Institution: University of Wolverhampton

Unit of Assessment: 11 Computer Science and Informatics

Title of case study: Digital innovations in cybersecurity to support small and medium-sized enterprises (SMEs)

Period when the underpinning research was undertaken: 2016 - 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:
Professor Amar Aggoun	Professor of Visual Computing	2016 - Present
Professor Prashant Pillai	Professor of Cybersecurity	2018 - Present
Dr Haider Al-Khateeb	Reader in Cybersecurity	2018 - Present
Dr Zhraa Alhaboby	Lecturer in Public Health	2018 - Present
Dr Ali Sadiq	Lecturer in Computing	2019 - Present
Dr Nikolaos Ersotelos	Lecturer in Computer Science	2019 - Present

Period when the claimed impact occurred: 2018 - 2020

Is this case study continued from a case study submitted in 2014? N

1. Summary of the impact

Our research developed innovative and cost-effective cyber solutions for online safety and has gone on to have substantial impacts on small medium-sized enterprises (SMEs) in the UK and overseas. It provided better protection in people's homes and businesses against modern advanced online threats. In Nigeria, our free training programme for businesses has enabled over 1,500 SME employees to become more resilient to cyberattacks during the COVID-19 pandemic. In the UK, our technology-sharing project SOLVD has brought new software to cybersecurity companies through a partnership programme with Telford & Wrekin Council. Furthermore, our new spin-out company Onlyn Shield Ltd is bringing cost-effective pioneering security solutions to the UK market.

2. Underpinning research

The COVID-19 outbreak has impacted daily lives, with more people accessing their work data from home while looking after their families. This situation has been exploited by cybercriminals to attack people and businesses. The Wolverhampton Cyber Research Institute (WCRI), established in 2017, brings together academics from the School of Mathematics and Computer Science and builds on the established strength of its members in the areas of cyber incident response, online safety, artificial intelligence, and cyber-physical systems. In an ever-changing online world, the expertise within the group has been utilised to support online safety against substantial risks. Many individuals/organisations do not have the resources to deploy expensive cybersecurity solutions; therefore, our research aims provide free training and cost-effective software to businesses and people around the world. The following findings [F] have been key in that mission:

F1. Forensically-enabled methods for proactive incident response

The Internet is an enabler for cyber-attacks including the victimisation of vulnerable groups (e.g. children, disabled people) which includes radicalisation, bullying, stalking and grooming. However, the Internet can also provide an environment for near-real-time detection and mitigation. Novel methods have been designed by our researchers to identify, assess risk and cover the forensic preservation of various types of cyber incidents. A model has been developed to leverage distributed ledger technology and Internet of Medical Things (IoMT) data to detect stressful events [R1]. For example, when bullying takes place, the model will allow quicker and better decision-

making, while revolutionising aspects related to compliance, double-entry, confidentiality, and privacy. To provide a proof of validity, the concept of "Digital Witnesses" (DW) is introduced to the context of our work where data produced by digital devices becomes fully documented [R2] to support incident response methodologies in smart environments [R3]. DW helps to make sure that event reconstruction is viable, and data integrity -and therefore admissibility- to a Court of Law can be achieved with A Chain-of-Custody (CoC) maintained in near real-time [R2].

F2. Assessing information gleaned from web browsers to preserve user privacy

The data collection of online browsing habits of individuals can enable effective advertisement targeting and retargeting. However, these data collection practices can cause leakage of private data belonging to website visitors (end-users) without their knowledge. Furthermore, this data can be utilised to enable cyberstalking. [R4] presents a new method (AdPExT) to extract third-party parameter key-value pairs at an individual key-value level. This feeds into a process to monitor and analyse what personal data is collected by online servers. Furthermore, a survey gathered the perceived sensitivity sentiment for various representative tracking parameters to help in the risk assessment of visited websites.

F3. Parameter reduction technique for efficient classification with optimal decisions

Statistical classification has many applications including pattern recognition and decision-making, which is needed to support the digital solutions presented in this case study. However, existing classification techniques that were proposed previously for eliminating data inconsistency could not achieve an efficient parameter reduction in soft set theory, which affects the obtained decisions. Meanwhile, the computational cost made during the combination generation process of soft sets could cause machine infinite state, this is known as nondeterministic polynomial time. An efficient soft set reduction-based binary particle swarm optimized by biogeography-based optimizer (SSR-BPSO-BBO) algorithm was developed [R5]. It generates an accurate decision for optimal and sub-optimal choices. Additionally, a novel COVID-19 optimizer Algorithm (CVA) was developed based on an efficient optimizer algorithm that can solve non-deterministic polynomial-time hardness (NP-hard) in addition to applied optimization problems [R6].

3. References to the research

The research papers have been published following a rigorous peer-reviewed process. Research questions were investigated empirically and contributed to the knowledge base. Content from the papers have been utilised to generate funding and deliver impacts on commerce, practitioners, delivery of professional services, and public awareness. R1 has been underpinned by 2 Innovate UK grants (see below).

R1. Ersotelos, N., Bottarelli, M., Al-Khateeb, H.M., Epiphaniou, G., Alhaboby, Z., Pillai P. & Aggoun, A. (2021). Blockchain and IoMT against Physical Abuse: Bullying in Schools as a Case Study. *Journal of Sensor and Actuator Networks*, 10(1). https://www.doi.org/10.3390/jsan10010001. (Published online 29th December 2020).

R2. Ahmadi-Assalemi, G., Al-Khateeb, H.M., Epiphaniou, G., Cosson, J. & Pillai, P. (2019). Federated Blockchain-based Tracking and Liability Attribution Framework for Employees and Cyber-Physical Objects in a Smart Workplace., *12th Annual International Conference on Global Security, Safety and Sustainability (ICGS3)*, London, UK: IEEE, 16 – 18 Jan 2019. https://www.doi.org/10.1109/ICGS3.2019.8688297.

R3. Ahmadi-Assalemi, G., Al-Khateeb, H. M., Epiphaniou, G. & Maple, C. (2000). "Cyber Resilience and Incident Response in Smart Cities: A Systematic Literature Review". *Smart Cities*, 2020, 3, 894-927. https://www.doi.org/10.3390/smartcities3030046.

R4. Woensdregt, J.W., Al-Khateeb, H.M., Epiphaniou, G. & Jahankhani, H. (2019). AdPExT: Designing a Tool to Assess Information Gleaned from Browsers by Online Advertising Platforms. *12th Annual International Conference on Global Security, Safety and Sustainability (ICGS3)*, London, UK: IEEE, 16 – 18 Jan 2019. https://www.doi.org/10.1109/ICGS3.2019.8688328.

R5. Sadiq, A.S., Tahir M.A., Ahmed A.A. & Alghushami, A. (2020). Normal parameter reduction algorithm in soft set based on hybrid binary particle swarm and biogeography optimizer". *Neural Computing and Applications*, 32, 12221–12239. https://www.doi.org/10.1007/s00521-019-04423-2.

R6. Hosseini, E., Ghafoor, K.Z., Sadiq, A.S., Guizani, M. and Emrouznejad, A. (2020). "COVID-19 Optimizer Algorithm, Modeling and Controlling of Coronavirus Distribution Process," *IEEE Journal of Biomedical and Health Informatics*, 24(10), 2765-2775. DOI: https://www.doi.org/10.1109/JBHI.2020.3012487.

Underpinning Grants
Al-Khateeb, H. Safe Internet surfing with an intelligent child-centred shield against harmful content. Innovate UK. GBP30,502. April 2019 – July 2019. Underpins R1.

Al-Khateeb, H. VACCYNE - an intelligent child-centred shield against harmful communications. Innovate UK. GBP58,932. September 2019 – February 2020. Underpins R1.

4. Details of the impact

Our research helped SMEs to transform their employees' understanding of cyber threats and the ability to deploy appropriate security controls and incident response. Additionally, our research aided SMEs to bring innovations to the market. The following impacts [I] have been realised:

I1. Impacting understanding of and response to online risk for SMEs in Nigeria
Our research on innovative cyber solutions against online threats [F1] and user privacy [F2] has informed training of thousands of employees to become more resilient to cyberattacks during the COVID-19 pandemic. The pandemic has raised the issue of cybersecurity in relation to the new normal of expecting staff to work from home. This has increased the possibility of state-sponsored, phishing and ransomware attacks.

Through the Cybersafe Foundation, a Nigerian based Non-Governmental Organisation (NGO) on a mission to facilitate a safer internet for everyone with digital access in Nigeria, employees from over 1,500 SMEs across Nigeria are now better informed about how to protect themselves and the businesses they work for from cyber threats. The project was delivered in partnership with the UK Government through its Foreign and Commonwealth and Development office (FCDO) under the initiative *Safe Digital Community During COVID-19*, and we were the only University to contribute to the programme. Our findings on forensically enabled methods incident response [F1] and user privacy [F2] were used to create educational materials, including slides, handouts, videos and other reference materials [C1], aimed at arming employees with the knowledge and skills required to identify, protect, detect, defend and respond to COVID-19 instigated cyber threats. In October 2020, the free 8-week virtual programme was delivered to 3057 participants, across 1504 SMEs, in 35 states across Nigeria, via an eLearning platform and biweekly live conferences [C1].

This represents a hugely significant push forwards in the cybersecurity training available to SMEs in a country where such training is almost non-existent. The UK Government's Head of Digital Access Programme and Country Adviser indicated:

> "This project demonstrates the UK Government's continued support for Nigeria and its digital sector, recognizing the tech ecosystem's role in inclusive growth and development," [C2].

The Founder of Cybersafe further commented that:

> "This training raised the bar in cybersecurity preparedness for Small and Medium Scale Businesses in Nigeria who until this time were indeed worst prepared to defend against prevalent cyber-attacks" [C1].

Feedback from the attendees was very positive with comments such as: "The training opened my eyes to cloud data privacy, practical ways to secure web applications, cloud computing, how to

secure my passwords, etc", "as a staff (member) of a local trading organisation, joining the training helped me to learn how to protect my organization from cyber-attacks and how to secure my business for the future", and , "the lessons learned from this training were helpful in my daily task of ensuring the protection of my clients' and organisations"

In terms of the success of the course in enhancing cyber resilience, the Founder of Cybersafe further clarified that "57% of beneficiaries could not identify a phishing email before training" but following training on incident response", and that "83% beneficiaries now understand prevalent attack vectors and preventive measures" [C1]. Furthermore, "76% of beneficiaries have now implemented one or more security controls" [C1].

Overall, the training campaign was transformative and impactful, with SMEs continuing to enrol their employees for the training programme in 2021. This is a prime example of how high quality cyber research can be used to significantly benefit businesses, who would otherwise been financially unable to access such expertise.

I2. Developing skills of UK based SMEs during the pandemic

The effect of the COVID-19 crisis on SME performance across the UK is immense. In the year prior to the pandemic, 80% of SMEs reported stable or growing revenue. However, after the pandemic begun, 80% of SMEs say their revenues are declining. Research on forensically enabled incident response [F1], user privacy [F2] and efficient classification [F3] helped to establish SOLVD, a new initiative formed between the University of Wolverhampton and Telford & Wrekin Council to improve knowledge and skills for the digital economy in the region. Through free workshops, seminars and 1-to-1 sessions, up until December 2020, SOLVD has helped 2 businesses to find growth opportunities at this challenging time by learning about emerging digital technologies. The Co-founder of Lockdown Cyber Security Ltd commented

> "The SOLVD workshop provided us with new technology to use within our business, which adapted our business plan and brought it to life, maintaining our business agility and creating the roadmap to assist in the creation of our software prototype", "This experience has shown the value the University can bring, to start-up businesses, throughout its business journey." [C4].

I3. Bringing innovations to market

The findings on cyber-attacks [F1] and online browsing [F2] were used to create new software and form a new SME, the spin-out company Onlyn Shield Ltd (Company number: 112462631), registered in 2020. The product is an intelligent safeguarding software platform to protect children from harmful online communications at schools and households. With the increase in online activity due to the COVID-19 pandemic, and recent studies showing 1 in 4 children have been exposed to racism or hate messages online, the need for such innovative software has never been more prevalent. Onlyn Shield offers quicker intervention and better filtering capabilities than previous alternatives, with the ability to address emerging threats targeting children on social media. The project also aims at achieving Incident Response and safer Internet surfing without having to block popular services and websites.

The Market Validation Report [C5] for Onlyn Shield Ltd was compiled as part of the CyberASAP programme, and included data collected from a conference attended more than 30 teachers, with 7 interviews with headteachers and 18 interviews with parents. Given a relatively low product annual license fee of GBP35 per family or GBP7 per pupil, the overall annual UK Market Potential was estimated at approximately GBP266,000,000, with sales potential for Onlyn Shield of GBP5,320,000 aiming for 2% market penetration, with potential growth to GBP18,620,000 (7% market penetration), and further potential global growth beyond the UK market. This indicates a huge potential market for Onlyn Shield making it a significantly viable product, both in terms of potential revenues, but also in terms of the potential benefits to families who will have access to a cheap and effective tool for keeping their children safer online.

Overall, in a world where online risks have never been more prevalent, our research is being used to good effect to provide solutions to businesses and people who otherwise may not have the financial means to protect themselves.

5. Sources to corroborate the impact

C1. Cybersafe Foundation, Letter of Appreciation.

C2. Cybersafe Foundation, Press Release.

C3. Cybersafe Foundation, Testimonials from Trainees.

C4. Testimonial by Co-founder of Lockdown Cyber Security.

C5. Market Validation Report and Presentation (VACCYNE project).