RISCS
Research Institute in Science of Cyber Security

ANNUAL REPORT 2018

EPSRC
Engineering and Physical Sciences Research Council

National Cyber Security Centre

UCL
DEPARTMENT OF SCIENCE, TECHNOLOGY, ENGINEERING AND PUBLIC POLICY

Contents

Research Institute in Science of Cyber Security

The Research Institute in Science of Cyber Security (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 communities, RISCS promotes and supports the development of scientific 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. Recognising that cyber security is a contested concept, RISCS operates within a national and international cyber security framework to establish a coherent set of research principles. These principles focus on the deployment of scientific methods and the gathering of evidence to produce sound interventions and responses to cyber security challenges.

We actively seek to maximise collaboration amongst our diverse community through a culture of open publication, sharing and expanding our network. Through this collaboration, RISCS develops techniques that enable communities to anticipate emergent cyber security issues from public policy, social practice and technological perspectives. Our end goal is to deliver a world-class portfolio of activity and research findings that maximises the value of social, political and economic research into cyber security and which results in a set of scientifically based options that individuals, institutions and nation states can use to respond to imminent and long term cyber security challenges. RISCS is managed by a team based in the Department of Science, Technology, Engineering and Public Policy (STEaPP) at University College London (UCL).

To find out more visit: www.riscs.org.uk

Science, Technology, Engineering and Public Policy, UCL

UCL STEaPP explores 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 Sciences, 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

With thanks to….

Emma Bowman, RISCS Administrator

Alex Chung, Research Associate, ECSEPA

Ruth Dollard, Research Coordinator, UCL STEaPP

Laura Pullen, UCL STEaPP

Amaka Nwosu, Photographer

Layton Thompson, Photographer

Director's Message

Welcome to the 2018 Annual Report for the Research Institute in Science of Cyber Security (RISCS). RISCS has undergone a number of changes this year and as the new Director, I'm pleased to have this opportunity to update you. We have had a productive year and outline here some of the exciting plans we have for 2019 as we continue to draw on the dynamism of cyber security research and deliver impactful findings to our community of stakeholders.

Changes to the RISCS Leadership Team

Perhaps most significantly, our founding Director, Professor M. Angela Sasse has stepped down. She will be taking up a new opportunity as Professor of Human-Centred Security at Ruhr-University Bochum in Germany. Angela has been incredibly important to the research community that focuses on the human and organisational factors of cyber security. During her time at UCL, Angela has been a prolific researcher setting a positive example (and a high bar!) for women in engineering and computer science. In addition to her exceptional research credentials, Angela has developed strong, ongoing relationships with stakeholders beyond academia. As a result, she has a powerful international reputation for her research and her leadership and she will be greatly missed as Director of RISCS. Angela will continue to participate in the RISCS community through the Cyber Readiness for Boards project.

We have also experienced a change in the team on the NCSC side. Susan A worked closely with Angela to establish RISCS – perhaps in a climate that was generally less alive to the human and organisational factors of cyber security. Susan's determination to work collaboratively with the academic community provided a strong foundation for RISCS. She and Angela worked together to develop the NCSC password guidance issued in 2016. They also championed a broad range of projects that reflected the diverse methodological, practice-based, and theoretical spaces that inform cyber security today. Susan's commitment and intellectual contribution will be missed and we wish her well in her new role.

Helen L has taken over as Technical Director for RISCS. Helen has a degree in Physics and, having worked at DSTL, the Ministry of Defence and The Insolvency Service, she joined GCHQ nearly ten years ago. She has worked in the research space of GCHQ and the NCSC during that time, initially focusing on the material properties of semiconductors before moving on to lead the Engineering Processes and Assurance team. Helen is now the Technical Director of the Sociotechnical Security Group in the NCSC.

Helen is supported by Sam B as Deputy Technical Director and together, they have been extremely important to RISCS this year. They have worked with us to restructure RISCS and to clarify many aspects of how we work – both within the Institute and also with regard to our collaborations with the NCSC. Sam has taken an active role in helping to design interventions like the Metrics Workshop that we held in May and he is also the NCSC lead on the Cyber Readiness for Boards project. As RISCS Director, I'm very grateful to both Helen and Sam for their commitment, energy and engagement.

In March, I was delighted to be invited to take up the role of Director of RISCS. My background is in the international politics of cyber security and Internet governance. I moved from Cardiff University to UCL in October 2017 to join the multi-disciplinary Department of Science, Technology, Engineering and Public Policy (STEaPP). Within STEaPP, I have established the Digital Policy Lab with the aim of supporting policy making to adapt to the pace of change in society's integration of digital technologies. For the past three years, I have been the Co-lead on the Standards, Governance and

Policy stream of the UK wide PETRAS research hub on the cyber security of the Internet of Things. I am the PI on the RISCS ECSEPA project, the RISCS Cyber Security Policy Mapping project, and the RISCS Cyber Readiness for Boards project. I am also the PI on an EPSRC project looking at international cooperation on critical infrastructure in the IoT and Co-I on PACE - a TIPS2 project with colleagues from Cardiff Computer Science that explores Privacy Aware Cloud Ecosystems.

Alongside these changes, we are fortunate to have Lizzie Coles-Kemp continue on as Deputy Director of RISCS and Geraint Price continue as Chair of the Practitioner Panel. In her capacity as Deputy Chair, Lizzie will continue to focus on knowledge exchange and engagement.

Activities in 2018

We hosted two RISCS community days in 2018 with a third to come in October. In February, our first meeting featured range of international speakers who eloquently addressed the 'Science of Cyber Security' from positions of considerable experience. On day two, the community members had the opportunity to attend one of two workshops; one was on Developer-Centred Security which forms one of the current research pillars of RISCS. The second workshop was on Scientific Methods and Approaches which links into our new Scientific Advisory Board that Professor David Wall has agreed to chair (see below).

In May, our community days focused on decision making and cyber security. We looked first at the use of cyber security metrics, drawing on related experience with measuring outcomes in healthcare and other fields and as a means of communicating risk to the board. We then ran a workshop at which we collated views on which metrics are useful/possible from different perspectives including business leaders, policy makers and the security community. The report (available on our website) makes interesting reading and forms the basis of a larger package of work that we will pursue in 2019 with the NCSC. Following on from this day of discussing ways to quantify cyber security, we moved to the world of decision making under deep uncertainty to consider the implications of the 'smart family' in 2030. Working with Futures and Foresight specialist, Ine Steenmans, we asked participants to explore a range of questions about how the Internet of Things would be integrated into family life and what 'key security alerts' might arise. The findings from this workshop are also available on our website.

In terms of the research agenda of RISCS, our work has largely been clustered around a few key themes. 'Developer Centred Security' is a novel perspective on secure software development that supports and enriches the secure development guidance produced by the NCSC. We hope to deliver tangible support to software developers through these projects. The 'You Shape Security' work is focused on shaping a security culture. This links to some of the RISCS work from Phase 1 – particularly the CySeCa project which has some work coming out later this year. 'Supporting the Board' is a new package of work intended to provide long-overdue support to business leaders. The first project, Cyber Readiness for Boards is just getting underway and this will be instrumental in the continuous evolution of the NCSC's Board Toolkit.

Coming up this year…

There are two main objectives that we intend to pursue in 2019. The first is to strive to develop more effective and systematic ways to return our RISCS research findings to industry and policy stakeholders in a useable format. Cyber security is referred to as a 'wicked problem'. This means that it is complex, open-ended, intractable and difficult to manage because of interdependencies with other policy making solutions or business decisions. The UK has one of the world's best higher education and research sectors but it is not always clear that excellence in research translates into work that is accessible and helpful to business and policy communities. We believe that RISCS has a role to play in facilitating this transfer of knowledge and we are working on developing mechanisms to support our research teams to do this. As a first step, watch for our new series of *RISCS Research Briefs* which we will begin to produce and circulate later this year.

Linked to this first objective is our intention to stimulate a critical debate about methodologies employed in cyber security research. To this end, we have established a Scientific Advisory Board chaired by Professor David Wall from the University of Leeds. The Board exists to help RISCS to improve and sustain the scientific quality of its work, to help it achieve its aims and goals, to champion rigorous and actionable research for the policy and practitioner communities and to help resolve methodological tensions in the work carried out by the RISCS community in order to increase confidence in the knowledge produced.

This coming year will also see a line up of dynamic new multi-disciplinary projects in RISCS. We are pleased to announce a new cyber crime-focused research programme, commissioned by the Home Office, via funding from the National Cyber Security Programme. We look forward to updating the RISCS community in the coming months on the progress of these exciting projects and to working closely with both the Home Office and the project PIs.

The RISCS community is comprised of people who recognise that there are a whole set of cyber security challenges that cannot be addressed by technological solutions alone. We understand that organisational and human factors are, and always will be, fundamental elements of improving cyber security outcomes. For those reasons, we know that it is essential to work across disciplinary and sectoral boundaries to think creatively and innovatively about the implications of technology for the human condition. This is both a UK project and a global one and RISCS has a role to play in facilitating the exchange of knowledge, research and solutions to problems between all parties at both levels. Our activities in 2019 will reflect that.

Madeline Carr
London, October 2018


Projects

Addressing Cybersecurity and Cybercrime via a co-Evolutionary aPproach to reducing human-relaTed risks (ACCEPT)

The ACCEPT project's overall aim is to develop a framework through which we can analyse the behavioural co-evolution of cybersecurity/cybercrime ecosystems and effectively influence behaviours of a range of actors in the ecosystems in order to reduce human-related risks. This will be done by combining knowledge drawn from social sciences (criminology, psychology, business), engineering, and physical sciences (computer science, security engineering) to create a theoretical socio-technical framework and a set of software tools. The framework and tools are intended to help organisations both to personalise and contextualise communications and provide feedback to users in a more human-centric manner. They will draw on both our understanding of human behaviour – how criminals target victims and why victims fall prey to scams – and emerging ICT technologies such as machine learning and mobile computing.

The Project has seen progress on improving the computational ontology on cybercrime, widening the knowledge base about cybercrime and cyber security related human behaviours, undertaking a number of interviews and workshops with stakeholders, and investigations into use cases and scenarios. A key outcome is the confirmation of the following three use cases in relation to human-in-the-loop (HITL) approach around which software development and empirical studies will be carried out:

- Location privacy: a HITL approach can help us better understand human behaviour in location sharing especially in cross-source sharing scenarios. This will eventually help human users to better manage their location sharing behaviours;
- Cyber fraud and scam: a HITL approach can help us to better understand human behaviours of potential victims of cyber fraud. This use case will produce findings that will help educate users to be more cautious about these risks;
- Reporting of semantic attacks: a HITL approach can help us to encourage reporting of semantic attacks. This case will help inform approaches to educating users to improve their resilience and the performance of their reports.

The decision to focus on these use cases were based upon a number of factors and practical considerations. These included feedback from stakeholders, the likelihood of gaining access to real-world data, the time required to develop software tools, and the complexity of the empirical studies. With the now confirmed use cases, the project team has progressed into the software development phase. We are also discussing new research collaborations with a potential partner institution, to apply software tools they have developed to the study of the last use case.

While the project is still in its early stage, the work has already helped inspire another EPSRC-funded project “PriVELT: PRIvacy-aware personal data management and Value Enhancement for Leisure Travellers” (EP/R033749/1). PriVELT will focus on privacy protection of leisure travellers and significantly overlaps with the first use case of the ACCEPT project. Led by the ACCEPT PI (Shujun Li) and Xiao Ma (previously of the ACCEPT project), the work we have done so far in the ACCEPT project has contributed to a report produced by the WPI lead, Michael McGuire, titled “Into the Web of Profit - Understanding the Growth of the Cybercrime Economy” (Bromium 2018). The work in the ACCEPT project also led to a special issue on “Cybercrime: interdisciplinary approaches to cutting crime and victimisation in cyber space” for the Springer open access journal *Crime Science*, which is currently being edited.

Related Activity:

- Chair at HHMC 2017 (Workshop on Hybrid Human-Machine Computing) (September 2017)
- Invited talk: ACCEPT Project at The Economics and Human Aspects of Cyber-Security workshop, Kent University (November 2017)
- Interviews with five cybersecurity experts on dynamic/evolutionary aspects of data breaches (2017-2018)
- Co-editing a special issue on Cybercrime: interdisciplinary approaches to cutting crime and victimization in cyber space, to be published in the open access journal Crime Science: An Interdisciplinary Journal by Springer.
- Keynote talk: "Human Factors in Cyber Security: User authentication as a use case" at ISWRACS (International Symposium and Workshop on Research Advances in Cyber Security) 2018, organized by the Hindustan Institute of Technology & Science (Hindustan University), India (January 2018)

Research Databases and Models:

- A searchable database of key cybersecurity incidents between 2010-2016 is being created.

EPSRC Reference:	EP/P011896/2
Principal Investigator:	Professor Shujun Li (University of Surrey)
Other Investigators:	Dr Hervé Borrion (University College London)
	Professor Paul Ekblom (University College London)
	Dr Shaun Helman (Transport Research Laboratory Ltd)
	Professor Roger Maull (University of Exeter)
	Dr Michael McGuire (University of Surrey)
	Dr Sotiris Moschoyiannis (University of Surrey)
	Professor Irene Ng (University of Warwick)
	Professor Ganna Pogrebna (University of Birmingham)
	Dr Helen Treharne (University of Surrey)

CyberSecurity Across the LifeSpAn (cSALSA)

The goal of the cSALSA project is to take a lifespan approach to understanding how cyber security is understood and how that relates to risk and behaviour. Prior work supports the idea that there are unique security challenges at different life stages. Many changes occur during a lifetime: the resources people have to draw on (family, friends, work colleagues) change, and the power structures within these relationships also shift over time. These changing states play a part in determining how individuals interact with technology products. This project seeks to study questions such as how these factors intertwine and interact to determine individual responses.

As the CyberSecurity Across the LifeSpAn (cSALSA) project began in Spring 2017, this report covers the previous 14 months. The project began with a collaborative effort between partners in Bath, Northumbria and Portsmouth to collect extensive data on the public's understanding of cybersecurity. This led to almost 1000 submissions from across the country, ranging from the age of 14 to 90 years old. The Bath partners have manually coded these responses and conducted four studies to reveal the structure of the public's lay understanding of cybersecurity. Simultaneously, Northumbria have been conducting workshops with older adults (in collaboration with U3A), and interviews with individuals who are socially isolated and those who are well connected. Portsmouth have conducted a large literature review of the links between physiology (e.g. tiredness, stress) and risk behaviours. Finally, work at Bath on creating a dictionary of cybersecurity based on the earlier definition work is continuing at pace, where the base dictionary and a cybersecurity corpus are being created in order to begin validation and word sense disambiguation of the tool.

cSALSA researchers have presented their work at the Behavioural and Social Science in Security (BASS18) conference, and organised (with cSALSA-funded ECR / PhD support) a workshop on security and privacy for vulnerable older users at MobileHCI. Two PhD researchers (funded by University scholarships) have also been appointed to work on the project, and cSALSA supported a research visit by Prof Briggs to our partners in Canada. Over the next year, we plan to complete the work on the dictionary and meaning of cybersecurity, and to conduct in-depth research across young people / families, working age population and older adults before returning to the measurement of cybersecurity in collaboration with industrial partners.

Publications:

- Williams, E., Polage, D. (2018) 'How persuasive is phishing email? The role of authentic design, influence and current events in email judgements'. *Behaviour & Information Technology.* 1-14.

Related Activity:

- IE Conference presentations with NCSC on phishing (2018)
- DCMS discussion / co-working on segmentation & metrics (2018)

EPSRC Reference:	EP/P011454/1
Principal Investigator:	Professor Adam Joinson (University of Bath)
Other Investigators:	Professor Debi Ashenden (University of Portsmouth)
	Professor Pam Briggs (Northumbria University)
	Dr Emily Collins (University of Bath)
	Professor Lynne Coventry (Northumbria University)
	Dr Simon Jones (University of Bath)
	Darren Lawrence (Cranfield University)
	Dr Ana Levordashka (University of Bath)
	Ben Morrison (Northumbria University)
	Dr Kate Muir (University of Bath)
	Dr James Nicholson (Northumbria University)
	Samantha North (University of Bath)

Detecting and Preventing Mass Marketing Fraud (DAPM)

The DAPM project focuses 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.

Our recent activity includes:

- Analysis and investigation of 25 extended exchanges between a single victim and scammers. This work looks at how scammers build and maintain trust, and how victims respond. A stage model will then be developed.
- Work identifying distinctive semantic indicators of scammer profiles on dating websites and patterns in the choices of scammer personas, photographs used, and so on.
- Work investigating the geography of online romance scams. From this research, it can be seen that scammers in different countries target different types of victims in a variety of countries. There is also variation in marital status and occupation among targets of different genders.
- Collaboration with Southampton City Council and Trading Standards, looking at their procedures around preventing and detecting cybercrime. This work also looked at a local 60+ Silver Surfers group and the level of support given to prevent older people becoming victims of online fraud.
- Ethics issues associated with repeat scam victims and with victim-offenders.
- Ethics of scam-baiting, an investigation.

A number of publications are under review or due to be submitted before the project comes to an end in December 2018. A stakeholder meeting is due to be held in London at the end of the year to share findings from the project. Invitees will include academics, law enforcement agencies, dating website staff and Home Office staff.

Publications:

- Edwards, M., Suarez-Tangil, G., Peersman, C, Stringhini, G, Rashid, A & Whitty, M (2018). 'The Geography of Online Dating Fraud'. Paper presented at Workshop on Technology and Consumer Protection, San Francisco, United States, 24/05/18 - 24/05/18.
- Whitty, M. T. (2018). 'Do You Love Me? Psychological Characteristics of Romance Scam Victims', *Cyberpsychology, Behavior and Social Networking* 21(2), 105-109.
- Whitty, M. T. (2018). 'It's just a game: Developing a framework to understand cyberfraud from a Nigerian cultural perspective'. *International Journal of Cyber Criminology, 12, 89-106.*
- 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.*

Related Activity:

- Stringhini, G., provided evidence to the International Relations Committee of the House of Lords on cybercrime risks to the UK, specifically mass marketing fraud.
- Gumtree-the online advertising site--is currently taking advice from DAPM about fraud-prevention.

EPSRC Reference:	EP/N028112/2
Principal Investigator:	Professor Tom Sorell (University of Warwick)
Other Investigators:	Professor Michael Levi (Cardiff University)
	Professor Awais Rashid (Bristol University)
	Professor M. Angela Sasse (Ruhr-University Bochum)
	Dr Gianluca Stringhini (Boston University)
	Professor Monica Whitty (University of Warwick)

Evaluating Cyber Security Evidence for Policy Advice (ECSEPA)

The ECSEPA project seeks to provide support for the cyber security policy community in the UK, specifically those civil servants who provide short and longer term policy advice, either in response to specific crisis incidents or in the context of longer term planning for national security and capacity building. We regard this cohort as having particular significance to UK cyber security for a number of 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 has three main objectives:

1. Evaluate what exactly constitutes the evidence presented to and accessed by UK policy advisors, how they privilege and order 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 policy making that can be used to make recommendations for improvement and that can be re-applied to other public, private, and international cohorts.

During the project's first year, we completed a series of project deliverables. We conducted, transcribed and analysed 15 interviews with policy advisors. These interviews gave us valuable insight into the evidence sources used in cyber security policy advice, the general challenges and organisational issues that policy advisors face, and the areas in which they feel in need of additional support. We presented the highlights at the Global Internet Governance – Actors, Regulations, Transactions and Strategies (GIG-ARTS) conference in April 2018 (see below).

The interviews formed the basis for a two-month online survey which closed on 31 July 2018. It was designed to learn more about the kinds of evidence the broader UK policy community use in their work, how they evaluate evidence, and how they can be better supported. The survey is essential to help us understand what makes their jobs difficult and what changes or interventions could make it easier. With crucial assistance from the NCSC in helping us circulate the survey, 69 responses were received which satisfactorily met our target for this phase. We are now analysing the results from phase one data collection and we have presented a preliminary summary to our NCSC colleagues in September 2018. Next steps include incorporating the findings from the interviews and survey into the design of our upcoming ECSEPA Policy Crisis Games. This interactive game geared towards the policy community employs simulated cyber security scenarios to gain a glimpse into policy response and incident management, and to get a feel for how evidence is used and consumed in practice and under pressure. A pilot game will be undertaken in late 2018, with the main game in early 2019 involving participants from cross-government departments. Designed to promote a two-way knowledge exchange, the games will not only facilitate data gathering but also provide a forum through which the policy community can learn about how current research on evidence usage may apply to their work. Publications arising from the games' findings will be presented back to the policy community in the latter half of 2019.

In tandem to the work above, we created an interactive map of the UK cyber security governance landscape. This was based partly on the interviews and largely on desk-based research. The map includes departments, teams, programmes, and initiatives. Once the map was drafted, we hosted a Validation Workshop in London with representatives from over ten government departments as well as an EPSRC officer and UCL researchers. We will release the map back to the policy community along with a policy brief to reflect our findings.

Publications:

- 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., Dawda, S., Hussain, A., Shaikh, S., and Carr, M., (2018). 'Cybersecurity Policy*',* in *Encyclopedia of Security and Emergency Management,* LR Shapiro and MH Maras eds. Springer Nature.

Related Activity:

- Paper presentation titled, 'Cyber Security Capacity Building: Strengthening Policy Advice' at the Global Internet Governance – Actors, Regulations, Transactions and Strategies 2018, 26-27 April, Cardiff University.
- Paper presentation titled, 'An Evidence Quality Assessment Model for Cybersecurity Policymaking'. *Critical Infrastructure Protection XII*, IFIP, 12-14 March 2018, USA.
- Presentation of cyber security governance landscape map to policy, practitioner, and academic communities at the ECSEPA Mapping Validation Workshop, 8 February 2018, London.

EPSRC References:	EP/P011691/1, EP/P01156X/1
Principal Investigators:	Dr Madeline Carr (University College London)
	Professor Siraj Shaikh (University of Coventry)
Other Investigators:	Dr Alex Chung (University College London)
	Mr Atif Hussain (University of Coventry)
	Dr Emma Moreton (University of Coventry)

Leveraging the Multi-Stakeholder Nature of Cyber Security

This project is designed to leverage the distributed, multiple human stakeholder nature of cyber security by developing a novel framework (with the necessary scientific underpinning) to improve user access to tailored cyber security information. It develops a cutting-edge, data-driven Online CYber Security decision support System (OCYSS). This approach is designed to directly address an acute shortage of availability and access to highly qualified cyber security experts by both small-to-large scale users from government to industry.

In the last 12 months, the project team and ongoing work has grown quickly. Drs Josie McCulloch and Zack Ellerby have joined the team, with backgrounds in Computer Science and Psychology respectively. In addition, a number of PhD students are focussing on theoretical work underpinning the capture, modelling and reasoning with uncertain data, specifically when said data is captured in interval-valued form. Beyond the project team which includes colleagues at CMU, USA, the project has been supported by collaborations with Michigan Tech University and the University of Missouri, USA.

The ongoing work itself has focussed on three key strands:

- Refinement and validation of the interval-valued response format – employed to capture uncertainty from cyber security experts. A primary study contrasting participant responses when using traditional ordinal scales versus interval-valued scales has been conducted with exciting initial results on the type of information captured – which is not available through standard, discrete single-point questionnaires. An arising publication will be submitted later this year.
- The software development of an open-source toolkit enabling the rapid generation of questionnaires using an interval-valued response format has reached a milestone – with a Beta version completed in the summer of 2018. Working with the NCSC, the toolkit will be evaluated and refined over the next 18 months, followed by public release.
- Substantial advances in the handling and in particular the aggregation of interval-valued data have been made. These advances are important, as they allow the combination and comparison of individual interval responses (e.g., from individual experts). See publications.

Beyond the project itself, the related work has also expanded, with a three year Knowledge Transfer Partnership (KTP) with JP Morgan winning approval for co-funding by Innovate UK in July 2018.

Going forward, in parallel to continuing the wider work programme, a second study focussing on the specific nature of the uncertainty captured through interval-valued questionnaires is scheduled to launch in the autumn of 2018. The study is designed around a workshop setting with participants responding to tailored questionnaires using a kit of tablet computers. Coming to a workshop near you in 2018-2019, so keep your eyes peeled!

Publications:

- Kabir, S., Wagner, C., Havens, T.C., Anderson, D.T. and Aickelin, U. (2017) 'Novel similarity measure for interval-valued data based on overlapping ratio', *IEEE International Conference.*
- Havens, T.C., Wagner, C., Anderson, D.T., (2017) 'The Arithmetic Recursive Average as an Instance of the Recursive Weighted Power Mean', *Proceedings of the IEEE International Fuzzy Systems Conference.*
- Havens, T.C., Wagner, C., Anderson, D.T., (2017) 'Efficient modeling and representation of agreement in interval-valued data' *Proceedings of the IEEE International Fuzzy Systems Conference.*
- Agrawal, U., Pinar, A., Wagner, C., Havens, T.C. , Soria, D., Garibaldi, J.M. (2018) 'Comparison of Fuzzy Integral-Fuzzy Measure based Ensemble Algorithms with the State-of-the-art Ensemble Algorithms', *International Conference on Information Processing and Management of Uncertainty in Knowledge-Based Systems, 329-341* (Springer)
- Islam, M.A., Anderson, D.T., Du, X., Havens, T.C. and Wagner, C. (2018) 'Efficient Binary Fuzzy Measure Representation and Choquet Integral Learning', *International Conference on Information Processing and Management of Uncertainty in Knowledge-Based Systems, 115—126* (Springer)

EPSRC Reference:	EP/P011918/1
Principal Investigator:	Professor Christian Wagner, (University of Nottingham)
Other Investigators:	Dr Travis D Breaux, (Carnegie Mellon University, USA)
	Dr Stephen Broomell, (Carnegie Mellon University, USA)
	Professor Jonathan Garibaldi, (University of Nottingham)
	Professor Derek McAuley, (University of Nottingham)

Mapping Security Theories

The focus of this research programme is to better understand the relationships between the security of the individual, the security of the state and the security of the digital. A core part of this programme is to explore how Information Security as a discipline and as a practice relates to the broad and rich security theory landscape that can be found in the disciplines of Sociology and in Politics and International Relations. By drawing on this security theory landscape, the information security community may be able to both expand security practice and to better understand how the protection of information is linked to other forms of security – thus making an information security strategy more comprehensive. Security as experienced by people and institutions is a multi-dimensional problem and therefore needs multiple theoretical lenses and analyses to understand and positively respond to information security challenges.

The Everyday Safety and Security research programme has produced the Security Theory Map (STM) as a digital prototype that maps security theory from ancient Greek times to the present day. It enables security researchers and practitioners to examine their own security interests and concerns from a range of different theoretical perspectives, and to identify previously unacknowledged assumptions, relationships, and genealogies in concepts associated with the practice of information security.

The map is designed to enable researchers and security practitioners to drill down into the detail of each theory, to select and save this to a personalised interactive map showing the parts of theory that they have connected most strongly with, and which shows how these parts are related to one another. Exporting the map makes it possible to share maps, made by individuals or teams, across teams or organisations. This activity has the potential to stimulate detailed discussions comparing how information security issues and challenges can be handled in different ways by looking at these issues through different theoretical lenses and from different security positions.

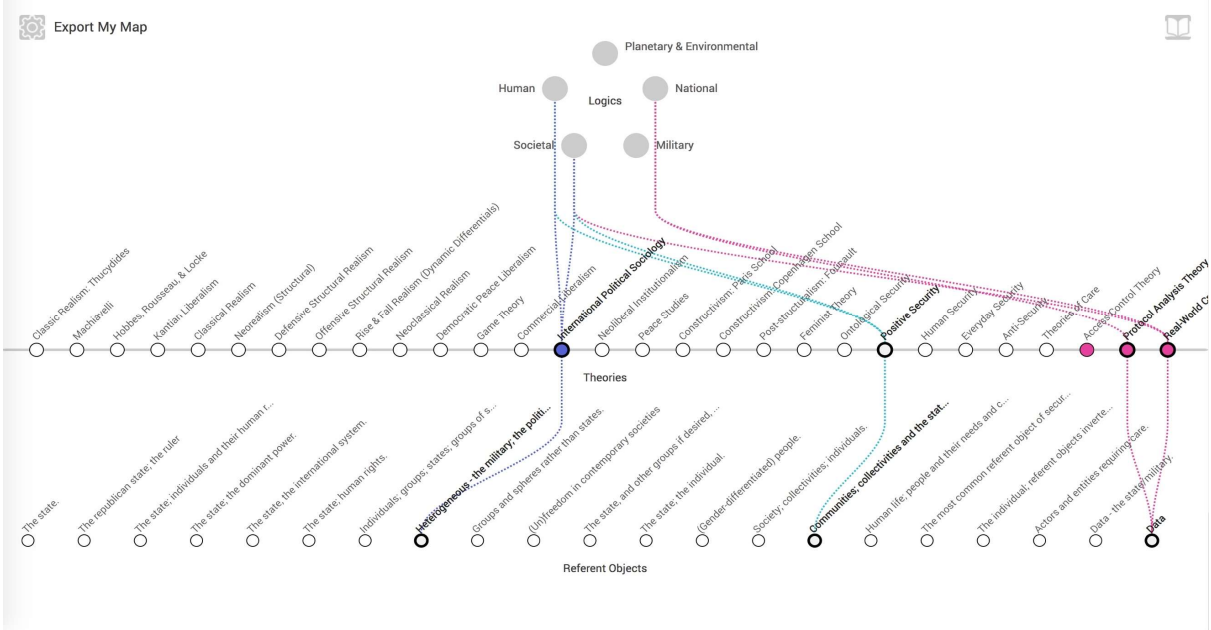


Figure One: The STM Prototype

To make the map usable, the STM groups security theories into security logics and the user of the map can then see how individual theories are linked to these logics. The map can be queried at a number of levels, which represent the constituent parts of the theories: agents of security, typical interventions and strategies, primary sources, the referent objects of security (the elements to be protected), the potential source of resilience that the operationalisation of a theory offers, and the threats posed to the referent objects. By providing multiple ways in which to interrogate theories of security, the STM functions a little like a synonyms and antonyms dictionary; it enables users to view

not only those aspects of theory that are closely related to a particular security focus or strategy, but also to see the opposites of these and to take this into account when designing security.

While the STM is not a definitive map, it promises to continue to grow and evolve with the feedback of researchers in many areas of security study and from the information security practice community. We are running workshop engagements for both academic and practice communities during 2018-19, with refinements added as a result of feedback. Please contact lizzie.coles-kemp@rhul.ac.uk if you would like to join or organise one of these workshops.

Publications:

- Coles-Kemp, L., & Hansen, R. R. (2017, July). Walking the line: The everyday security ties that bind. In International Conference on Human Aspects of Information Security, Privacy, and Trust (pp. 464-480). Springer, Cham.
- Coles-Kemp, L., Jensen, R. B., & Talhouk, R. (2018, April). In a New Land: Mobile Phones, Amplified Pressures and Reduced Capabilities. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (p. 584). ACM.
- Ashenden, D. M., Coles-Kemp, L., & O'Hara, K. (2018). Why Should I?: Cybersecurity, the security of the state and the insecurity of the citizen. Politics & Governance, 6(2), 41-48.
- Coles-Kemp, L., & Ashenden, D. (2017). 'An Everyday Story of Country Folk' Online? The Marginalisation of the Internet and Social Media in The Archers. In Custard, Culverts and Cake: Academics on Life in The Archers (pp. 249-267). Emerald Publishing Limited.

EPSRC Reference:	EP/N02561X/1
Fellow:	Professor Lizzie Coles-Kemp (Royal Holloway)
Researcher:	Mr Claude Heath (Royal Holloway)

EconoMical, PsycHologicAl and Societal Impact of RanSomware (EMPHASIS)

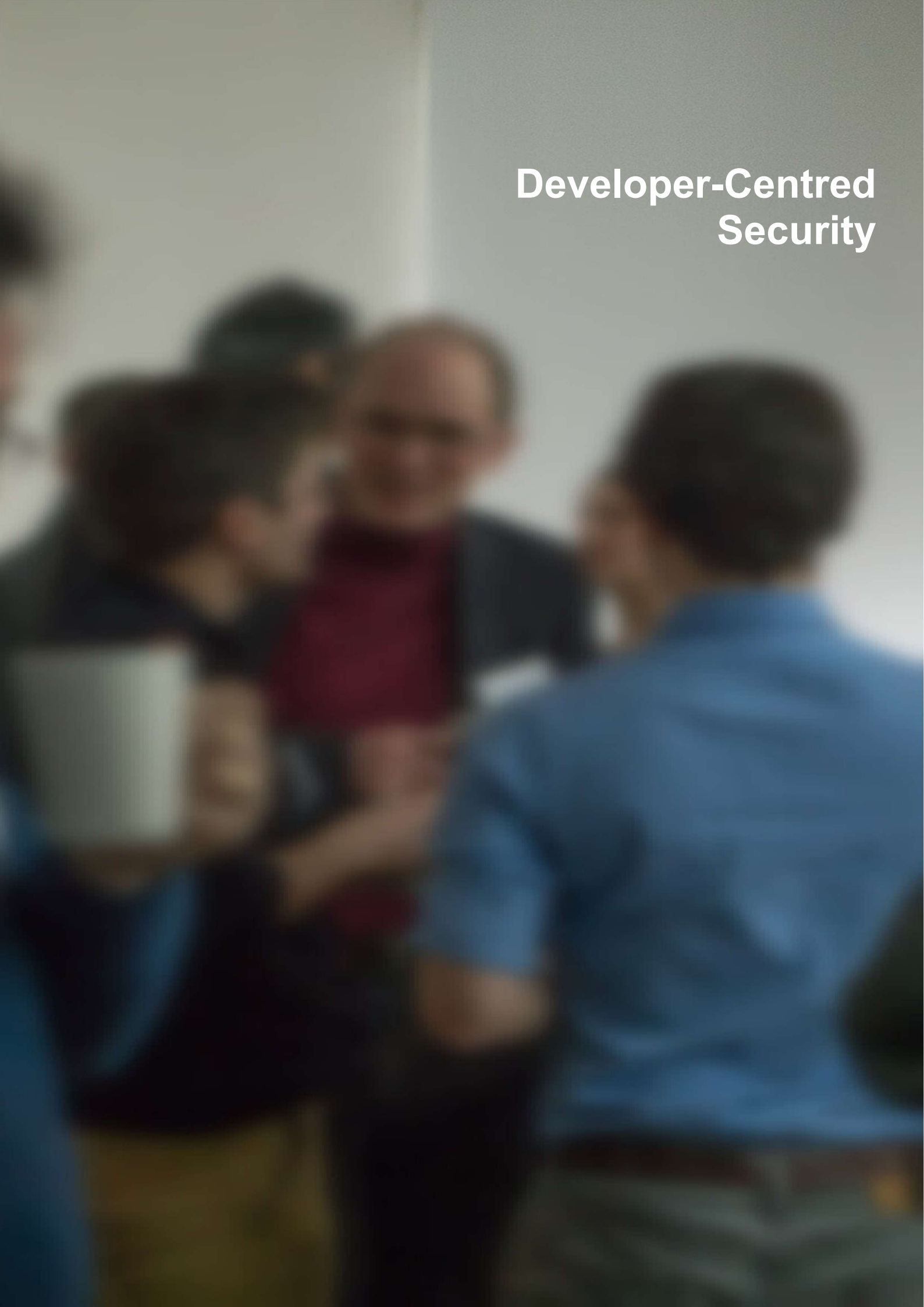
The EMPHASIS project asks the following research questions: Why is ransomware so effective, and why are there so many victims? Who is carrying out ransomware attacks? How can police agencies be helped? What interventions are required to mitigate the impact? The overall goal is to strengthen society's resistance to ransomware to make it less effective, protect and prepare potential victims, (whether organisations or citizens), and pursue the criminals.

The EMPHASIS ransomware project has made excellent progress on the economic and game-theoretic understanding of ransomware, culminating in a paper at the Workshop on the Economics of Information Security, with more to follow. Interviews with ransomware victims and a large scale cybercrime victimisation survey are currently underway and will lead to an increased understanding of ransomware crime stories and victim profiles. The project is pursuing several threads of technical, criminological, and psychological analysis using data gathered in the project and obtained from law enforcement agencies.

Publications:

- de Balthasar, T., Hernandez-Castro, J. (2017) 'An Analysis of Bitcoin Laundry Services'. In: *Lipmaa H, Mitrokotsa A, Matulevičius R (eds) Secure IT Systems. NordSec 2017. Lecture Notes in Computer Science, vol 10674*. Springer, Cham
- Wall, D.S. and Boiten, E. (2017) 'NHS caught out by WannaCry - now scrambling to catch up.' *Public Sector Focus,13, pp. 24-25. 2017*
- Boiten, E.A. (2017) 'WannaCry report shows NHS chiefs knew of security danger, but management took no action The Conversation,' 2017

EPSRC Reference:	EP/P011772/1
Principal Investigators:	Professor Eerke Boiten (DeMontfort University)
	Professor Tom Chen (City University)
	Professor Stephen McGough (Newcastle University)
	Professor David Wall (Leeds University)
Other Investigators:	Dr Budi Arief (University of Kent)
	Dr Edward Cartwright (DeMontfort University)
	Professor Julio Hernandez-Castro (University of Kent)
	Dr Anna Stepanova (University of Coventry)



Developer-Centred Security

Developer-Centred Security

By Helen L, NSCS

The RISCS Developer-Centred Security research portfolio (which complements the NCSC's guidance on secure software development and deployment) aims to help understand why things aren't working, and what we can do to better support developers and their organisations to write less buggy code. Our research shows that the following steps support developers to write more secure code:

- appreciate that security fundamentals are hard to get right
- acknowledge that developers are not necessarily security experts
- help stimulate conversations about cyber security from an early stage
- facilitate collaboration between security experts and developers
- reward and motivate developers - both intrinsically and through the work environment
- select tools and techniques that developers find usable
- promote a blame-free culture that encourages developers to report incidents (so that the team can learn from mistakes and continuously improve)

It's important to note that there are different kinds of motivators:

- intrinsic motivators relate to the work itself (such as clear goals, challenging and creative problem-solving tasks, recognition of quality work and autonomy)
- extrinsic motivators relate to externally driven factors (such as good management, creating a blame-free environment, a sense of belonging, rewards and incentives)

Of all the different motivators, the research has highlighted that creating a blame-free environment, where developers feel at ease with discussing their experiences without fear of being penalised for their 'mistakes', is the most important. It's not about addressing 'who did it?' but 'what caused it?'

It's important to remember that preventing every vulnerability in software is unrealistic, and often not a cost-effective business model. Development practices should include accepting the inevitability of such problems, and organisations should 'plan for security flaws'. Understanding this balance between prevention vs reducing harm is a crucial part of a risk management approach. Having confidence in being able to identify the leaks in a software development pipeline (and understanding how they can be 'mopped up' in a blame-free environment) is a crucial part of empowering developer-centred security.

Most importantly, a developer-centred approach to security enables coders to do what they do best: applying their creativity and knowledge to develop new functionality that enables us to do more and businesses to thrive.

Many tools and learning resources don't consider what the developer is trying to do, instead focusing on what they must *not* do. However, there are tools being developed under the RISCS Developer Centred Security research umbrella that aspire, eventually, to pro-actively support developers to write more secure code. These are outlined in the following projects.

You Get Where You're Looking For: The Impact of Information Sources on Code Security

Sascha Fahl's project, with Yasemin Acar and Marten Oltrogge, looks at the impact of "citizen developers" on software security. A relatively new phenomenon, citizen developers are users who create new business applications for use by others instead of professional developers using development and runtime environments sanctioned by corporate IT. Often they use code generators. There are a lot of these; they are easy to use; and laypeople can create apps using a mouse and drag-and-drop. However, the development process is a black box, and it's hard to know what's happening inside. Fahl set out to ask two research questions; are generated apps widely used and what is their impact on code security?

There are two types of generators: those you download and run on your own machine, and those you use online. Fahl began by building analysis tools to identify these generated apps. Running these tools across 2.2 million Android apps, he found 250,000 generated apps with 1.1 billion collective installs. All of these came from a list of approximately 25 online generators. Analysis of the generated apps found they did duplicate known issues, but also added new problems, such as using a single signing key to sign up to 30,000 apps. Put simply, he was seeing automated lack of security.

The result of this work was a paper that will be presented at *IEEE Symposium on Security and Privacy* in May 2018. Respondents commented that this was an important piece of work that has highlighted a scaled security issue. Future work will look at who is using these generators, information that will be needed to answer the question of how to make them more secure but still easy to use. The researchers are also planning coordinated disclosure.

Publications:

- Acar, Y., Backes, M., Fahl, S., Kim, D., Mazurek, M.L., Stransky, C. (2016) 'You Get Where You're Looking For: The Impact of Information Sources on Code Security': *2016 IEEE Symposium on Security and Privacy (SP)*

Principal Investigator	Professor Sascha Fahl (Ruhr-Universität Bochum)
Other Investigators:	Ms Yasemin Acar (Leibniz University Hannover)

Interventions to Improve Software Security in Development Teams

Charles Weir (Lancaster University) works on the Magid Research Project with a team including Ingolf Becker (UCL), Lynne Blair (Lancaster), Awais Rashid (Bristol) and Angela Sasse (UCL). Prior work had identified a range of inexpensive interventions to help teams with software security. Now, the team have developed a lightweight 'Developer Security Essentials' package of workshops to introduce these to a development team. Over the last year they have used this with teams in three widely different companies and recorded the process. Using dual coding of the transcribed sessions, the researchers identified what aspects of the package worked effectively, and where improvements are necessary.

The results have been encouraging: two of the teams adopted new and effective security assurance techniques; the other reported improved communication and identified that their software security was already very effective. Based on detailed feedback from the research, the team have developed an improved package, designed to be introduced without the support of security or research professionals. They have also created web-based collateral to support adopters of the package. This offers a potential 'viral' distribution model, where development teams can adopt the package without active support from the researchers.

The Magid team are now trialling this improved package with a larger range of software development teams. In future, they look to encourage wide scale adoption of packages of this kind, to empower developers and play a much-needed role in improving software security for all end users.

Publications:

- Weir, C., Blair, L., Becker, I., Sasse, M.A., and Noble, J. (2018) 'Light-touch Interventions to Improve Software Development Security.' *IEEE Cybersecurity Development Conference, IEEE Computer Society.*
- Weir, C., Blair, L., Noble, J., Becker, I., Sasse, M.A. Developer Cyber Essentials: 'Trialling Interventions to Improve Development Security'. (2018) *Lancaster.*
- Weir, C. and Ford, N. (2018) 'Secure Development Handbook.'.

Principal Investigator:	Professor Charles Weir (Lancaster University)
Other Investigators	Dr Ingolf Becker (University College London)
	Dr Lynne Blair (Lancaster University)
	Professor Awais Rashid (University of Bristol)
	Professor M. Angela Sasse (Ruhr-University Bochum)

Impact of Gamification on Developer-Centred Security

Manuel Maarek (Heriot-Watt), Sandy Louchart (Glasgow School of Art), Léon McGregor (HW) and Ross McMenemy (GSoA) are studying the impact of gamification on developers using coding-based games, competitions, interactions for education, and securing coding games. The main research question: does gamification have a greater impact on security or non-security tasks? The researchers' hypothesis is that it does, based on the impression that adversarial discussions are easy for security, a trigger that can be activated by putting the task inside a game.

Each participant is given six programming tasks; three have a security focus and three do not. They work in two settings, performing these tasks as part of a sequence of online programming exercises or as part of an online game with programming exercises. As control groups, the security tasks were chosen to partially replicate Sascha Fahl's and Yasemin Acar's SOUPS 2017 paper, and the effect of gamification was studied by comparing security and non-security tasks.

Publications:

- Maarek, M. Louchart, S., McGregor, l and McMenemy. R. Co-created design of a serious game investigation into developer-centred security. In Games and Learning Alliance, 7th International Conference (GALA 2018), Palermo, Italy, 2018.
- Acar, Y., Stransky, C., Wermke, D., Mazurek, M.L. and Fahl, S. Security Developer Studies with GitHub Users: Exploring a Convenience Sample. In Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017), 2017.
- Rojas, J.M., White, T.D., Clegg, B.S. and Gordon Fraser. Code Defenders: Crowdsourcing Effective Tests and Subtle Mutants with a Mutation Testing Game. In Proceedings of the 39th International Conference on Software Engineering, Piscataway, NJ, USA, 2017. IEEE Press
- Ruef, A., Hicks, M., Parker, J., Levin, D. Mazurek, M.L. and Mardziel, P. Build It, Break It, Fix It: Contesting Secure Development. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, CCS '16, pages 690–703, New York, NY, USA, 2016. ACM.

Principal Investigator:	Professor Manuel Maarek (Heriot- Watt University)
Other Investigators:	Dr Sandy Louchart (Glasgow School of Art)
	Mr Léon McGregor (Heriot- Watt University)
	Mr Ross McMenemy (Glasgow School of Art)

How Developers and Security Experts View Big Data

Laura Kocksch spent eight months in companies looking at data innovation versus security and observed a clash of philosophies. She does not see security as just a technical definition that can be inculcated into developers; many do already think about security and have their own picture of what it is.

Her previous research showed that there may be good organisational reasons for bad security. Extra work solving security problems rarely gets developers any credit and they often struggle to keep up with this extra workload. They liked their training, which stuck with them for six or seven months after the training ended, but still needed organisational support. If, for example, security doesn't count as a feature request it does not form part of their accountable work practices. Longstanding industry sectors such as energy and insurance are starting to take on big data, and are accordingly making changes in their data infrastructure, which might offer a good opportunity for security by design.

For this project, she spent eight months inside companies studying the tension between data innovation and security, where the company sees big data as a big opportunity but believes that security always holds it back. She found a complete clash of cultures, which raised questions of how to translate between them to enable cross-disciplinary understanding. Social science has long-standing ideas of how this might work.

Kocksch has a number of questions. Where and when does security come up? When in the processes is it important to the developers to talk about security? What does it mean to them? These things need to be defined. Certain concepts that focus on establishing symmetrical discussions might apply, such as boundary objects and trading zones.

A questioner asked if the concept of "security as a service" would be helpful, so that the security team would take the humble approach of offering help to developers rather than saying no to things. Kocksch agreed that the people she talked to call the security department "the department of No", often for good reasons. Kocksch is trying to open up the network of connections that are there, rather than trying to define big data. A key issue is whether the two different groups want to work together; Kocksch has found that both groups feel there is a new infrastructure opportunity, but the problem remains that they have completely different goals.

Publications:

- Poller, A., Kocksch, L., Türpe, S., Epp, F. A., & Kinder-Kurlanda, K. (2017, February). Can Security Become a Routine?: A Study of Organizational Change in an Agile Software Development Group. In *CSCW* (pp. 2489-2503).
- Kocksch, L., Korn, M., Poller, A., & Wagenknecht, S. (2018, in publication). Caring for IT Security: Accountabilities, Moralities, and Oscillations in IT Security Practices.

Research team:	Dr Laura Kocksch (Ruhr-Universität Bochum)
	Professor Estrid Sørensen

Motivating Jenny to Write Secure Software: Community and Culture of Coding

This project is examining the role of developer motivation in the production of secure code, with a focus on professional developers who are not security specialists. Previous research has found that successful developers are rarely motivated by reading documentation or studying manuals. Instead, peer-to-peer interactions, within the team, within the organisation, and within wider developer communities are more likely to bring about lasting cultural change. Furthermore, developer communities that transcend organisation boundaries can be very influential in directing behaviour and identifying technical solutions. This project is looking at individual motivation and interactions within their communities, examining how personal and social identities can be used to influence behaviour, with the goal of identifying how to motivate developers to write secure software.

Starting from existing research into developer motivation, the project aims to:

1. Develop an empirically-grounded model of why and how non-specialist developers can be motivated to adopt secure coding practices and to effectively integrate existing security technologies into their software development practice; and

2. Produce a practitioner pack for creating and propagating a security culture across software teams

To do this, we are characterising our target 'Jenny' or 'Jennies' using personas, conducting online and face-to-face ethnographic studies of developers, and engaging with practitioner communities through conference, workshop and individual interactions. For our face-to-face studies, we are collaborating with two distinct software organisations. For off-line studies, we have been focusing on StackOverflow, and will collaborate with a range of companies in the UK and in Ireland, Brazil and Japan.

We have developed a persona template for characterising developers, which is informed by existing work on motivation, security and social psychology. A set of preliminary personas has been defined based on literature and practitioner reports. Data collected in our various studies and interactions is being used to refine and develop these preliminary personas. A shorter version of the template was evaluated with developers at the Extreme Programmers London Meetup at the end of November 2017.

Our studies so far have shown that: online conversations about security are influential in shaping developer perceptions and values; security is part of the daily practice of developers, e.g. through code reviews, when accessing data, and as users of various third party platforms and libraries; and developers regard security as necessary, but it can also be a barrier to getting work done.

Motivation to work is a complex and very individual concept, which makes it challenging to understand, and security is, in part, a social phenomenon. Within both online and offline developer communities, whether at team, organisational, or professional level, there are influential individuals and conversations that emerge which affect the way secure coding is practised. Early indications are that in many ways, security is 'just' another aspect of code quality, and hence the motivational factors that sit around it are not different to motivational factors for any other attribute of code quality.

Publications:

- Lopez, T., Tun, T.T., Bandara, A., Nuseibeh, B., Sharp, H., & Levine, M., (2018). An Investigation of Security Conversations in Stack Overflow: Perceptions of Security and Community Involvement. 1st International Workshop on Security Awareness from Design to Deployment, International Conference of Software Engineering, 2018. Gothenburg, Sweden, 27 May 2018

Related Activity:

- Presentation at XP 2018 (Porto, Portugal): International Workshop on Secure Software Engineering in DevOps and Agile Development at XP 2018 on 25 May 2018. The presentation was called “Security Conversations in Practice”
- Invited presentation and workshop: Helen Sharp & Tamara Lopez. Motivating Developers: Community and Culture of Coding. Extreme Programmers London Meetup, 30 November 2017.
- Workshop: Tamara Lopez, Helen Sharp and Thein Tun gave a workshop on Secure Code Development in Practice at the SPA Conference in London on 2 July 2018
- Workshop: Tamara Lopez, Helen Sharp and Thein Tun gave a workshop on Secure Code Development in Practice at the SPA Conference in London on 2 July 2018
- In April-May 2018, Tamara Lopez collaborated with researchers from Leibniz (Acar, Schrader), Ruhr (Fahl) and Saarland Universities (Gröber) on a qualitative study examining security library selection practices.
- Workshop: Tamara Lopez, Helen Sharp and Thein Tun gave a workshop on Secure Code Development in Practice at the SPA Conference in London on 2 July 2018
- We have been discussing with Charles Weir (Lancaster University) the interventions he has developed and assessed, and how they may be integrated in this project's practitioner pack.
- We have been discussing with members of the EPSRC-funded Johnny project regarding how best to leverage our two sets of studies.

Principal Investigator:	Professor Helen Sharp (The Open University)
Other Investigators:	Professor Arosha Bandara (The Open University)
	Professor Mark Levine (University of Exeter)
	Ms Tamara Lopez (The Open University)
	Professor Bashar Nuseibeh (The Open University)
	Dr Thein Tun (The Open University)

Why Johnny Doesn't Write Secure Software: Secure software development by the masses

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. Currently, little is understood about the security behaviours and decision-making processes of Johnnys engaging in software development. The overall aim of this EPSRC-funded project is to develop an empirically-grounded theory of secure software development by Johnnys. Our focus is on understanding:

1. what typical classes of security vulnerabilities arise from Johnny's mistakes,
2. why these mistakes occur, and
3. how we may mitigate these issues and promote secure behaviours.

Studies undertaken

In 'Using cryptography APIs securely – visual building blocks', (van der Linden, Rashid, Williams, and Warinschi, 2018), we focused on a key aspect of the modern software developers' potential to write secure software: their (lack of) success in using cryptography APIs securely. In particular, we set out our vision toward secure cryptography-API use by young and inexperienced developers, by moving them away from the actual source-code. We proposed to adopt visual programming to use targeted visual metaphors - derived empirically through participatory design - to offer building blocks for the most-needed cryptography functionality. Ongoing further work intends to connect such building blocks to automatically-generated code that provides key functionality, for example using CogniCrypt's existing generation of source-code which uses cryptography APIs correctly.

In an online study of active, published, mobile app developers, we focused first on understanding what they think affects the security of the apps they write, followed by an in-depth task-based study assessing the prevalence of solutions favouring security. We captured detailed qualitative data of participants' reflections on their solutions, allowing us to understand to what extent their actions align with their motivations and intentions. ('Setting the baseline: what characterizes Johnny's attitude towards security?')

On-going studies

'Mapping the intervention space: how are we trying to support Johnny?'

This ongoing analysis of literature from different research areas - including software security, software engineering, and human-computer interaction – aims to understand potential interventions to influence Johnny's secure software development practices. We intend to produce conceptual models which address the intervention needs for different contexts in which Johnny may develop software, as well as different behaviours for which Johnny needs support. The study will also map the landscape of existing security interventions, in order provide a research agenda for the community.

Publications

- van der Linden, D, Rashid, A, Williams, EJ & Warinschi, B 2018, 'Safe Cryptography for All: Towards Visual Metaphor Driven Cryptography Building Blocks' Paper presented at First International Workshop on Security Awareness from Design to Deployment, International Conference on Software Engineering, 2018, Sweden
- Weir, C., Rashid, A., & Noble, J. (2017).'I'd Like to Have an Argument, Please: Using Dialectic for Effective App Security.' In EuroUSEC 2017: the 2nd European Workshop on Usable Security. Reston, VA: Internet Society.
- Weir, C., Rashid, A., & Noble, J. (2017). 'Developer Essentials: Top Five Interventions to Support Secure Software Development'. Lancaster: Lancaster University
- Weir, C., Rashid, A., & Noble, J. (2016). 'Reaching the Masses: A New Subdiscipline of App Programmer Education'. In FSE 2016: Proceedings of the 2016 24th ACM SIGSOFT International Symposium on Foundations of Software Engineering. (pp. 936-939). New York: ACM.
- Lopez, T., Petre, M., & Nuseibeh, B. (2016). 'Examining active error in software development.' In VL/HCC: IEEE Symposium on Visual Languages and Human-Centric Computing (pp. 152-156). IEEE Press.
- Weir, C., Rashid, A. & Noble, J. 'How should mobile app programmers learn security? comparing and contrasting expert views' In Proceedings of International Workshop on Security Information Workers at SOUPS, 2016.
- Lopez, T., Petre, M., & Nuseibeh, B. (2012). 'Getting at ephemeral flaws.' In CHASE: Proceedings of the 5th International Workshop on Co-operative and Human Aspects of Software Engineering (pp. 90-92). IEEE Press.
- Tun, T. T., Jackson, M., Laney, R., Nuseibeh, B., & Yu, Y. (2009). 'Are your lights off? Using problem frames to diagnose system failures.' In RE'09: 17th IEEE International Requirements Engineering Conference (pp. 343-348). IEEE Press.

EPSRC Reference:	EP/P011799/1
Principal Investigators:	Professor Awais Rashid (Bristol University)
Other Investigators	Dr. Dirk van der Linden (Bristol University)
	Professor Bashar Nuseibeh (The Open University)
	Professor Marian Petre (The Open University)
:	Dr. Irum Rauf (The Open University)
	Dr. Thein Tun (The Open University)

Supporting the Board

Cyber Readiness for Boards

The role of boards in contributing to a broader agenda of cyber security is well established. Cyber security is discussed at 80% of board meetings, it is regarded as a top concern for CEOs (and *the* top concern for investors – according to the PWC Global Investor Survey, 2018) and yet, only 11% of corporate directors believe their boards have a high level understanding of cyber risk (survey by NYSE Governance Services). 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. Consequently, the NCSC and RISCS have initiated a research agenda to provide support to boards in making sound assessments of cyber risk.

In order to better understand board decision-making processes on cyber security, this project takes 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 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:

- 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 multi-disciplinary team builds on established methods from three fields to bring something genuinely new to the study of board level cyber risk assessment. The researcher team has the expertise to understand the human, organizational, commercial, technical, policy, and wider environmental factors that shape decision-making about business risk. The project has outstanding collaborative partners which are essential to gaining access to boards, including Lloyds Register Foundation, Axelos, Hermes EOS, Brunel Pension Partners and the Environmental Agency Pension Fund.

The outputs from this project will contribute significantly to state of the art research into the intersection of board cyber risk assessment. Through the development of a comprehensive framework for identifying, understanding and improving the internal and external factors that influence board decision-making in this context, the narrow focus on cyber risk will be opened up to include a range of factors not previously taken into account. Not only will this be useful as a tool for future analysis of cyber governance, it will lay the foundation for future researchers to incorporate other similar environmental factors.

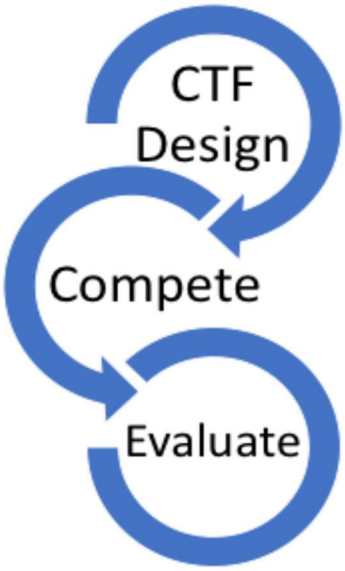
Principal Investigators:	Dr Madeline Carr (UCL)
Other Investigators	Professor M. Angela Sasse (Ruhr-Universität Bochum)
	Dr Tony Moore (Reading University)
	Professor Andreas Hoepner (Reading University)
:	Professor Siraj Shaikh (Coventry University)
	Dr Simon Parkin (UCL)

RISCS Short Projects

Capture the Flag Exercises

A Capture The Flag competition (CTF) is a game in which different teams compete to solve different cyber security puzzles in a time-constrained exercise. This project uses jeopardy-style completion, where the contestants are provided clues in the form of answers and must phrase their responses in the form of questions. This type of competition involves different categories of problems - namely, challenges. Each of these challenges represents a cyber security question that the team must solve in order to earn a number of points. The goal of this project is to understand if a Capture The Flag competition (CTF) can influence the way practitioners confront security. The project is divided into three phases: (i) the design, implementation and development of a CTF competition; (ii) the actual competition, and; (iii) the collection of feedback and an assessment to evaluate how the competition influences the way in which they do security. The methodology used in this project is based on the waterfall model, where each of these phases are executed sequentially as shown in Figure 1.

Figure 1: The methodology of the CTF project.



Phase One of the project involved the development of the software infrastructure as well as the challenges for the CTF competition. The focus of the challenges was refined following three meetings with a well-known high street retailer, who was given access to a demonstration of the competition. The next steps will include running the competition among a group of its technical employees, followed by evaluation of how running this awareness exercise influenced their approach to computer security.

Principal Investigators:	Dr Gianluca Stringhini (Boston University)
Other Investigators	Dr Simon Parkin (University College London)
	Professor M. Angela Sasse (Ruh-rUniversität Bochum)
	Dr Guillermo Suárez de Tangil (Kings College London)

Supporting Data Security and Privacy in the Home

The researchers investigated the use of internet-connected technology in the home. In the first part of the research, they interviewed 36 participants about the routine aspects of their use of and cohabitation with the internet-connected devices from categories other than entertainment and communications that they own and use in their homes.

Based on these interviews, the researchers went on to survey the social context and usage of these devices in order to understand how home users can be better supported in securing their domestic infrastructure. In the first part of this two-part study the researchers interviewed two nationwide Internet Service Providers, finding that reputation, legal requirements, cost, limitations imposed by privacy laws and lack of contextual knowledge are all factors in determining whether and how they will intervene. In the second part, the researchers reviewed best practices in network security and evaluated three home network routers in terms of their capability of supporting these best practices in a simple and usable way.

Publications:

- Nthala, N., Flechais, I., 'Informal Support Networks: an investigation into Home Data Security Practices' *SOUPS@USENIX Security Symposium 2018: 63-82*

Principal Investigator:	Professor Ivan Flechais (University of Oxford)
Other Investigators:	Martin Kraemer (University of Oxford)
	Norbert Nthala (University of Oxford)

Separating Security Science from Pseudo-Science: A Systematisation of Knowledge (SoK) review of survey constructs measuring security behaviour

In a scientific intervention to support the NCSC's 'People: The Strongest Link' policy, the researchers studied the scientific validity of the surveys organisations use to identify constructs associated with compliant and non-compliant security behaviour and to measure the effectiveness of interventions to change behaviour. The underlying assumption is that these surveys can measure employee compliance with security policies and identify rule-breakers. The questions used in these surveys have been drawn from numerous disciplines such as psychology and organisational behaviour and repurposed for the security context. A literature review found little methodological rigour in adopting these constructs, most of which have been reused from existing literature; the review also found 217 newly created "security constructs". The resulting resource will be useful for academics and practitioners for exploring the existing survey constructs and building meaningful surveys without the need to re-invent them.

Related activity:

- Security Constructs Database*: https://verdi.cs.ucl.ac.uk/constructDB/*

Principal Investigator:	Professor M. Angela Sasse (Ruhr-University Bochum)
Other Investigators:	Dr Ingolf Becker (University College London)

ECSEPA Mapping Project

'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.

A Mapping Project research assistant was hired between November 2017 and March 2018 to carry out research tasks designated for this project phase. This included a series of infographics that provide a clear visual guide to cyber security governance in HMG, based on a number of interviews and stakeholder meetings. Along with this, we have drafted a report for the policy and research communities that documents the results of the desk-based work and the validation workshops. We are now feeding these results into a jointly authored journal article (with the ECSEPA team) that contributes to the broader debates about global governance of complex policy issues like cyber security. The dissemination of the latter part of the research is currently being managed in collaboration with key stakeholders and the funder.

The primary impact ambition of the team is directed to bringing benefit to the civil service and policy community. To do this most effectively, we are drawing support from the NCSC team, from POST, and from the Director for Policy in UCL STEaPP. Together, we are developing a series of policy engagements that will be incorporated into the broader ECSEPA policy impact plan.

Principal Investigator:	Dr Madeline Carr (University College London)
Other Investigators:	Professor Siraj Shaikh
	Dr Alex Chung (University College London)
	Ms Sneha Dawda (University College London)
	Mr Atif Hussain

Appendix 1: 2018 Community Meeting Programs

February 7, 2018 RISCS Community Meeting

10.00 – 10.30	Coffee and Registration
10:30 – 10:45	Welcome
10.45 – 11.30	Conducting impactful cyber security research Yasemin Acar *(Leibniz University Hannover)*
11.30 – 12.00	Doing Social Science and Computer Science: Obstacles and Opportunities Shari Lawrence Pfleeger *(Pfleeger Consulting Group)*
12.00 – 12.30	Foundational Cybersecurity Research: Improving Science, Engineering, and Institutions- reflections on key recommendations from the US National Academies Report Roy Maxion *(Carnegie Mellon University)*
12.30 – 12.50	Strength of Evidence in Cyber Security User Studies Thomas Gross *(Newcastle University)*
12.50 – 13.50	Lunch
13.50 – 15.30	Future of Community Meetings: strategic direction, priority problem spaces and methods of engagement Lizzie Coles-Kemp (RISCS Deputy Director)
15:30	Round-up session
16.00	Close

February 8, 2018: Developer Centred Security Workshop

09:30 – 09:50 Welcome & Introduction (Helen) (20 min)

Helen will open the day by discussing the aims of the Developer Centred Security (DCS) research and community and how it supports secure software development, where we are now (from the perspective of the NCSC) and what she hopes to achieve from the day.

09:50 – 11:00 "Developers Den" (70 min) hosted by Nicola

Bringing together researchers, industry practitioners and users, to work through the challenges faced in practice together, is an important aspect of the RISCS community. This section will enable this feedback loop between the DCS researchers, practitioners developing tools to help software developers and the developers themselves.

Introductory 5-10 minute pitches of their tools/ techniques will be delivered by:

- Secure Code Warrior
- Drie
- The UK Hydrographic Office (Security Champions)
- Thoughtworks (Sensible Conversations)

Our (friendly) panel of DCS researchers and developers will ask questions and offer feedback on what they have heard, based on their work and experience, before discussion and questions are opened up to the community.

Panellists: Prof. Helen Sharp, Prof. Awais Rashid, Dr Sascha Fahl, Dr Yasemin Acar, Charles Weir, Manuel Maarek, Michael Brunton-Spall, Harry Metcalfe.

11:00 – 11:25 Coffee (25 min)

11:25 – 12:15 "Reverse Panel Session" (50 min) hosted by Sam

This section turns a panel session on its head. Seniors across government and industry will be invited to pose questions, or articulate their challenges, to the DCS community on the topic of secure software development and how it can and can't currently be effected in their organisations.

These questions may be delivered in person, by video or by email...and any member of the floor can catch the mic to offer their answer, observation or ideas in response. We will record the responses and send them back to the senior that asked the question.

12:15 – 13:10 Lunch

13:10 – 14:45 "Lightning Talks" (75 min) hosted by Ceri

(There will be a 15 minute coffee/ comfort break during this session at a convenient point.) The DCS researchers involved in the following projects will provide a 5-7 minute 'lightning talk' on either their research project, or in response to what they have heard during the day. The remainder of their 15 minute slot will be used for questions, comments, war stories etc from the floor.

- Motivating Jenny to write secure software (PI: Prof. Helen Sharp)
- Why Johnny doesn't write secure software: secure software development by the masses (PI: Prof. Awais Rashid)

- You Get Where You're Looking For: The Impact of Information Sources on Code Security (Dr Sascha Fahl, University of Hannover)
- Trialling Interventions to Improve Software Security in Development Teams (Charles Weir, Lancaster University)
- Impact of gamification on Developer-Centred Security (Manuel Maarek, Heriott-Watt University)

14:45 – 15:15 Networking, Discussion & Questions (30 min) hosted by Helen

A chance to grab another coffee and take part in a facilitated discussion about the DCS topic. Those that want to network can use this time to have those important one-to-one conversations.

15:15 – 15:30 Wrap up – summary of the day and next steps (Helen) (15 min)

Helen will close by summarising the day, and proposing the next steps and required support from the NCSC and others for this important topic of research.

February 8, 2018: Scientific Methods and Approaches for Cyber Security

09:30 – 09:50 Welcome & Introduction (Thomas Gross)

We will open the workshop by outlining what we hope to achieve in terms of outcomes. This will be followed by polling the participants on:

- Which practical and lived cyber security issues would you want to see addressed by scientific inquiry?
- How could science contribute?

09:50 – 10:50 Cyber Security Scholarship: The field and disciplines that form the field (David Wall & Lizzie Coles-Kemp)

Drawing on a wide range of experiences, David and Lizzie will sketch out the complex scientific landscape that shapes our understanding of relevant cyber security issues. They will identify the different fields of science that need to be brought to bear when analysing and designing effective interventions for cyber security problems that people and organisations experience. The session will present a range of scientific methodologies and approaches, consider how they make a difference at their best, as well as ask questions of effectiveness, quality and representativeness.

10:50 – 11:05 Coffee

11:05 – 11:50 State-of-Play of Scientific Methods: Our field and others
(Kovila Coopamootoo & Thomas Gross)

This session asks the question: “How well is Science doing in creating reliable and practically relevant results?” “What could possibly go wrong?” “What difference will that make for practitioners?” We will make observations on our own field in an accessible way, at first. Then, we consider problems that other fields have faced in their endeavour to deliver rigorous and effective science as well as some of the solutions with which the sciences responded to those problems.

11:50 – 12:15 Key Scientific Concepts: A Community Discussion (Plenum)

This session will form one foundation of a structured group discussion in the afternoon. We invite the participants to write their ideas and concepts on moderation cards in answer to the following questions:

- What are the pivotal elements of scientific methodology in cyber security that we need to get right?
- What obstacles do we need to overcome for strong science supporting cyber security practice?
- What do we stand to gain from a strong scientific methodology?
  We collect the concepts offered by the plenum for a subsequent clustering.

12:15 – 13:00 Lunch

13:00 – 13:45 Shaping the Way Ahead (Plenum)

We will start with presenting the clustering of the concepts elicited from the plenum in the previous session. We’ll engage in a discussion on the clusters to reach consensus on the important topics, and then offer participants an opportunity to display their own priorities with stickers. The outcome of the session

is a visual representation of the crucial concepts together with the weighting by the audience.

13:45 – 14:45 Discussions in Focus Groups

This is an opportunity to join a discussion that is at the heart of the matter for you. We will create up to five focus groups on topics derived from the prioritization of the previous phase. The focus groups are first to settle on concrete and accessible examples that illustrate the situation to a broad audience. While topics can range from hallmarks of strong scientific evidence all the way to how science can best impact the needs of practitioners, we ask all focus groups to propose guiding principles as well as concrete steps to take for different stakeholders (e.g., scientists, scientific committees, funding bodies, publishers, practitioners). With the help of a rapporteur and a scribe, the focus groups will each produce a flipchart with a visualization of their discussion.

14:45 – 15:30 Lightning Presentations of the Focus Groups (Plenum)

Armed with a flipchart including the summary of their discussion, the rapporteurs of the focus groups will report back to the plenum. We will have 6-minute presentations with room for questions from the plenum.

15:30 – 16:00 Wrap-Up & Next Steps (Thomas Gross)

We will summarize the outcomes of the day, make decisions on how to proceed and outline next steps. As an outcome, the workshop yields recommendations to be fed back to the RISCS Scientific Sub-Board. Overall, we intend to create a position paper together with the RISCS Scientific Sub-Board.

May 23, 2018: Metrics and Healthcare

09:30 – 10:00 Registration (Please join us for tea & coffee.)

10:00 – 10:45 Welcome and announcements

10:45 – 12:30 Use of metrics in the healthcare sector

To frame our two-day discussion into the use of metrics in decision making, we begin with a great line up of speakers who will discuss the use of metrics in the healthcare sector. This is a valuable use case because the interpretation of complex inputs in healthcare is crucial to informing risk decisions around data-sharing and public safety. It is also useful because it intersects with many of the IoT security issues that will frame our workshop into *Uncertainty and Complexity in the IoT* tomorrow.

David Reeves, NHS Digital
Data Security and Protection Toolkit: David will introduce us to the new data security compliance and journaling mechanism for the whole of Health and Social Care. How is data gathered and how is progress against Dame Fiona Caldicott's new 'data security standards' demonstrated for regulators and peer organisations?

Helen Dawes, Oxford Brookes University
Missing and false data: Helen will outline the potential of linking information of body functioning and other factors to inform understanding of if, why, and how interventions work. She will discuss this in the context of our transition to a health care system that supports the population to live with and manage conditions in the community.

Cliff Lake, Public Health England
Cliff will talk to us about how epidemiological data gathered from numerous sources is geospatially visualised to inform important public safety decisions on the ground.

13:30 – 15:30 Interactive Workshop: Use of metrics for communicating risk to board/policy communities

In this session, we will consider how to apply cyber metrics to decision-making more generally, and raise questions about how data is best presented to the board and the policy community. We want to explore the potential for metrics to help but we also want to take a critical approach to the underlying values that can shape metrics – and consequently, decisions.

Madeline Carr (RISCS Director) and Sam B (NCSC) will give a short presentation in order to lead into an Interactive workshop in which we'll be drawing out some of the different perceptions about which metrics the cyber security community is willing and able to provide as compared to which metrics the board/policy community wishes to have provided to them.

15:30 – 16:00 Wrap up and overview of Day Two: Decision Making Under Uncertainty

On the second day, we bring together some of the research emerging to support decision making under uncertainty or in complex systems. In this brief taster, we quickly introduce several key approaches and outline the objectives and goals of tomorrow's workshop.

16:00 – 18:00 Drinks Reception

May 24, 2018: Decision Making Under Uncertainty

10:00 – 11:00 Dealing with Uncertainty

Following on from yesterday's focus on metrics, we move today into the domain of uncertainty. When decisions must be taken without the benefit of the kind of certainty or clarity that metrics might provide, there are a whole set of different assumptions and approaches that come into play. This morning we have a number of presentations that will briefly introduce some of the emerging work in this space including:

- **Madeline Carr (RISCS):** There are a number of innovations for dealing with uncertainty that are emerging from the policy community including the World Economic Forum's work on Agile Governance as well as regulatory sandpits. While these may not be fully evolved at this stage, they point to a kind of iterative policy making that leaves scope to accommodate change or address decisions that later prove to be less than ideal.
- **Helen L (NCSC):** Helen will give an outline of some of the techniques that the NCSC has researched around orienting in problem space and complex problem solving. She will also provide an overview of the Cynefin Framework which highlights some of the risks of treating complex problems simply.
- **David Tuckett (CRUISSE):** Challenging Radical Uncertainty in Science, Society and the Environment is a network established to bring academics from disciplines in mathematical, physical, psychological, social and other sciences together to better understand and help practitioners who are making difficult decisions. David will introduce some the emerging thinking on this with a view to applying it to cyber security decision making.

11:00 – 11:30 Morning tea

11:30 – 13:00 Interactive Workshop: Uncertainty and Complexity in the Internet of Things

Drawing on our multi-disciplinary community as well as a range of invited policy and industry guests, we will be facilitating a workshop to help push thinking about a problem emanating from the Internet of Things. In order to help us engage with the work on complexity and uncertainty explained in the previous session, we will look at 'smart families' and their use of IoT circa five years into the future. The format of the session will enable people to explore their own uncertainties as representatives of their discipline or sector, as individuals who relate to the concept of family, and as contributors to multi-disciplinary research. Near term, medium term and long term uncertainty will be explored.

The outcomes of this workshop will be:

- A familiarisation with emerging thinking on uncertainty/complexity that may be useful in research into cyber security problems.
- Insight into some of the concerns about the IoT that emerge from different disciplines and sectors.

13:00 – 14:00 Lunch

14:00 – 15:30 Interactive Workshop continued...

October 18, 2018: Incentives and Impact

This Community Meeting extends the work we did together in May this year where we looked at a couple of themes; how to quantify cyber security (and some of the problems with doing that) and then, when meaningful metrics are not available, how those involved in decision making under deep uncertainty can best be supported.

This Meeting focuses on two themes: 'Incentives in Cyber Security' and 'Realising impact from research'. In the morning, we'll explore the spectrum of levers that are available to influence better cyber security behaviours. We'll discuss what has already been done and what research opportunities exist.

The afternoon session will continue the conversations at the Research Institutes Conference the day before about how impact from the academic research across all four Research Institutes can be most effectively delivered back to the stakeholder community. We'll collaboratively discuss what we can put in place in RISCS to promote this in 2019.

Morning Theme: Incentives

As part of the National Cyber Security Strategy the Government is committed to ensuring that the UK has the right regulatory framework in place for cyber security across the wider economy. To help inform this we need to understand the spectrum of incentives and interventions available and their wider impact on our economy and society. All whilst sitting against the backdrop of a constantly evolving technology and cyber security landscape.

The options and opportunities for potential incentives and their socioeconomic impact will form the centre of our discussions this morning, as we seek to understand what has been done already and what is yet to understand. RISCS brings cyber security experts across government, industry and academia alongside experts from wider fields across social science to explore this complex space further and discuss what research could support this national level objective.

09:30 – 09:40 Welcome & Introduction (Dr Madeline Carr, Director of RISCS)

09:40 – 10:00 DCMS Regulation & Incentives Review (Emma Green, DCMS)

10:00 – 11:10 'Innovation in the Spectrum of Incentives' invited talks from:

- Market Design (Will Jones, Royal Holloway)
- Cyber Insurance - helping our customers manage their Cyber risk pre and post event (Gareth Wharton, Hiscox Insurance)
- Building your human firewall: Innovation in cyber security education and awareness (Vicki Gavin, Northview Group)

11.10 – 11.25 Tea and Coffee

11.25 – 11.30 Open IoT Assessment Tool (Mark Simpkins)

11:30 – 12:30 Panel discussion: (Helen L, Chair) What has been done already in terms of incentives and what is left to understand?

This panel builds on the morning session to look at:

- The mechanisms that have been implemented and relied upon in the past
- How effective existing incentives have been
- What kind of innovation in incentives holds most promise

Panellists:

- Rob Carolina, Royal Holloway, University of London
- Jonathan Cave, University of Warwick
- Pam Briggs, Northumberland University
- Evie Monnington-Taylor, Behavioural Insights Team

12:30 – 13:15 Lunch

Afternoon Theme: Realising impact from our academic research

Seeing our research findings implemented in the real world can be very satisfying for researchers. But it is not always clear how to disseminate our work to best effect. While we recognize that academic journal articles or conference papers don't necessarily resonate with the policy community or industry, what actually are the channels through which we can best reach them? This session will bring in reflections from the Research Institutes Conference the previous day and build on them through a dialogue between academics and the policy community.

13:15 – 13:30 Introduction (Madeline Carr)

13:30 – 13:45 Keynote: The view from NCSC Comms Team: (Senior NCSC Speaker)

13:30 – 14:50 Panel discussion: What is Impact? (Madeline Carr, Chair)

Panellists:

- Sarah Foster, DCMS
- Helen L, Technical Director Sociotechnical Security Group, NCSC
- Senior NCSC Speaker
- Professor. Lizzie Coles-Kemp, RISCS Deputy Director

14:45 – 15:00 Tea and coffee

15:00 – 15:50 Facilitated workshop: Reaching stakeholders through research

15:50 – 16:00 Wrap up and next steps (Madeline Carr)