RISCS

Research Institute in Sociotechnical Cyber Security

ANNUAL REPORT

2019

RISCS

Research Institute in Sociotechnical Cyber Security

Contents

DIRECTOR'S MESSAGE 3

RISCS STRUCTURE AND RESEARCH THEMES 6

RISCS RESEARCH STOCKTAKE 8

RISCS PROJECT UPDATES 11

ACCEPT: Addressing cyber security and cybercrime via a co-evolutionary approach to reducing human-related risks 12
cSALSA: Cyber Security Across the Lifespan 14
DAPM: Detecting and Preventing Mass Marketing Fraud 15
ECSEPA: Evaluating Cyber Security Evidence for Policy Advice 16
EMPHASIS: Economical, Psychological and Societal Impact of Ransomware 19
Leveraging the Multi-Stakeholder Nature of Cyber Security 20
Cyber Readiness for Boards 22
Motivating Jenny to Write Secure Software 24
Why Johnny Doesn't Write Secure Software 27

SHORT PROJECT UPDATES 29

Data Security in the Home 30
ECSEPA Mapping Project 31
Impact of Gamification 34
Software Security in Development Teams 36
Visualising access control policies 38

CYBERCRIME PROJECTS 39

Advanced modelling of cyber criminal careers: New technology and intelligence from online evidence bases 40
Case by case: Building a database on cybercriminal business models 41
Connecting delayed pre-commitment with cyber awareness in order to address the perception gap and present bias 42
Gentle Interventions for Security (GIFS) 43
Evaluating criminal transactional methods in cyberspace as understood in an international context 44
Investigative interviewing of cybercrime victims to gain best evidence 45
Online Ties Taking Over (OTTO)? A longitudinal study into actual vs. perceived cybercriminal behaviour of offline vs. online social ties among youth 46
Victims of Computer Misuse Crime 47

Director's message

Welcome to the RISCS 2019 Annual Report. We look forward to this opportunity to provide an update on our activities over the past 12 months and to foreshadow our plans for 2020. Over the course of 2019, we have engaged in a period of quite intense reflection and evaluation about the structure, function and direction of RISCS. The UK cyber security ecosystem has grown and changed significantly over the lifespan of RISCS and so has our own community. We wanted to take some time this year to consider our place in this ecosystem as well as how we can best contribute to shaping the future of global sociotechnical cyber security research. We've drawn heavily on our Advisory Board through this process and we're very grateful to them for their expertise and input.

One of the changes we have made is to our name. In recognition of the ways that cyber security research has matured over the past eight years and of the focus of our community, we have changed our Institute's name from 'Research Institute in Science of Cyber Security' to 'Research Institute in Sociotechnical Cyber Security'. Obviously, this name change should not suggest that we place any less emphasis on evidence or rigorous methodologies – these continue to be central to our work, as they are for most cyber security researchers in 2020. However, it does provide more clarity about the type of cyber security research that we focus on in RISCS and that will be important to us as we move into the next phase of our growth.

Below, we list some of our highlights from this year as well as plans for 2020.

CYBER LIABILITY AND CYBER INSURANCE WORKSHOP: APRIL 10 AND 11

In early April, RISCS held two workshops in London that looked at the complexities of liability in cyber security and at the role (both current and potential) of cyber insurance. We had a range of fascinating presentations from the insurance sector, from RISCS academics, and from cyber security practitioners in the NHS before embarking on a scenario-based workshop designed by RISCS Scientific Advisory Board member, Dr Ine Steenmans. The workshop explored the many forms of known, latent, and unknown liabilities that intersect with financial and legal chains of accountability. We also discussed whether and how cyber insurance could provide a lever to promote better cyber risk management. On the following day, we took stock of the previous day's findings in an interactive workshop to identify knowledge gaps and implications for future research. This work was instrumental in developing what will be our next funding call on Economic Incentives (to be launched early 2020) and in providing an evidence base for the NCSC's upcoming Cyber Insurance Buyers Guide. This workshop was testament to the value of bringing a diverse multidisciplinary set of minds together to work on complex sociotechnical cyber security problems.

This work provided an evidence base for the NCSC's upcoming Cyber Insurance Buyers Guide.

WHITE HALLS AND IVORY TOWERS: JUNE 27

Strengthening our research impact and the extent to which we reach out to external stakeholders was a key goal for us in 2019. We have focused these efforts largely on our interactions with the UK policy community in the first instance – with more work on industry and the third sector to come in 2020. In pursuit of this, we collaborated with Sarah Foster (DCMS) and Jenny Bird from the Policy Impact Team in UCL STEaPP to run a policy workshop at the ACE-CSR Conference. ***White Halls and Ivory Towers*** allowed us to gather valuable insight into the reasons why technical researchers abstain from participating in knowledge exchange activities with the policy community. The findings from this event informed a subsequent funding proposal for the Policy Impact Unit to support RISCS researchers in these activities (see below).

INNOVATE UK GLOBAL EXPERT MISSION TO SINGAPORE: SEPTEMBER 30 – OCTOBER 5

In my capacity as Director of RISCS, I visited Singapore as part of an Innovate UK Global Expert Mission. While there, I met with the Singapore National Research Foundation, the Cyber Security Agency and many private sector and academic stakeholders. There is a real appetite in Singapore for work on the human and organisational factors of cyber security and we are now exploring the potential for collaboration between the RISCS community and colleagues in Singapore. There are numerous opportunities for RISCS researchers in the form of live implementations of cyber-physical systems in Singapore that would provide scope for joint research projects. We are working with the British High Commission on an exchange program to take some RISCS researchers to Singapore in early 2020.

ROUNDTABLE ON RISCS STRUCTURE, DIRECTION AND RESEARCH THEMES: NOVEMBER 22

By November, we had developed a number of initiatives, plans and proposals that had been discussed with our Advisory Board and upon which we wished to seek input from our community. We hosted a roundtable to present our ideas and to encourge an open discussion on them. We had a very engaged and active conversation about our proposed plans and took away a lot of great feedback. We've had strong support for our plans and following the input we received at this workshop and from our Advisory Board, we are pleased to be able to present the following agenda for 2020.

New Funding Call on Economics and Incentives: We are delighted to announce an open funding call specifically targeted at work that expands our evidence based knowledge on the economics of and incentives for cyber security. The work that we have done as a community through various workshops over 2018 and 2019 has demonstrated that there is a lot more to understand about the economics of cyber security. It has also become clear that this is an area in which the RISCS community has plenty to offer. We will be funding up to five 12-month projects in the first quarter of 2020.

Airbus Human-Centric Cyber Security Accelerator Programme: Sponsored by Airbus and the Welsh Government, Kevin Jones (CISO, Airbus) and Ceri J (NCSC) have pioneered the creation of a human-centric accelerator. The Accelerator, led by Dr Phil Morgan of Cardiff University, will offer placements for qualifying university students and establish collaboration opportunities with research teams and businesses. The expectation is that RISCS will be a significant cog in the initiative: feeding in research that can be trialled and refined in an industry setting.

Impact Support: Developing more effective mechanisms for delivering impact through our RISCS research led us to trial a few different things this year. Supported by our findings from the ***White Halls and Ivory Towers*** event, we have developed two key initiatives to take forward in 2020. The first is the implementation of 'Impact Lenses' (the first of which will be the NHS) which will form test beds or use cases allowing us to both demonstrate the real world applications for our work (transferrable more widely) while simultaneously providing support to an important component of the UK social fabric. The second exciting initiative that we can announce here is that we have formed a partnership with the Policy Impact Unit at UCL to bring on board a part time Policy Impact Officer. This person will work with RISCS researchers to help them to share their work with the UK policy community. We recognise that this is a specialist skill and not one that academics necessarily possess or have time to develop. We believe that the Policy Impact Officer is a missing link in UK academic-policy collaboration.

> **There is a lot more to understand about the economics of cyber security - and the RISCS community has a lot to offer in developing that knowledge.**

RISCS Fellows: When the RISCS community was smaller and more niche, having the Director develop and curate the community activities made sense. But the sociotechnical research community has grown rapidly over recent years and we want to draw on the depth and breadth of expertise of our members more comprehensively now. For this reason, we are introducing RISCS fellows to begin to devolve this leadership function. These Fellows will be provided with a budget and comprehensive support from the RISCS team to develop and implement a community agenda aligned to one of our research themes. This new, expanded structure will allow us to maximise the input of the talented, creative and ambitious people we have in the RISCS community. It will also allow for RISCS sub-communities to thrive and develop in a more bottom-up manner, supported fully by the infrastructure that we have in place across the Institute.

We believe that all of this sets us on the path to an exciting, dynamic year for RISCS in which we continue to think creatively about how best to carry out and pull through sociotechnical research into cyber security. We're absolutely committed to contributing fully to the already high functioning, collaborative community of UK research and innovation. In doing so, we will also strengthen our links internationally, bringing RISCS research to a global platform and acting as a portal for the world's best sociotechnical cyber security researchers to engage with our community here.

Many thanks again to everyone who has supported us, challenged us, worked alongside us and engaged with us this year. You make RISCS what it is.

Professor Madeline Carr, RISCS Director

Research Institute in Sociotechnical Cyber Security

The Research Institute in Sociotechnical Cyber Security is the UK's first academic Research Institute to focus on understanding the overall security of organisations, including their constituent technology, people and processes. RISCS takes an evidence based and inter-disciplinary approach to addressing cyber security challenges. By providing a platform for the exchange of ideas, problems and research solutions between academia, industry, and both the UK and international policy community, RISCS promotes and supports the development of scientifically rigorous sociotechnical approaches to cyber security. Central to the RISCS agenda is the application of bodies of knowledge to stimulate a transition from 'common practice' to 'evidence-based best practice' in cyber security.

UCL Department of Science, Technology, Engineering and Public Policy (UCL STEaPP)

The UCL Department of Science, Technology, Engineering and Public Policy (UCL STEaPP) is the host institution for RISCS. STEaPP academics explore how scientific and engineering expertise can meaningfully engage with public decision making and policy processes to tackle pressing global issues and improve public wellbeing.

UCL STEaPP is a uniquely policy-oriented department which sits across three UCL faculties: the world class Faculty of Engineering, the Bartlett Faculty of the Built Environment and the Faculty of Mathematical and Physical Sciences.

To find out more visit: www.ucl.ac.uk/steapp

REPORT AUTHORS
Madeline Carr
Alex Chung
Emma Bowman

RISCS MANAGEMENT TEAM

Madeline Carr
RISCS Director, UCL

Helen L
Technical Director, Sociotechnical Security Group, NCSC

Lizzie Coles-Kemp
Deputy Director, Royal Holloway University of London

Geraint Price
Chair of Practitioners' Panel, Royal Holloway University of London

Awais Rashid
Chair of the Scientific Advisory Board

Alex Chung
Research Fellow, UCL STEaPP

Emma Bowman
RISCS Institute Administrator, UCL

RISCS ADVISORY BOARD

Alex Ashby
ESC Labs Ltd

JP Cavanna
Lloyds Register Foundation

Lizzie Coles-Kemp
Royal Holloway University of London

Peter Davies
Thales

Samantha Dowling
UK Home Office

Emma Green
DCMS

Kerry Gibson
Ministry of Defence

Chris Hankin
Imperial College London

Larry Hirst
former Chairman of IBM Europe, Middle East and Africa

Shari Lawrence Pfleeger
Pfleeger Consulting

Paul Lewis
Elsevier

John Madelin
Cognizant

Aad van Moorsel
Newcastle University

Geraint Price
Royal Holloway University of London

Adam Shostack
Shostack Associates

Paul Taylor
KPMG

RISCS SCIENTIFIC ADVISORY BOARD

Awais Rashid (Chair)
University of Bristol

Thomas Gross
University of Newcastle

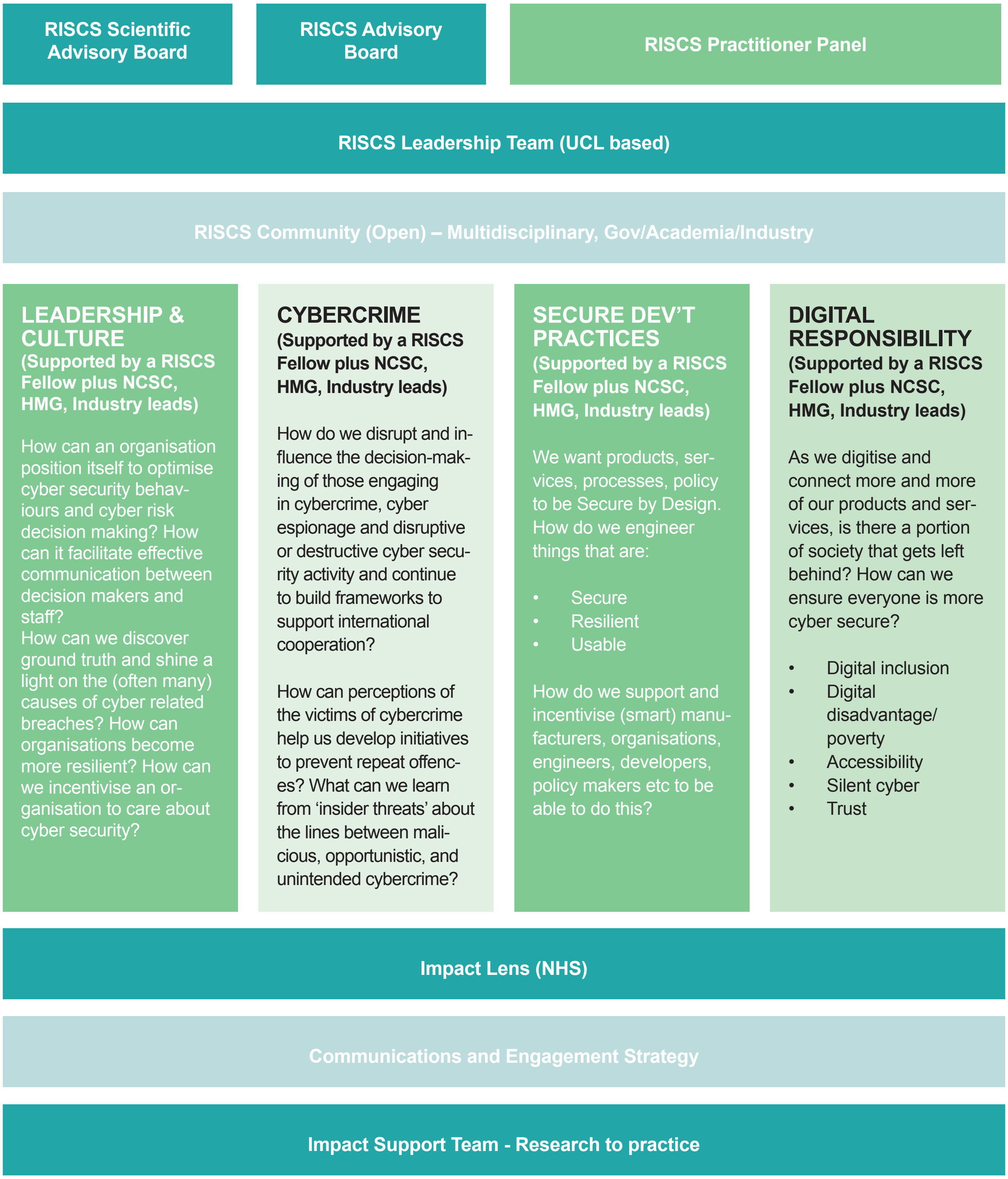
Shujun Li
University of Kent

Ine Steenmans
University College London

David Wall
University of Leeds

RISCS Structure and Research Themes

In 2019, we introduced four research ‘themes’ into RISCS. These provide structure and strategy to our work and have been drawn from those issues that we feel are most relevant to supporting the UK’s efforts in improving sociotechnical cyber security. The research themes allow us to build sub-teams of interested academics, policy makers, industrial partners and NCSC leads. They also create areas of critical mass and focus that are large enough to attract funding from other sources to facilitate real change. These themes and the structural diagram below are the framework for how RISCS will operate through 2020 and into 2021.



RISCS Scientific Advisory Board

RISCS Advisory Board

RISCS Practitioner Panel

RISCS Leadership Team (UCL based)

RISCS Community (Open) – Multidisciplinary, Gov/Academia/Industry

LEADERSHIP & CULTURE

(Supported by a RISCS Fellow plus NCSC, HMG, Industry leads)

How can an organisation position itself to optimise cyber security behaviours and cyber risk decision making? How can it facilitate effective communication between decision makers and staff?
How can we discover ground truth and shine a light on the (often many) causes of cyber related breaches? How can organisations become more resilient? How can we incentivise an organisation to care about cyber security?

CYBERCRIME

(Supported by a RISCS Fellow plus NCSC, HMG, Industry leads)

How do we disrupt and influence the decision-making of those engaging in cybercrime, cyber espionage and disruptive or destructive cyber security activity and continue to build frameworks to support international cooperation?

How can perceptions of the victims of cybercrime help us develop initiatives to prevent repeat offences? What can we learn from ‘insider threats’ about the lines between malicious, opportunistic, and unintended cybercrime?

SECURE DEV’T PRACTICES

(Supported by a RISCS Fellow plus NCSC, HMG, Industry leads)

We want products, services, processes, policy to be Secure by Design. How do we engineer things that are:

- Secure
- Resilient
- Usable

How do we support and incentivise (smart) manufacturers, organisations, engineers, developers, policy makers etc to be able to do this?

DIGITAL RESPONSIBILITY

(Supported by a RISCS Fellow plus NCSC, HMG, Industry leads)

As we digitise and connect more and more of our products and services, is there a portion of society that gets left behind? How can we ensure everyone is more cyber secure?

- Digital inclusion
- Digital disadvantage/ poverty
- Accessibility
- Silent cyber
- Trust

Impact Lens (NHS)

Communications and Engagement Strategy

Impact Support Team - Research to practice

Research Themes

LEADERSHIP AND CULTURE

Cyber security is central to the health and resilience of any organisation and this places it firmly within the responsibility of the Board. But it also means that enabling and facilitating good cyber security practices spans the whole of an organisation and is not simply the remit of the IT or technical teams.

Supporting those people in leadership positions of an organisation to make the best possible decisions about cyber security practices is desperately needed. This includes:

- Support to navigate cyber risk management,
- Providing accurate and relevant data/ information presented in the most effective way,
- Understanding the economics and incentives of cyber markets,
- Facilitating a shared narrative and language between leaders, staff and cyber security experts

This theme will draw through previous RISCS research as well as the Cyber Readiness for Boards research project currently in progress. It will harvest the outputs of the recent work into economics, regulation and incentives by RISCS, NCSC and DCMS to provide input into future cyber security policy and legislation.

CYBERCRIME

Understanding how people behave, both individually and in groups, is a central research theme for the Sociotechnical Research Group, RISCS' partner in the NCSC. To date, this work has mostly been focused on those people whose intentions are non-malicious and who simply want to do a good job. To understand the full spectrum of people in cyber security, we need to understand the intentions, drivers and behaviours of those who have more malicious aspirations as well as those who inadvertently find themselves as “accidental insiders”. This is important for policymakers and practitioners for helping inform how best to prevent and deter people from getting involved in cyber crime in the first place, as well preventing re-offending amongst those who are already involved.

This research theme pulls together the cybercrime research projects funded by Home Office funded by the Home Office, via the National Cyber Security Programme and will further expand to include work that can provide insights into topics such as insider threat, online harms and supporting victims of cybercrime.

SECURE DEVELOPMENT PRACTICES

Secure by Design is extremely high on HMG's list of priorities, whether that is to facilitate secure by default IoT commodity products for the consumer or reducing online harm by ensuring that companies have the right processes and systems in place to fulfil their obligations. Secure by Design is the first cousin of Safety by Design and Privacy by Design, and the three need to work in harmony (via both a cross-government and global collaborative effort) to ensure clarity for manufacturers, developers and engineers.

There is a plethora of advice, guidance, standards, and frameworks that has existed for a number of years for secure software development. However, real-world evidence and our own RISCS portfolio of Developer Centred Security has demonstrated that these resources have struggled to engage and be relevant to software developers. Existing resources also contain little on usability and resilience.

This theme will continue this work and expand the remit to reach across a number of engineering and manufacturing disciplines and sectors to address this issue and support businesses to embed security during the development or update of their products and services.

DIGITAL RESPONSIBILITY

As we digitise and connect more and more of our products and services, we need to ensure that cyber security remains inclusive and that everyone is more secure. This theme will work across different existing research areas such as digital inclusion, digital disadvantage / poverty, digital accessibility, and trust, but through a cyber security lens. It will expand as required to deliver actionable advice into the various cyber security initiatives that HMG delivers, as well as important insights into UKRI led programmes such as Online Harms.

Research Stocktake

RISCS is now entering its eighth year and, we felt it would be useful to provide an overview of what we have produced over this time. Alex Chung has been working this year on a Research Stocktake to bring together the outputs of the many research projects and activities that RISCS has co-ordinated. These pages provide some of our history and how the Research Institute and its research activities have evolved over time. They also provide insight into the difference that our work has made to the UK cybersecurity ecosystem.

'Phase 1' of RISCS began in October 2012 with £3.8 million in funding over three and a half years from a partnership of GCHQ, the Department for Business, Innovation, and Skills, and the Engineering and Physical Sciences Research Council (EPSRC), part of the Research Councils' Global Uncertainties Programme (RCUK). RISCS was tasked with creating an evidence base that would allow both the RISCS researchers and security practitioners to answer two questions: How secure is my organisation? How can I make better security decisions? The four projects that evolved from these questions were:

PRODUCTIVE SECURITY

PI: Prof Angela Sasse

GAMES AND ABSTRACTION

PI: Prof Chris Hankin

CYBER SECURITY CARTOGRAPHIES

PI: Prof Lizzie Coles-Kemp

CHOICE ARCHITECTURE

PIs: Prof Aard Van Morsel & Pam Briggs

The NCSC and HMG have enjoyed some excellent pull through and impact from these projects that include:

- NCSC Password Guidance
- NCSC You Shape Security Guidance
- RISCS, HP Enterprises & NCSC White Paper: "Awareness is just the First Step"

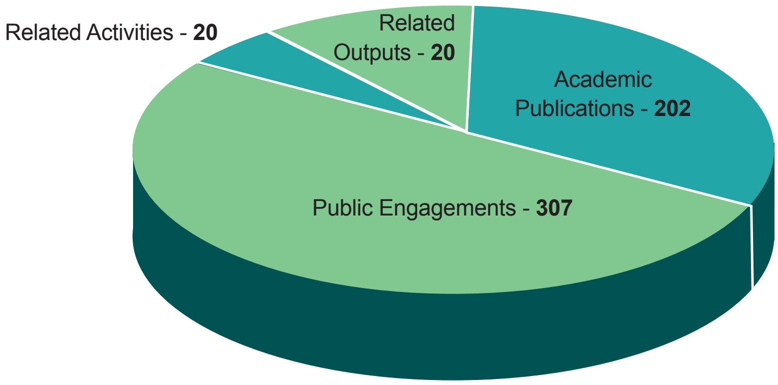
RISCS is now approaching the end of 'Phase 2'. In this phase, funding has predominantly come from the National Cyber Security Programme (NCSP) budget (with a small amount from EPSRC for administrative costs).

The main activities and projects in this Phase have centred around the topics:

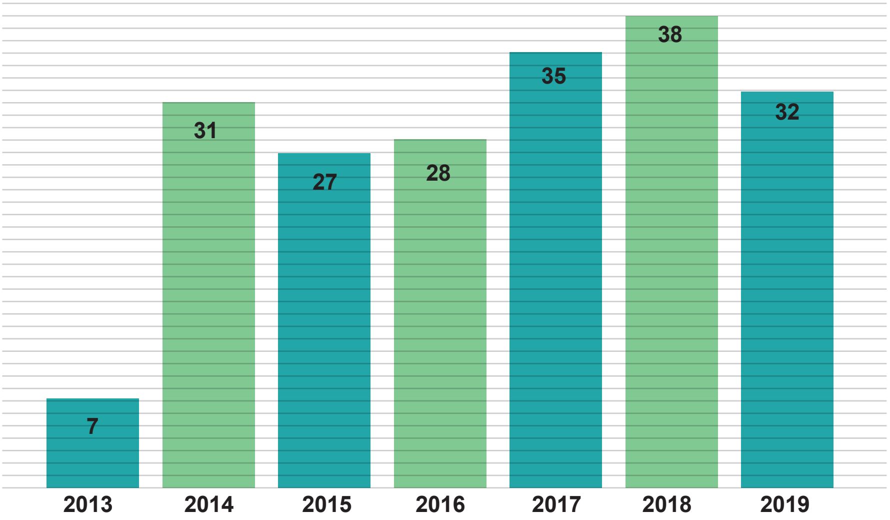
- Developer Centred Security
- Cyber Crime
- Supporting the Board
- Economics and Incentives
- IoT

This research has produced material that has fed into the NCSC's Board Toolkit as well as two pieces still in draft: Software Engineering Best Practice and Cyber Insurance Advice and Guidance Buyers Guide. The pages of this Annual Report document ongoing research projects and also the long-tail impact of some projects that continue to produce impact beyond their formal term of funding. In addition, below are some infographics that provide insight at a glance into our activities and outputs.

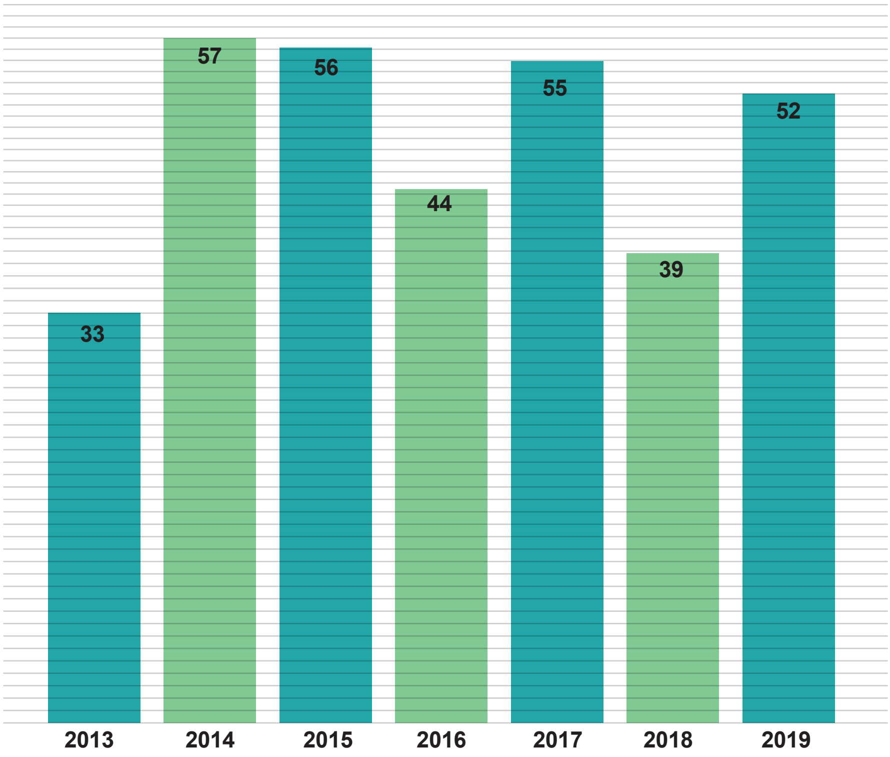
RISCS Outputs and Activities 2013 - 2019 (39 Projects)



RISCS Academic Publications 2013 - 2019



RISCS Stakeholder Engagements 2013 - 2019



RISCS at a glance: Research and Policy Impacts

RISCS academic publications contributed to:

- NCSC Engineering Best Practice (forthcoming)
- NCSC Cyber Insurance Buyers Guide (forthcoming)
- NCSC You Shape Security Guidance, 2019
- NCSC Board Toolkit, 2019
- NCSC People are the Strongest Link campaign 2017
- US NIST Password Guidance, 2017
- US National Academies of Science Report, 2017
- NCSC Password Guidance, 2015
- RISCS, HP Enterprises and NCSC White Paper, 2015

RISCS related activities contributed to:

- ENISA Cybersecurity Culture Guidelines, 2019
- DCMS Secure by Design Guidance, 2019
- NCSP-Local & MHCLG St George's House Report, 2019
- UK Parliamentary expert witness testimony, 2018
- UK Parliamentary expert witness testimony, 2017
- Fraud prevention advice to Gumtree, 2017
- DCMS Cyber Security Regulation and Incentives Review, 2016

RISCS

Project updates

RISCS

Research Institute in Sociotechnical Cyber Security

RISCS (PHASE 2)
PROJECT UPDATES:

ACCEPT: Addressing Cyber security and Cybercrime via a co-Evolutionary aproach to reducing human-relaTed risks

PROJECT LEAD: Professor Shujun Li, University of Kent

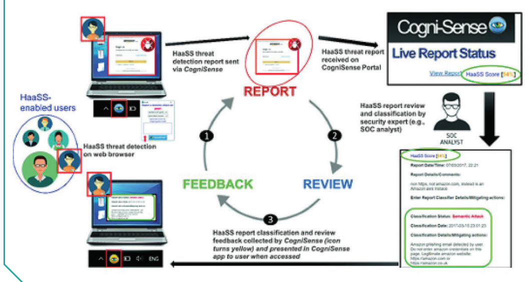
THE AIM OF THIS PROJECT IS TO DEVELOP A NEW SCIENTIFIC, evidence-based framework for guiding the development of software tools to tackle problems associated with human-related risks in the cyber security and cybercrime ecosystems, particularly with a view to countering the rapidly evolving threats in the cyber-physical world. ACCEPT focuses on two problematic areas: how to enhance the effectiveness and efficiency of the cyber threat intelligence collection process from people, and how to help people to be more informed about cyber threats and behave more securely. To successfully develop real-world systems that address these issues, a holistic framework is needed to guide system designers and to effectively engage individual users of those systems.

As the project concludes in early 2020, we are busy with the final phase of two main use cases. To design a system that truly grounds itself in robust evidence and addresses real-world challenges, that system should be tested ‘in the wild’ with real users. To this end, the project team have devised two use cases through which two separate contextualised software systems are being developed and will be piloted before we can recommend them for wider deployment. The two use cases are human-related privacy risks within hybrid transportation networks based on a segmentation based approach, and Human-as-a-Security-Sensor (HaaSS) with a feedback loop for more user-centric and interactive security reporting.

Use case one looks at privacy risks caused by location sharing online (e.g., via Google Maps). A mobile app is being developed to allow individual users to monitor how they share location information and to selectively report data to the project team in order to help others and be helped. By “help others”, we mean that the data shared can be aggregated on the project team’s side to understand the collective behaviour of all participating users so that we can have more useful intelligence to decide how to support those users who need help. By “be helped”,

> **“A mobile app is being developed to allow individual users to monitor how they share location information.”**
>
> ***Shujun Li***

Figure 1. The HaaSS System with a Feedback Loop
Source: PriVELT project poster


HaaSS threat detection report sent via CogniSense
REPORT
HaaSS threat report received on CogniSense Portal
Cogni-Sense
Live Report Status
View Report
HaaSS Score [94%]
HaaSS-enabled users
HaaSS threat detection on web browser
1
2
HaaSS report review and classification by security expert (e.g., SOC analyst)
SOC ANALYST
FEEDBACK
REVIEW
3
HaaSS report classification and review feedback collected by CogniSense (icon turns yellow) and presented in CogniSense app to user when accessed
ENG

we mean that by actively sharing data, each participating user will have an opportunity to gain a better understanding of their own location sharing behaviour and privacy risks, especially compared with others, and to "pull" useful feedback (situational awareness information, advice, and recommendations, etc.) on how to adapt their behaviour to better protect themselves. The word "pull" is important here as the project team's server will aggregate (pseudo-)anonymised data to form segment-specific feedback to all users without actually storing their personal data (e.g., name and email address). The pulling is done by the user's mobile app which periodically checks with the project server to download what the app considers useful for that individual. This is based on the segment that the user belongs to, therefore achieving "personalisation" and "contextualisation" without the need for the project server to store sensitive personal data. In this use case, we plan to recruit users "in the wild" by putting the developed app on Google Play, with the project team simulating the role of organisations and cyber security experts who provide cyber security services to individuals (e.g., LEAs and cyber security awareness campaigns). If our experiment gives positive evidence, we will try to influence relevant organisations to repeat our experiment in a more realistic environment (e.g., LEAs serving potential victims and their carers).

Use case two takes as its starting point an existing security incident reporting system called 'Human-as-a-Security-Sensor' (HaaSS) also called Cogni-Sense, developed by George Loukas's group at the University of Greenwich, an unfunded partner of the project. By adding a feedback step into HaaSS, we create a closed-loop system to allow more user-centric interactions between users (reporters) and the organisations receiving such security reports. This use case simulates the widely used security reporting systems in many organisations, and does not aim at completing anonymising data submitted from users. Instead, we aim to validate our hypothesis that the feedback loop will help change the users' behaviour positively so that they become more willing to report and their reports become more accurate over time as their knowledge about cyber attacks improves. The system is designed to allow easy upgrading of existing open loop reporting systems, to facilitate deployment in the real world. Our planned experiment in the project will be a pilot with a simulated IT department (played by the project team) working with recruited human participants, but if the experiment produces positive evidence, we will try to promote the new security reporting system to organisations and conduct more realistic experiments in real-world environments.

Professor Shujun Li, University of Kent

Shujun Li is Professor of Cyber Security at the School of Computing and Director of the Kent Interdisciplinary Research Centre in Cyber Security (KirCCS), University of Kent. His research interests are mostly around the interplay between cyber security and privacy, human factors, digital forensics and cybercrime, and multimedia computing. His work also involves practical applications of AI, especially human-in-the-loop AI and human-machine teaming. He is on the Scientific Advisory Board of RISCS.

PUBLICATIONS

- *Pogrebna, G., Renaud K, Taratine B. (2019). 'The many faces of active cyber.' Network Security, 2019(2), pp. 20.*
- *Pogrebna, G., Skilton M. (2019). 'Navigating New Cyber Risks: How Businesses Can Plan, Build and Manage Safe Spaces in the Digital Age.' (1st edition). Springer Nature Switzerland AG: Palgrave Macmillan.*
- *Ng, Irene C.L., Wakenshaw, S. (2019). 'Service Ecosystems: A timely worldview for a connected, digital and data-driven economy.' Handbook of Service Dominant Logic Sage Publications Ltd.*
- *Morris J, Becker I, Parkin S. (2019). 'In Control with no Control: Perceptions and Reality of Windows 10 Home Edition Update Features. Workshop on Usable Security (USEC).'*
- *Michael McGuire. (2019). Social Media Platforms and the Cybercrime Economy.*
- *Islam T. et al. (2019) 'A Sociotechnical and Co-evolutionary Framework for Reducing Human-Related Risks in Cyber Security and Cybercrime Ecosystems.' In: Wang G., Bhuiyan M., De Capitani di Vimercati S., Ren Y. (eds) Dependability in Sensor, Cloud, and Big Data Systems and Applications. DependSys 2019. Communications in Computer and Information Science, vol 1123. Springer, Singapore*

RISCS (PHASE 2) PROJECT UPDATES:

CSALSA: Cyber Security Across the Lifespan

PROJECT LEAD: Professor Adam Joinson, University of Bath

THE CSALSA PROJECT FOCUSSES ON HOW CYBER SECURITY is understood by people over the course of their lives and how that (changing) understanding relates to their risk and behaviour. Prior work has demonstrated that there are unique security challenges at different life stages and understanding more about these distinctions is significant. Many changes occur during an individual's lifetime including the resources we draw upon (family, friends, work colleagues), and the power structures within these relationships which also shift over time. These changing factors play a part in determining how individuals interact with technology products and services. This project studies how these factors intertwine and interact to determine individual responses.

To explore this, cSALSA ran a highly interactive and successful workshop in March 2019 on 'communicating about cyber security'. We invited policy makers and practitioners from across government. We looked in depth at how people talk about cyber security, and where they seek advice. Subsequently, the project team has worked with the Home Office and Multi-Agency Commissioning Group (MACG) on cyber security awareness, as well as supporting the refresh of 'cyberaware'.

Our research papers from the cSALSA project are now beginning to appear. We are delighted to have had work accepted to ACM CHI and SOUPS that has explored older adults cyber security and the ways in which experts and users differentially value security behaviours like updating.

We now have a working dictionary for the automated analysis of cyber security texts - look out for its release in early 2020. The dictionary will allow researchers and practitioners to analyse cyber security texts - including interviews and press articles - using automated systems in seconds rather than months. For instance, we have recently run a comparison of over 1000 press and trade articles from the 1990s to the present day, and have identified patterns in how the press have been reporting cyber security. Specifically, over time, articles have become more focused on threats and incidents, with less emphasis on how to protect ourselves.

> **"There are unique security challenges at different life stages and understanding these is important."**
>
> ***Adam Joinson***

Professor Adam Joinson, University of Bath

Adam is Professor of Information Systems at the University of Bath. He conducts research on the intersection between technology and behaviour - including work on communication patterns, influence, security and privacy, and how design can influence behaviour.

PUBLICATIONS

- *Jones S, Collins E, Levordashka A, Muir K, Joinson A. (2019). What is 'Cyber Security'?. doi: 10.1145/3290607.3312786*

RISCS (PHASE 2)
PROJECT UPDATES:

Detecting and Preventing Mass Marketing Fraud **(DAPM)**

PROJECT LEAD: Professor Monica Whitty, University of Melbourne

THE DAPM PROJECT RAN IN 2016 and focused on understanding why individuals are scammed online, the stages involved in these scams, who is likely to become a victim and how these scams can be detected. Mass-marketing fraud (MMF) is a type of fraud that exploits mass communication techniques (e.g., email, Instant Messenger, bulk mailing, social networking sites, telemarketing) to con people out of money. It is easy to underestimate the frequency of this category of fraud. As Whitty points out, there are more victims of computer fraud than there are people whose homes are broken into. The project continues to generate valuable impact and outputs.

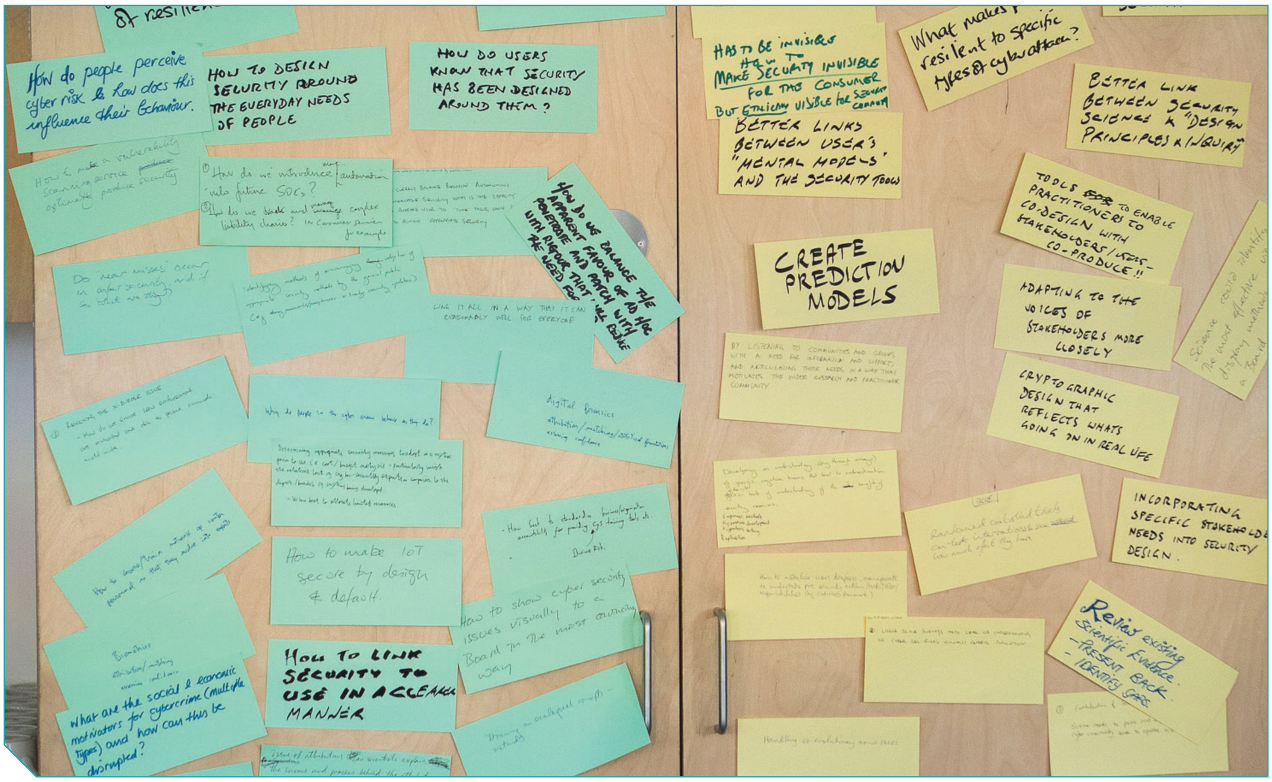
Professor Monica Whitty, University of Melbourne, Australia

Monica holds a full-time Chair in Human Factors in Cyber Security at the University of Melbourne and a part-time Chair in Human Factors in Cyber Security at the University of Warwick. She is also a committee member of the Global Futures Council on Cyber Security for the World Economic Forum. She is a cyber-psychologist whose research over the last 20 years has focused on how individuals behave in cyberspace.

PUBLICATIONS

- *Whitty, M. T. (in press). Predicting susceptibility to cyber-fraud victimhood. Journal of Financial Crime.*
- *Whitty, M. T. (in press). Who can spot an online romance scam? Journal of Financial Crime*

> **“There are more victims of computer fraud than there are people whose homes are broken into.”**
>
> ***Monica Whitty***


How do people perceive cyber risk & how does this influence their behaviour.
HOW TO DESIGN SECURITY AROUND THE EVERYDAY NEEDS OF PEOPLE
HOW DO USERS KNOW THAT SECURITY HAS BEEN DESIGNED AROUND THEM?
HOW DO WE BALANCE THE APPARENT FAVOUR OF AD HOC PENETRATE AND PATCH WITH RIGOUR THAT... THE NEED FOR
How to make IoT secure by design & default
HOW TO LINK SECURITY TO USE IN A CCEAKA MANNER
How to show cyber security issues visually to a Board in the most convincing way
What are the social & economic motivators for cybercrime (multiple types) and how can this be disrupted?
digital forensics
HAS TO BE INVISIBLE
How TO MAKE SECURITY INVISIBLE FOR THE CONSUMER BUT ETHICALLY VISIBLE FOR SECURITY COMMUNITY
What makes ... resilent to specific types of cyberattacks?
BETTER LINKS BETWEEN USER'S "MENTAL MODELS" AND THE SECURITY TOOLS
BETTER LINK BETWEEN SECURITY SCIENCE & "DESIGN PRINCIPLES & INQUIRY"
TOOLS ~~FOR~~ TO ENABLE PRACTITIONERS TO CO-DESIGN WITH STAKEHOLDERS/USERS - CO-PRODUCE!!
CREATE PREDICTION MODELS
BY LISTENING TO COMMUNITIES AND GROUPS WITH A NEED FOR INFORMATION AND SUPPORT, AND ARTICULATING THEIR NEEDS IN A WAY THAT MOTIVATES THE WIDER RESEARCH AND PRACTITIONER COMMUNITY
ADAPTING TO THE VOICES OF STAKEHOLDERS MORE CLOSELY
CRYPTOGRAPHIC DESIGN THAT REFLECTS WHATS GOING ON IN REAL LIFE
INCORPORATING SPECIFIC STAKEHOLDER NEEDS INTO SECURITY DESIGN.
Review existing Scientific Evidence. - PRESENT BACK - IDENTIFY GAPS
LINK IT ALL IN A WAY THAT IT CAN REASONABLY WELL FOR EVERYONE

RISCS (PHASE 2) PROJECT UPDATES:

Evaluating Cyber Security Evidence for Policy Advice (ECSEPA)

PROJECT LEAD: Professor Madeline Carr, University College London

THE ECSEPA PROJECT WAS DESIGNED TO PROVIDE SUPPORT for the cyber security policy community in the UK, specifically those civil servants who rely upon various sources of evidence to provide short and longer-term policy advice. We regard this cohort as particularly significant to UK cyber security for several reasons. First, they are a relatively small and disparate group, with varying levels of technical expertise and experience in this field. Second, their responsibility and impact go well beyond their own organizations to shape the national and international landscape. As such, their decisions are acutely important to the UK's global standing. And finally, there is a real lack of research to support these people, either in identifying specific challenges they face or in developing more effective mechanisms for the work they do.

ECSEPA had three main objectives:

1. Evaluate what exactly constitutes the evidence presented to and accessed by UK policy advisors, how they privilege and order that evidence and what the quality of that evidence is.
2. Identify the particular challenges of decision making in this context and evaluate how effectively policy advisors make use of evidence for forming advice.
3. Develop a framework to assess the capacity of evidence-based cyber security policymaking that can be used to make recommendations for improvement and that can be re-applied to other public, private, and international cohorts.

Over the course of the project, we worked very closely with colleagues in HMG, in local government, and in a range of allied agencies and organisations to understand the constraints, challenges and opportunities for support that characterises cyber security policy making in the UK. We first carried out 15 in-depth, confidential interviews with key stakeholders about how they work with evidence. These interviews helped us to develop a set of survey questions that were circulated more widely. We had 69 responses from the UK cyber security policy community, which was indicative in itself, of the interest in this work and the strong desire for more support amongst this cohort. We then used the responses to the survey questions to design a 'policy crisis game' in which we developed an escalating cyber security crisis, fabricated evidence for the participants, and observed their decision making processes as they worked in teams to develop policy alternatives to the scenario.

> "The decisions of civil servants working on cyber security have significant impact on the UK's global standing."
>
> MADELINE CARR

During the final phase of the project from autumn 2018 through late 2019, we completed a number of project deliverables. These included an analysis of our online survey results to show the different types of evidence sources used in cyber security policymaking; feeding these findings into the design of the ECSEPA Policy Crisis Game; hosting two games with government specialists; and disseminating our findings through numerous public engagement activities.

The first game was a condensed version that piloted in October 2018 with a selected cohort of government specialists who had deep technical expertise. They were asked to evaluate a set of fabricated evidence as the crisis presented to them unfolded. The responses submitted by these technical specialists served as a benchmark against which to compare and assess the responses submitted by the policy specialists who participated in the second game. We analysed any discrepancies between the two cohorts to draw out policy implications with regards to evidence engagement and evaluation during a cyber incident and we are working on publishing our findings in technical proceedings over the coming year.

As the ECSEPA project wound down over the latter half of 2019, we took various opportunities to apply our learnings and present our work at national events and international conferences.

- One of the contexts to which the project has contributed is the UK government's effort to establish a community of practice around cyber incident and policy response. We have been invited by several public sector organisations to apply our understanding and approach to the design and running of cyber crisis games at their events between 2018 and 2019. The Ministry of Housing, Communities and Local Government (MHCLG) requested our support with the facilitation of the National Cyber Security Programme (NCSP) Pathfinder Regional Multi-Agency Cyber Exercise 2019 which took place in Westminster, London in January 2019.
- In May, at the request of the London Resilience Group and London Fire Brigade, we helped to create and facilitate a workshop for the conference 'Strategic Coordination Summit: Cyber Emergency Response'. The scenario featured a cyber-physical incident which was designed to explore strategic incident response framework and advisory coordination mechanisms.
- As we had supported the running of the London and Geneva editions of the 2018 Cyber 9/12 Strategy Challenge, we were invited back to a stakeholder meeting in late 2018 at the Royal United Services Institute (RUSI) to feed back our experience and help improve the 2019 competition.
- We have also presented our project findings at a number of public sector and academic events to validate our findings. By sharing our insights at the UK Authority's Public Sector Cyber Forum and Cyber4Good events, we learned just how much our findings on the common challenges faced by policymakers working in cyber security resonated with the audience.
- By presenting our work at the NCSP's Autumn Showcases which took place in Manchester, Bristol and Birmingham in late 2018, we supported MHCLG's efforts aimed at promoting a better understanding of the roles that key national strategic partners play and increasing awareness about the importance of cyber resilience.
- As a follow up from that event, MHCLG invited us to deliver a policy-focused session during a two-day NCSP 2019 consultation event in June at Windsor Castle's St George's House. At that meeting, we highlighted the complexity of the cyber security policy landscape and informational issues in policymaking. The coping mechanisms employed by the policy community in their evaluation of cyber security evidence were discussed, along with suggestions for how research can better support policymaking. This series of collaborations led to the publication of a consultation report after the event and further work on the value of establishing CERT capabilities in the local public sector.

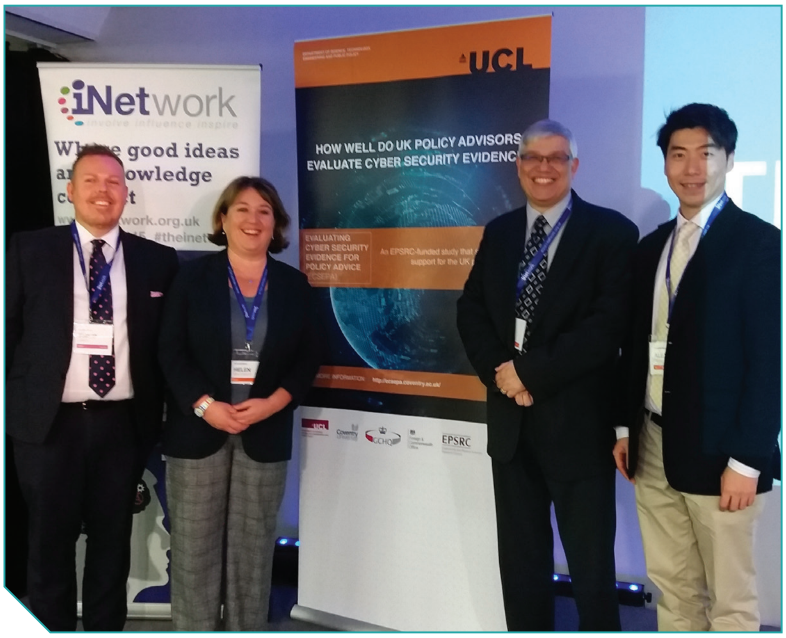
At the Data for Policy 2019 international conference at UCL, the ECSEPA team delivered a presentation based on a joint-authored paper, 'Cyber capacity building and knowledge sharing: The UK policy community's perception of the National

Cyber Security Centre (NCSC).' This talk explored UK policymakers' views on the relevance of NCSC provisions to their work, and their engagement experiences with the NCSC. The presentation also touched upon areas of intervention suggested by the policy community which could help strengthen knowledge sharing practices.

In early 2020, we will be submitting the write-up of our analysis and findings for publication in journal articles and technical proceedings. We will also continue to feed our findings back to the diverse communities and policy stakeholders with whom we have been engaging closely through our work. For ECSEPA updates, visit ***https://www.ucl.ac.uk/steapp/research***

Professor Madeline Carr, UCL

Professor Carr is the Director of the Digital Technologies Policy Lab which supports policy making to adapt to the pace of change in society's integration of digital technologies. Her research looks at the implications of emerging technology for national and global security, international order and global governance. Professor Carr has published on cyber norms, multi-stakeholder Internet governance, the future of the insurance sector in the IoT, cyber security and international law, and the public/private partnership in national cyber security strategies. Her book US Power and the Internet in International Relations is published by Palgrave MacMillan. Professor Carr was the co-lead on the Standards, Governance and Policy stream of the UK's £24M PETRAS research hub on the cyber security of the Internet of Things. She is now the lead on the Economics and Law lens of the new PETRAS National Centre of Excellence in Cyber security of the IoT. Professor Carr is a member of the World Economic Forum Global Council on the IoT. She is also the Deputy Director of a new Centre for Doctoral Training in Cyber security at UCL which focuses on the interdisciplinary nature of these problems.


iNetwork
involve influence inspire
Where good ideas and knowledge connect
UCL
HOW WELL DO UK POLICY ADVISORS EVALUATE CYBER SECURITY EVIDENCE
EVALUATING CYBER SECURITY EVIDENCE FOR POLICY ADVICE
EPSRC

PUBLICATIONS

- *Chung A, Dawda S, Carr M. (2020, forthcoming). 'Engaging with Evidence in UK Cybersecurity Policymaking'.*
- *Chung A, Dawda S, and Carr M. (2020, forthcoming). 'Policymaking Practices and Evidence Pathways in UK Cybersecurity'.*
- *ECSEPA and RISCS contributed to the St George's House Consultation Report by MHCLG: 'Local Leadership in a Cyber Society 3: Building Resilience Together – Lessons for the Future'. Windsor Castle, September 2019.*
- *Hussain A, Shaikh S, Chung A, Dawda S. and Carr M. (2018). 'An Evidence Quality Assessment Model for Cybersecurity Policymaking'. Critical Infrastructure Protection XII, IFIP.*
- *Chung A, Carr M, Dawda S, Hussain A, and Shaikh S. (2018). 'Cybersecurity: Policy', in Encyclopedia of Security and Emergency Management, LR Shapiro and MH Maras eds. Springer Nature.*

RISCS (PHASE 2) PROJECT UPDATES:

EMPHASIS: Economical, Psychological and Societal Impact of Ransomware

PROJECT LEAD: Professor Eerke Boiten, De Montfort University

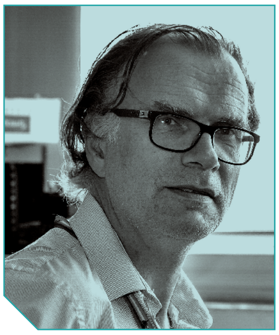
THE EMPHASIS PROJECT SETS OUT TO ANSWER THE FOLLOWING RESEARCH QUESTIONS: Why is ransomware so effective, and why are there so many victims? Who is carrying out ransomware attacks? How can police agencies be helped? What interventions are required to mitigate the impact? The overall goal is to strengthen society's resistance to ransomware to make it less effective, protect and prepare potential victims, whether organisations or citizens, and pursue the criminals.

In order to do so, the project gathers data from Law Enforcement Agencies (which have agreed to closely collaborate with the project), through surveys of the general public and SMEs, and through interviews with stakeholders. The data will be analysed using script analysis, behavioural analysis, and other profiling techniques, leading to narratives regarding the criminals, the victims, and the typical ransomware scenario. Economical and behavioural models of ransomware will then be constructed and used to improve ransomware mitigation and advice, as well as support for law enforcement.

The field of ransomware has evolved as we are seeing more targeted attacks, including at public organisations. We are focused on the development of advice for the best response, which still includes ensuring that paying the ransom is the very last resort. Recent activity includes developing "business models" for ransomware criminals from an economic perspective, and analysing ransomware victimisation experiences to inform recommendations for law enforcement.

Professor Eerke Boiten, De Montfort University

Eerke set up and led Kent's interdisciplinary Research Centre in Cyber Security in 2011, and moved to De Montfort University in 2017, where he now leads the Cyber Technology Institute, freshly accredited as an ACE-CSR, as well as the School of Computer Science and Informatics. Originally a formal software engineering researcher, he now looks at, and comments publicly on, many aspects of cyber security and privacy. His current research projects are in cybercrime, cryptography, privacy impact assessment, refinement and cyber intelligence sharing.



> **"The overall goal is to strengthen society's resistance to ransomware."**
>
> ***Eerke Boiten***

PUBLICATIONS:

- *Cartwright A, Cartwright E. (2019). Ransomware and Reputation. Games, (2), doi: 10.3390/g10020026*
- *Cartwright E, Hernandez Castro J, Cartwright A. (2019). To pay or not: game theoretic models of ransomware. Journal of Cyber security, (1), doi: 10.1093/cybsec/tyz009*
- *Cartwright E, Stepanova A, Xue L. (2019). Impulse balance and framing effects in threshold public good games. Journal of Public Economic Theory, (5), doi: 10.1111/jpet.12359*
- *Hull G, John H, Arief B. (2019). Ransomware deployment methods and analysis: views from a predictive model and human responses. Crime Science, (1), doi: 10.1186/s40163-019-0097-9*
- *Pont J, Abu Oun O, Brierley C, Arief B, Hernandez-Castro J, "A Roadmap for Improving the Impact of Anti-Ransomware Research", In: A. Askarov, R. Hansen, W. Rafnsson (eds) Secure IT Systems, NordSec 2019, Lecture Notes in Computer Science, vol 11875, Springer, Cham, pp. 137-154, 2019.*
- *Connolly L and Wall D.S. (2019) 'The Rise of Crypto-Ransomware in a Changing Cybercrime Landscape: Taxonomising Countermeasures, Computers and Security. Available online, https://doi.org/10.1016/j.cose.2019.101568*
- *Connelly L and Wall D.S. (2019) 'Hackers are making personalised ransomware to target the most profitable and vulnerable'. The Conversation*
- *Connolly L and Wall D.S. (2019) 'Cyber security: Think like the enemy', Computing, 16th July*
- *Wall D.S. (2019). 'Ransomware attacks on cities are rising – authorities must stop paying out'. The Conversation*

RISCS (PHASE 2)
PROJECT UPDATES:

Leveraging the Multi-Stakeholder Nature of Cyber Security

PROJECT LEAD: Professor Christian Wagner, University of Nottingham

MODERN IT SYSTEMS ARE COMPRISED OF A VERY LARGE number of different components and features, making them both diverse and complex. They are commonly spread out across multiple locations, and their inner workings are frequently best understood by different individuals both within and outside a given organisation (e.g. within third party organisations providing key components). A first challenge therefore in understanding the level of vulnerability of a system, is to obtain information on the different aspects and components of a system from this range of individual experts, or 'stakeholders'—each with their own perspective, expertise and individual level of (un)certainty in respect to the vulnerability of given components. At the same time, modern IT systems change rapidly, which means that many repeated assessments may be required to maintain up-to-date vulnerability estimates. This is a problem, as there are too few experts available to make these assessments for what is an ever-growing number of increasingly complex systems.

This project's key objectives are to overcome these two challenges—establishing a strong scientific basis for efficient collection and effective integration of uncertain information from a variety of experts, or other individuals, in order to take advantage of these varied inputs and perspectives to create comprehensive vulnerability assessments that are greater than the sum of their parts. To achieve this, the project combines interdisciplinary strands of research at the interface of quantitative social and computer science.

Our first line of research aims to develop and validate methods to more efficiently extract richer information content from individual responses, with minimal added effort or complexity. One practical example of this is the development of open source software to facilitate more information-rich 'interval-valued' responses, which capture a range representing the uncertainty or variability associated with each response. The initial public release of this software ('DECSYS'—Discrete and Ellipse-based response Capture SYStem), was made at the end of June 2019. Shortly afterwards, a presentation and demonstration of the capabilities of DECSYS was given at our research partner's institution, Carnegie Mellon University, Pittsburgh. A paper with the same purpose was also presented at the 2019 IEEE International Conference on Fuzzy Systems, in New Orleans.

Alongside this, a poster presentation was made at the MathPsych 2019 conference in Montreal, Canada. This summarised experimental results demonstrating the effectiveness of the interval-valued response method in capturing response uncertainty arising from a range of sources. Another paper, which investigated the added value provided by capturing uncertainty in expert ratings in the context of vulnerability assessments of cyber systems, was presented at the 14th International Conference on Critical Information Infrastructures Security (CRITIS) and won the Young CRITIS Award.

Our second line of research focuses on comparing and developing methods for effective integration, handling and modelling of interval-valued data obtained through these new information rich modes of responding. This work is essential as it underpins how one can make best and efficient use of rich information captured from various experts to inform vulnerability assessment of real systems – enabling timely mitigation to be put in place, e.g. via the introduction of additional controls. Much of this work leverages and develops existing work in the area of interval arithmetic and

> "Modern IT systems are commonly spread out across multiple locations, and are frequently best understood by different individuals both within and outside a given organisation"
> *Christian Wagner*

fuzzy sets, which offer an established way to handle data containing uncertainty, or disagreement between input sources. More specifically, interval arithmetic provides the fundamental building blocks for manipulating data which is interval-valued, rather than numeric, while fuzzy sets offer set-theoretical modelling of aggregates of such data, while minimising model assumptions and data loss (e.g. such as from outlier removal). Outputs from this line of work within the project in 2019 included a second paper presented at the FUZZ-IEEE conference, titled 'On Comparing and Selecting Approaches to Model Interval-Valued Data as Fuzzy Sets'. This examined two different methods of aggregating interval-valued responses into fuzzy sets, using real-world data to demonstrate how the methods differ and highlighting which is more appropriate given the assumptions of the data.

Two further journal papers, focusing on modelling and comparison of information in the form of fuzzy sets, were also accepted this year. The first concerns the selection of similarity measures for comparing type-2 fuzzy sets—evaluating common properties between all current options and assessing whether and why certain methods may miss certain properties of the data and the real-world effects that this may have. This is published in Information Sciences. The second explores the relationship between similarity measures and thresholds of statistical significance in the context of fuzzy sets, and is published in IEEE Transactions on Fuzzy Systems. This work is important for determining the conditions under which it may or may not be appropriate to draw meaningful inferences about any differences observed between data in this format.

In 2020, the project is set to conduct a final study to comprehensively demonstrate and show the utility, importance and value of the proposed framework to efficiently capture rich, uncertain quantitative input in order to generate comprehensive assessments based on human insight. Achieving this provides a direct pathway to access and leverage essential insight held by experts across the world. The resulting information can be used directly or can be combined with additional information sources (such as arising from network monitoring), providing a sociotechnical approach to comprehensive vulnerability assessment of value to IT system owners and their stakeholders in the public and private sector.

Professor Christian Wagner, University of Nottingham

Christian Wagner is a Professor of Computer Science at the University of Nottingham and founding director of the Lab for Uncertainty in Data and Decision Making (LUCID). His work ranges from decision support in cyber security and environmental management to personalisation and control in manufacturing. He has led and co-led a number of research projects with partners from industry and government with an overall value of around £10m and co/developed multiple open source software frameworks, making cutting edge research accessible to research communities beyond computer science.

PUBLICATIONS

- *Ellerby, Z., McCulloch, J., Young, J., & Wagner, C. (2019, June). 'DECSYS–Discrete and Ellipse-based response Capture SYStem'. In 2019 IEEE International Conference on Fuzzy Systems*
- *McCulloch, J., Ellerby, Z., & Wagner, C. (2019, June). 'On Comparing and Selecting Approaches to Model Interval-Valued Data as Fuzzy Sets'. In 2019 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE). IEEE.*
- *Ellerby, Z., McCulloch, J., Broomell, S., Wagner, C. (2019) 'The added-value of interval-values – capturing individual response uncertainty'. (MathPsych - Poster presentation): https://osf.io/chuz8/*
- *Ellerby, Z., McCulloch, J., Wilson, M., & Wagner, C. (2019). 'Exploring how Component Factors and their Uncertainty Affect Judgements of Risk in Cyber-Security'. arXiv preprint arXiv:1910.00703.*
- *McCulloch, J., Ellerby, Z., & Wagner, C. (2019). 'On the Relationship between Similarity Measures and Thresholds of Statistical Significance in the Context of Comparing Fuzzy Sets.' IEEE Transactions on Fuzzy Systems.*
- *McCulloch J, Wagner C. (2019). 'Measuring the Directional or Non-directional Distance Between Type-1 and Type-2 Fuzzy Sets With Complex Membership Functions'. IEEE Transactions on Fuzzy Systems, (7), doi: 10.1109/TFUZZ.2018.2882342*

RISCS (PHASE 2) PROJECT UPDATES:

Cyber Readiness for Boards

PROJECT LEAD: Professor Madeline Carr, University College London

> “Board level approaches to cyber risk cannot be understood in isolation of board level approaches to other business risks.”
>
> MADELINE CARR

THE ROLE OF BOARDS IN CONTRIBUTING TO A BROADER AGENDA OF NATIONAL CYBER SECURITY IS WELL ESTABLISHED. Cyber security has been designated a Tier 1 threat to the UK. With 83% of UK critical infrastructure in private hands and the largest digital economy of the G20, the boards of private sector organizations have been identified as critical to enhancing cyber security and resilience. As we move rapidly into more complex technological ecosystems like the Internet of Things which allows not only for data and system breaches but for physical consequences, the relevance of cyber risk assessment is expected to significantly increase in scale and in scope.

Much of the work on how boards understand cyber security focuses on a particular challenge - that of communicating abstract, technical information to a non-specialist audience. While this is acknowledged to be an issue for board risk assessment, it is inadequate as an explanation for shortcomings because it is not a board specific challenge. Communicating technical (or medical, legal, scientific) risk to any non-specialist audience carries the potential for misinterpretation or a lack of understanding. This applies in academia, policy communities, and the general public as well as between boards and cyber security specialists.

Therefore, in order to better understand board decision-making processes on cyber security, we take a multidisciplinary approach tailored to the role of the board rather than tailored to cyber security as an issue of concern. The starting point for this research project is the assertion that board level approaches to cyber risk cannot be understood in isolation of board level approaches to other business risks. Focusing too narrowly on the issue of cyber security obscures broader factors that may have significant implications. This research project looks holistically (and therefore, differently) at how boards approach cyber risk assessment. It qualitatively and quantitatively evaluates a range of existing and proposed interventions. And it develops a framework for improving structures of cyber risk governance.

The overarching aim of this project is to extend existing research on board responses to cyber risks (which largely focus on communication challenges) in order to identify, understand, and account for broader internal and external decision-making factors. There are three clear research objectives around which this project is structured. Each work package explicitly addresses one or more of these.

- Elicit and describe factors influencing current cyber risk decision-making at board level in order to develop a model for evaluating and improving this in the future.
- Develop an understanding of the broader landscape on cyber risk decision-making that includes, but goes beyond, the cyber security executive level / board interaction.
- Evaluate and refine interventions for board development and improvement in cyber risk decision-making.

This project employs a multi-disciplinary and mixed methods approach to address the research objectives. In order to address the aims and objectives of the research project, we work collaboratively and across disciplinary divides to bring in four key explorations:

- An evaluation of training interventions: Axelos is a leading provider of training on cyber risk assessment. They acknowledge that evaluating to outcomes of their programs is essential to continuing to improve and develop their and any similar training interventions.
- An assessment of how boards evaluate cyber risk 'evidence': The 2017 Cyber Breaches Report found that non-specialists reported difficulty evaluating information and advice on cyber security and that they exhibited a lack of trust in the sources they had to rely upon. Understanding which material is most useful to boards and why is essential to better supporting their risk assessments and decision making.
- An investigation into the significance of board composition: Only 29% of businesses in the UK have a board member who is responsible for cyber security. This is one area of possible focus but there are many diverse factors of board composition that can impact on risk assessments. Board composition has to be considered in the context of the boards' capacity to evaluate evidence and the extent to which training programs can help address inadequacies in this area.
- The impact of investor pressure on board decision-making on cyber risk: While some have sought to explain cyber security as a commercial trade-off, the role of investors in shaping board level decision-making on risk has not been taken into account. This work package will help to establish if further engagement with NEDs provides some possible forward momentum for addressing cyber risk assessment.

Each of these four work packages is led by a co-investigator with relevant expertise. Significantly, though, these work packages intersect with and inform one another which allows for the development and validation of a comprehensive framework.

RISCS (PHASE 2) PROJECT UPDATES:

Motivating Jenny to **Write Secure Software**

PROJECT LEAD: Professor Helen Sharp, Open University

> “It is vital to help developers spot security-relevant decisions as they are encountered, to develop their sense of when security is needed and why: to sensitise them to security.”
> *Helen Sharp*

SOFTWARE DEVELOPERS, WHETHER PROGRAMMERS, testers, designers or product managers, typically make hundreds of decisions every day. Very few of those decisions have security implications. So, it is vital to help developers spot security-relevant decisions as they are encountered, to develop their sense of when security is needed and why: to sensitise them to security. Working out how best to achieve this has been the focus of the Motivating Jenny project.

When the project started, its aim was to investigate how to motivate professional software developers, who are not security specialists, to write code that is more secure. Based on research into motivation for software engineering conducted over many years (Sharp et al, 2009; Franca et al, 2018), we took an ethnographic approach to this question. Ethnographic studies can provide an in-depth understanding of the realities of everyday software development practice, i.e., they help to uncover not only what practitioners do, but also why they do it (Sharp et al, 2016). This approach was novel in the security research arena, and highly appropriate because motivation is a very individual concept. In practice, taking an ethnographic approach meant studying software practitioner activities through collaborations with organisations, and engaging with practitioners through face-to-face meetups, online forums and online questionnaires. From the beginning, two organisations agreed to take part in our studies, and over the course of the project, a third organisation adopted one of our practical outputs, to help trial its use. We also interacted with various practitioner groups, deployed an online questionnaire in the UK, India and Brazil, and conducted an in-depth study of questions and comments with a security tag, posted on Stack Overflow up to January 2018.

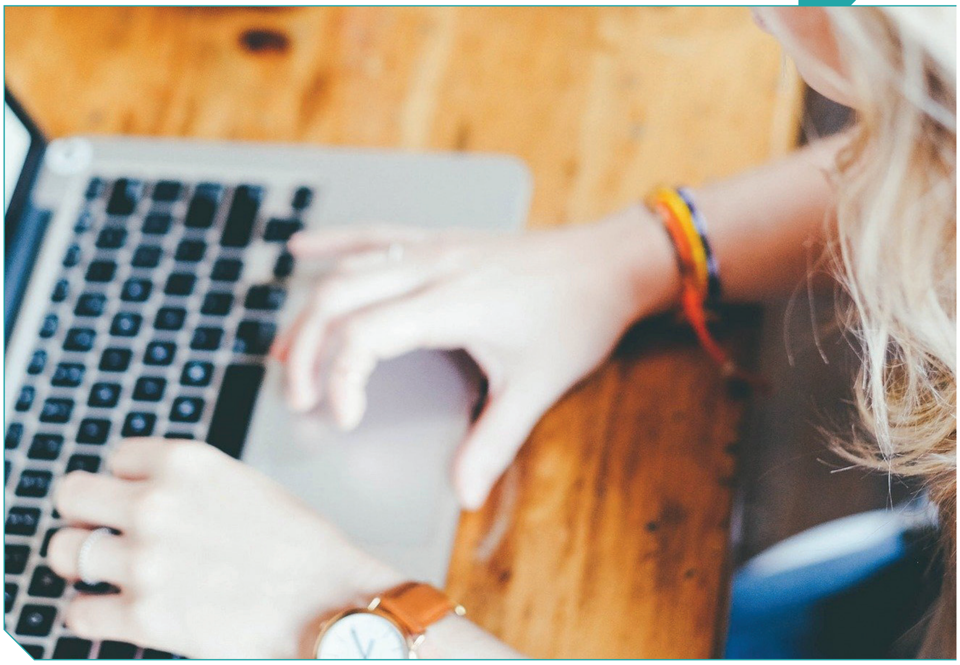
Over the course of the project, we have observed five different responses to tasks that involve security, depending on context rather than on individual motivations. This understanding has emerged from the combination of empirical research with practitioners, and theoretical frameworks, and is underpinned by theoretical and practical insights into developer motivation, developer profiles, attitudes to security and daily development activities.

Each response has positive and negative value in practice, depending on the developer’s own profile and career stage, the context within which the task is located, and how well current knowledge can be translated into specific action for this task. Note that these represent responses rather than lasting attitudes, and several can co-exist in any one developer at the same time. A particular response will come to the fore depending on the situation being considered.

- Worry: “I worry about security. Sometimes I am aware that things could be done better, but I don’t always have the ability to make changes or to make better security a priority.”
- Follow: “I don’t think a lot about security. There are security policies and measures in place where I work and I am able to rely on existing mechanisms in frameworks and infrastructure.”
- Explore: “I am interested in security, I think it is a fascinating topic. I don’t know why, but I just got curious and started reading up and learning things. At some point I realised I know more than others.”
- Engineer: “I believe software should be made secure through engineering. If you say ‘write this piece of software’ I will write it so it does this thing and no other things. Software that does what it is specified to do and nothing else will be secure.”
- Float: “I wouldn’t say I’m an expert, but I have a good understanding about how security works in my organisation. I do this by solving problems that come up and by helping others solve problems.”

There could be the tendency to see a developer exhibiting a strong engineering response as motivated, and one exhibiting a worrying response as lacking knowledge or competence but these need to be seen in context. The responses are signals that can be used to identify areas for improving security practice. For example, if three developers on Project Y are all worrying then that indicates a need for further investigation.

The issue of how to develop more secure coding practices is therefore less about how to motivate developers to write more secure code, and more about creating the conditions within which developers can apply appropriately the knowledge they have gained through other educational and awareness activities. Hence our focus moved towards how to sensitise developers to security.



An articulation of the theoretical findings is still being developed, but these findings have been embedded in four practical outputs. These are presented in detail on our website motivatingjenny.org, together with downloadable packages of materials designed to support practitioners to apply our findings. Each has been developed and deployed with practitioners, and is being actively trialled by practitioners. For example, P1 has been used by our third collaborator, an international business insurance company. They have adopted and adapted P1 for their own use. Specifically, they have used the workshop in their induction programme for new staff. Not only did the inductees provide positive feedback about the approach taken, but our collaborator confirms that the workshop has helped them change the way in which they talk to other areas of the business about security, making those interactions more constructive. Each pack can be tailored to the specific context of a team or organisation, and we provide guidance for tailoring the materials. The four packages are summarised below:

- **P1: Security in the World:** a card-based workshop to inspire awareness using structured discussions of real-world incidents. P1 has been run three times by the research team in different practitioner settings (Lopez et al, 2019), and has also been adopted by our third collaborator (as described in the previous paragraph)
- **P2: Security in the Community:** guidelines to help developers adapt their use of Stack Overflow and other online forums to achieve security. P2 materials have been discussed with and presented to practitioner audiences (Lopez et al, 2020).
- **P3: Security and Me:** a questionnaire designed to identify different attitudes to software security, to form a basis of discussion and reflection. The questions ask about individual work attributes (likes/dislikes and general goals/values) to allow practitioners and teams to loosely associate their own security responses and personal attributes with the tasks/projects that are being undertaken by teams or individuals at the time the questions are answered. This questionnaire has been deployed in India, Brazil and the UK to consolidate our understanding about developer profiles, in particular, motivation factors that are relevant in modern software development contexts, and the prevalence of the responses to security listed above, in a range of organisational settings.
- **P4: Security between Us:** a lego-based workshop to promote learning and discovery about a team's own projects and the context within which security is embedded. P4 has been run several times in our second collaborator organisation, and has been very well-received by developers and managers as a positive and novel approach to exchange experiences and to learn about their working context.

These packages will be of particular interest to developers and managers, while the theoretical developments in motivation and developer profiles will be of particular interest to researchers

.

Study methods and participants

The first organisation was UK-based, with teams located around the world. They were engaged in producing staff scheduling software used by a range of global clients, and developed software using an agile approach. They had been taken over recently by a large American company in the same domain. In this organisation, we spent time at their offices, attended daily ceremonies and meetings, talked informally to staff, and observed how software is developed on a daily basis. This was followed up with more detailed interviews and a workshop. Together, these activities gave us an in-depth view of where security features in day-to-day activities, how developers approach their daily development work, and the significance of security work to individual developers, as well as to the company.

The second organisation was also UK-based and had a strong track record in engineering solutions to tricky technological problems. They had recently been bought by a consultancy company and were integrating themselves into this working environment during our study. In this organisation we interviewed senior technical managers, spent time in the company's offices, talked with members of staff, and conducted selected interviews. We also presented at their weekly technical meetings to discuss our work and the findings, and ran several workshops.

In parallel with these on-site studies, the examination of StackOverflow posts aimed to uncover the significance of security to the developers in this environment, by examining how they talk about it. A strength of including this data corpus is that their security conversations can be observed unobtrusively and analysed in depth. Our field work confirms that developers refer to this and similar online Q&A sites within their daily work.

Professor Helen Sharp, Open University

Helen is Professor of Software Engineering in the Computing and Communications Department of The Open University. She is also Associate Dean for Research, Scholarship and Enterprise in the Faculty of Maths, Computing and Technology. Her main research interest focuses on the human and social aspects of software engineering, leveraging her expertise in both Interaction Design and Software Engineering.

PRESENTATIONS:

- *Lopez, T. presented (2019) "Strategies for Managing Risk in Professional Secure Software Development" at The Social and Behavioural Science for Cyber Security Conference 2019, 25th September, 2019.*
- *Sharp, H. and Lopez, T. (2019) Invited talk at Lancaster University for Security Lancaster research group. "Secure Code Development in Practice: community and culture" 30th January 2019*
- *Lopez, T. and Sharp, H. (2018) "Secure Code Development in Practice", Presentation at mini-SPA 2018, Leeds 26th November*

PUBLICATIONS:

- *Lopez, T., Tun, T.T, Bandara, A., Levine, M., Nuseibeh, B. & Sharp, H. (2019) 'Taking the Middle Path: Learning about Security through Social Interaction' IEEE Software, doi: 10.1109/MS.2019.2945300*
- *Lopez, T., Sharp, H., Tun, T.T., Bandara, A., Levine, M., and Nuseibeh, B. (2019) 'Talking about security with professional developers', In: 7th International Workshop Series on Conducting Empirical Studies in Industry (CESSER-IP), 28 May 2019, Montréal, Canada, doi: 10.1109/CESSER-IP.2019.00014w*
- *Lopez, T., Tun, T.T, Bandara, A., Levine, M., Nuseibeh, B. & Sharp, H. (2019) 'An Anatomy of Security Conversations in Stack Overflow' ICSE 2019, Software Engineering in Society track*
- *Lopez, T., Sharp, H., Tun, T.T., Bandara, A., Levine, M., and Nuseibeh, B. (2019) 'Hopefully We Are Mostly Secure': Views on Secure Code in Professional Practice', in Proceedings of CHASE 2019, workshop at ICSE 2019, doi: 10.1109/CHASE.2019.00023*

RISCS (PHASE 2)
PROJECT UPDATES:

Why Johnny Doesn't Write **Secure Software**

PROJECT LEAD: Professor Awais Rashid, University of Bristol

DEVELOPING SOFTWARE IS NO LONGER THE DOMAIN of the select few with deep technical skills, training and knowledge. A wide range of people from diverse backgrounds are developing software for smart phones, websites and IoT devices used by millions of people. Johnny is our pseudonym for such developers (following Whitten and Tygar's pseudonym for typical users). Currently, little is understood about the security behaviours and decision-making processes of such developers engaging in software development. The overall aim of this EPSRC-funded project is to develop an empirically-grounded theory of secure software development by the masses. Our focus is on understanding:

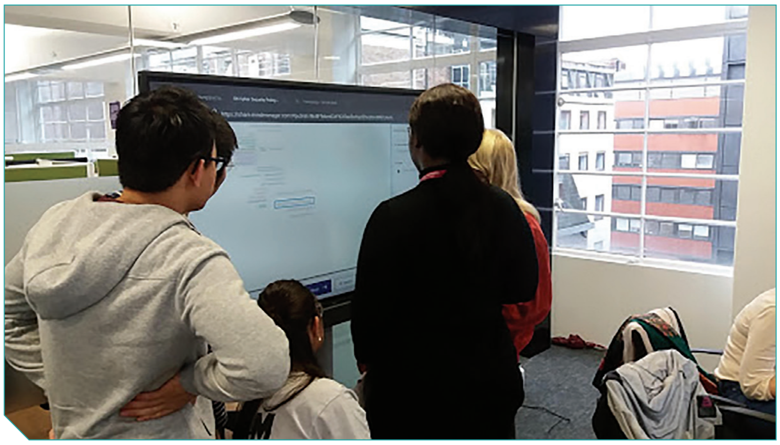
- what typical classes of security vulnerabilities arise from their mistakes,
- why these mistakes occur, and
- how we may mitigate these issues and promote secure behaviours.

To achieve this, we designed a number of studies. First, working with a number of researchers from different disciplines, we designed a study meant to understand developers' reasoning and decision-making across the different kinds of software development tasks they typically come across--why these mistakes occur. This includes not only having to deal with source-code and potential vulnerabilities, but also with less technical aspects, such as considering social aspects of whom to trust when seeking testers for software, or when asking for help, or the decisions that come from monetisation, such as the potential impact of advertisement libraries on security, or the longer-term implications of typical clauses in software licensing agreements. We designed a task-based study where we had 44 mobile app developers engage with these kinds of tasks, prioritising their solutions, and reasoning about their choices: *why* they think they make particular decisions. We found that developers really only frequently consider security when directly facing code (e.g., fixing vulnerabilities), but in many software development activities choices perceived to be secure may only be an illusion, with rationales indicating little to no security considerations.

> **"In many software development activities choices perceived to be secure may only be an illusion, with rationales indicating little to no security considerations."**
>
> ***Awais Rashid***

We also undertook an analysis of over 2400 Stack Overflow posts where developers struggle with using cryptography libraries and identified 16 underlying usability issues. We analysed these further in the light of usability principles proposed in literature to identify four "usability smells" where the principles are not being observed.

Following up on these findings, we designed further experimental psychology studies on how cognitive biases may play into developers' decision-making on trusting particular people or resources (such as code fragments on Stack Overflow), which so far indicate that developers places trusts in people (and the resources they provide) based on *their* perception of those people, which may not be an accurate view of reality at all. This provides further in-depth understanding of why these mistakes occur, especially in software development tasks where developers are not directly engaged in writing code. We further collaborated with cognitive scientists and software engineers to design a psychometric instrument to elicit developers' attitudes towards handling of



personal data in their software, to allow for quantifiable measurements of the extent to which they care about minimizing the data they capture of users, placing users in control of their own data, and using such personal data for monetization.

While further studies are still in progress, some of the key findings from this project as described above are already of interest to developers themselves, as well as policy makers intending to support developers in writing more secure software. Understanding that secure software development is about more than just writing secure code, and stimulating a critical reflective attitude towards the choices developers make and what potential impacts these may have on the security of their software should be an important aspect of mitigating these aspects and promoting secure behaviour.

Professor Awais Rashid, University of Bristol

Awais Rashid is Professor of Cyber Security and Head of the Cyber Security Group at the University of Bristol. He is also Director of the EPSRC Centre for Doctoral Training in Cyber Security – Trust, Identity, Privacy and Security in Large-Scale Infrastructures. Prior to joining Bristol, he was founder and co-director of the Security Lancaster Institute at Lancaster University. Awais has longstanding experience of leading large, multi-partner, interdisciplinary projects with a total value in excess of £20M. His research focuses on security of large-scale connected infrastructures (the overall vision and focus of the Bristol Cyber Security Group) with particular attention on how humans, devices and software intersect in complex ways – leading to cyber security vulnerabilities. Awais is Chair of the RISCS Scientific Advisory Board.

PRESENTATIONS:

- *Yu, Yijun; Wang, Xiaozhu; Dil, Anton and Rauf, Irum (2019). Teaching the Art of Computer Programming at a Distance by Generating Dialogues using Deep Neural Networks. In: 28th ICDE World Conference on Online Learning, 3-7 Nov 2019, Dublin, Ireland, (In Press).*
- *The Johnny project was introduced at an Institute of Coding's Cyber security workshop on 28th Feb, 2019 held at The Open University. Many SMEs and the wider community attended.*
- *Nikhil Patnaik, Joseph Hallett, Awais Rashid: Usability Smells: An Analysis of Developers' Struggle With Crypto Libraries. Proceedings of the 15th Symposium on Usable Privacy and Security, Santa Clara, CA, USA 2019.*
- *D. van der Linden, I. Hadar, M. Edwards, A. Rashid: Data, data, everywhere: quantifying software developers' privacy attitudes, Proceedings of the 9th International Workshop on Sociotechnical Aspects in SecuriTy (STAST). Springer, 2019.*
- *The Johnny project is participating in an initiative to provide a new form of pedagogy to teach programming concepts. This will be further extended towards teaching secure coding practices. Read our paper here: Teaching the Art of Computer Programming at a Distance by Generating Dialogues using Deep Neural Networks (2019) (http://oro.open.ac.uk/62778/)*

Short project updates

In 2016 We funded a series of short projects that ran until 2017-18. These were useful either for supplementing larger, existing projects or for developing nascent ideas that may later form the basis of a new funding application for a more substantial body of work. As is often the case, research projects continue to generate impact and outputs long after the funded period expires. Consequently, we provide updates here on some of our short projects that have officially concluded but nevertheless, have news to report for 2019.

RISCS
Research Institute in Sociotechnical Cyber Security

Security in the Home

PROJECT LEAD: Professor Ivan Flechais, University of Oxford

THE AIM OF THIS PROJECT WAS TO INVESTIGATE SOCIAL RELATIONSHIPS and their role in home data security. The study had two phases. The first was a qualitative exploration of how people make decisions based on 50 semi-structured interviews with UK home users that focused on security decision-making and were analysed using Grounded Theory. The second phase used those results to inform a quantitative study to validate and generalise the qualitative findings. The researchers are still studying the statistics derived from 1,032 UK residents.

The project team found there is a complex culture around responsibility and duty of care. Home users take initiatives to protect themselves, but some also assume responsibility for others, though they are far more likely to offer unsolicited advice to family members than to friends. Those who offer advice feel the need to make good on situations where they have offered bad advice, a responsibility that's determined by the social relationship.

In 2019, Dr Norbert Nthala and Prof Ivan Flechais were successful in progressing the ideas behind the project to the second year Cyber Academic Startup Accelerator Programme competition run by Innovate UK. This competition aimed to identify and support academic ideas for spinout companies. We were successful in progressing our work through all three phases of the competition and are currently working on building this into a social enterprise. .

Dr Ivan Flechais, University of Oxford

Ivan Flechais is Associate Professor of Human-Centred Security in the Department of Computer Science at Oxford, and has over 15 years' experience in undertaking academic research in the area of secure systems design, usable security and privacy, and exploring the security and privacy challenges of home users.

> **"Home users take initiatives to protect themselves, but some also assume responsibility for others, though they are far more likely to offer unsolicited advice to family members than to friends."**
>
> *Ivan Flechais*

PRESENTATIONS:

- *Nthala, N & Flechais, I. (2018). Rethinking Home Network Security. EuroUSEC 2018*
- *Kraemer M J, Flechais I, & Webb H. 2019. Exploring Communal Technology Use in the Home. In Proceedings of the Halfway to the Future Symposium 2019 (HTTF 2019), ACM, New York, NY, USA, Article 5, 8 pages.*
- *Chalhoub G & Flechais I 2020 (To appear). "Alexa, are you spying on me?": Exploring the effect of User Experience on the Security and Privacy of Smart Speaker Users. HCI International 2020.*

SHORT PROJECTS

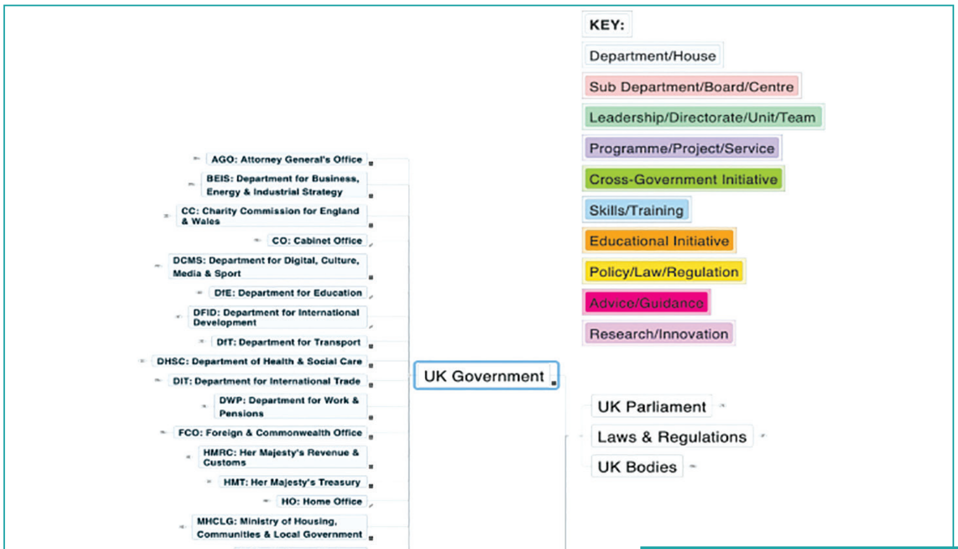
ECSEPA Mapping

PROJECT LEAD: Dr Alex Chung, ECSEPA Project Team, UCL STEaPP

'CYBER SECURITY POLICY MAKING IN THE UK: Mapping the Landscape' is a RISCS-funded spin-out research project from the ECSEPA main project. It emerged from the realisation that there is a lack of clarity about how cyber security is organised within HMG – even for those who work at the heart of it. Understanding where cyber security policy is being developed and implemented, how different issue bases interact and coincide, where there is duplication and where there are gaps, is essential to understanding how a complex, rapidly developing policy landscape like this one should be organised so as to be most effective.

Although the Mapping Project officially concluded in 2018, we had a huge amount of interest and engagement in this work from the UK policy community over 2019. Based on input and feedback from stakeholders, Professor Carr and Dr Alex Chung invested further in fully developing our map of UK cyber security policymaking landscape from a PDF version into a fully interactive digital map. Time-stamped May 2019, the map is currently being hosted on RISCS website and it is publicly accessible for viewing in Internet browser: www.riscs.org.uk/ecsepa-map

> **"The project emerged from the realisation that there is a lack of clarity about how cyber security is organised within HMG – even for those who work at the heart of it."**
>
> *Alex Chung*



KEY:
- Department/House
- Sub Department/Board/Centre
- Leadership/Directorate/Unit/Team
- Programme/Project/Service
- Cross-Government Initiative
- Skills/Training
- Educational Initiative
- Policy/Law/Regulation
- Advice/Guidance
- Research/Innovation

UK Government
- AGO: Attorney General's Office
- BEIS: Department for Business, Energy & Industrial Strategy
- CC: Charity Commission for England & Wales
- CO: Cabinet Office
- DCMS: Department for Digital, Culture, Media & Sport
- DfE: Department for Education
- DFID: Department for International Development
- DfT: Department for Transport
- DHSC: Department of Health & Social Care
- DIT: Department for International Trade
- DWP: Department for Work & Pensions
- FCO: Foreign & Commonwealth Office
- HMRC: Her Majesty's Revenue & Customs
- HMT: Her Majesty's Treasury
- HO: Home Office
- MHCLG: Ministry of Housing, Communities & Local Government
- MOD: Ministry of Defence
- MOJ: Ministry of Justice
- UKSA: UK Statistics Authority

UK Parliament

Laws & Regulations

UK Bodies

GLA: Greater London Authority

Northern Ireland (NI) Executive

As part of our dissemination plan, developed jointly with UCL's Policy Impact Unit, we undertook a series of public engagements to release the map to those communities that we envisioned would benefit most from this package of work. This included circulating the map to our project stakeholders working in government ministries and organisations (Cabinet Office, FCO, Home Office, Mayor's Office London, etc), demonstrating the map in closed sessions (NCSC, DCMS, MHCLG, MOD, etc) and launching the map at public sector events in 2018 and 2019.

The international reach of our public engagement activities is evident from the events at which we featured the mapping project. These ranged from a live demonstration at UCL given to a visiting delegation from Thailand to discussions with Singapore government officials during an Innovate UK Expert Mission to Singapore.

To maximise the educational value of the map, we incorporated live demonstrations into our teaching curriculum over the course of 2018 to 2019. We engaged at all levels to do this. For instance, we explained the thinking behind the mapping research to two A-Level students during their six-week placement at UCL as part of the In2ScienceUK initiative.

We took part in the UCL undergraduate Connected Curriculum 2019 initiative by giving an interview and a demonstration to a student's video project for her module on Criminal investigation and Intelligence. We showed her how the map could be used to navigate the policy and regulation ecosystem concerning different types of cyber security and digital forensics evidence.

At the post-graduate level, we presented the mapping project to UCL's PhD and Master's in Public Policy students on various occasions, including through a presentation by our former colleague who created the first iteration of the map, Ms Sneha Dawda. Sneha returned as a guest speaker to share research insights from her experience working on the project.

The map was particularly relevant to the MPA Digital Technologies and Public Policy students. They enjoyed a hands-on experience where they explored the map using touch-screen interactive panels. During these in-class exercises, they gained knowledge about policy challenges during cross-government collaboration and coordination. Similarly, the map was used as a training tool for smaller cohorts of students where they learned about cyber security incident response and management, especially in preparation for student competitions such as the Cyber 9/12 Strategy Challenge in which UCL has been competing for the third year running.

Currently, we are working with a range of stakeholders to develop bespoke 'sub-versions' of the map which HMG departments and other groups may use to showcase their work on policy outputs and delivery. These bespoke maps are also proving useful as sector specific versions to better suit their own policy needs (e.g. for staff training). To accompany our public engagement activities, we will be releasing a research brief in 2020 to highlight the parts of our research findings that contextualise the policy challenges faced by the government in organising cyber security in the UK.

Dr Alex Chung, ECSEPA Project Team, UCL STEaPP

Alex Chung is a Research Fellow in University College London's Department of Science, Technology, Engineering and Public Policy (UCL STEaPP) and RISCS Fellow in the Research Institute in Science of Cyber Security (RISCS). He is working on an EPSRC-funded project, 'Evaluating Cyber Security Evidence for Policy Advice' (ECSEPA). His research interests include cyber security policy, organised crime and consumer protection. He is the author of Chinese Criminal Entrepreneurs in Canada, Volume I & Volume II, which are based on his PhD undertaken at Oxford University.

RELATED ACTIVITIES

- *UCL Case Study for industry handbook: Map demonstration for cyber incident and policy response exercises during the MPA Digital Technologies and Public Policy session (https://www.ucl.ac.uk/steapp/news/2019/nov/new-project-examines-role-interactive-displays-university-learning). Featured in A Seatwo, A Chung, Y Yu, M Carr and W Tso, Interactive Display in Blended Learning. A joint project by UCL, Oxford University, and BenQ Corporation; forthcoming publication in 2020.*
- *Presentation titled, 'Policy Challenges in UK cyber security: Understanding the role of evidence.' UKAuthority's Cyber4Good event in London, December 2019.*
- *Presented the ECSEPA Mapping project and demonstrated the map to UCL's Connected Curriculum undergraduate student video project, December 2019.*
- *Closed door validation sessions held to demonstrate ECSEPA Map for stakeholders from NCSC, DCMS, MHCLG, and DSTL: various dates throughout 2019.*
- *Collaboration with MHCLG to develop a sectoral map focusing on the local public sector. In progress, started in October 2019.*
- *Collaboration with DCMS to develop a bespoke map focusing on NCSS objectives and policy outputs. In progress, started in July 2019.*
- *Presented the ECSEPA Mapping project to two A-level students during their UCL placement for In2ScienceUK, August 2019.*
- *Presentation titled, 'ECSEPA: Mapping the UK cyber security policy landscape'. Visiting delegation from the Thai Digital Economy Promotion Agency and Fiscal Policy Research Institute, UCL, April 2019.*
- *Three presentations and demonstrations of the ECSEPA Map to UCL's MPA classes: October 2019, November 2018 and October 2018.*
- *wo presentations and demonstrations of the ECSEPA Map to UCL's MPA cohorts as part of Cyber 9/12 Strategy Challenge training programme in January 2019 and January 2018.*
- *Presented ECSEPA Mapping Tool and Policy Crisis Game to Government Security Group: Public Sector Cyber Working Group, 2018.*

SHORT PROJECTS

Impact of Gamification

PROJECT LEAD: Dr Manuel Maarek, Heriot Watt University

THE IMPACT OF GAMIFICATION WAS A SHORT PROJECT which was funded as part of the RISCS Developer-Centred Security call. The aim of this project was to assess the impact of gamification (the application of game-playing principles to other areas of activity) on developers using coding-based games, competitions, interactions for education, and secure coding games.

The outcomes of the project led to the development of an experimental platform to evaluate the impact that serious games could have on developer-centred security. We designed and developed a serious game prototype presented at the Games and Learning Alliance (GaLA 2018) and ran a pilot study in 2018, the findings of which led to a restructuring of the experiment (presented at the European Workshop on Usable Security (EuroUSEC 2019). We have now based our experiment platform on a GitLab instance and have adapted the experiment and game to be longitudinal as the time to play the game and do the programming tasks were too long for a single instance experiment. The game is available at https://www.macs.hw.ac.uk/games-dcs/

Another positive outcome of this project is that research assistant Léon McGrégor moved into a PhD programme at HWU under my supervision. This will allow us to continue our collaboration on this topic through an EPSRC DTA scholarship.

> “The outcomes of the project led to the development of an experimental platform to evaluate the impact that serious games could have on developer-centred security.”
>
> *Manuel Maarek*

We organised a workshop in May 2019 on the wider topic of serious games in cyber security. The SGCS19 Workshop on Serious Games for Cyber Security was sponsored by SICSA Cyber Nexus
https://www.macs.hw.ac.uk/sgcs19/
https://twitter.com/hashtag/sgcs19?src=hash

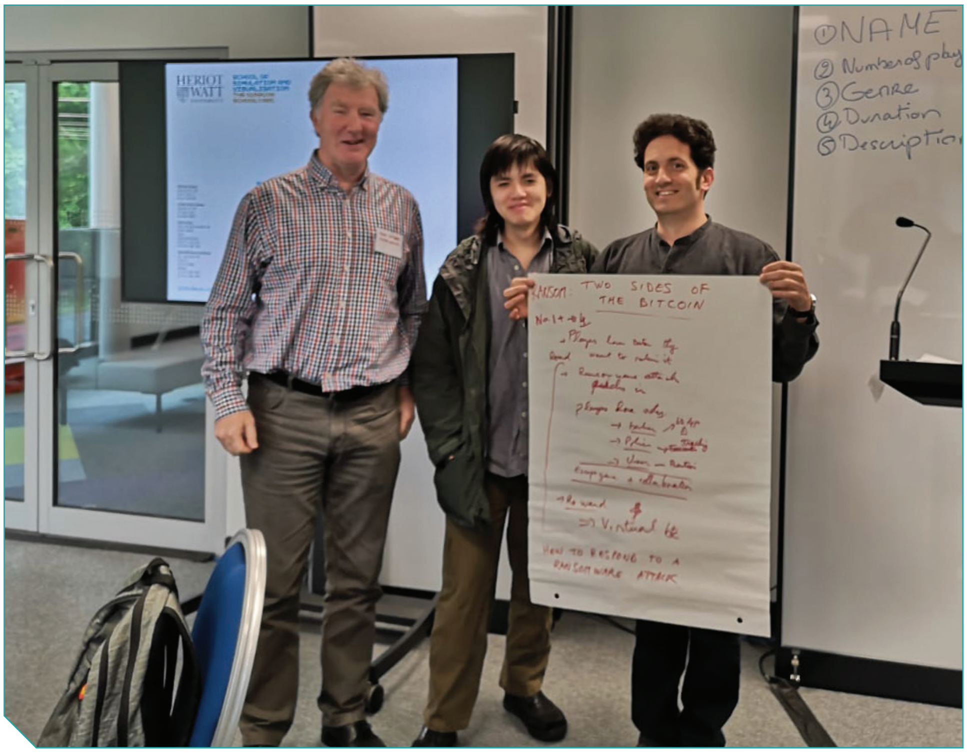
In addition to the presentations of the two papers we published, we presented our work at a seminar in IBM Watson in April 2018, at the SGCS19 workshop in May 2019, and at DemoFest in November 2019.

Finally, in December 2019 we were awarded funding to take this research further through the EPSRC call "People at the Heart of Software Engineering". This three-year project will start in early 2020. Titled "Serious Coding: A Game Approach to Security for the New Code-Citizens", it is led by Lynne Baillie (HWU) with co-investigators from HWU (Manuel Maarek, Hans-Wolfgang Loidl, Rob Stewart), from the Glasgow School of Art (Sandy Louchart, Daisy Abbott), from the University of Saint Andrews (Adam Reed), and in collaboration with Civic Digits.

Manuel Maarek, Heriot Watt University
Manuel Maarek is Assistant Professor in the Computer Science Department of the School of Mathematical and Computer Sciences at Heriot-Watt University in Edinburgh. His research interests are in programming language, type theory, formal methods and their application to the safety, security, and liability of software.

PUBLICATIONS

- *Maarek, M., McGregor, L., Louchart, S., McMenemy, R., 2019b. How Could Serious Games Support Secure Programming? Designing a Study Replication and Intervention. Presented at the EuroUSEC European Workshop on Usable Security, Stockholm, Sweden, pp. 139–148. https://doi.org/10.1109/EuroSPW.2019.00022*
- *Maarek, M., Louchart, S., McGregor, L., McMenemy, R., 2019a. Co-created Design of a Serious Game Investigation into Developer-Centred Security, in: Gentile, M., Allegra, M., Söbke, H. (Eds.), Games and Learning Alliance, Lecture Notes in Computer Science. Springer International Publishing, pp. 221–231. https://doi.org/10.1007/978-3-030-11548-7_21*


①NAME
② Number of play
③Genre
④Duration
⑤Description
HERIOT WATT
RANSOM: TWO SIDES OF THE BITCOIN
→ Virtual
HOW TO RESPOND TO A RANSOMWARE ATTACK

SHORT PROJECTS

Software Security in Development Teams (The Magid Project)

Software Security in Development Teams (The Magid Project)

THE MAGID PROJECT AT SECURITY LANCASTER, Lancaster University, is aimed at creating, refining and disseminating a package of techniques to help developers in teams to deliver more secure software without the direct support of security experts. The project continues to develop a package of low-cost workshops to help development teams to improve their development security. Working with Ingolf Becker of UCL, Angela Sasse of RU Bochum and Lynne Blair of Lancaster, this year we have carried out interventions with teams in ten very different organisations, ranging from a security-focused government team to a one-programmer team in a small company. In all we worked with more than 90 programmers, testers, project managers and product managers; and in each case there were identifiable and sustained improvements in security-related activities of the team involved.

> “The results of this work have highlighted the importance of the relationship between developers and the product management function in each organisation.”
> *Charles Weir*

We have presented the interventions at sessions in two developer conferences, and at internal conferences in two international software development companies.

In research terms, the results of this work have highlighted the importance of the relationship between developers and the product management function in each organisation. We have modified the workshops to include methods to address this relationship and the results have been encouraging. Further work will focus on this relationship and ways to improve the effectiveness of this dialogue in improving security.

Professor Charles Weir, University of Lancaster

Charles is now a Researcher at Security Lancaster, within Lancaster University, UK. He is passionate about improving the security skills of teams of professional software developers. Previously, he set up the mobile application development company, Penrillian, and ran it successfully for 15 years, employing up to thirty people and with a total turnover well over £20M. Charles also helped introduce object-oriented and agile methods to the UK, and was technical lead for the world's first smartphone.

PUBLICATIONS

- *Weir, C., Becker, I., Noble, J., Blair, L., Sasse, M. A. & Rashid, A., 23/10/2019, (Accepted/In press) In: Software - Practice and Experience. 37 p. Interventions for Software Security: Creating a Lightweight Program of Assurance Techniques for Developers*
- *Weir, C., Blair, L., Becker, I., Noble, J., Sasse, A. & Rashid, A., 25/05/2019, Proceedings of the 41st International Conference on Software Engineering: Software Engineering in Practice Track. Sharpe, H. & Whalen, M. (eds.). IEEE*
- *https://www.securedevelopment.org/writings/*

Visualising access control policies

PROJECT LEAD: Dr Charles Morisset, University of Newcastle

A COMMON PROBLEM AMONG SECURITY PRACTITIONERS is maintaining access control policies when they have hundreds of rules, they may be misconfigured, and they may have to be periodically updated for changes in policy. Practitioners have to go through these files, which encode many hundreds or even thousands of rules in a markup language called XACML in order to understand what they can change. Even for technically trained experts, these files are difficult to read.

In 2017, Morisset's project studied visualising these using different options such as maps, user roles, permissions, and multilateral grids: making complex policies easier to understand at a glance should mean fewer errors that can leave networks vulnerable. An online demonstration shows the design the group came up with, an ongoing effort called VisABAC, for the visualisation of attribute-based access control policies, and a test for visitors to take to help assess the effectiveness of these design changes.

Dr Charles Morisset,
University of Newcastle

Charles Morisset is a Senior Lecturer in Security at the University of Newcastle. His main research interest is on quantitative techniques for security systems, in particular, those related to authorisation policies. He has a formal methods background, and is interested in the process of formalisation, which consists in expressing a concrete problem within a formal model, in order to understand and analyse it.

> **"Making complex policies easier to understand at a glance should mean fewer errors."**
> *Charles Morisset*

PUBLICATIONS

- *Charles Morisset, David Sanchez: VisABAC: A Tool for Visualising ABAC Policies. ICISSP 2018: 117-126*
- *Charles Morisset, David Sanchez: On Building a Visualisation Tool for Access Control Policies. ICISSP (Revised Selected Papers) 2018: 215-239*
- *An open-source tool which is currently used for undergraduate and postgraduate cyber-security teaching (https://gitlab.com/morisset/visabac)*

Cybercrime Projects

In 2018 RISCS expanded its interdisciplinary research community to develop further collaboration between the social sciences and cyber security professions. This was complemented by development of a new cybercrime focused research programme, commissioned by the Home Office, via funding from the National Cyber Security Programme. The research programme comprises both longer-term, multi-year research projects as well as shorter-term research.

RISCS

Research Institute for Sociotechnical Cyber Security

CYBERCRIME PROJECTS

AMoC: Advanced Modelling of Cyber Criminal Careers – New technology and intelligence from online evidence bases

PROJECT LEAD: Professor Awais Rashid, University of Bristol

CYBERCRIME IS NOT A SOLITARY AND ANTI-SOCIAL ACTIVITY, but one where social interaction plays a critical role in the recruitment, training and professional advancement of criminals. AMoC's multidisciplinary approach will form a detailed understanding of the characteristics of cyber offenders, their behavioural patterns and their career progression and lifecycle in cybercrime by combining expertise in intelligent technologies and security informatics with methodological social science approaches in psychology, (socio)linguistic theory and law enforcement.

The overall aim of this project is to tackle cybercrime by understanding the social and economic development of cyber criminal careers, and will be achieved by: analysing different evidential sources to engender a better understanding of the characteristics of cyber offenders and how communities thereof react to interventions and; developing new techniques and software tools that support law enforcement agencies to detect and investigate cyber offenders, cyber threats and online networks. To date, AMoC's research on the known characteristics and motivations of offenders engaging in cyber-dependent crimes indicates that while the knowledge-base is expanding, evidence on these topics remains limited. Existing research is constrained by methodological limitations and difficulties in accessing offender populations. For example, many studies describe low-level or loosely-defined forms of cyber criminality, self-reported in student or youth populations, rather than technically sophisticated attackers. Anonymous online surveys of cyber criminal venues have greater potential to access this latter population, but are limited by doubt about the accuracy of self-reported accomplishments or skill. Police case data is also used, but relatively small numbers of prosecutions for cybercrime, relative to traditional offending, hamper generalisability of results, particularly when focused on technically sophisticated attackers. This highlights the need for more objective measures of cybercriminals, and greater focus on technically sophisticated attacker populations. AMoC's later stages will tackle these challenges through large-scale data mining of cybercriminal forums.

The tools developed through AMoC will support the future efforts of cybercrime investigators to:

- Detect cyber offenders and analyse their criminal activities and behaviours;
- Assess the degree of importance and urgency of different types of evidence to establish cyber offenders' danger to society;
- Acquire useful evidence in a timely manner.

Professor Awais Rashid,
University of Bristol

Professor Awais Rashid is Professor of Cyber Security and Head of the Cyber Security Group at the University of Bristol. He is also Director of the EPSRC Centre for Doctoral Training in Cyber Security – Trust, Identity, Privacy and Security in Large-Scale Infrastructures. Prior to joining Bristol, he was founder and co-director of the Security Lancaster Institute at Lancaster University. Awais has longstanding experience of leading large, multi-partner, interdisciplinary projects with a total value in excess of £20M. His research focuses on security of large-scale connected infrastructures (the overall vision and focus of the Bristol Cyber Security Group) with a particular attention to how humans, devices and software intersect in complex ways – leading to cyber security vulnerabilities.

> "To date, AMoC's research on the known characteristics and motivations of offenders engaging in cyber-dependent crimes indicates that while the knowledge-base is expanding, evidence on these topics remains limited."
>
> *Awais Rashid*

CYBERCRIME PROJECTS

Case by Case: Building a Database of **Cybercriminal Business Models**

PROJECT LEAD: Dr. Jonathan Lusthaus, University of Oxford

> “We want to help law enforcement identify vulnerabilities in organizational structures and to target disruptive interventions effectively.”
>
> *JONATHAN LUSTHAUS*

THIS PROJECT FOCUSES ON THE BUSINESS models of cybercriminal groups. Its goal is to build a database of closed cybercrime cases that illustrates different group structures. This will move the discussion of cybercriminal organisations from generalities to a richer micro-level understanding, thereby making it more feasible for law enforcement to identify vulnerabilities in organizational structures and to target disruptive interventions effectively.

To ensure its feasibility and to erect solid foundations, the project began with a design phase, which took place from October 1 2018 until March 31 2019. Along with other preliminary work, this involved holding a series of workshops with law enforcement and other stakeholders held in Amsterdam, London and Pittsburgh. Since October 1 2019, work on the 10 case studies has begun, making use of interviews with investigators and judicial data. In the first instance, this is taking place with the Metropolitan Police Service in London. In 2020, the remaining case studies will be collected from a range of law enforcement partners across the UK. At the conclusion of the project, the database will be stored by the Home Office with the intention to provide access to other (vetted) researchers.

Dr. Jonathan Lusthaus, University of Oxford

Jonathan is Director of the Human Cybercriminal Project in the Department of Sociology and a Research Fellow at Nuffield College, University of Oxford. He is also an Adjunct Associate Professor at UNSW Canberra Cyber.

Connecting delayed pre-commitment with cyber awareness in order to address the perception gap and present bias

PROJECT LEAD: Dr Anna Cartwright, University of Coventry

> **“Our focus is on the barriers that small organizations face in adopting cyber best practice.”**
> ***Anna Cartwright:***

THIS PROJECT IS LOOKING AT HOW TO IMPROVE CYBER-SECURITY IN SMALL BUSINESSES (less than 50 employees) and charities. Our focus is on the human-aspects of the cyber-security and the barriers that small organizations face in adopting cyber best practice.

As part of the project we are asking small organizations to complete a cyber-security health check with KITC Solutions (the University of Kent student led IT consultancy). The health check is built around the NCSC Small Business Guide. At the end of the health-check we are trialing an intervention designed to help overcome procrastination. Before and 3 months after the health check we survey the participants about cyber behavior in their organization. This allows us to explore the effect of the health-check and intervention.

As part of the project we are also developing a typology of small business behavior using our own data and that from the Cyber Breaches Survey, which also considers how amenable businesses might be to cyber advice and adoption of behavioural tools to overcome procrastination.

To support the project we are coordinating with regional cyber protect officers in Kent and the Midlands. We are also engaging with regional business and charity support organizations such as Voluntary Action Leicestershire, Coventry Council, Coventry and Warwickshire Chambers of Commerce. More information about the project is available at ***https://cyberprotect.our.dmu.ac.uk.***

Gentle Interventions for Security **(GIFS)**

PROJECT LEAD: Dr Emily Collins, University of Cardiff

SUMMARY

AS A RESPONSE TO INCREASING THREATS, technology is becoming more secure by default. However, users are still at the centre of cyber security. Users are responsible for making a large number of security related decisions on a daily basis, despite a lack of understanding of the risks involved. Heavy handed approaches that force users to behave in a particular way (e.g. stringent password guidelines; Inglesant and Sasse, 2010) fail to create the secure environments they aim to achieve, instead encouraging users to identify workarounds in order to maintain the usability of the system. Similarly, existing interventions often neglect to appreciate the timeliness of many security behaviours, and how simply informing users of ideal behaviours may not be sufficient to break ingrained habits. As a result, individuals will continue to perform unsafe behaviours, despite the risks they carry. Alternative ways of encouraging behaviours may therefore be a more effective solution to empowering users to behave securely.

Drawing from the literature and theoretical frameworks surrounding habit formation in health-related behaviours (Gardner et al., 2012, 2011) and from successful ambient "nudge" interventions in the areas of work-breaks and health (Rodríguez et al., 2015), this project aimed to explore the potential for ambient displays (such as small, desktop light boxes) to gently encourage more secure habits in workplace office contexts at times tied specifically to the behaviour in question. One of the important features of this project was a user-centred approach, aiming to identify what security behaviours should be the focus, and the form the ambient displays should take through the research itself, and iterating our displays before conducting a final evaluation.

To this end, taking a mixed methods approach, this project aimed to: (i) identify how security behaviours could be encouraged or discouraged through ambient displays, (ii) identify the most effective ambient features to use in such interventions, (iii) develop an ambient display in line with this research and finally, (iv) evaluate the effectiveness of such a display on security behaviours.

PROGRESS

WE BEGAN WITH AN EXTENSIVE LITERATURE REVIEW to identify guidelines for ambient displays. Once these were established, we conducted exploratory research in the form of online questionnaires and participatory design workshops to identify what behaviours people most needed support in performing, and what users wanted the ambient displays to do, and how they should do it. A behaviour that emerged as especially important and appropriate was locking computers, with participants arguing for light-based feedback and sensors that avoided too many wires or user-input.

Using inexpensive Adafruit Circuit Playgrounds, we were then able to develop a light-based display that provided feedback to users in the form of coloured lights when they failed to lock their computers when they left their desks, using data collected from proximity and light sensors.

Finally, we installed a total of 13 devices (see Figure 1) in three offices over a 4-6 week period. We collected self-reported behaviour and attitudes towards computer locking before and after this period as well as behavioural data, and also conducted exit interviews with participants. We will be installing a further 18 devices for a second round of data collection early this year.

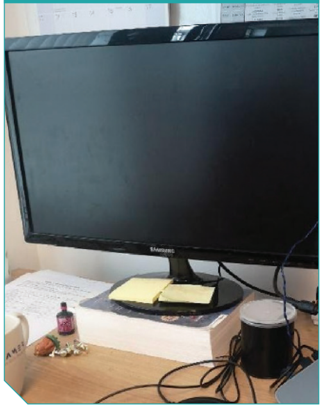
"Heavy handed approaches that force users to behave in a particular way fail to create the secure environments they aim to achieve."

Emily Collins:

Dr Emily Collins, University of Cardiff

Dr Collins is a Lecturer in Human Factors in Psychology at Cardiff University. Her research uses principles and methods from Psychology and Human Computer Interaction to explore novel ways to support people in making safer and healthier choices, with a particular focus on cyber security behaviours. More broadly, she is interested in using technology to create positive outcomes through applied, mixed methods and interdisciplinary research.

Figure 1. The hardware installed on one participant's computer



Evaluating criminal transactional methods in cyberspace as understood in an international context

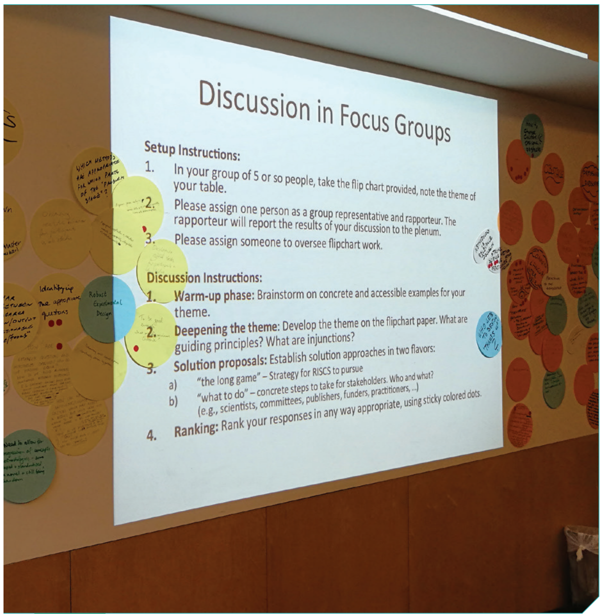
PROJECT LEAD: Rajeev Gundur, Flinders University

THIS PROJECT, NOW APPROACHING COMPLETION, is an exploration of what is currently known in the academic and grey literature about the financial aspects of various cybercriminal business models. Our project has three prominent characteristics: it is multilingual; it provides background on education, law enforcement strategy, and regulation vis-à-vis cybercrime in countries with significant internet user bases; and it analyses how cybercriminals conduct financial transactions, to the extent of our understanding of these transactions.

The project has surveyed over 500 documents across five languages. Findings so far suggest that the current literature does not adequately document the criminal process or verify claims about how criminal interactions and transactions unfold in consistent ways. It also shows that while the English-language literature may mention some of the concerns that exist in non-English speaking contexts, these issues are severely underdeveloped. Moreover, literature is revealing that there is an asymmetric representation of concerns from the developing world, likely underwritten by a lack of capacity or transparency. Ultimately, these findings indicate that, despite the global nature of cybercrime, cybercrime research tends to focus on a relatively narrow set of concerns that pertain primarily to western, English-speaking audiences.

To understand transactions in reference to cybercrime, this research has developed a typology of economic ecosystems and transaction types that cybercriminals use. It has identified products and services that cybercriminals leverage to transact value and it shows how cybercriminals access these products and deploy them.

> **"Despite the global nature of cybercrime, research tends to focus on a relatively narrow set of concerns that pertain primarily to western, English-speaking audiences."**
> *Rajeev Gundur:*



Discussion in Focus Groups

Setup Instructions:

1. In your group of 5 or so people, take the flip chart provided, note the theme of your table.
2. Please assign one person as a group representative and rapporteur. The rapporteur will report the results of your discussion to the plenum.
3. Please assign someone to oversee flipchart work.

Discussion Instructions:

1. **Warm-up phase:** Brainstorm on concrete and accessible examples for your theme.
2. **Deepening the theme:** Develop the theme on the flipchart paper. What are guiding principles? What are injunctions?
3. **Solution proposals:** Establish solution approaches in two flavors:
   a) "the long game" – Strategy for RISCS to pursue
   b) "what to do" – concrete steps to take for stakeholders. Who and what? (e.g., scientists, committees, publishers, funders, practitioners, ...)
4. **Ranking:** Rank your responses in any way appropriate, using sticky colored dots.

WHICH METHODS ARE APPROPRIATE FOR WHICH PARTS OF THE "PROBLEM SPACE"?
Robust Experimental Design
WHO GETS TO DEFINE THREATS?

Rajeev Gundur, Flinders University, South Australia

Rajeev Gundur is a lecturer at Flinders University. He previously taught for the University of Liverpool in Singapore where he lectured on cybercrime and transnational organized crime. He is the prize chair for the International Association for the Study of Organized Crime (IASOC). Rajeev's work focuses on illicit enterprise in both online and offline contexts.

CYBERCRIME PROJECTS

Investigative interviewing of cybercrime victims to gain best evidence

PROJECT LEAD: Professor Eerke Boiten, De Montfort University

> **“The dynamics of cybercrime investigations are complicated by many factors.”**
>
> ***Eerke Boiten:***

THIS PROJECT AIMS TO STUDY AND IMPROVE TECHNIQUES for police interviewing of cybercrime victims. There is a range of evidence available regarding best practice in terms of how police can best interview traditional crime victims. However, the experience of being a victim of cybercrime is likely to differ in a number of ways to traditional crime, for example, in terms of eliciting technical information regarding the crime and the potential impacts on victim cognitive function and memory retrieval from use of digital devices. Alongside difficulties with the apparent anonymity of offenders and the need to build rapport with victims, these types of issues may potentially present law enforcement different types of challenges when it comes to interviewing cybercrime victims, as compared to victims of traditional crime. This research will therefore focus on better understanding the types of interviews with victims being conducted by law enforcement, how they are conducted, the challenges interviewers face and how they could be improved (for example whether more cognitive interview techniques should be employed). The project is in its final stages, with results currently being written up.

CYBERCRIME PROJECTS

Online Ties Taking Over?
A longitudinal study into actual vs. perceived cybercriminal behaviour of offline vs. online social ties among youth

PROJECT LEAD: Dr Marleen Weulen Kranenbarg

THIS LONGITUDINAL PROJECT AIMS TO ADDRESS THE RESEARCH QUESTION 'To what extent is there a causal relationship between individuals' social ties and their cybercriminal behavior?'. The project also investigates whether peer effects differ for cyber delinquent and traditional delinquent behavior. Research from traditional crime areas suggests there is a strong relationship between an individual's criminal behavior and the criminal behavior of their social ties. This project aims to explore whether this is true also of cyber offenders, building on initial evidence suggesting that cyber criminals tend to have more cybercriminal social ties than non-offenders. However, this project aims to address some methodological issues with previous research by employing more reliable longitudinal methodologies and obtaining direct measures of peer offending behaviours, rather than just measuring perceptions.

The research includes young people in the Netherlands, with survey data to be collected in 3 waves. Online surveys examine self-reported cybercriminal behaviour of a high-risk sample of juveniles and young adults (aged 12-23) together with those of respondents' social peers. It will distinguish between online and offline social peers. As a result, it will explore the extent of any causal relationship between social ties (either traditional or online) and cybercriminal behaviour. The longitudinal aspect will help to distinguish between peer influence and peer selection as shifting social relationships (and changes in self-reported behaviour) are explored over time. The first wave of data collection started in September 2019 and ended in November 2019. A total of 12 schools participated, resulting in a sample of 891 respondents. As the research question requires longitudinal data, there are no preliminary results yet. The next wave of data collection is planned for January-February 2020.

The findings from this research will help to build the evidence base regarding our understanding of cyber offenders and the factors that influence cyber offending behavior. This in turn will help to inform policymakers and law enforcement regarding how interventions could be designed to target these factors and prevent young people from becoming involved in cybercrime.

Dr Marleen Weulen Kranenbarg

Dr. Marleen Weulen Kranenbarg is an assistant professor at VU Amsterdam, The Netherlands. Her research mostly focuses on cyber-dependent offenders. In her doctoral dissertation she empirically compared traditional offenders to cyber-offenders on four important domains in criminology: 1. offending over the life-course, 2. personal and situational risk factors for offending and victimization, 3. similarity in deviance in the social network, and 4. motivations related to different offense clusters. She recently started the OTTO project, a large-scale longitudinal study into actual vs. perceived cybercriminal behaviour of offline vs. online social ties among youth. Marleen is also a research fellow of the NSCR (Netherlands Institute for the Study of Crime and Law Enforcement), board member of the ESC Cybercrime Working Group, and part of the steering committee of the IIRCC (International Interdisciplinary Research Consortium on Cybercrime).

> **"The findings from this research will help to build the evidence base regarding our understanding of cyber offenders and the factors that influence cyber offending behaviour."**
>
> *Marleen Weulen Kranenberg*

CYBERCRIME PROJECTS

Victims of Computer Misuse Crime

PROJECT LEAD: Professor Mark Button, University of Portsmouth

> “The research has highlighted the significant impact that computer misuse crime has on many victims.”
>
> *Mark Button*

THE AIM OF THIS PROJECT IS TO INVESTIGATE THE EXPERIENCES OF VICTIMS OF COMPUTER MISUSE OFFENCES. The changes in questions to the Crime Survey for England and Wales (CSEW) had exposed almost half of all crime was now accounted for by fraud and computer misuse offences. Both areas have been lightly researched compared to other volume crimes, but for the latter the gaps in knowledge are even more stark with very few studies.

This project embarked with the broad aims to:

- To examine the nature and impact of computer misuse related crime on victims; and
- To assess the support provided to such victims and identify better means to prevent such crime.
- To examine the experiences and perceptions of those victims who have experienced a law enforcement response.

Over the last year the team has conducted an online survey of 252 individual victims of computer misuse, conducted 52 depth interviews with 38 individual and 14 SME/O victims; along with stakeholder interviews, review of the literature and analysis of websites where victims report.

The research has highlighted the significant impact the crime has on many victims, the limited changes in security behaviours that victimisation often brings, as well as exploring the gaps in victim support - among many other findings. Findings from the study have already been used by HMICFRS as part of their inspection of the police response to cyber-dependent crime, published in October 2019. A full report of all the findings will be published early in 2020. The report that will be published will highlight a variety of recommendations directed at various bodies to help improve the treatment of victims and better equip them to reduce further victimisation. These findings and recommendations were also discussed at a seminar in London attended by representatives from the Government, police and key stakeholders held in early December.

Professor Mark Button, University of Portsmouth

Professor Mark Button, who is Director of the Centre for Counter Fraud Studies at the University of Portsmouth, has led the project which included the colleagues: Dr Lisa Sugiura, Dean Blackbourn, Dr Victoria Wang, Dr David Shepherd and Dr Richard Kapend.

RISCS

Research Institute in Sociotechnical Cyber Security

Ministry of Housing,
Communities &
Local Government

National Cyber
Security Centre
a part of GCHQ

Department for
Digital, Culture,
Media & Sport

Home Office

UCL
DEPARTMENT OF SCIENCE,
TECHNOLOGY, ENGINEERING AND
PUBLIC POLICY

EPSRC
Engineering and Physical Sciences
Research Council

Lloyd's Register
Foundation

AIRBUS