RISCS

# Annual Report 2017

# Annual Report 2017

Research Institute in Science of Cyber Security | Department of Computer Science

University College London | Gower Street | London | WC1E 6BT

## Research Institute in Science of Cyber Security

Advisory Board Members:

Alex Ashby, Controlesc.com
Kerry Bell, Dstl
Lizzie Coles-Kemp, Royal Holloway, University of London
Peter Davies, Thales
Chris Hankin, Imperial College London
Larry Hirst, formerly of IBM
Shari Lawrence Pfleeger, I3P
Aad van Moorsel, Newcastle University
Geraint Price, Royal Holloway, University of London
Martin Sadler, HP Labs
Adam Shostack, Shostack & Associates

Participating Universities:

This Annual Report and the preceding 2013, 2014 and 2015 Annual Reports may be downloaded from the RISCS website at www.riscs.org.uk

# Introduction

As Director of RISCS, am pleased to report that our Phase 2 has steamed ahead in 2017: we have an impressive portfolio of research projects and community, funded by the National Cyber Security Centre (NCSC) and the Engineering and Physical Science Research Council (EPSRC), and a growing community of engaged researchers and practitioners driving cyber security research and practice forward.

At the start of Phase 2 in 2016 the EPSRC TIPS project Detecting and Preventing Mass Market Fraud (DAPM), lead by Prof. Monica Whitty from the University of Warwick joined. DAPM has already published several highly regarded studies on both victims and perpetrators of fraud, and engaged with industry and law enforcement to develop effective strategies for detecting and preventing fraud. In 2017, six projects funded by the EPSRC Human Dimensions of Security call have joined RISCS:

- EMPHASIS: EconoMical, PsycHologicAl and Societal Impact of RanSomware, led by Prof. Eerke Boiten at De Montfort University
- ACCEPT: Addressing Cybersecurity and Cybercrime via a co-Evolutionary aPproach to reducing human-relaTed risks, led by Prof. Shujun Li at the University of Kent
- cSaLSA: Cyber-Security across the Life Span led by Prof. Adam Joinson from Bath University
- Leveraging the Multi-Stakeholder Nature of Cyber Security, led by Dr Christian Wagner at Nottingham University
- Why Johnny Doesn't Write Secure Software, led by Prof. Awais Rashid at Lancaster (who will be moving to Bristol in 2018)
- Evaluating Cyber Security Evidence for Policy Advice: the other human dimension, led by Prof. Madeline Carr at Cardiff University

We are also honoured that two eminent researchers who have been part of the RISCS community from the start have decided to associate major fellowships they have won with RISCS. Prof. Lizzie Coles-Kemp from RHUL – who is also the Deputy Director of RISCS - was awarded an EPSRC TIPS Fellowship to study ***Everyday Safety-Security for Everyday Services***. A digital economy and society needs empowered consumers and citizens. Lizzie's pioneering research has shown that their needs, values and preferences have hitherto not been represented as part of cyber security goals, and developed methods for eliciting and representing these in tools that security practitioners can employ. Dr Thomas Gross from Newcastle University won a highly competitive European Research Council (ERC) starting grant for his project CASCAde *Confidentiality-Preserving Security Assurance*, and shown great leadership in developing a new strand on improving experimental methods and results for security experiments.

The first major project funded by the NCSC as part of RISCS-2 – ***Motivating Jenny to Write Secure Software***, led by Prof. Helen Sharp from the Open University, was awarded after an open call that was developed on the basis of a RISCS workshop with leading UK and international researchers and practitioners on secure software development. The researchers of the 'Johnny' and 'Jenny' projects, together with other interested researchers and practitioners from the NCSC and industry, have now formed a sub-community to share methods and results so we can rapidly identify support for developers and organisational changes that will make software development more robust.

The engagement between researchers and practitioners is one of the key features of the RISCS community – it is the input of, and feedback from practitioners which helps us to conduct quality research with immediate benefits. Members of the RISCS Practitioner Panel, chaired by Dr Geraint Price from RHUL, shaped both the call for the developer-centred security project and our forthcoming project call on information and metrics 'Supporting the Board' in making better decisions about cyber security. This is a topic that has been core to the RISCS mission from the start, but has received a significant new steer and impetus through our work with the PP.

In 2017, the NCSC funding also supported 11 Small Grants projects to that enabled RISCS researchers to explore emerging cyber security challenges and promising avenues, with topics ranging from smart buildings and smart home security to security advice for small businesses and consumers buying a new computer. The results of those grants produced many surprises and insights for new investigations, and I highly recommend them for identifying new topics you might like to engage on, or indeed provide funding for.

**Professor M. Angela Sasse**

Director

Research Institute in Science of Cyber Security

# DAPM: Detecting and Preventing Mass-Marketing Fraud

This interdisciplinary project has made some progress in the last year in attempting to understand why individuals are taken in and tricked out of money from mass-marketing fraudsters, the stages involved in these scams, who is more likely to be scammed and methods to detect these scams. Some of our studies are detailed below:

**Surveyed victims of MMFs:** We carried out a survey of 1000s of victims of MMF victims (one-off and repeat victims) and non-victims to learn more about susceptibility to cyber-fraud victimhood. This research found that some demographic details and psychological dispositions (e.g., impulsivity, addictive measures), online risky routine behaviours (e.g., shopping, banking) predicted victimhood. What was a surprising result of this research was that those who sought out information online to protect themselves from cyber attacks were more likely to be scammed and more likely to become repeat victims.

**Interviewed victims of MMFs:** We have interviewed about 40 victims in the last year to learn more about why they were scammed and the persuasive strategies employed by criminals to trick victims, differences and similarities in the typologies of cyberscams, victims' understanding of cyber security and changes, if any, in victims' cyber security practices subsequent to the scam. These interviews have helped us map out different types of scams and discover more about how criminals trick victims. We have learnt more about the stages involved in the scams. Moreover, we have learnt about the gaps in victims' knowledge of cyber security and continued vulnerabilities after being scammed. We have elucidated that some advice is neither helpful nor preventative. We have disseminated these findings to government organisations in the UK and Australia and made suggestions on how they might support victims after they have been scammed to help prevent future victimisation.

**Interviewed near-victims of MMFs:** We have interviewed about 5 near victims of MMF to learn how they managed to notice and resist becoming scammed. Moreover, we have examined whether these 'near victims' are likely to be victims in the future or whether they have adequate knowledge and protections to prevent becoming victims.

**Analysis of emails written between victims and criminals:** We have conducted grounded theory analysis on communications between victims and criminals to gain more in-depth insights into the trusting relationships developed by scammers, their techniques used at different points in the scams (e.g., authority, trust, love, a sense of urgency etc.). These psychological examinations have informed the computer scientists who will seek out further evidence to support these psychological theories via machine learning, deep learning and linguistic analysis.

**Experiments to improve manual detection:** We have also run psychological experiments to improve human detection of scams. Instructions were developed based on insights provided by the computer scientists as well as the psychological findings. Although we are still in the midst of running these studies we have found that our own interventions have been successful at improving human detection.

**Experiments to improve detection via data analysis:** We have analysed publicly available data from scam-baiters (people who knowingly respond to scam emails, engaging with the fraudster to waste their time and inconvenience them). Based on textual content, a system was designed which can accurately separate advance fee email conversations from regular professional and personal emails. In addition, the system can identify both the fraudster and the potential victim with a high level of accuracy based on their exchanges. The scam-baiter text was also analysed using linguistic markers to develop a model of the different persuasive strategies and stages used by scammers-solicitation, formal extraction, irritation, personal appeal and abandonment.

Computer Scientists on the project are examining data from a wide variety of fake and real online dating profiles, looking at information including marital status, ethnicity, occupation, age and profile pictures. In conjunction, a linguist is looking at the language that is used, descriptions, sentence structure and word patterns. This multi-disciplinary approach has allowed the team to produce a tool which is very effective at detecting scam dating profiles.

**Engaging with other organisations:** Throughout the project, we have been working with relevant organisations to understand the problems in their areas and disseminating our findings with an aim to reducing the incidence of MMF. This has included Gumtree, online dating sites, Action Fraud and the London Mayor's Office. Partners on this project include ACCC (Australian Competition and Consumer Commission), Barclays, CIFAS, City of London Police, Action Fraud, Federal Trade Commission, Fraud Help Desk (Netherlands), Fraud Women's Network, Southampton City Council, Royal Canadian Mounted Police, Scamalytics and Western Australian Police.

Updates of our latest findings can be found on our webpage: http://www2.warwick.ac.uk/fac/sci/wmg/research/csc/research/dapm/

## Related Activity

Sorell, T, and Whitty, M. T. (June, 2017). Victim-Offenders in Scams. *Joint paper presented at a conference on cybercrime held at Nuffield College, Oxford.*

Whitty, M. T. (June, 2017). Detecting and Preventing Mass-Marketing Fraud & the UNDERWARE workshop. *RISCS Community Meeting*

Whitty, M. T. (July, 2017). Detecting and preventing mass-marketing fraud: An interdisciplinary approach. *International Conference on Cybercrime and Computer Forensics, Queensland, Australia, July 17 – July 18,* 2017.

## Publications

Whitty, M.T., Edwards, M., Levi, M., Peersman, C., Rashid, A., Sasse, A., Sorell, T., & Stringhini, G. (2017). *Ethical and social challenges with developing autonomous agents to detect and warn potential victims of Mass-marketing fraud* (MMF). 26th World

Wide Web, 2017, Cybersafety2017: 2nd International Workshop on Computational Methods in CyberSafety. (Accepted 9/2/16).

Whitty, M. T. (in press). Do you Love Me? Psychological characteristics of romance scam victims. *Cyberpsychology, Behavior, and Social Networking*

Whitty, M. T. (September, 2017). Cyberpsychology. *Keynote at 8th Annual Psychology Postgraduate Conference, Queen's University, Belfast.*

## Grant Details

**EPSRC Reference:** EP/N028112/1

**Title:**
DAPM: Detecting and Preventing Mass-Marketing Fraud (MMF)

**Principal Investigator:**

Whitty, Professor M *(University of Warwick)*

**Other Investigators:**

Rashid, Professor A *(Lancaster University)*
Levi, Professor M *(Cardiff University)*
Sasse, Professor MA *(University College London)*
Sorell, Professor T *(University of Warwick)*
Stringhini, Dr G *(University College London)*

**Research Associates:**

Briazu, R *(University of Plymouth)*
Edwards, M *(Lancaster University)*
Mudhar, JK *(University of Warwick)*
Peersman, Dr C *(Lancaster University)*
Suarez de Tangil, Dr G *(University College London)*

**Project Management:**
Bailey, J *(Project Manager)*
Sherliker, B *(Project Co-ordinator)*

# Cyber-Security across the Life Span (cSaLSA)

Part of Adam Joinson's work focuses on what "cyber security" actually means to both lay people and experts. A professor of information systems at the University of Bath, Joinson's newest project is cSALSA: Cyber Security Across the Life Span. Launched in April 2017, the three-year project has a long list of partners, primarily behavioural and cognitive psychologists, plus one computer scientist. Among the project's partners are Pam Briggs (Northumbria University); Debi Ashenden (University of Portsmouth and the Centre for Research and Evidence on Security Threats); Darren Lawrence (Cranfield University); and researchers at Pacific Northwestern Labs, Carleton University, BAe Systems, and others.

The goal of the project is to take a lifespan approach to understanding how cyber security is understood and how that relates to risk and behaviour. There are many reasons for pursuing this approach. First, prior work supports the idea that there are unique security challenges at different life stages. Briggs's early work suggests a U-shaped curve of vulnerability, with the oldest and youngest as most vulnerable to particular types of threat. Many other changes also occur during a lifetime: the resources people must draw on change as family, friends, work colleagues, and the power structures within these relationships shift over time. Power systems in particular can be quite important; the 21st century has seen the rise of the teen guru who knows the passwords for the family router. In addition, goals change throughout life as people aspire to and then achieve independence, stability, family, and security. These changing states also play a part in determining how individuals interact with technology products.

So, the cSALSA project seeks to study questions such as how these factors intertwine and interact and determine individuals' responses. What protective steps do they take to understand risk? How do individuals deal with large-scale social and technological change? Age is not the only factor; cohort is also significant in determining an individual's social networks, families, cognitive ability, technical understanding, and skills. Individuals also vary according to the vulnerabilities that are available for attackers to exploit.

The model the researchers are developing to be shared among all the partners draws on approaches used for diseases to express individuals' varying levels of exposure, which help to determine how they respond: whether they avoid thinking about it, seek as much information as they can find about it, or adapt to the changing situation. Each of these responses leads to a different outcome.

There are three main strands the project seeks to pull together over the course of its three years. One, define cyber security in everyday language; two, develop the results of year one into a dictionary for testing how different groups of people talk about cyber security; and three, create metrics from a series of interactions to study how to measure risk in cyber security tools, using the understanding gained from the first two years.

Currently, the researchers are working on definitions. Classical definitions pose the problem of having sharp boundaries. They define elements that are necessary and sufficient; then everything that has those elements fits in the definition and everything lacks one or more of those elements is excluded.

But "cyber security" may include vastly different phenomena: hacktivism, cyber crime, cyber terrorism, and cyber warfare all fit within that one term. In addition, risk, by its nature, is fuzzy: we speak of degrees of risk, just as we speak of degrees of security or protection. More fuzzy definitions and, especially, boundaries are needed to capture this. Cognitive psychologists have prototyped approaches that attempt to capture the degree by which something is or is not included. In this approach, exemplars are found for a superordinate category, some of which may be better than others – we might see a robin as a better exemplar of the superordinate "bird" than a penguin. For cyber security, exemplars might be information protection, with an opposing example of identity fraud or loss of bank card details.

Among the possible applications of this work are contributions to theory creating links between security and privacy; the development of a dictionary that can be used to analyse discussions; improvements to the design of awareness and training materials; improvements to the design of security products and features; and the development of workplace metrics and measures.

## Grant Details

**EPSRC References:** EP/P011454/1
EP/P011667/1
EP/P011446/1

**Title:**

Cyber-Security across the Life Span (cSaLSA)

**Principal Investigators:**

Joinson, Professor A *(University of Bath)*
Ashenden, Professor D *(University of Portsmouth)*
Briggs, Professor P *(University of Northumbria)*

**Other Investigators**:

Coventry, Professor L *(University of Northumbria)*
Jones, Dr S L *(University of Bath)*
Lawrence, Mr D *(Cranfield University)*

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

Researchers and practitioners have acknowledged human-related risks among the most important factors in cybersecurity, e.g. an IBM report (2014) shows that over 95% of security incidents involved "human errors". Responses to human-related cyber risks remain undermined by a conceptual problem: the mind-set associated with the term 'cyber'-crime which has persuaded us that that crimes with a cyber-dimension occur purely within a (non-physical) 'cyber' space, and that these constitute wholly new forms of offending, divorced from the human/social components of traditional (physical) crime landscapes. In this context, the unprecedented linking of individuals and technologies into global social-physical networks - hyperconnection - has generated exponential complexity and unpredictability of vulnerabilities.

In addition to hyperconnectivity, the dynamic evolving nature of cyber systems is equally important. Cyber systems change far faster than biological/material cultures, and criminal behaviour and techniques evolve in relation to the changing nature of opportunities centering on target assets, tools and weapons, routine activities, business models, etc. Studying networks and relationships between individuals, businesses and organisations in a hyperconnected environment requires understanding of communities and the broader ecosystems. This complex, non-linear process can lead to co-evolution in the medium-longer term.

The focus on cybersecurity as a dynamic interaction between humans and socio-technic elements within a risk ecosystem raises implementation issues, e.g. how to mobilise diverse players to support security. Conventionally they are considered under 'raising awareness', and many initiatives have been rolled out. However, activities targeting society as a whole have limitations, e.g. the lack of personalisation, which makes them less effective in influencing human behaviours.

While there is isolated research across these areas, there is no holistic framework combining all these theoretical concepts (co-evolution, opportunity management, behavioural and business models, ad-hoc technological research on cyber risks and cybercrime) to allow a more comprehensive understanding of human-related risks within cybersecurity ecosystems and to design more effective approaches for engaging individuals and organisations to reduce such risks.

The project's overall aim is therefore 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. To achieve the project's overall aim, this research will:

- Be theory-informed: Incorporate theoretical concepts from social, evolutionary and behavioural sciences which provide insights into the co-evolutionary aspect of cybersecurity/cybercrime ecosystems.
- Be evidence-based: Draw on extensive real-world data from different sources on behaviours of individuals and organisations within cybersecurity/cybercrime ecosystems.
- Be user-centric: Develop a framework that can provide practical guidance to system designers on how to engage individual end users and organisations for reducing human-related cyber risks.
- Be real world-facing: Conduct user studies in real-world use cases to validate the framework's effectiveness.

The new framework and solutions it identifies will contribute towards enhanced safety online for many different kinds of users, whether these are from government, industry, the research community or the general public.

This project will involve a group of researchers working in 5 academic disciplines (Computer Science, Crime Science, Business, Engineering, Behavioural Science) at 4 UK research institutes, and be supported by an Advisory Board with 12 international/UK researchers and a Stakeholder Group formed by 12 non-academic partners (including LEAs, NGOs and industry).

**The main objectives of the project include:**

1. To develop a more comprehensive understanding of the key (co-) evolutionary trajectories of human behaviours in cybersecurity and cybercrime ecosystems.
2. To compile a knowledge base including evidential and theoretical information to assist solution designers and crime preventers to out-innovate adaptive cybersecurity offenders.
3. To develop a cybercrime ontology with an internally-consistent glossary that can make the cybercrime knowledge base machine readable for automated processing.
4. To produce a practical framework for reducing human-related cyber risks, which incorporates theoretical concepts and needed software tools for better user engagement via personalisation and contextualisation.
5. To validate the developed framework in selected real-world use cases.

**Use cases:**

**Use Case 1) Human-related cyber risks within global transaction and exchange networks.**

Example scenarios in this use case include transactions involving: (traditional) currencies – specifically the use of money mules for online banking attacks and reshipping mules for online credit card frauds; virtual currencies – specifically bit-coin and block-chain based frauds; objects – specifically trade of stolen or fake goods (e.g. vehicles and diamonds).

**Use Case 2) Human-related cyber risks within hybrid transportation networks.**

Examples include organised crime (e.g. theft) of connected vehicles, cyber attacks on rail infrastructures, pirates collecting intelligence on ships in order to plan physical attacks, etc. This can be built on TRL's extensive research work in the transportation sector, the project team's previous work in a recently-complete project POLARBEAR (led by the project PI Li) and an ongoing project EP/N028295/1 (led by the project CI Treharne).

The use cases will be focused in Year 2 of the project, and in the first year the project will study more scenarios to decide what use

cases should be selected. Input from the project's Stakeholders Group and Advisory Board will be sought for the final choices. The project also welcomes wider stakeholders and the general public to inform us about the most important use cases the project should choose. **Expected deliverables:**

A socio-technical framework combining both theoretical concepts and technical tools to facilitate better understanding of human behaviours in cyber security and cybercrime context, sufficiently adaptable to accommodate future developments

- A structured knowledge base of evolution of cybercrime and human-related risk
- A cyber risk and cybercrime ontology (and an internally-consistent glossary derived from this), and a machine-readable knowledge database with related tools which allow automatic knowledge visualisation
- Various tools for handling different data sources to capture information for the knowledge base
- Various tools for supporting risk management and personalised/contextualised cyber risk communications to individuals
- A set of typical cyber risk and cybercrime use cases and scenarios where human behaviours play a key role, with possible intervention points, and accounts of the wider implementation process to realise those interventions in practical terms, including mobilisation and partnership issues
- Various indicators (metrics and qualitative analysis) of findings out of two focused real-world use cases to which the above framework and tools are applied
- Research papers summarising our work and research findings
- A public-facing document with recommendations for future actions of all stakeholders including suggestions and insights for business managers, policy makers and law makers to adjust their strategy towards crime prevention and victimisation reduction in the medium-to-long term.

## Grant Details

**EPSRC Reference:** EP/P011896/1

**Title:**
ACCEPT: Addressing Cybersecurity and Cybercrime via a co-Evolutionary aPproach to reducing human-relaTed risks

**Principal Investigator:**
Li, Dr S *(University of Surrey)*

**Other Investigators:**
Borrion, Dr H *(University College London)*
McGuire, Dr M *(University of Surrey)*
Maull, Professor R *(University of Surrey)*
Ng, Professor ICL *(University of Warwick)*
Pogrebna, Dr G *(University of Birmingham)*
Stevens, Professor A *(Transport Research Laboratory Limited)*
Stringhini, Dr G *(University College London)*
Treharne, Dr H E *(University of Surrey)*

# Leveraging the Multi-Stakeholder Nature of Cyber Security

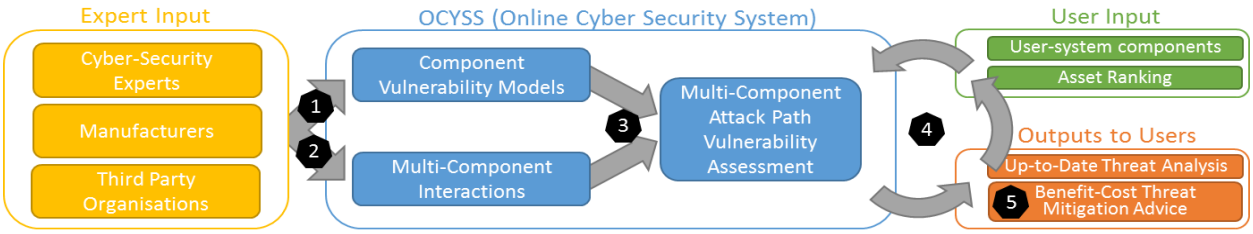



*Fig. 1 Structure of the OCYSS framework, highlighting de-coupling and integration of multi-stakeholder insight and information.*

The project brings together researchers from the Lab for Uncertainty in Data and Decision Making (LUCID) at the University of Nottingham, UK and Carnegie Mellon University, USA, with domain experts from the NCSC to build on initial work in the area of system vulnerability assessments by cyber security experts in order to develop the basis for a rapid, adaptive, vulnerability assessment platform.

Cyber Security (CyS) is a distributed, multi-stakeholder problem. It is distributed because the expertise to comprehensively assess the level of security of a given IT system is commonly not all available in one location, e.g. the IT system component detail is available within a company, while detail on operating system software vulnerability may be available to the OS manufacturer and further expert insight may be available to public security agencies, such as CESG. It is a multi-stakeholder problem because a number of human stakeholders, from IT designers to users with varying levels of expertise, need to effectively communicate and work together in order to deliver systems with an appropriate level of CyS assurance.

This 'Leveraging the Multi-Stakeholder Nature of Cyber Security' project is designed to enable leveraging the distributed, multiple human stakeholder nature of CyS by developing a novel framework with the necessary scientific underpinning to improve stakeholder access to knowledge operationalised as a data-driven Online CYber Security decision support System (OCYSS). Fig. 1 captures the structure of the eventual framework, highlighting the role of OCYSS to effectively integrate expert and user inputs, capturing individual component vulnerabilities as well as vulnerabilities arising from the interaction/combination of individual components, to efficiently deliver appropriate, user-tailored, balanced, informed and up-to-date threat analysis and decision support to users.

A key strength of the OCYSS framework is the decoupled data gathering combined with strong data integration. By efficiently making use of available CyS expertise, the approach is designed to directly address an acute shortage of highly qualified CyS experts by both small-to-large scale users from government to industry. To enable this approach the project addresses the following scientific challenges (numbered in Fig. 1):

1. Comprehensive, efficient and continuous rating and modelling of component vulnerabilities.
2. Capture of multi-component interactions and dependency information.
3. 'Lossless' integration of individual component vulnerability models with multi-component interaction information to deliver comprehensive attack path vulnerability assessments with quantified uncertainty.
4. Meaningful communication of CyS assessment and analyses outputs to users to enable them to make informed mitigation and security investment decisions. This includes the communication of vulnerability levels of user-specific component sets and attack paths.
5. Enabling detailed user asset-value rating and associated cost-benefit analysis of threats and appropriate mitigation prioritisation, i.e. providing decision support on whether/where to invest or improve security levels based on asset-at-risk value; in particular when uncertainty is high.

## Progress in the Year to Date

While the 'Leveraging the Multi-Stakeholder Nature of Cyber Security' project's recruitment has been delayed and is expected to complete in autumn 2017, after which the project will have run for three years, substantial progress has been made, in particular on the techniques for comprehensive vulnerability capture and integration of resulting data.

We have developed paper-based prototypes of interval-valued questionnaires which enable the richer capture of vulnerability levels in comparison to ordinal scales (e.g., as in Likert scales). Focussing on the very different application context of manufacturing, the paper based questionnaires have been used in multiple trials to capture complex information (such as the perceived flavour of juice) from series of consumers. The resulting interval-valued data has been modelled using a recently developed Interval-Agreement-Approach, capturing the agreement across sources (participants) and minimising data-loss and assumptions. Finally, the models were then shown to provide a useful and effective basis for reasoning.

Beyond the research, an international workshop with approximately thirty experts on computational intelligence, data fusion and uncertain data processing was held in Rothley, UK, in July 2017. The workshop focussed on the identification of both academic/theory-led priorities in the domain, and on the opportunities in addressing urgent, real-world challenges in cyber security.

## Related Activities

- LUCID Workshop with thirty international computational intelligence experts on handling uncertainty and challenges in Cyber Security.
- Open source software development for the efficient and effective capture of vulnerability assessments including associated uncertainty.

## Publications


- H. Hibshi, T. D. Breaux and C. Wagner, *"Improving security requirements adequacy*," 2016 IEEE Symposium Series on Computational Intelligence (SSCI), Athens, 2016, pp. 1-8.
- S. Miller, C. Wagner, U. Aickelin, J. M. Garibaldi, *"Modelling cyber-security experts' decision making processes using aggregation operators,"* Computers & Security, Vol. 62, 2016, pp. 229-245.


## Grant Details

**EPSRC Reference:** EP/P011918/1

**Title:**

Leveraging the Multi-Stakeholder Nature of Cyber Security

**Principal Investigator:**

Wagner, Professor C *(University of Nottingham)*

**Other Investigators:**

Garibaldi, Proessor JM *(University of Nottingham)*
McAuley, Professor D *(University of Nottingham)*

# Evaluating Cyber Security Evidence for Policy Advice

The ECSEPA project seeks to provide support for cyber security policy makers in the UK, specifically those civil servants who provide short and long 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 goes well beyond their own organisations 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.

Specifically, ECSEPA sets out to examine how policy staff, often in time-critical scenarios, are asked to assess evidence from a mix of sources including official threat intelligence, academic sources, and industry threat reports. They draw upon this diverse evidence base to make judgments on threat, risk, mitigation and consequences, and offer advice shaping the national regulatory landscape, foreign and domestic security policy, and a range of public and private sector initiatives. But the assessment of evidence is a particularl problem in this policy context.

Some evidence can be contradictory and it can also potentially carry within it particular agendas or goals that may raise questions for policy advisors about its rigour and reliability. The 'politicisation' of cyber security evidence is increasingly problematic as states sometimes privilege threat intelligence from sources located within their sovereign borders rather than based on the quality of the research they produce.

In addition, it has proven extremely difficult to conclusively attribute cyber attacks and to quantify the cost of cyber insecurity. This lack of certainty means that evidence can only support policy makers' decisions and evaluation of cyber security risks, threats and consequences to an extent.

And finally, the landscape of cyber security is developing rapidly and spans many issue areas including national security, human rights, commercial concerns, and related infrastructure vulnerabilities. Consequently, policy staff must work to balance a range of sometimes conflicting interests that compete for attention and they must do so in a field with little precedent to draw upon.

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

This project was designed in close collaboration with colleagues in the UK cyber security policy community, especially the NCSC and the Foreign Commonwealth Office. In recognition of the diverse and complex factors at play in this research, we've brought together a multi-disciplinary team that includes Madeline Carr, Associate Professor of International Relations and Cyber Security (UCL), Siraj Ahmed Shaikh, Professor of Systems Security (Coventry), Alex Chung (PhD Law, Oxford) and Emma Moreton (PhD Corpus Linguistics, Birmingham).

## Progress to date

ECSEPA is in early stages – it began on June 1 this year. Our first few months have been taken up with desk based research and literature reviews. We have also started on a mapping exercise in order to produce an infographic of where cyber security policy making is situated across HMG. In addition, we have begun some linguistic analysis of threat reports and policy documents so that we can better understand the kind of language and terminology that impact on how policy staff evaluate evidence.

Over the last quarter of 2017, our intention is to interview people who work on UK cyber security policy to better understand exactly which evidence they draw upon and how they privilege it, what *they* think of that evidence in terms of its usability and reliability, and what problems they see in their evaluation of cyber security evidence.

In 2018, we will draw upon the outcomes of this research as well as the expertise of colleagues in the Berkeley Center for Long-Term Cybersecurity to design a 'cyber policy crisis game'. This will allow us to simulate the evidence evaluation process and we will be inviting interested UK cyber security policy staff to participate. An analysis of the game will provide data on a range of factors including which evidence is most useful, which background knowledge (level of technical literacy etc) is most useful, and significantly, how UK policy staff can be better supported in their roles.

## Grant Details

**EPSRC Reference:** EP/P011691/1
EP/P01156X/1

**Title:**

Evaluating Cyber Security Evidence for Policy Advice

**Principal Investigator:**

Carr, Dr M *(Cardiff University)*
Shaikh, Professor S *(Coventry University)*

**Other Investigators:**

Chung, Dr A *(Oxford University)*
Moreton, Dr E *(Birmingham University)*

# Why Johnny Doesn't Write Secure Software

The aim of the three-year EPSRC-funded Why Johnny Doesn't Write Secure Software project, which began in April 2017, Awais Rashid (Lancaster University) explained to the June 2017 RISCS meeting, is to develop an empirically grounded theory of secure software development by the masses. The project's collaborators include others at Lancaster University: Charles Weir, John Towse, and newcomer Dirk van Linden. From elsewhere, it includes Pauline Anthonysamy (Google Switzerland); Bashar Nuseibeh, Marian Petre, and Thein Tun (Open University); Mark Levine (Exeter); Mira Mezini (ITU Darmstadt), Elisa Bertino (Purdue); Brian Fitzgerald (Lero); Jim Herbsleb (Carnegie Mellon); Shinichi Honiden (National Institute of Informatics, Japan). This project has close links to the complementary Motivating Jenny to Write Secure Software project.

The last decade has seen a massive democratisation of how software is developed. In the early days of the software industry, a would-be programmer would pursue a university degree, learn software development, and then work in a software house. With recent developments such as the Arduino, the Raspberry Pi, mobile phone apps, and the Internet of Things, virtually anyone may become a developer writing software that is then deployed to people around the world. "Johnny" may be working in a software house or may equally be working in their own time from their living room on software that comes into contact with amyriad other systems around the world on a regular basis. How does that person think about security? What decisions do they make, and what drives them? This project will study a range of software in apps and devices that captures the range of "Johnnies" actually engaged in writing software in today's world.

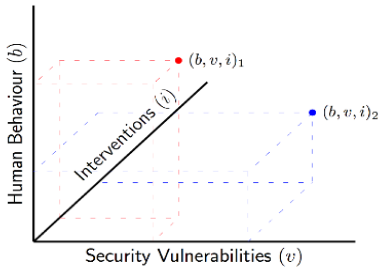
The project seeks to answer three main questions:

What typical classes of security vulnerabilities arise from developers' mistakes?

Why do these mistakes occur? Are the APIs so complicated to use that they produce mistakes, as suggested by recent work from Darmstadt. Are there other factors, such as their own misconceptions about security and how the software they write is supposed to handle it?

How may we mitigate these issues and promote secure behaviours?

The project's first objective is to characterise developers' approach to producing secure software by examining the artefacts produced and eliciting the developers' awareness, attitudes, and assumptions about security. Do they think it is someone else's job? Do they care about security? Rashid suspects the project team will find a range of responses: some will care, some won't; some will fail because the tools they are given make it hard to do secure programming. All of this will make it possible to determine how developers' assumptions, behaviours, and awareness relate to the mistakes that appear in their software.




*Schematic rendering of three degrees of secure software development: developers' personal characteristics; those characteristics' associated vulnerabilities in software; and the degrees of intervention to mitigate against them.*

Next, the project will investigate the factors that affect developers' security behaviours. The researchers seek to understand not only what their security design strategies are, but also to mitigate their biases and accommodate constraints such as pressure to meet market deadlines. Many apps have very short lifetimes; these are constraints that need to be understood. Based on this work, the project hopes to develop and evaluate a range of cost-effective interventions for steering developers away from poor security design decisions, taking into account both the kinds of vulnerabilities to be avoided and the types of behaviour to be discouraged.

Earlier work studying developers' approach to error detection and recovery by Tamara Lopez and Marian Petre (Open University) ethnographic analysis of how developers work found three main stages of error detection and recovery. First: detect that something has gone wrong. Second: identify what's wrong. Third: Undo the effects. In this context, errors can be beneficial because they show something has gone wrong.

With James Noble (Victoria University), Weir and Rashid have carried out complementary work to understand how developers learn about security and what encourages good security behaviour. This research found a pattern in the many interviews conducted with experienced people in industrial secure software development: challenges to what developers do encouraged them to engage with security. These challenges come from many directions: automated testing tools; pentesters and security experts; product managers; feedback from end users; the team's own brainstorming sessions; and discussions with other development teams. All of these help developers think more about security and how to embed it in software.

The project hopes to build on this prior work as well as a small grant recently completed by Weir studying effective ways to intervene. Developers, Rashid concluded, do need our help. The project is eager to engage with others, receive critical feedback, and populate the space. Those interested can contact the project at contact@writingsecuresoftware.org.

## Grant Details

**EPSRC Reference:** EP/P011799/1

**Title:**

Why Johnny doesn't write secure software. Secure software development by the masses

**Principal Investigator:**

Rashid, Professor A *(Lancaster University)*

**Other Investigators:**

Levine, Professor M *(University of Exeter)*
Nuseibeh, Professor B *(The Open University)*
Petre, Professor M *(The Open University)*
Towse, Dr JN *(Lancaster University)*
Tun, Dr T *(The Open University)*

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

Surveys have shown that many real-world security vulnerabilities are related to a few classes of attack such as code injection. There are also good practices and technologies for detecting and preventing such vulnerabilities in code, such as input sanitisation and non-escaping strings. Yet, it is not clear why professional software developers do not always adopt these practices and technologies as a matter of course. This project examines the role of developer motivation in the production of secure code.

Motivation plays an important role in software development and it has a significant influence on project productivity and code quality. Successful developers are rarely motivated by reading documentation or studying manuals. Peer-to-peer interactions and assessments are more likely to bring about lasting cultural change within the developer community. This is evident in the widespread adoption of object-oriented technologies and agile development practices, for example. This project plans to focus on individual and group behaviours, examining how personal and social identities can be used to influence behaviour in self and in peers. Two specific aims of the project are:

A1. 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.

A2. Develop guidelines for creating and propagating a security culture across software teams.

In addressing these research aims, we will be engaging with the developer community in both online and off-line settings, using a range of methods including ethnographic and constrained task studies. For online studies, we will involve online communities such as StackExchange groups. For off-line studies, we will collaborate with a range of companies including members of Agile Business Consortium (ABC) Ltd and with international partners in Ireland, Brazil and Japan.

This is a joint project between The Open University and Exeter University, and is a sister project of the EPSRC-funded *Why Johnny doesn't write secure software? Secure Software Development by the masses.*

## Progress in the Year to Date

The project has just started in August 2017. We are currently consolidating the team's understanding of relevant literature, confirming developer collaborators, and conducting an initial detailed study of how motivation factors manifest in online discussion forums.

Updates of our latest progress are available on the project website motivatingjenny.org

## Publications


França, C. Sharp, H., & Da Silva, F. Q. (2014) *Motivated software engineers are engaged and focused, while satisfied ones are happy*. In ESEM: Proceedings of the 8th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (no. 32). ACM Press.

Sharp, H., Baddoo, N., Beecham, S., Hall, T. and Robinson, H.M. (2009) *Models of motivation in software engineering*. Information and Software Technology 51(1) (pp. 219-233).

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.

Lopez, T. (2016). *Error Detection and Recovery in Software Development*. PhD Thesis, the Open University.

Sach, R.J. (2013*) The Impact of Feedback on the Motivation of Software Engineers*. PhD Thesis, the Open University.

Sharp, H., Dittrich, Y. and deSouza, C. (2016) *The Role of Ethnographic Studies in Empirical Software Engineering*. IEEE Transactions on Software Engineering. 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.


## Related Activities

*Invited Talk*: Helen Sharp, Motivating Jenny to Write Secure Software: Community and Culture of Coding, RISCS Community Meeting, UCL, 22 June 2017

*Panel:* Helen Sharp and Bashar Nuseibeh, *Every little helps? Supporting the transition to secure software development processes,* RISCS Community Meeting, UCL, 22 June 2017

*Invited Talk:* Helen Sharp, Motivating Jenny to Write Secure Software: Community and Culture of Coding, ACE Nottingham, 29 June 2017

## Grant Details

**NCSC Reference:**

**Title:**

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

**Principal Investigator:**

Sharp, Professor H *(The Open University)*

**Other Investigators:**

Bandara, Professor A *(The Open University)*
Levine, Professor M *(University of Exeter)*
Lopez, Ms T *(The Open University)*
Nuseibeh, Professor B *(The Open University)*
Tun, Dr T *(The Open University)*

# Everyday Safety and Security – an EPSRC fellowship research programme

## By Lizzie Coles-Kemp, Professor of Information Security, Royal Holloway University of London

Phase Two of RISCS is home to a family of research projects and programmes that focus on the intersection between the individual and the digital. One of these research programmes is Everyday Safety and Security, funded under the EPSRC TIPS fellowship scheme and comprising a number of projects related to RISCS' main focus. The Research Fellow is Lizzie Coles-Kemp and she is supported by postdoctoral research fellow Claude Heath. She also works with collaborators Rikke Jensen (Royal Holloway University of London) and René Rydhof Hansen (University of Aalborg) on a project by project basis. Lizzie, Claude and Rikke are part of Royal Holloway's Information Security Group.

The focus of the Everyday Safety and Security 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. The research revisits and extends existing theories of security as it digs deeper into these relationships. It will go on to develop novel security techniques and mechanisms for use in the delivery of everyday essential digital services, such as digital health, welfare, housing and employment services. The first year of the fellowship has just been completed and there are four years remaining.

Lizzie has spent the first twelve months primarily working with refugee groups in Sweden and Denmark together with fellow Royal Holloway and RISCS member, Rikke Jensen. Rikke and Lizzie have been working with participant groups through narrative and collage building, to better understand how the mobile phone is used, its importance for security and the roles it plays in interacting with institutions such as the state, schools and families. In Phase 2 of this work, Lizzie and Rikke are exploring further how the design and delivery of state refugee re-settlement policies and approaches affect feelings of safety and security in refugee communities, and the roles the mobile phone plays in engendering and responding to those feelings. They are working closely with teachers, community workers and policy makers to produce practical outputs that can support safer mobile phone use during times of insecurity as well as contributing to the theoretical understanding of individual and state securities.

*'Smart For Whom? An IoT Roundtable and W 1'Smart For Whom? An IoT Roundtable and Workshop', at the Health Foundry, London, in September 2017 with participants from digital health startups.*

Claude has spent the first twelve months developing a map of the full spectrum of security theories, for use in the design of public policies and services. As part of this work he has been conducting focus groups on the topic of IoT using creative engagement techniques such as story boarding and LEGO modelling. In this work, he discovered that clarity and fit, trust-building, and active participation are the principles needed for co-creating IoT security interventions that sufficiently engage users. Clarity and fit is important, helping IoT users to better understand the relevance of security features and the reasons why their engagement is necessary in supporting IoT security, since these should support their everyday activities. If the relevance of the security design is not clear and transparent, Claude's participants were doubtful as to whether users would trust and follow IoT security requirements. The focus groups were unanimous in their views about trust-building, and the findings indicate that there is a fundamental mistrust in many of the business models that have led to the propagation of smart devices, specifically regarding the intentions of institutions who harvest large quantities of user data from IoT. Claude's participants articulated very clearly that trust must be built up through encountering smart services that fit into their lives, as much as through smart devices. This relationship to technology needs to be repaired if users are to carry out security tasks not just for their own benefit but also for the benefit of businesses and the state. Claude also discovered that IoT security features were more likely to succeed if people were actively consulted in the use of IoT as it is introduced into settings such as the workplace, schools and shared community spaces.

In Year 2 of the fellowship, Claude is working on practical ways in which such active participation in these issues can be encouraged and supported. He is also continuing to develop the map of theoretical approaches, for use by academics, security practitioner groups and policy makers. Something we hope to present in RISCS' annual review for 2018!

### Grant Details

**EPSRC References:** EP/N02561X/1
**Title:**

ESSfES: Everyday Safety-Security for Everyday Services

**Principal Investigators:**

Coles-Kemp, Professor L *(Royal Holloway, University of London)*

**Other Investigators**:

Heath, Dr C *(Royal Holloway, University of London)*
Jensen, Dr R *(Royal Holloway, University of London)*

# Update on NCSC Small Grants 2016-17

## Visualising access control policies

**Professor Charles Morrisset (Newcastle University)**

Charles Morisset's talk at the June 2017 RISCS meeting reported on his work with David Sanchez, a recent MSc graduate from Newcastle University, on visualising access policies to help people make better decisions. Funded by a small NCSC grant, the project finished in January 2017.

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

Morisset's project studied visualising these using different options such as maps, user roles, permissions, and multilateral grids: making complex policies easier to understand at a glance should mean fewer errors to leave networks vulnerable. An online demonstration shows the design the group came up with, an ongoing effort called VisABAC, for the visualisation of attribute based access control policies, and a test for visitors to take to help assess the effectiveness of these design changes. A significant difficulty for the project is that there is no benchmark for reading access control policies and therefore no way to answer the simple question: does this approach work to improve the situation or not? Morisset is hoping RISCS participants will be able to help answer this question.

In the meantime, the researchers conducted a test in which they recruited 32 students, gave them the tool, identified the policy, and asked them to find the attributes. The results suggested that graphics are helpful with new policies but tend to be ignored once people have formed a mental model of how the policy works.

For future work, Morisset wants to:

- consider helping security experts;
- consider the general problem of understanding access control;
- integrate multiple and appropriate visualisation techniques;
- fully integrate with XACML and role-based access control.

Morisset also hopes to be able to use these designs to extend the ability to understand access control policies to non-technical people.

## UNDERWARE: UNDERstanding West African culture to pRevent cybercrimEs

**Professor Monica Whitty (Cyber Security Centre, University of Warwick WMG)**

The overall objective of this project is to gain a greater understanding of West African culture in order to:

- scientifically evaluate current methods employed to prevent and deter cybercrime that emanates from West Africa;
- develop and test new methods to prevent and deter cybercrime (that emanates from this region).

A literature review was conducted on scholarly and grey literature examining cybercriminal culture in West Africa; West African culture in general, and research on deterrence and prevention programmes for cybercrimes.

In addition, a workshop was held, where academics from West Africa presented their research on cybercriminals in the region, and a number of law enforcement officers spoke about the problems they face and their views on the way forward in dealing with cybercrimes.

Attendees including members of the RISCS community as well as other academics that have expertise in this area; employees of intelligence UK agencies; UK law enforcement officers, policy makers and members working in relevant areas in industry were invited to ask questions of the speakers and make comments on the presentations.

The workshop highlighted poignant points that might help us understand the popularity of cybercriminals within Nigeria as well as the reasons why the problem persists. The speakers, in the main, agreed that cybercrimes, especially fraud, are deemed less immoral than most other crimes (e.g., theft) by West Africans and that poverty and corruption were major causal factors of cybercrimes. Notably, cybercrime is a cheap and low difficultly/skilled crime to move into and given that criminals believe they are unlikely to be penalised it is also a low risk crime.

Rationalisations used by cybercriminals was noted by many of the speakers. They also noted that criminals, in the main, provide excuses for their bad behaviour. The shared view that 'white' Westerners deserved to be scammed given the harm they had caused West Africans in the past was mentioned by most speakers. However, it was also noted that West Africans are just as likely to scam other West Africans and so this clearly contradicts the 'West deserve it' discourse.

Most speakers discussed how these crimes are organised – using loose structures with networks across the world. Different groups within the structures had different skills and they would be called upon as needed when committing cyberfraud, for instance. It is believed that there is a large diaspora of Nigerians in many countries that are called upon to assist criminals with their crimes. The use of spirituality was discussed by most speakers, and while these practices seemed bizarre in many ways to Westerners, speakers warned the audience that these practices are deemed to be very serious and real – and are not only enablers to crimes but, in some cases, prevent arrests – due to law enforcements' shared beliefs. Although poverty was believed to be a causal factor, speakers noted that education did not help prevent cybercrimes. Instead, being a university student increased the chances that someone would be a cybercriminal. Cybercriminals stood out at universities (with expensive cars, and dressed in bling) and other students sought them out to join their gangs. Law enforcement had however, used this opportunity to catch out more cybercriminals. Being educated, however, seemed to be more typical of Nigerian cybercriminals than other West African cybercriminals. The understandings highlighted by law enforcement were particularly interesting and elucidate the need for further academic work. Academic work, however, is limited by how far it might penetrate into the criminal realm and so working together with law enforcement is clearly important as we advance the science in this field.

## Beyond Dissemination

**Rikke Jensen and David Denney**
**(Royal Holloway, University of London)**

The overarching aim of this study by Rikke Jensen and David Denney was to better understand how academics can demonstrate the impact of their cyber security research and move it beyond purely academic dissemination. This small grant project, funded by NCSC, was born of the researchers' own frustrations when trying to determine the extent to which their DSTL-funded research into social media use by military personnel had fed into MoD policy and practice. Instead of finding answers, they were simply told to trust that the research and its findings would be taken seriously by military leadership and policy makers.

The dissemination study created an opportunity to speak to a wide range of stakeholders from both inside and outside academia and discuss expectations about how collaboration might facilitate better usage of academic research. The researchers expressed their concern that research findings tend to disappear into a vortex, which they call "The Void". The issues they were interested in were well summed up by the CISO of a global organisation, cited in the presentation, who told them that academic research was generally not well disseminated outside of academic circles and did not reach him in a form that's useful in the real world. Accordingly, they set out to find ways to present academic work that might foster greater impact. One simple idea was producing new forms of output, such as one-page summaries, a seemingly small thing but a big change from the usual 100-page report or technical article.

Jensen and Denney conducted a small group of interviews with stakeholders who had engaged with academics in previous research projects, asking what impact meant to them, how important it was, what it looks like, what their expectations were, what kinds of partnerships they saw as useful, and how to do things differently. Alongside that, they conducted a separate study on impact case studies submitted to the 2014 Research Excellence Framework (REF2014) where they used cyber security-related keywords to explore how research projects demonstrated impact. In the process of identifying impact from cyber security projects, they found that the way REF2014 categorises case studies is somewhat arbitrary. These two pieces of research exposed a profound split between non-academics, who want to understand from the outset what the effect of the research will be, and researchers, who feel that impact is too narrowly defined. For academics, navigating this difference is a challenge.

Their main findings:

- Impact is a dynamic process that can and should occur at every stage of the research cycle;
- Stakeholders' expectations in relation to cyber security research were varied and sometimes conflicting;
- The way impact was categorised and assessed in REF2014 appeared to be arbitrary, and assumes an agreed understanding of the meaning of "impact";
- Over-emphasising impact in cyber security research creates divisions between people-oriented and technical-oriented research.

It emerged in the interviews that "impact" is not a generic concept but a differentiated one. Several models were proposed by interviewees. A DSTL fellow proposed two options: a transactional model, in which stakeholders learn from the research when the findings are delivered, and a co-creation model, in which expertise is shared and participants learn from each other throughout. Crucially, which model is being followed needs to be specified at the outset. An external RCUK champion proposed four types of impact: pedagogical, in which the research is turned into teaching material; intellectual, the research influences policy-making and decisions; instrumental, the research delivers tools, capabilities, and techniques; and polemical, going public with the results when any attempt to demonstrate impact has failed. Of these, intellectual impact is the one that's difficult to document. Polemic can be a high-risk strategy. Finally, a data analyst from the MoD offered a mnemonic checklist called "TEPID OIL": training, equipment, personnel, infrastructure, doctrine (and policy), organisation, information, logistics. Using that model, impact has to be shown in all those categories.

The big question moving forward into more impact-driven research is the meaning of "impact" to various stakeholders. Academics use the notion of impact every day as if there's a common meaning, but, as this small study shows, it's much more nuanced. An additional finding that surfaced is that some stakeholders feel exploited when, from their point of view, academics come in, take data, and disappear. A cultural change is necessary: researchers must build their relationships with stakeholders early on in the research cycle and on a basis of genuinely wanting to engage with the problems that have been identified by stakeholders.

## Eye Tracking Devices

**Shujun Li and Patrice Rusconi (University of Surrey)**

This is a small research grant for purchasing a high-end eye-tracker and conducting some preliminary user studies on some eye-racking experiments in different cyber security and privacy applications.

Summary of outcomes:

- A high-end eye-tracker Tobii TX3-120 was purchased.
- Together with other two low-end eye-trackers, they have supported several experiments of COMMANDO-HUMANS (joint Singapore-UK project, UK part funded by EPSRC EP/N020111/1, http://www.commando-humans.net/), an Innovate UK and DCMS co-funded KTP project H-DLP (http://www.surrey.ac.uk/cs/research/projects/h-dlp.htm), an MSc dissertation project in 2016-17 year on privacy policies of online social networks.
- Two Psychology UG students and an overseas visiting UG student from Italy participated in some eye-tracking experiments in 2016-17 year.
- A number of new Psychology UG students are being recruited for new eye-tracking experiments.
- A Best Paper Award at HAS 2017 (part of HCII 2017) for one of the eye-tracking experiments (in the context of COMMANDO-HUMANS project):
- Haiyue Yuan, Shujun Li, Patrice Rusconi and Nouf Aljaffan, "When Eye-tracking Meets Cognitive Modeling: Applications to Cyber Security Systems," in Human Aspects of Information Security, Privacy and Trust:5th International Conference, HAS 2017, Held as Part of HCI

International 2017, Vancouver, BC, Canada, July 9-14, 2017, Proceedings, Lecture Notes in Computer Science, vol. 10292, pp. 251-264, Springer, 2017, http://epubs.surrey.ac.uk/813689/

- A number of local researchers at Surrey have benefited from the eye-trackers and new interests of using them were generated beyond cyber security.
- New collaboration with Surrey's School of Tourism and Hospitality Management due to common interests on eye-tracking, which led to a new research bid just submitted (today!) to EPSRC DE TIPS2 call.
- A series of new eye-tracking experiments and research projects are being planned.
- The evidence gained from the eye trackers will lead to the purchase of a number of mobile eye-trackers to be funded by the University of Kent, as part of the equipment of the newly established Cyber Security Lab.

## Welcome and effective cyber security advice in the sales context

**M. Angela Sasse & Simon Parkin (UCL) and Lynne Coventry (University of Northumbria)**

The project is part of a broader RISCS research stream to develop effective and actionable cyber security advice to consumers and citizens.

The sales professionals who help us select devices that might be vulnerable to cyber attacks could be a welcome and trusted source of security advice for customers purchasing computing equipment and other devices. The study was carried out by RISCS academics in collaboration with the major retailer, and with input from the Home Office Cyber Aware and NCSC staff.

The researchers visited four branches, interviewing 85 customers who were about to buy a laptop or tablet, or had just bought one, and 30 members of staff across four UK stores. Participants in this exercise were self-selecting. Our result showed that the majority trusted sales staff to make them aware of cyber security risks and point them towards effective measures. Even though most had concerns and questions, and were open to receiving advice, they were not aware of resources like Cyber Aware; those who were complained that advice they had seen was confusing or not actionable; they also mentioned that the equivalent of law enforcement advice on physical crime prevention was missing. Many relied on paid or unpaid advice and assistance from friends, family, or IT service providers. The research is now continuing to explore the role of different parties in providing advice and support to consumers.

## Developer Essentials: Top Five Interventions to Support Secure Software Development

**Charles Weir, Awais Rashid (Lancaster University) and James Noble (Victoria University, NZ)**

Cyber security is a big and increasing problem. Almost every week we hear of a new exploit or security breach that leads to major concerns about our digital infrastructure. Software systems are at the very heart of this digital infrastructure. Therefore, while there may be many commercial, social and practical factors that contribute, it is certain that the decisions of software development teams must have a significant impact on the vulnerability of those systems.

In this research we explored ways in which outside actors – such as management, coaches, security teams, industry bodies, and government agencies – may positively influence the security of the software created by development teams, while keeping the development competitive and practically viable. This means that the costs of such 'interventions' need to be acceptable relative to the risks that they address.

We interviewed 14 specialists in introducing software security to development teams. Based on a rigorous analysis of their responses, we were surprised to find that three of the most cost effective and scalable interventions are 'cultural interventions' – ones that work to influence the working of development teams, rather than the artefacts they produce:

1. Developing a 'threat model' and using that model to achieve commercially negotiated, risk based agreement how threats are to be addressed;
2. A motivational workshop engaging the team with the genuine security problems as they affect their specific projects, while making it clear how they are to address those problems; and
3. Continuing 'nudges' to the developers to remind them of the importance of security.

The other two low-cost and effective interventions relate to the code produced:

4. The use of source code analysis tools; and
5. The informed choice of components based on their security quality.

We therefore suggest that providing guidelines, technical support and mentoring in each of these five interventions will have a significant effect on improving the security quality of code developed in future.

## Quantifying the impact of password policy change

**Ingolf Becker, Simon Parkin and M. Angela Sasse (UCL)**

A new password management system was deployed in an organisation with 100,000 employees in August 2016. Employees were moved from fixed-length passwords (8 characters, complexity 3, expiring after 150 days) to a variable-length password scheme requiring complexity 3 with an expiry dependent on the length and strength of the password. The 'Longer Password Longer Life' (LPLL) was created by an experienced systems administrator who was motivated by the high cost of helpdesks for resetting passwords and user complaints, but unaware of the research literature or the NCSC Guidance. The intent was to change to a '3-words-strung-together' scheme as promoted by the government Cyber Aware advice, but organisation committee responsible for security policies mandated that existing 'complexity 3' requirements remained in force. This presented a unique opportunity for researchers to examine and directly measure the impact of large-scale changes to password policy through before-and-after comparison. Through direct collaboration with the organisation's IT team the researchers were able to obtain and analyse system logs on password behaviour, and combine them with employee interviews. 6 months after the change, the strength of passwords use by staff were not significantly different from previously – the majority of users tried LPLLs but changed back to

previous type of passwords. The workload on the help desk was larger than anticipated.

## Helping a High Street Bank to help their customers to be secure online: Developing a customer-focused security awareness maturity framework and associated metrics

**Simon Parkin and M. Angela Sasse (UCL)**

The project involves a review of the information security awareness activities that a UK High Street bank offer to their individual customers and small and medium business customers (SMEs). These are face-to-face information/training sessions and webinars.

While there is a clear indication that customers are interested in receiving guidance from the bank – the sessions are well attended and there is 'customer pull'– the bank currently has no measures for effectiveness. Indications are that customers feel better informed, but there is no mechanism for knowing if they have changed behaviour and/or feel more confident.

The project carried out observations of the training events and customer-centred evaluation. We found that customers were keen to receive cyber security advice from their bank - particularly advice on recent and specific threats - and tried to spread what they had learnt to colleagues within their company. However they were unsure of how that advice mapped onto general security advice that is proffered by a range of stakeholders, such as government and law enforcement. To encourage and help customers to move 'beyond awareness', i.e. ensure they deploy the right technical procedures and countermeasures, and ensure staff are able to understand and follow processes and countermeasures to secure their accounts. We have identified six specific topics areas in the delivery of security advice and engagement with customers where this can happen; Signpost consistent security advice; State which stakeholders should receive what advice; Reach non-attendees; Relate to attendees' existing competencies; Measure expectations over time, and; engage customers when the threat landscape changes.

# RISCS Phase 1 Update

## Choice Architecture for Information Security (ChAISe)

### Publications


Briggs, P., Coventry, L. & Jeske, D. (2017). The Design of Messages to Improve Cybersecurity Incident Reporting. Lecture Notes in Computer Science, Springer.

Jeske, D., McNeill, A.R., Coventry, L. and Briggs, P. (2017). Security information sharing via Twitter: 'Heartbleed' as a case study. Int. J. Web Based Communities, Vol. 13, No. 2, 172-192.

Nicholson, J., Coventry, L., & Briggs, P. (2017). Can We Fight Social Engineering Attacks By Social Means? Assessing Social Salience as a Means to Improve Phish Detection. Symposium on Usable Security and Privacy (Symposium on Usable Privacy and Security – SOUPS 2017).

Briggs, P., Jeske, D and Coventry, L. (2016). Behaviour Change Interventions for Cybersecurity: Using Protection-Motivation Theory as a Framework. In L. Little, E. Sillence and A. Joinson (Eds) Behavior Change Research and Theory: Psychological and Technological Perspectives. Elsevier.


### Grant Details

**EPSRC Reference:** EP/K006568/1
**Title:**

Choice Architecture for Information Security

**Principal Investigator:**

van Moorsel, Professor A *(Newcastle University)*

**Other Investigators:**
Laing, Dr CD *(Northumbria University)*
Gross, Dr T R *(Newcastle University)*
Briggs, Professor P *(Northumbria University)*
Coventry, Dr L *(Northumbria University)*

## Productive Security

### Related Activity

Invited talk. MA Sasse 17th October 2016 *Case study: Implementing effective defence against the insider threat without ruffling feathers* 15th Noord Infosec Dialogue, Marlow

Invited talk MA Sasse 1st November 2016 *Managing your privacy - What choice do you really have?* Google Security and Privacy Week, Zurich, Switzerland

Keynote talk, MA Sasse, 9th November 2016 *Securing the Digital Society - why we need a multidisciplinary approach*, Opening Ceremony for Beautiful New World: Safety for People in CyberSpace (SecHuman) project, Bochum, Germany

Invited talk, MA Sasse, 7th December 2016, *Awareness supporting the transition to secure behaviours*, SASIG Conference, London

Invited talk, MA Sasse, 13th December 2016, *Working together to meet the cyber challenge*, Rise to the Challenge: Cyber Security, London

Invited speaker, MA Sasse, 11th January 2017, *How Safe Is Your Password?,* BBC Radio 4 Moneybox Programme, London

Panel moderator, MA Sasse, 27th January 2017, *Password-Based Protection of Privacy and Personal Data: Friend or Foe?*, CPDP Conference, Brussels, Belgium

Invited talk, MA Sasse, 2nd February 2017, Fast Stream Conference, London

Distinguished Lecture, MA Sasse, 8th February 2017, *Why Johnny, Jane, and their friends won't encrypt: Barriers to the adoption of secure messaging tools*, Lancaster University, UK

Invited talk, MA Sasse, 22nd February 2017, *Design a training programme that works with the way people naturally behave,* The European Information Security Summit (TEISS), London

Invited talk, MA Sasse, 28th February 2017, HOSAC Conference, Royal Society, London

Invited talk, MA Sasse, 3rd March 2017, Security and usability in the development process - Insights from 3 case studies, Keele University Seminar, Newcastle

Invited talk, MA Sasse, 15th March 2017, Stream Two "People are the Strongest Link", Session One, CyberUK 2017, Liverpool

Invited talk, MA Sasse, 16 March 2017, TAKE AWARE Conference, Neuss, Germany

Invited talk, MA Sasse, 20 April 2017*, Can we make the Internet of things secure enough for humans?,* IoT meets Cyber Security, Edinburgh UK

Invited talk, MA Sasse, 20th May 2017. *Protect what people value – and they will value security*, GREPSEC III meeting, San Jose, USA

Invited talk, MA Sasse, 24th May 2017, *Can we make people value IT security?,* Wheeler Lecture, Cambridge UK

Invited talk, MA Sasse, 6th June 2017, Data Protection Workshop, Infosecurity Europe 2017

Fireside chat, MA Sasse, 25th September 2017 *Fostering Cyber Security and Enabling People to be the Strongest Link - how do we get there? Understanding the Human Dimensions of cyber security,* 3rd Annual Energy Cyber Security Executive Forum, London

Invited talk, MA Sasse, 28th September 2017, WIRED Security Event 2017,. London

Invited talk, MA Sasse, 1st October 2017, *Is trying to protect your privacy futile?,* New Scientist LIVE, London

### Publications


S. Dodier-Lazaro, R. Abu-Salma, I. Becker, and M. Sasse, 'From Paternalistic to User-Centred Security: Putting Users First with Value-Sensitive Design', in CHI 2017 Workshop on Values in Computing, 2017. UCL Discovery

Becker, I. F., Parkin, S., & Sasse, M. A. (2017).Finding Security Champions in Blends of Organisational Culture.Proocedings of EuroUSEC '17. Internet Society.

S. Dodier-Lazaro, I. Becker, J. Krinke, and M. A. Sasse, 'No Good Reason to Remove Features: Expert Users Value Useful Apps over Secure Ones', in: Tryfonas T. (eds) Human Aspects of Information Security, Privacy and Trust. HAS 2017. Lecture Notes in Computer Science, vol 10292. Springer, Cham. Previously published as a UCL Computer ScienceResearch Note, University College London, Computer Science, London, WC1E 6BT, United Kingdom, 17/03, Feb. 2017.

The Security Blanket of the Chat World: An Analytic Evaluation and A User Study of Telegram, R Abu-Salma, K Krol, S Parkin, V Koh, K Kwan, J Mahboob, Z Traboulsi, .2nd European Workshop on Usable Security (EuroUSEC 2017)

Murdoch, S.J., Becker, I., Abu-Salma, R., Anderson, R., Bohm, N., Hutchings, A., Stringhini, G. (2017). Are payment card contracts unfair? (Short paper).

Abu-Salma, R., Sasse, M.A., Bonneau, J., Danilova, A., Naiakshina, A., Smith, M. (2017). Obstacles to the Adoption of Secure Communication Tools.


### Grant Details

**EPSRC Reference:** EP/K006517/1

**Title:**

Productive Security: Improving security compliance and productivity through measurement

**Principal Investigator:**

Sasse, Professor MA *(UCL)*

**Other Investigators:**

Pym, Professor D *(UCL)*