Institution: Bournemouth University		
Unit of Assessment: 11		
Title of case study: Productive security and privacy by design: building security and privacy tools into the earliest stages of software development		
Period when the underpinning research was undertaken: 2015 – 2020		
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:**
Dr Shamal Faily	Principal Lecturer in Systems Security Engineering	2013 – current
Dr Jane Henriksen-Bulmer	Lecturer in Computer Science	2013 – current
Dr John McAlaney	Associate Professor in Psychology	2014 – current
Period when the claimed impact occurred: 2014 – 31 December 2020		
Is this case study continued from a case study submitted in 2014? No		

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

When designing secure, private software products, it was identified that user experience (UX) was often hugely diminished. Researchers at Bournemouth University (BU) devised a solution to this problem which has primarily:

- enabled global rail consultancy Ricardo Rail to win new business worth GBP50,000,
- allowed the UK's Defence Science and Technology Laboratory (DSTL) to improve battlespace risk management,
- saved money for regional charities in their preparations for the implementation of GDPR.

It also led to the development of new teaching materials, adopted by universities in the UK and US, and a leading educational publisher, and the creation of new commercial products.

2. Underpinning research (indicative maximum 500 words)

Faily has shown how personas – as a vehicle for UX (user experience) techniques in general – can be instrumental in incorporating security into software design prior to architectural design and software development. He demonstrated how the activity of creating personas leads to better security requirements and how the elicitation and management of personas can be incorporated into integrated tool-support [R1]. He has also shown how personas based only on assumptions can help find security problems once software has been developed and where the design data is sub-optimal [R2].

Beyond the development of software, Faily's research has also shown how security awareness campaigns can be centered around the creation and validation of personas, particularly when such campaigns tackle human factors and related risks [R3].

Since 2016, Faily and McAlaney have collaborated on a number of research projects with DSTL – an executive agency, sponsored by the Ministry of Defence which ensures scientific innovations contribute to the defence and security of the UK. Together, they have identified factors that influence how security analysts interpret risk, as well as principles for designing software used by cybersecurity risk-based decision-makers [R4].

Since 2015, BU research has explored whether the design techniques and tools for security are equally applicable when considering privacy, particularly in helping organisations make sense of the General Data Protection Act's (GDPR) impact on their products and services. Henriksen-Bulmer's work has shown that, by building on Nissenbaum's theory of Contextual Integrity, practical processes for assessing privacy risk can be devised and potentially tool-supported [R5, R6].

Insights from the underpinning research have informed the evolution of the open-source CAIRIS (Computer Aided Integration of Requirements and Information Security) platform. CAIRIS, which is maintained by Faily and his team, was initially created to understand the conceptual relationship between security, usability and software engineering concepts. However, it has since evolved to illustrate the form of tool-support that software engineers, UX researchers and security engineers might use when designing usable and secure software [R1]. In 2018, CAIRIS was used to demonstrate how very early-stage design models could be validated for potential non-compliance with the principles of the GDPR Act [R7].

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

R1-7 have been subject to rigorous peer review.

R1: Faily, S. (2018). *Designing Usable And Secure Software With IRIS And CAIRIS*. Cham: Springer International Publishing. (Copy available on request.)

R2: Faily, S. (2015). "Engaging stakeholders during late-stage security design with assumption personas," *Information and Computer Security,* Vol. 23 (no. 4), pp. 435-446. https://doi.org/10.1108/ICS-10-2014-0066

R3: Ki-Aries, D. and Faily, S. (2017). "Persona-centered information security awareness," *Computers and Security,* Vol. 70, pp. 663-674. https://doi.org/10.1016/j.cose.2017.08.001

R4: M'manga, A., Faily, S., McAlaney, J. and Williams, C. (2017). "Folk Risk Analysis: Factors Influencing Security Analysts' Interpretation of Risk," Proceedings of the 13th Symposium on Usable Privacy and Security (SOUPS 2017), Santa Clara, USA, Usenix. https://www.usenix.org/system/files/conference/soups2017/wsiw2017-mmanga.pdf

R5: Henriksen-Bulmer, J., Faily, S. and Jeary, S. (2018). "DPIAs for Charities: The DPIA Data Wheel," Privacy and Identity: Proceedings of the 13th IFIP International Summer School on Privacy and Identity Management, Vienna, Austria, Springer. https://www.researchgate.net/publication/327437377_DPIAs_for_Charities_The_DPIA_Data_Wheel

R6: Henriksen-Bulmer, J., Faily, S. and Jeary, S. (2019). "Privacy risk assessment in context: A meta-model based on contextual integrity," *Computers and Security*, Elsevier. https://doi.org/10.1016/j.cose.2019.01.003.

R7: Coles, J., Faily, S., Ki-Aries, D. (2018). "Tool-supporting Data Protection Impact Assessments with IRIS and CAIRIS," Proceedings of the 5th IEEE International Workshop on Evolving Security and Privacy Requirements Engineering, IEEE, pp. 21-27. https://www.researchgate.net/publication/328457983_Tool-Supporting_Data_Protection_Impact_Assessments_with_CAIRIS

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

Impact on industry

Our research has been adopted by Ricardo Rail (RR), a global consultancy that provides technical expertise, assurance and specialist engineering services to rail companies around the world. BU's research enabled RR clients to better understand emergent qualities of their systems such as safety, security and usability and the relationship between them [E1a]. RR uses the term ‘digital resilience’ to describe this area of development.

Since 2018, RR has highlighted its enhanced capability in this area – which is based on BU’s research – in GBP700,000 of bidding activity, with approximately GBP50,000 being won to date in new contracts [E1b]. ‘Without the partnership with Bournemouth, [this new capability] would not be on our radar. [BU’s] research has allowed us to market ourselves as providing a cutting edge service…. It has been fundamental in enhancing our existing Human Factors [HF] capabilities as part of our wider digital resilience offering.’ [E1a]

RR’s first application of the research was on a project conducting cyber security risk analysis of a rolling stock platform developed by a major UK-based manufacturer. By modelling personas developed by BU, RR was able to identify and investigate threats and control measures in greater detail, which would not have been the case otherwise. ‘Not only did [it] rationalise existing assumptions, it also helped to identify new vulnerabilities… the outcome for the client was a richer understanding of the threat landscape for its products, which enabled them to develop responses during early design stages.’ [E1c]

The project also resulted in approximately GBP10,000 in revenue, ‘an extra level of satisfaction from a client who already had a very high degree of satisfaction’, and the potential for further work with the client’s customers [E1a].

Impact on UK government
DSTL uses ‘the best science and technology capabilities’ to respond to the MoD’s needs regarding current operations and future defence strategy. A key element is its support of military operations in rapidly changing situations in coalition with other nations. It is therefore essential that risk-based decision-making is understood across organisational boundaries.

DSTL has used BU’s research to support its work with Defence Spectrum Management ‘to ensure defence use of the electromagnetic spectrum [signals such as radio, infrared or radar] is efficient’ and remove the potential for conflict between different users [E2]. Current spectrum management toolsets are not capable of supporting network managers to make informed, risk-based decisions. DSTL confirms that BU’s research ‘supports the specification of new risk-aware toolsets that will increase the efficiency of spectrum utilisation’ [E2].

Impact on UK charities
In 2018, when the new GDPR legislation was introduced, UK charities grappled with their preparations and the lack of clarity about what charitable organisations were expected to do to demonstrate compliance. We began working with regional charities to demonstrate how techniques and tools resulting from our research could help.

Working with StreetScene - a renowned UK addiction rehabilitation charity - we evaluated the readiness of its existing policies and procedures using our privacy risk assessment processes and tools [E3]. The charity used Henriksen-Bulmer’s research to ‘review, analyse and justify every piece of data we now hold... It was also used as a training tool for staff, showing them how to consider data in terms of GDPR’ [E3].

By providing this training to StreetScene, and 50 participants from other charities across the region, we helped them reduce the amount of time and resources they currently spend on privacy compliance activities, allowing them to re-direct more funds to their charitable goals. ‘Doing this for ourselves gave us an understanding that could not have been achieved if someone else had done it for us... it has improved working practice around our data collection and use. The biggest benefit for all of us was to be shown a way through that made [GDPR] understandable and not at all scary. It gave us confidence, which is priceless.’ [E3]

Educational impact and software development
BU’s research has been utilised in education and a Software-as-a-Service (SaaS) platform:

- Pearson includes CAIRIS as an essential course component in the Cloud Computing specification for both its Higher National Certificate and Diploma [E4, p.192].
- The University of Kentucky uses CAIRIS to ‘allow students some hands-on experience. CAIRIS [fits] the bill… as it deals with requirements and security… has a system perspective… [and] is mature enough to have documentation and sample problems’ [E5].
- Faily’s book on IRIS and CAIRIS [R1] and the CAIRIS platform have been central components since 2017 in BU’s advanced undergraduate/postgraduate course unit on Security by Design [E6a], with students using CAIRIS with industry clients in final-year projects. iQHealthTech used it to carry out a GDPR privacy impact assessment of a prototype patient-led application: ‘…this work was a contributing factor to our evolving understanding and focus in security by design.’ [E6b]
- Faily’s work on CAIRIS (supported by approximately GBP110,000 in Innovate UK funding) has provided the technological foundation for HuaHana, a SaaS platform that enables UX and security designers to find security problems early by analysing and visualising product design data [E7].

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

E1:
E1a. Ricardo Rail. (2019). Testimonial letter, 10 December.
E1b. Ricardo Rail. (2021). Email, 8 February.
E1c. Thron, E., (2019). Why Human factors matter in rail cyber security. [Blog] *Ricardo Rail: News*, Available at: https://rail.ricardo.com/news/why-human-factors-matter-in-rail-cyber-security (Accessed 9 February 2021).

E2: Defence Science and Technology Laboratory. (2020). Testimonial letter, 8 December.

E3: StreetScene. (2019). Testimonial letter, 30 July.

E4: Pearson Education Limited. (2020). *Higher Nationals: Cloud Computing*. 1st ed. Pearson Education Limited, p. 200.

E5: University of Kentucky, US. (2020). Letter, 17 December.

E6:
E6a. Faily, S., (2020). *FST L6/L7 Security By Design*. [online] Rl.talis.com. Available at: https://rl.talis.com/3/bournemouth/lists/98B6E668-7203-597A-76CD-CECB6E78F48C.html (Accessed 27 January 2021).
E6b. iQHealthTech. (2020). Email, 11 December.

E7: Huahana.com. (2021). *Huahana - Enabling Agile Teams To Create Digital Products And Services With Security And Privacy Designed In*. [online] Available at: https://huahana.com (Accessed 13 March 2020).