved cybersecurity awareness among 820 older people in the North East of England
E4	Two testimonials from the National Cyber Security Centre (NCSC): a) Paul Waller (Head of Research, NCSC Capability), b) Ceri Goncalves Jones (former NCSC employee)	Corroborates Northumbria's input into UK cybersecurity policy development
E5	UK Government Office for Science report 'Using behavioural insights to improve the public's use of cyber security best practice' (2014)	Report produced by Northumbria's psychology department (Coventry, Briggs, Blythe, Tran), showing impact on policy and how behaviour change theories can be used to improve cybersecurity behaviours
E6	UK Government Office for Science report 'The Internet of Things: Making the most of the Second Digital Revolution' (2014) and screenshot of PETRAS website	Corroborates impact on cybersecurity policy in the UK and the role of Northumbria research in PETRAS
E7	Compilation of three reports from the European Commission, Joint Research Centre (all from 2016): 'The effect of warning messages on secure behaviour online' (p1); 'Nudging online security behaviour with warning messages' (p51); 'Testing the effect of the cookie banners on behaviour' (p97)	The three reports corroborate that Northumbria's researchers acted as external consultants in forming EC's thinking on cybersecurity
E8	European Commission, High Level Group of Scientific Advisors report 'Cybersecurity in the European Digital Single Market' (2017)	The report draws on Northumbria's IMPRINTS research project findings. Corroborates impact on EU cybersecurity policy
E9	UK Government, Department for Digital, Culture, Media and Sport 'Secure by Design: Improving the cyber security of consumer Internet of Things' (2018)	Corroborates that Northumbria's researchers contributed to creation of policy guidelines for secure consumer behaviour in the UK
E10	House of Commons, Science and Technology Select Committee report 'Current and future uses of biometric data and technologies' (2015)	Corroborates impact on cybersecurity policy in the UK