RISCS

Project Catalogue

Introduction

Knowledge exchange between technical, academic and policy actors is a key priority for RISCS. We are deeply engaged with the academic and policy communities in the UK, delivering high impact work that routinely shapes guidance, advice, and policy processes. One challenge that always comes up is around the ability of those who need research to access it, and to have the information they need at their fingertips.

Through discussions with policy stakeholders in 2020, we identified a need for a summary of particular evidence of interest from RISCS projects, as well as more awareness of how projects are progressing and any upcoming outputs. This catalogue is intended to be a succinct summary of completed and ongoing projects tailored for a policy audience.

We hope that the catalogue will offer opportunities for future collaborations between sectors and for RISCS research to feed into policy decisions and analysis where there are synergies.

The document is complementary to the materials on the RISCS website and can be read in conjunction with the RISCS Annual Report 2021.

How to use this catalogue

The projects are presented chronologically but coloured icons indicate the associated research themes as shown.

- Leadership and Culture
- Cybercrime
- Secure Development Practices
- Digital Responsibility
- Anticipation and Futures Literacy
- Quantification and Cyber Risk

If more detail is required on any of the project, you can request more information (for example via a meeting with researchers or through development of a policy briefing) on certain projects of interest by contacting us by email.

The published research findings are available in a separate annex of publications.

If you have any questions or comments, please feel free to get in touch with the RISCS Team at riscs.administrator@ucl.ac.uk

Contents

Ransomware: The Role of Cyber Insurance (RaCI)

Dates: July 2021 – April 2022

Lead researchers: Dr Jason Nurse, Dr Gareth Mott, Sarah Turner, *University of Kent*; Jamie MacColl and James Sullivan, *RUSI*; Edward Cartwright, *De Montfort University;* and Anna Cartwright, *Oxford Brookes University*.

Overview: This project follows on from the "Incentisizing cyber security through cyber insurance" project. It seeks to understand the role of cyber insurance in handling the challenges posed by ransomware. Specifically, it will answer the following questions:

- How has the rise in ransomware losses changed the cyber insurance market and cyber insurance coverage?
- Can cyber insurers help make organisations more secure or resilient against ransomware?
- What is the current role of insurers when a ransomware incident occurs?
- How has this role changed and where may it be headed?
- What are the incentives and disincentives to victims paying ransoms?
- What sort of public–private partnerships between the insurance industry and government would be effective for tackling ransomware?
- Is ransomware coverage sustainable for the insurance industry?

Policy implications: The research findings will help decision-makers to navigate cyber risk management approaches, understand ransomware challenges in the context of cyber insurance, and provide clear and actionable recommendations that can be adopted by governments and practitioners alike.

Methods: Literature review, stakeholder interviews and workshops.

Funders: NCSC

Security Economics of the Supply Chain for Connected Places

Dates: March 2021 – April 2022

Lead researchers: Dr Manos Panaousis and Professor George Loukas, *University of Greenwich.*

Overview: This project is investigating how we can better understand the economic drivers involved in Connected Places supply chains. The first phase has involved looking at some existing smart cities and reviewing the makeup of their supply chains and the nature of the companies involved. Drawing on the NCSC Cyber Security Principles for Connected Places, as well as Chartered Institute of Information Security, resources and the academic literature where applicable, the project aims to design a model case of a typical connected place. In this instance the project looked at a smart traffic light system, and its supply chain to understand how the different cyber security principles can be practically applied to this case.

The project also hopes to propose an economic feasibility assessment framework, to analyse the NCSC Cyber Security principles for Connected Places. This will involve identifying expenditures involved in delivering these capabilities and activities required to implement the Connected Places principles, along with examining the damages they prevent. The project has proposed a control feasibility assessment framework.

Policy implications: This research can help to develop a better understanding of how best to incentivise players in this ecosystem and articulate the risk involved in a lack of adherence to the recommended principles.

Funders: NCSC.

Stories of Cyber Security (SOCS)

Dates: April 2021 – March 2022

Lead researchers: Professor Genevieve Liveley, *University of Bristol*.

Overview: This project examines the potential for stories and storytelling to inform and support more effective communication of cyber security good practice and policy. The first phase of the project mapped what the 'storyworld' of this narrative ecosystem looks like – identifying problem areas where narrative dynamics are weak and failing to engage key stakeholders. It adopted a systems thinking approach to the narrative analysis of a portfolio of stakeholder stories that interact across the ecosystem of cyber security. The second phase of the project analyses the dynamics of these varied interactions and suggests practical recommendations for employing different narrative strategies in cyber security communications.

Policy implications: This project maps the relationships between key audiences and storytellers (including policymakers) across the cyber security ecosystem and makes recommendations for employing different strategies in cyber security policy communications.

One of the project's key discoveries is that the NCSC's narrative role in this ecosystem is best understood as that of the 'donor' or 'helper' – a classic mentoring or caring character whose prime function is often to help 'heroes' defeat 'villains'. The free provision of tools and services, and work supporting people to take charge of their own cyber security, align well with this 'donor' or 'helper' characterization. As do metaphors and narrative tropes emphasizing the role of the NCSC in mentoring, advising, and supporting others. The project has also found that the NCSC's core mission and strategic narrative is that of the 'quest' – which emphasises teamwork, profits, optimism, and future possibilities. A full report detailing these findings will be published later in 2022.

Methods: Literature review, stakeholder interviews and workshops.

Funders: NCSC, RISCS.

Cyber Readiness for Boards (CR4B)

Dates: September 2019 – September 2021

Lead researchers: Professor Madeline Carr, *UCL*

Overview: The role of boards in contributing to a broader agenda of national cyber security is well established. 83% of UK critical infrastructure is in private hands, so boards of private sector organisations have been identified as essential to enhancing cyber security and resilience. The relevance of cyber risk assessment is expected to increase in scale and in scope as technological ecosystems become increasingly complex.

This project investigated how corporate boards assess cyber risk and make decisions about investments in cyber security, working with the assertion that board-level approaches to cyber risk cannot be understood in isolation of other business risks. The aim of this project was to extend existing research on board responses to cyber in order to identify, understand, and account for broader internal and external decision-making factors.

The project had three key objectives:

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

Policy implications: The project developed a range of practical and actionable interventions to improve board decision-making about cyber risk which is relevant to NCSC guidance for boards and the DCMS cyber security breaches work, as well as for the next cyber security strategy beyond 2021.

Outputs include briefings for policy audiences to communicate key findings, a joint report with Axelos (a leading provider of board level training on cyber risk assessment) on improvements for board training, and written guidance for boards.

Outputs will be disseminated to relevant audiences in 2022.

Methods: Interviews, surveys, qualitative and quantitative data analysis, literature review

Funders: RISCS, Lloyds Register Foundation

External collaborators: Axelos, The Access Group. Other organisations, as well as board members, non-executive board members and senior cyber security practitioners were also involved.

Leveraging the Multi-Stakeholder Nature of Cyber Security

Dates: April 2017 – September 2021

Lead researchers: Professor Christian Wagner, *University of Nottingham*

Overview: Cyber security is a challenging, distributed, multi-stakeholder problem. It is distributed in the sense that the expertise to comprehensively assess the level of security of a given IT system is usually available from different locations). 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 cyber security.

The project involved developing a framework with scientific underpinning to improve user access to tailored cyber security information. The tool, named 'Online Cyber Security Decision Support System' (OCYSS), is designed for small-to-large scale users in government and industry sectors, to address the shortage of availability and access to highly qualified cyber security experts they might otherwise require.

The OCYSS tool is designed to efficiently deliver appropriate, user-tailored, balanced, informed and up-to-date threat analysis and decision support to users. It will do this by integrating inputs from experts and the user to efficiently capture, handle and integrate richer cyber security data (such as from vulnerability assessments).

The research has also considered how to collect richer data that carries uncertainty (such as precisely how many tools are available to an expert to protect from attack) from people, using interval-valued rating scales. They have developed software 'DECSYS', which stands for 'discrete and ellipse-based response Capture system', to permit electronic capture of such data. This has received funding from the NCSC and was made available in late 2019.

Policy implications: DECSYS aims to expand the capacity of senior practitioners and policymakers to make better decisions, such as cyber investment decisions. The tool could help decision makers discern whether to invest in specific vulnerability controls or to diversify financial resources into mitigating a range of vulnerabilities. The tool was trialled with DSTL in 2019. The research team are looking for further engagement with both Government and industry stakeholders in order to better understand how decision makers can best make use of the uncertainty responses gathered.

Find out more: Lab website with links to the software tools: https://www.lucidresearch.org/decsys.html

Methods: Empirical studies, including surveys, combined with re-analysis of existing datasets. Software development in parallel.

Funders: EPSRC and NCSC (supported the software development).

External collaborators: Carnegie Mellon University (US), NCSC (UK), JPMorgan and Chase.

Cyber Protect: Protecting Businesses in the Eastern Region from the Risk of Cybercrime

Dates: June 2020 – March 2021

Lead Researchers: Dr Christian Kemp, Adrian Winckles, Kelly Coulter, *Anglia Ruskin University*

Project Overview: This study examined how we may better support businesses in the Eastern Region to make long-term, sustainable improvements in cyber security behaviours and practices. To achieve this, the research evaluated the work of the cyber-protect network in the region with a view towards locating ways in which the delivery of NCSC messaging to business communities may be improved and reinforced. Interviews with a wide sample of SMEs in the East were integral when highlighting the complex challenges that businesses have faced when seeking to introduce and maintain long term positive behavioural change. It is anticipated the data may help to develop tools to help improve the impact that protect officers have when engaging with Eastern businesses. For example, the research team are exploring a cyber-protect 'engagement tool' that could simulate a live attack to illustrate key vulnerabilities and modes of attack to a business audience. The intention is for any new tools to be accompanied by relevant metrics to help measure long-term behaviour change.

The research also evaluates the relationship between cyber-insurance and low levels of cybercrime reporting amongst SMEs in the Eastern Region.

Policy implications: As a key part of the UK's National Cyber Security Strategy, the Cyber Protect Network is responsible for the delivery of NCSC cyber security guidance and messaging to UK businesses. The research will help to generate recommendations for improvements the Protect Network could implement to further develop its impact on long-term cyber resilience practices amongst businesses in the Eastern region. These recommendations aimed to support the cyber-protect network to maximise engagement and outreach between protect officers and SMEs, update the format/structure of cyber-awareness training and inputs, improve key impact metrics and address new challenges posed by Covid 19.

Methods: 20 interviews with Cyber-protect officers and policing stakeholders. 30 interviews with representatives from a sample of SMEs based across the Eastern Region.

Find out more: Please email Dr Christian Kemp (Christian.kemp@aru.ac.uk) – website in development.

Funders: Home Office

External Collaborators: Essex Police, Essex Chambers of Commerce, Eastern Region Special Operations Unit, Eastern Region Cyber-Resilience Centre

Follow up work: The work has contributed to the development of the Eastern Region Cyber-Resilience Centre and the Essex Strategic Cyber-Crime Board.

Cyber Security Quirks: Personalised Interventions for Human Cyber Resilience

Dates: May 2020 – March 2021

Lead researchers: Dr John Blythe and Dr Inka Karppinen, *Cybsafe*

Project overview: Existing work in the cyber security field has primarily been focussed on raising security awareness by 'fear' appeals as a means to change behaviour. There has been little work on the role of personalisation harnessing individual differences. Together with poorly understood barriers to security behaviour change they have led to fairly generic 'one-size-fits-all' informational campaigns that do not serve people effectively. Thus, research lags behind interventions used within the public health sphere. Moving away from generic security awareness raising, approaches that are tailored to people's needs and apply behavioural change techniques are needed. The overall objectives of this project were to:

- identify factors for personalisation;
- assess the usability of a personalised behaviour change intervention; and
- evaluate the effectiveness of the intervention for changing cyber security behaviour.

A rapid evidence assessment, guided by theoretical and evidence-based research, was conducted to achieve the first objective. Barriers to security behaviour change were also identified.

The study also focused on the evaluation of the personalised intervention including a usability study and experimental evaluation of the effectiveness of the intervention for changing behaviour.

Policy implications: People's idiosyncrasies are not served by the current awareness and behaviour change campaigns. Exploring the use of behaviour change techniques and personalised interventions are important for advancing current campaigns that are group-level in focus and static in delivery.

Many groups (such as older adults) are under-represented in awareness campaigns. Differences that influence the degree to which an individual engages in an intervention, are rarely considered. This project will adjust intervention content and delivery to suit individual variability. Furthermore, this innovative approach will focus beyond using 'fear' to change behaviour by using structured approaches (e.g. Behaviour Change Wheel) to apply behaviour change techniques that are appropriate for the cyber security behavioural barriers. Personalisation of behaviour change techniques, alongside other personalisation factors (e.g. age and personality), will allow us to understand what combination of interventions works for individuals. These findings will have wider implications on the way which cyber security behaviour change initiatives are rolled out to the general public.

Find out more: To find out more about the project please contact research@cybsafe.com

Funders: Home Office

External collaborators: None

A Framework to Model and Incentivise Cyber Security Investment Decisions (MERIT)

Dates: April 2020 – March 2021

Lead researchers: Dr Manos Panaousis, *University of Greenwich* and Dr Michail Chronopoulos, *City, University of London*.

Overview: This project sought to address the challenges of quantifying the benefits of investment in cyber security. It is common for cyber security budgets to cover overlapping elements through diverse service agreements. Through economic modelling, this project aimed to minimise cyber security risks by guiding organisations to optimally invest their budget for cyber controls.

The team produced:

- A software tool that visualises decisions about investing in cyber security controls;
- A knowledge base of controls along with their costs; and
- A threat-based risk assessment modelling using the MITRE ATT&CK® – a globally accessible knowledge base of adversary tactics and techniques based on real-world observations of cyberattack.

Policy implications: This work could benefit cyber security policymakers who will be able to tailor existing cyber security policies and best practises to incentivise and regulate the use of any required baseline defences and appropriate levels of investments in cyber security controls.

The work is intended to be useful for cyber security accreditation (such as for IASME and NCSC) and to incentivise businesses by saving them money.

Methods: mathematics, software development, cyber security engineering

Funders: RISCS

External collaborators: IASME Consortium, Professor Chris Hankin, *Imperial College London*

Follow on work: We are collaborators on the European CUREX project, the European SECONDO project, and the SecurityBudget project to produce a cyber security dashboard to support SMEs.

Economic Metrics for Supporting Cyber Security Investment Decision-Making

Dates: April 2020 – March 2021

Lead researchers: Dr Yulia Cherdantseva and Dr Izidin El Kalak, *Cardiff University*

Overview: For Small and Medium Enterprises (SMEs) in the UK, an average cost of a cyber security breach varies between £3,650 and £9,270. According to the DCMS Cyber Security Breaches Survey, 78% of businesses consider cyber security as a high priority. More work is needed to support SMEs to take appropriate action. While there are many approaches they can take, such as score cards or risk portfolios, techniques can be costly and difficult to implement for SMEs who have limited resources.

This project involved an empirical study on the use of economic metrics (both quantitative and qualitative) by Boards and technical experts for supporting decision-making on cyber security investments. It looks at advantages and disadvantages of different metrics, how effective they are for supporting decision making and how they could be made more appealing for Boards.

Policy implications: The project resulted in A Best Practice Guide for SMEs on Cybersecurity Investment Decision-Making which is aimed at assisting them to make well-informed cyber security decision. It aims to equip cyber security professionals with an actionable guidance on how to "sell security to their bosses" which may lead to the improvement in the cyber security posture of SMEs. This should be a relevant and useful contribution to policy actors working to improve the cyber security of SMEs.

In the current landscape, where SMEs often have not yet implemented standardised cyber security decision processes, and where the application of investment metrics is either absent or inconsistent, it is critically important to produce a practically useful guide on the use of economic metrics for cyber security decision support. In the business context, the output of the project will equip cyber security professionals with an actionable guidance on how to "sell security to their bosses" which may lead to the improvement in the cyber security posture of SMEs.

Methods: Interviews with businesses as well as security vendors or consultants who work with them, qualitative data analysis

Find out more: A Best Practise Guide for SMEs on Cybersecurity Investment Decision-Making.

Funders: RISCS

Gamification Training to Protect Against Socially Engineered Cyber Attacks: An Evidence Based Design.

Dates: April 2020 – March 2021

Lead researchers: Justin Hempson-Jones and Nicolas Melendez, *Social Machines,* and Dr Francesca Salvi, *University of Portsmouth.*

Overview: Attacks that take advantage of human operator behaviour to compromise cyber security are often described as socially engineered cyber-attacks. For example, these include phishing (using email or voice-over-internet-protocol channels) in order to prompt users to divulge information or perform another compromising behaviour; social network exploitation; waterholing – where victims are lured to compromised websites and exploited, and baiting (leaving compromised material to lure individuals into compromising systems).

This research explored what types of training will best protect users against different types of attack. Evidence assessed through a systematic review was used to modify social engineering taxonomies to map our best current understandings of what works, where, how and why.

This was used to create a 'proof of concept': a set of fictional but practical use cases demonstrating how the taxonomy can be used to generate practical training packages for users.

Policy implications: The work aimed to support a more robust foundation for cyber protection training to help organisations to optimise cyber security behaviours and cyber risk decision making amongst employees. It will create a foundation for cyber security training in order to encourage take-up of training solutions based on a robust, evidence-based approach to gamified training in this area.

Methods: Systematic literature review, taxonomy development and illustrated proof of concept.

Find out more: https://socialmachines.co.uk/

Funders: RISCS

Incentivising Cyber Risk Management Behaviours: The Role of Cyber Insurance

Dates: April 2020 – March 2021

Lead researchers: James Sullivan, *RUSI* and Dr Jason Nurse, *University of Kent*

Overview: This project considers whether insurance could provide a significant lever to promote a step change towards better cyber risk management in organisations. It has two objectives:

- To develop a clear understanding of the positive outcomes that cyber insurance could have in improving cyber risk management practices, and consequently, to define how these outcomes may be championed to better direct secure behaviours in organisations, particularly SMEs.
- To research the extent to which knowledge from the other, more mature insurance portfolios – such as property, natural hazards, maritime, terrorism and health, may be leveraged to advance thinking and practice in cyber insurance.

The 'emerging insights' paper sets out key policy research gaps. It explores why the uptake of cyber insurance has been so low, the role of cyber insurance in improving cyber security behaviours and practises, scepticism on the value of cyber insurance and how cyber insurance can learn from other insurance sectors.

Following 50 stakeholder interviews with the insurance industry, SMEs and large businesses, academics and Government stakeholders, the team conducted workshops to explore the role of cyber insurance in business and its ability to incentivise security practices.

The occasional paper found that the shortcomings of cyber insurance mean that its contribution to improving cyber security practices is more limited than policymakers and businesses might hope. Although several means by which cyber insurance can incentivise better cyber security practices are identified, they have significant limitations. Interviewees consistently stated that the positive effects of cyber insurance on cyber security have yet to fully materialise. While some mature insurers are moving in the right direction, cyber insurance as a whole is still struggling to move from theory into practice when it comes to incentivising cyber security.

Policy implications: It is hoped that the research findings help decision makers to navigate cyber risk management approaches, understand challenges with incentives in the context of cyber insurance, and provide clear and actionable recommendations that can be adopted by policymakers and practitioners alike.

The RUSI occasional paper contains 13 direct, actionable recommendations relating to cyber risk management and the role of cyber insurance which could be adopted by policymakers and practitioners, with particular relevance to the DCMS market incentives programme.

Methods: Interviews, workshops, literature review, data analysis

Find out more:

- Project page on RUSI website
- Cyber security incentives and the role of cyber insurance (PDF)
- Occasional paper: Cyber insurance and the cyber security challenge (PDF)

Funders: RISCS

Keeping the Internet of Things Secure: Investigating Incentives for Internet Service Providers and Individuals in the UK and Japan

Dates: April 2020 – March 2021

Lead researchers: Dr Ingolf Becker and Dr Tristian Caulfield, *UCL*

Overview: Internet Service Providers (ISPs) have an ambiguous role in protecting users from cyber security vulnerabilities and in helping them recover from them. By working with a twin team in Japan, this project will determine which incentives and approaches might encourage (ISPs) and their customers to remediate compromised or vulnerable IoT devices, which present a growing risk to the security of the online ecosystem. The project will investigate the design and measurement of interventions and work with UK ISPs and customers to explore the suitability of different approaches in the UK.

Policy implications: This programme is relevant to the UK Government's secure by design agenda for Consumer IoT security, including the current proposals for regulating such 'smart' products.

Methods: Workshops, user studies

Funders: RISCS

External collaborators: Cybersecurity Laboratory at the National Institute of Information and Communications Technology in Japan

Case by Case: Building a Database on Cybercriminal Business Models

Dates: October 2018 – March 2021

Lead researcher: Professor Jonathan Lusthaus, *University of Oxford*

Overview: This project focused on the business models of cybercriminal groups. Its goal was to build a database of closed cybercrime cases that illustrates different group structures. This will move the discussion of cybercriminal organisations from generalities to a richer micro-level understanding, thereby making it more feasible for law enforcement to identify vulnerabilities in organisational structures and to target disruptive interventions effectively.

Policy implications: The project supported understanding of cyber offenders, their business models, the risk factors for offending and pathways - for overseas as well as UK based offenders. More broadly it will also help consider effectiveness of interventions to prevent people becoming involved in cyber crime and interventions to divert those on an offending pathway. This will help contribute to policy and law enforcement development in areas such as Cyber Prevent and Cyber Pursue. The project will support law enforcement through making it easier for them to identify vulnerabilities in organisational structures and to target disruptive interventions effectively.

Funder: Home Office

External collaborators: Dr Tom Holt, *Michigan State University*, Professor Edward Kleemans, *Vrije Universiteit Amsterdam*, Dr Rutger Leukfeldt, *Netherlands Institute for the Study of Crime and Law Enforcement*, Professor Mike Levi, *Cardiff University*, and Professor Federico Varese, *University of Oxford*.

Advanced Modelling of Cybercriminal Careers (AMOC): New Tech and Intelligence from Online Evidence Bases

Dates: January 2018 – March 2021

Lead researchers: Professor Awais Rashid, Dr Emma Williams, Dr Claudia Peersman, Dr Matthew Edwards, *University of Bristol*

Overview: Recent research in debriefing arrested criminals has identified that cybercrime is not a solitary and anti-social activity, but one wherein online social interactions play a critical role – namely, in the recruitment, training and professional advancement of criminals.

For this reason, investigating these social interactions is important to understanding the dynamics leading to initial engagement in cybercrime, continued careers and potential retirement. This project aimed to understand the social and economic development of cybercriminal careers.

To do this, the work focused on the potential for combining advanced data mining of these social interactions, with qualitative methods drawn from psychology, criminology and (socio)linguistics to form a detailed understanding of the characteristics of cyber offenders, their behavioural patterns and their career progression in cybercrime.

The project resulted in new techniques and software tools to support law enforcement agencies to detect and investigate cyber offenders, cyber threats and online networks.

These new tools will allow cybercrime investigators to detect cyber offenders, analyse their criminal activities and behaviour; assign degrees of importance and urgency to items of evidence in order to assess the potential danger to society, and find useful evidence in a timely manner.

Policy implications: The project findings will have relevance for law enforcement and policy stakeholders. The findings are intended to inform evidence-based approaches to disrupting cybercriminal activities on dark-net markets.

Methods: A web-based survey; qualitative analyses for building an assessment framework; quantitative analyses using text mining, natural language processing and machine learning techniques.

Find out more:
https://research-information.bris.ac.uk/en/projects/amoc-advanced-modelling-of-cyber-criminal-careers

Funders: Home Office

External collaborators: The National Crime Agency, the Dutch National High Tech Crime Unit, the Shadowserver Foundation and the UN Office on Drugs and Crime.

Why Johnny Doesn't Write Secure Software: Secure Software Development by the Masses

Dates: January 2018 – March 2021

Lead researchers: Professor Awais Rashid, *University of Bristol*, Professor Bashar Nuseibeh, Professor Helen Sharp, Professor Marian Petre, *The Open University,* Professor John Towse, Professor Mark Levine, *Lancaster University*

Overview: 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 such developers engaging in software development. The overall aim is to develop an empirically-grounded theory of secure software development by the masses. The focus is on understanding:

- What typical classes of security vulnerabilities arise from their mistakes,
- Why these mistakes occur, and
- How we may mitigate these issues and promote secure behaviours.

To achieve this, the researchers designed a study meant to understand developers' reasoning and decision-making across the different kinds of software development tasks they typically engage with and why these mistakes occur. The team found that developers really only consider security when directly facing code (such as when fixing vulnerabilities), and in many cases choices made in secure development that are perceived to be secure, actually are not.

The work then investigated how cognitive biases may play into developers' decision-making on trusting particular people or resources (such as code fragments on Stack Overflow). Findings so far indicate that developers place trusts in people (and the resources they provide) based on their perception of those people, which may not be an accurate view of reality. This provides further in-depth understanding of why these mistakes occur, especially in software development tasks where developers are not directly engaged in writing code.

As part of the project, psychometric instruments were designed to draw out developers' attitudes towards handling of personal data in their software.

Policy implications: Findings to date may already be of interest to developers themselves, as well as policy makers intending to support developers in writing more secure software. It has relevance to NCSC's secure development agenda.

Secure software development is about more than just writing secure code. The choices made by developers have potential to impact the security of their software. A critical, reflective attitude towards these choices could be an important component of promoting secure software development. The project is also exploring novel interventions which could lead to improved security cultures, as developers could engage in more secure behaviours without increasing their task load.

Methods: Interviews, surveys, online forum discussions.

Find out more: https://www.writingsecuresoftware.org

Funders: EPSRC

External collaborators: The Open University, UK; Lancaster University, UK; LERO (The Irish software research centre); National Institute of Informatics, Japan; Technical University of Darmstadt, Germany; Google.

Online Ties Taking Over (OTTO)?

A longitudinal study into actual vs. perceived cybercriminal behaviour of offline vs. online social ties among youth

Dates: January 2018 – December 2020

Lead researchers: Dr Marleen Weulen Kranenbarg, *Vrije Universiteit Amsterdam (VU)*, Professor Frank Weerman, *Netherlands Institute for the Study of Crime and Law Enforcement (NSCR)* and *Erasmus University Rotterdam*, Yaloe van der Toolen *VU* and *NSCR*.

Project overview: Research from traditional crime areas suggests there is a strong relationship between an individual's criminal behaviour and that of their social ties. This project is exploring the extent to which this is also the case for cybercriminal behaviour. It is also investigating whether peer effects differ for cyber and traditional criminal behaviour. This project is looking to identify whether this is true also for cyber offenders, building on initial evidence suggesting that cyber criminals tend to have more cybercriminal social ties than non-offenders. It aims to address some methodological issues of previous research by employing more reliable longitudinal methodologies and obtaining direct measures of peer offending behaviours, rather than just measuring perceptions.

The research included young people in the Netherlands, with survey data collected in 3 waves. Online surveys examine self-reported cybercriminal behaviour of a high-risk sample of juveniles and young adults (aged 12-23) together with those of respondents' social peers. It will distinguish between online and offline social peers. As a result, it will explore the extent of any causal relationship between social ties (either traditional or online) and cybercriminal behaviour. The longitudinal aspect will help to distinguish between peer influence and peer selection as shifting social relationships (and changes in self-reported behaviour) are explored over time.

Policy implications: The findings from this research have relevance to the Home Office's 'cyber prevent' theme in that it will help to build the evidence base around understanding cyber offenders and the factors that influence cyber offending behaviour. This in turn will help to inform policymakers and law enforcement on how interventions should be designed to target these factors and prevent young people from becoming involved in cybercrime.

Methods: Longitudinal study including online surveys

Funders: Home Office

Addressing Cybersecurity and Cybercrime Via a Co-Evolutionary Approach to Reducing Human-Related Risks (ACCEPT)

Dates: April 2017 – December 2020

Lead researcher: Professor Shujun Li, *University of Kent*

Overview: How can we enhance the effectiveness and efficiency of the cyber threat intelligence collection process from people? How can we help people to be more informed about cyber threats and behave more securely?

A holistic framework is needed to guide system designers and to engage users to develop real-world systems to address these questions. This project has involved two use cases:

- A case study on location privacy involved a survey of existing privacy scales and discovered a simpler way to combine all scales with a much smaller number of questions. The research team conducted a large panel survey and identified four typical user segments with different privacy attitudes, which can be used for personalised behavioural nudging. The hypothesis being tested here is that this will change the users' behaviour positively, making them more willing to report, and over time their reports become more accurate as their knowledge about cyber-attacks improves.
- Building on an existing security incident reporting system, the second case study involves creating a reporting software system which could turn a cumbersome experience into an intuitive one generating accurate and actionable data. By making the reporting process lighter, explicit and user-centric, the proposed design will not only prompt the user to report in the 'right' way but put the control over any identifiable and linkable personal data in their hands.

The framework developed as part of this project is intended to contribute towards improving online safety for many different kinds of users from different sectors, including the policy community, industry and the wider public.

Two software prototypes for the case studies described here have been produced and will be tested in further user studies.

Policy implications: The research team may look to explore potential avenues for collaboration with NCSC and DCMS, such as co-producing and publish policy or guidance documents that advise data consumers not just about the benefits of using the tool, but also what they should look for in the data it generates

Methods: Construction of a cybercrime ontology as the theoretical foundation. Use of empirical studies (surveys and behaviour monitoring via a mobile app) to collect evidence.

Find out more: https://accept.cyber.kent.ac.uk/

Funders: EPSRC

External collaborators: British Transport Police, Crossword Cybersecurity, Europol, HAT Community Foundation, Highways England, South East Regional Organised Crime Unit, IBM, Lloyds Banking Group, Metropolitan Police, NCC group, Neighbourhood and Home Watch Network, International Union of Railways, Surrey Police, Sussex Police.

Follow on work: One of the new use cases led to collaboration with another EPSRC project 'PriVELT' (EP/R033749/1) which is ongoing. Details can be found at https://privelt.ac.uk/

Cyber Security Across the Lifespan (CSALSA)

Dates: February 2017 – September 2020

Lead researchers: Professor Adam Joinson, *University of Bath*

Overview: The experience and understanding of cyber security is not the same for everyone. This project looked to address the fundamental challenge of how we can more fully understand a diverse range of cyber security experiences, attitudes and behaviours in order to design better, more effective cyber security services and educational materials. It considered how cyber security is understood by people over the course of their lives, and how that changing understanding relates to their risk and behaviour. People's attitudes and behaviours towards cyber security and risk change across the lifespan in sync with their goals and aspirations, cognitive abilities and knowledge and ability to control and adapt their cyber security behaviour.

The research included interviews with families to explore how they manage cyber security in their homes, and highlighted the management of cyber security as an evolving process of negotiation. While parents stated that managing family security in the digital age brought new challenges, they recognised similar challenges to previous generations, including 'stranger danger' and chain letters, where the principle is the same, but the medium is different.

Communications on cyber security might benefit from a reflection on this project finding – namely, that different groups have varied ways of defining cyber security terms. To this end, the research team produced a dictionary of key cyber security terms which reflects the terms most commonly understood and used by teenagers, working age adults and older adults. However, this variance is still not well understood.

Policy implications: This work found that the meaning of cyber security differs substantially between young people, those of working age, and older adults. This has implications for policy makers working on the national cyber security agenda because training and education materials might not have the impact they could if they are not recognised by people as being of concern. For example, the work established the ways that older adults communicate and receive information about cyber security and identified potential issues for the ways that government may wish to send out information targeted at older adults.

Communications on cyber security therefore need to address the finding that different groups have varied ways of defining cyber security terms.

Project findings have been communicated to the Home Office Cybercrime Unit and the DCMS Secure by Design Team.

Methods: Literature review, experiments, qualitative interviews with software developments

Find out more:
https://researchportal.bath.ac.uk/en/projects/cyber-security-across-the-lifespan-csalsa

Funders: EPSRC

External collaborators: NCSC, BAE Systems, HP Research Laboratories.

Evaluating Criminal Transactional Methods in Cyberspace as Understood in an International Context

Dates: October 2018 – May 2020

Lead researchers: R.V. Gundur, *Flinders University, Australia*, Michael Levi, *Cardiff University*, Volkan Topalli, *Georgia State University,* Marie Ouellet, *Georgia State University*, Maria Stolyarova, Lennon Yao-Chung Chang, *Monash University, Australia* and Diego Domínguez Mejía, *Flinders University.*

Overview: This project explored what is currently known about the financial transactions that cybercriminals carry out amongst themselves, and what they demand and receive from their victims. It provided an overview of the state of play in the countries of interest through five linguistic searches: in English, Russian, Chinese, Spanish, and French. For each of the five languages, the research team surveyed the organisations, structures and policies that are relevant to financial aspects of cybercrime and conducted a systematic review of the relevant literature.

The literature review examined the processes and attributes of cybercriminal acts and what is known about the actors behind them, and the specific financial strategies employed to facilitate and benefit from profit-generating crimes. Authors prioritised examinations of the victim-facing parts of crimes. They described how attacks happen: the vulnerabilities attackers exploit and processes behind how crimes unfold, in broad terms. Many claims within the grey literature were found to lack methodological rigour, making the asserted facts difficult to verify.

Most existing research focuses on developed economies and markets, leaving a significant gap in understanding as to how cybercrime affects rapidly expanding internet markets in developing economies and their users. There is an unequal representation of concerns from the developing world, likely due to a lack of capacity or transparency. The findings, to be published in due course, explore further evidence needs in this space.

Methods: Surveyed over 500 documents across five languages

Policy implications: This project has developed a typology of economic ecosystems and transaction types that cybercriminals use, to understand transactions in reference to cybercrime. It has identified products and services that cybercriminals leverage to transact value and it shows how cybercriminals access these products and deploy them. This is relevant to policy and law enforcement development in Cyber Prevent, as well as disruption. These findings, to be published in due course, explore further evidence needs in this space.

Find out more: Research articles in development

Funders: Home Office

Victims of Computer Misuse Crime

Dates: September 2018 – April 2020

Lead researchers: Professor Mark Button, Dr Lisa Sugiura, Dean Blackbourn, Dr David Shepherd, Dr Richard Kapend and Dr Victoria Wang, *University of Portsmouth*

Overview: This work had three broad aims:

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

The findings showed that most victims regard computer misuse crime as an equivalent crime to traditional crimes like burglary, with some considering it more serious, and a small minority regarding it as a lesser crime. The research demonstrated victims experience many of the impacts that other crime victims experience, with some overlap with fraud, including financial, psychological and emotional, health related, and reputational impacts. The research explored how individuals fell victim, which included being tricked by sophisticated social engineering, and illustrated that while some victims had poor security behaviours putting them at greater risk, some fell victim despite having good security procedures in place. Victims generally did not make major changes to their cyber security behaviour after falling victim.

Policy implications: The report made 12 recommendations to specific policy audiences. They include a number of suggestions around round the roles and responsibilities of Action Fraud, (including renaming it to the 'National Fraud and Cybercrime Reporting Centre'), how Action Fraud works with NCSC, and resources and schemes provided by Government and law enforcement to tackle computer misuse crime.

Methods: Literature Review, Website analysis, 8 stakeholder interviews, 52 victim interviews and a survey of 252 victims.

Find out more: Executive Summary, University of Portsmouth.

Funders: Home Office, Her Majesty's Inspectorate of Constabulary, Fire and Rescue Services.

Connecting Delayed Pre-commitment with Cyber Awareness in Order to Address the Perception Gap and Present Bias

Dates: January 2019 – March 2020

Lead researchers: Dr Anna Cartwright, *Coventry University*

Overview: This project investigated measures designed to improve cyber security behaviour in small organisations (with less than 50 employees). The primary aim of the project was to explore the potential for cyber security health-checks, coupled with a simple behavioural intervention (or 'nudge'), to improve cyber security behaviour in small organisations, built around the NCSC small business guide.

After the health-check, an intervention was trialled to help overcome procrastination, and participants were surveyed before and after the health check about cyber behaviour in their organization. This allowed for exploration of the effect of the health-check and intervention. A typology of small business behaviour was also developed to explore how amenable businesses might be to cyber advice and the adoption of behavioural tools to overcome procrastination.

Methods: Interviews with a range of parties - including Cyber Protect officers, cyber security experts, small business and charity owners and managers. Data analysis from the Cyber Security Breaches Survey.

Find out more: https://cyberprotect.our.dmu.ac.uk/

Funders: Home Office

External collaborators: Home Office, NCSC, Kent Police, Leicestershire Police.

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

Dates: August 2017 – January 2020

Lead researchers: Professor Helen Sharp, Professor Arosha Bandara, Dr Tamara Lopez, Dr Thein T Tun, *The Open University*, Professor Mark Levine, *Lancaster University*, Professor Bashar Nuseibeh, *The Open University* and *Lero*

Overview: The initial aim of this project was to investigate the role of developer motivation in the production of secure code. The project focused on developers who are not security experts. Specifically, it set out to 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.
- Guidelines for creating and propagating a security culture across software teams

Software developers, including programmers, testers, designers or product managers, typically make hundreds of decisions every day. Very few of those decisions have security implications. It is vital that developers spot security-relevant decisions as they are encountered, have a clear sense of when security is needed for different kinds of development tasks, and work in the right conditions to be able to act.

The Motivating Jenny project set out to understand how to develop more secure software. Rather than trying to motivate developers, this work found it is more important to sensitise developers to where security decisions are needed. For code to be more secure, developers need to learn how to recognise that security is needed and to apply the knowledge they have from awareness and skills training within the specific situations.

To achieve this, the research team identified four interventions and produced supporting packs for developers to adopt and adapt, which were developed with practitioners. There are four activity packages with clear instructions, freely downloadable from the website. The desired outcome of these activities is that teams of developers are empowered to develop more secure software.

Policy implications: This work identified a new way to tackle the problem of incentivising developer security: rather than focusing on motivating developers or providing incentives to improve security, it is better to focus on creating the environment and support for developers to apply the knowledge they gain through education and training.

Developers need to know when and how to apply the knowledge they have gained through education and training, so having knowledge is not enough. The practitioner packs produced within this project, with input from practitioners, support communities of developers to share and build on each other's experience and sensitise developers and build competencies to improve security. The project has provided both empirical evidence for this phenomenon and practical resources to achieve the change needed.

Methods: Ethnography underpinned all studies: in-situ observations, workshops, interviews, presentations at practitioner events, online forums, online questionnaires. Analysis through computer-mediated discourse analysis, motivation theory, situated learning.

Find out more: https://motivatingjenny.org/

Funders: RISCS

External collaborators: Support from NCSC and RISCS. Industrial collaborators: Workforce Software Systems; Oliver Wyman; Simply Business. International collaborators: Samsung labs, Brazil; UFSCAR, Brazil; Sapient, India.

Follow on work: The project underpinned the development of an EPSRC-funded project focusing on resilience and automation, funded until 2023: https://tinyurl.com/motivatingjenny

Economical, Psychological and Societal Impact of Ransomware (EMPHASIS)

Dates: April 2017 – December 2019

Lead researchers: Professor Eerke Boiten, *De Montfort University*, Professor David Wall, *University of Leeds*, Dr Stephen McGough, *University of Newcastle,* Professor Thomas Chen, *City, University of London*, Professor Julio Hernandez-Castro and Dr Budi Arief, *University of Kent*, Dr Anna Cartwright, *Coventry University*

Overview: This project investigated why ransomware (a type of malware which restricts access to a victim's computing resources and demands a ransom in order to restore access) is so effective as a crime and why so many people fall victim to it. It investigated who is carrying out the attacks, how to assist police agencies, and what interventions are required to mitigate the impact of these attacks. The project's main goal was to strengthen society's resistance to ransomware to make it less effective, protect and prepare potential victims - whether organisations or citizens, and help law enforcement pursue the criminals.

Policy implications: The project identified novel ways to detect a ransomware attack. The typical approach for detecting ransomware is by measuring statistical values of files in a target system or device but the researchers found that relying on this approach is not sufficient. This project combined typical detection methods with others in order to provide a better confidence that a ransomware attack is taking place, while minimising the false positives. They also considered using machine learning techniques for identifying new strains of ransomware through analysis of activity within a computer system. As with all forms of protection, access to information is a vital tool.

Although ransomware criminals are often keen to provide contact to themselves, for the purpose of facilitating the payment of ransom, there is a strong reluctance for victims to seek information from other channels, including those that may provide information about how to avoid payment. Providing mechanisms to help victims access pertinent information in this context is therefore essential.

The insight gained into this project informed policy development and discussions regarding information security management and cybercrime

Methods: Meetings with law enforcement organisations, evidence for policy review, and membership of advisory boards.

Find out more: The project blog is available at https://www.emphasis.ac.uk/

One of the team was a member of the HMIC-FRS external reference group cyber-dependent crime which produced the report: "Cyber: Keep the light on - An inspection of the police response to cyber-dependent crime". The report recommended that by 1 November 2020, the current police structure for the response to cyber-dependent crime should be revised. In doing so they should consider: the creation of a national police cyber-dependent crime network; the remit of any such network, how the network engages with other law enforcement agencies; and the tasking and co-ordinating responsibilities that will be required for the network to be effective.

Funders: EPSRC

External collaborators: National Crime Agency, Dun Laoghaire Institute of Art, Design & Technology, British Telecommunications Plc, University of Melbourne.

Follow on work: Connecting delayed pre-commitment with cyber awareness in order to address the perception gap and present bias.

Investigative Interviewing of Cybercrime Victims to Gain Best Evidence

Dates: February 2019 – December 2019

Lead researchers: Professor Eerke Boiten, *De Montfort University*

Overview: The aim of this project was to improve police interviews with victims of cybercrime. There was a range of evidence available regarding best practice in terms of how police can best interview traditional crime victims but interviewing of cybercrime victims differs from other types of crime. For example, there is a need to elicit technical information regarding the crime and the potential impacts on victim cognitive function and memory retrieval from use of digital devices. The work built understanding of the types of interviews with victims being conducted by law enforcement, how they are conducted, the challenges interviewers face, and how they could be improved.

This was intended to be achieved by:

- Exploring current practices and procedures and the cybercrime technology underpinning police interviews with victims of cybercrime in the UK.
- Identifying ways of improving the investigative interviewing of victims of cybercrime. This will include developing an interviewing protocol/guide and or/ training material taking into account insights from previous research, outcomes of the exploration of interviewing practices, and technological developments in malware and other cybercrime.
- Assessing the use of complex interviewing techniques, such as cognitive interviews, in cybercrime cases.

Funders: Home Office

Gentle Interventions for Security (GIFS)

Dates: November 2018 – November 2019

Lead Researchers: Dr Emily Collins, *Cardiff University* and Dr Joanne Hinds, *University of Bath*

Overview: Users are still at the centre of cyber security and are responsible for making a large number of security related decisions on a daily basis, despite a lack of understanding of the risks involved. Drawing from the literature and theoretical frameworks surrounding habit formation in health-related behaviours and from successful ambient "nudge" interventions in the areas of work-breaks and health, this project aimed to explore the potential for ambient displays (such as small, desktop light boxes) to gently encourage more secure habits in workplace office contexts at times tied specifically to the behaviour in question.

The project took a user centred approach, by conducting interviews which allowed the team to identify which cyber security behaviours to focus on, and how ambient displays could be useful for those behaviours.

The project aims were to:

- Identify how security behaviours could be encouraged or discouraged through ambient displays.
- Identify the most effective ambient features to use in such interventions.
- Develop an ambient display in line with this research and;
- Evaluate the effectiveness of such a display on security behaviours.

Policy implications: The findings are relevant to Problem 4 in the NCSC's sociotechnical problem book: 'How can security contribute positively to an organisation's culture?' In particular, the need to support people to behave securely in line with their values and the culture of their environment to help mitigate risks and support more secure ways of working. This project also contributes to broader understanding about how to better protect people and businesses against cybercrime.

Methods: User interviews, participatory design workshops, ambient display design, experimental testing.

Find out more: Contact the lead researcher, Dr Emily Collins, for more information at: collinse6@cardiff.ac.uk

Funders: Home Office

External collaborators: Dr Sarah Wiseman, Creative Technologist, Goldsmiths University of London.

Follow on work: The findings from this work are being integrated into larger projects exploring more broadly how ambient displays can be adapted for different cyber security behaviours and for different contexts.

Publications: One paper is currently under review with several others in preparation.

Evaluating Cyber Security Evidence for Policy Advice (ECSEPA)

Dates: October 2017 – October 2019

Lead researchers: Professor Madeline Carr, *UCL* and Professor Siraj Shaikh, *Coventry University*

Overview: Cyber security is considered a Tier One risk to National Security. Civil servants across Government are working on policy advice for cyber security - but what evidence do these policymakers rely on? What is the quality of that evidence? How effective are the judgements about threats, risks, mitigation and consequences based on that evidence?

ECSEPA was designed to provide support for the cyber security policy community. A mapping exercise identified exactly where cyber security policy development is taking place across Government, and what evidence is used in their decision-making processes. Policy crisis games brought together cyber security policymakers from across Government to build a picture of how cyber security policy recommendations are made. Finally, research on how civil servants working on cyber security policy use evidence led to the development of an evidence quality assessment model (EQAM) - designed as a first step towards a tool for policymakers to assess the effectiveness of the evidence they use in cyber security decision making.

Policy implications: Recognising that policymakers often use a limited range of evidence, the EQAM is a proposed method for policymakers, specifically civil servants who provide short- and long-term policy advice on cyber security, to measure the quality of evidence they use. The model is a simple two-dimensional map that positions evidence samples relative to each other based on two dimensions of evidence quality: source and credibility. The vertical axis captures the split in evidence sources between data and human sources. The horizontal axis expresses credibility based on the methodology and provider. For example, the vertical axis could place the value of data sources over the value of human sources in establishing the quality of evidence. Credibility is judged on a case-by-case basis (such as methods used and the evidence provider). The use of such a model could improve the quality of cyber security decision making, through the discussions around the use and quality of evidence it could prompt. The researchers are seeking input from senior policy stakeholders for further validation of the model.

The map provides a visualization of the complex, rapidly developing UK cyber security policy landscape. It is available for policymakers to download and edit to keep the information up to date.

Methods: Policy crisis games, design and testing of an Evidence Quality Assessment Model, mapping exercise.

Find out more:

- Project briefing: https://www.riscs.org.uk/new-riscs-policy-briefing-a-framework-to-assess-evidence-quality-in-cyber-security-policy-making/

Funders: EPSRC.

External collaborators: This project was supported by GCHQ/NCSC throughout, including through participation in the policy crisis games.

Follow on work: Findings from ECSEPA around the quality of evidence used in relation to cyber security and the experience of the policy crisis games have been taken forwards to the ongoing Cyber Readiness for Boards project.

Detecting and Preventing Mass Marketing Fraud (DAPM)

Dates: July 2016 – August 2018

Lead researchers: Professor Monica Whitty and Professor Tom Sorell, *University of Warwick*, Professor Awais Rashid, *University of Lancaster*, Professor Angela Sasse, *UCL*

Overview: This project developed novel techniques to detect and prevent online mass marketing fraud (MMF), a major and growing problem that generates significant social anxiety and psychological impact. MMF is a serious, complex and organised crime. Examples include foreign lotteries, advance-fee scams and romance scams. More effective prevention and detection techniques and strategies are needed to tackle this crime. To address this need, the project involved detecting assumed identities and persuasive messaging used by fraudsters and the factors leading to poor decision making by victims.

The project included academic and non-academic partners from law enforcement, regulatory bodies, industry, the third sector and citizens.

It provided insights into the psychological and technical factors that lead to poor decision-making by existing and prospective victims of such frauds to develop tools and techniques. These can form the basis of practical interventions in tackling such fraud. Ethical issues were also investigated.

Policy implications: This project developed algorithms, guidelines and practices that organisations can use to counter fraud. The research with project partners in law enforcement and intelligence agencies in different countries aimed to help them with in identifying fraudulent online content, tracing criminals and collecting appropriate forensic evidence to help increase chances of successful prosecution. The research publications also detail the ethical and social constraints involved in automated methods to prevent MMF and suggests considerations for using automated systems.

Methods: Algorithm development, global mapping of victims and fraudsters, development of victim typology.

Funders: EPSRC, ESRC

External collaborators: Federal Trade Commission, Barclays Bank plc, United Kingdom, Royal Canadian Mounted Police, City of London Police, the Australian Competition & Consumer Commission, CIFAS, Hampshire County Council, My Mate Your Date, Fraud Help Desk (Netherlands), Western Australian Police, Fraud Women's Network, Scamalytics, Online Dating Association.

Supporting Data Security and Privacy in the Home

Dates: Completed May 2018.

Lead researchers: Professor Ivan Flechais, *University of Oxford*

Overview: This project investigated social relationships and their role in home data security. It involved an exploration of how people make decisions based on 50 semi-structured interviews with UK home users that focused on security decision-making.

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

Policy implications: This work helped to uncover some of the motivations behind the prevalence of informal technical support. It highlighted the importance of targeting people who help others when crafting an intervention targeting home users and this has particular relevance for the NCSC and for Government departments focused on consumer security.

Methods: Interviews, surveys, grounded theory

Funders: RISCS

Follow on work: This project laid the foundation for a follow-on project funded by the Information Commissioner's Office, called "Informing the future of data protection by design and by default in smart homes". This project aimed to understand and investigate user needs related to how smart home devices handle, process and use personal data during their operation. In assessing this, the project sought to identify ways for devices to manage data more responsibly in the future. The work included a longitudinal study of smart home device use, in order to explore the usability, security, and privacy aspects of communal devices. Interviews were held with employees of a large UK-based smart home company to identify priorities and needs. The project then began the prototyping and field deployment of technology probes to explore new data protection approaches and concepts. Based on the results of this work, the researchers proposed user-centred design guidelines and recommendations to improve data protection in smart homes.

The findings of this study are available on a paper about the future of data protection by design and by default in smart homes: http://www.cs.ox.ac.uk/files/11860/casestudy-chi2020.pdf

Developer Security Essentials – The Magid Project

Dates: October 2017 – April 2018

Lead researchers: Dr Charles Weir, *Lancaster University*

Overview: Some software development teams are highly effective at delivering security, but others are not – which can be due to lack of care or expertise. This work proposed that a series of lightweight interventions (six hours of facilitated workshops delivered over three months) can improve a team's motivation to consider security and awareness of assurance techniques and change its security culture even when no security experts are involved.

Interventions were developed by surveying security professionals, followed by testing in three different organisations. These have now been delivered to many more, ranging from a security-focused government team to a single-programmer team in a small company. The research team worked with more than 90 programmers, testers, project managers, and product managers and in each case, there were identifiable and sustained improvements in security-related activities of the team involved.

The researchers have produced 'Security Essentials' – a half-day set of structured workshops to inspire and guide developers on security. This is available from the website linked below.

Policy implications: This work highlighted the importance of the relationship between developers and the product management function in every organisation. Further work will focus on this relationship and ways to improve the effectiveness of this dialogue in improving security.

Lightweight, facilitation-based interventions of the kind reported here offer the potential to help software development teams with limited current security skills to improve the security of their products. Wide scale adoption of programs of this kind will empower developers and play a much-needed role in improving software security for all end users. This may be relevant to the DCMS Incentives and Regulation programme of work.

Methods: Appreciative Inquiry and Grounded Theory survey of security professionals, Participatory Action Research study

Funders: RISCS, Lancaster University

Find out more: https://www.securedevelopment.org/

Impact of Gamification on Developer-Centred Security

Dates: November 2017 – March 2018

Lead researchers: Dr Manuel Maarek, *Heriott Watt University*.

Overview: The research investigated if serious games (games for which entertainment is not the main purpose) can help developers build more secure software. Results from the prototype game indicated that it did steer participants into focusing more on the security perspectives of their coding.

Policy implications: An EPSRC-funded follow-on project currently underway is looking to evaluate the approach of serious games for developer security as a result of these findings. It aims to produce a framework for creating serious games, a set of creative components and software components for secure coding as well as a series of games to teach secure coding to new coders. The research team plan to share these outputs with policy makers to advocate for the adoption of more secure software development practices.

Methods: Surveys.

Funders: RISCS

Find out more: The researchers created an online platform experiment for a coding-based game to engage and support developers with secure coding practices. It is available at: https://www.macs.hw.ac.uk/games-dcs/

External collaborators: Glasgow School of Art

Follow on work: EPSRC Funded project. Serious Coding: A Game Approach to Security for The New Code-Citizens: https://tinyurl.com/impactofgamification

Visualising Access Control Policies

Dates: December 2016 – January 2017

Lead researchers: Dr Charles Morrisett, David Sanchez, *Newcastle University*

Overview: Security practitioners have to maintain access control policies, sometimes with hundreds of rules, which may be misconfigured or have to be periodically updated. They are difficult to read, even to the technically trained eye. This work investigated how to make such complex policies easier to understand at a glance.

The researchers developed a tool 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. VisABAC presents a way to visually overview an access control policy, by disclosing details on demand and exploring policies graphically.

Users who tested the tool largely found it intuitive and easy to use, although they remarked that some training could have improved their response time. This experiment also showed that such a tool could be used to pass on the ability to understand access control policies to non-technical people.

The level of contribution VisABAC could provide to access control experts was not clear from this small study alone, but the work was intended to pave the way towards a larger scale experiment. It could result in fewer errors that leave networks vulnerable and is promising for authoring and editing access control policies.

Methods: Prototype design and surveys.

Funders: NCSC

Find out more: https://gitlab.com/morisset/visabac

Choice Architecture for Information Security

Dates: February 2013 – December 2016

Lead researchers: Professor Aad Van Moorsel, *Newcastle University*

Overview: This project sought to understand how people make decisions regarding their security and privacy, by examining the psychological factors involved in decision-making. The work identified nudging techniques that influence human behaviours. This finding can be useful in information security, as it will aim to modifying or changing individuals' behaviours that compromise their company's privacy and cyber security, instead of forcing more and more rigid security policies on employees.

The research team published an approach for practitioners to discuss and introduce nudges in design of privacy and security tools, based on the MINDSPACE framework of influences on behaviour change (such as the messenger and incentives). The approach, SCENE, is a co-creation based on five stages involving stakeholders: (i) Scenario elicitation; (ii) Co-creating nudges; (iii) Election of nudge(s) for further development; (iv) Nudge prototyping and (v) Evaluation of prototype(s). During these five stages, a nudge intervention is developed and evaluated. The framework acknowledges the role that users increasingly play in the security decision making process.

Policy implications: The proposed tool could help practitioners and academics to develop a strong evidence base for different interventions while being practical for organisations. It may be useful for policymakers looking at trade-offs between organisational security and practicality. The findings link to the DCMS area of research interest to: "evaluate what drives organisations' cyber security practices. This includes how to influence organisations to take action to protect themselves, identifying which actors to drive behaviour change, how decisions are made, and what information organisations would find useful in assessing risks and taking investment decisions."

Methods: Development of choice architecture, stealth tools and prototypes for the nudge intervention, evaluation.

Funders: EPSRC

External collaborators: Metropolitan Police

Follow on work: EPSRC Funded project (EP/R033595/1) FinTrust: Trust Engineering for the Financial Industry, which runs until July 2022.

Cyber Security Cartographies (CySeCa)

Dates: November 2012 – December 2016

Lead researchers: Professor Lizzie Coles-Kemp, *Royal Holloway*

Overview: Prior to this project, little research had been undertaken to understand how a security manager selects the appropriate control combination for cyber security in organisations. Risk management techniques do not include visualisation methods that can present a combined picture of organisational and technical asset compliance behaviours. This problem is exacerbated by the lack of systematic research of the cultural and organisational techniques used by organisations to protect their information.

This paucity of research results in limited practical guidance on cultural and organisational security management approaches.

The project goals were to:

- Explore how a security manager develops, maintains and uses visibility of both organisational and asset compliance behaviours for the management of cyber security risks;
- Better understand how organisational controls and technical controls are used in combination;
- Evaluate the use of different visualisations in the risk management process as a means to extend a security manager's ability to deploy combinations of organisational and technical controls in the cyber context.

The project involved the development of a storyboard approach called "Current Experience Comic Strip" which has enabled security practitioners to document and reflect upon how organisational controls are selected and maintained. A narrative method for gathering people's day to day experiences of using security technologies enabled participants to explore how security policies might be re-designed and shortened to improve their effectiveness.

The visualisations also provide a means for auditors and assessors to compare the compliance behaviours of two organisations.

Policy implications: This work informed NCSC thinking on cyber security skills sets (see link below). The 'Current Experience Comic Strip' were used in three sites at a Central Government Department to identify security practices. It is now referenced as one of the engagement mechanisms in the National Cyber Security Centre's engagement guidance.

Applying a human-centred perspective and design elicitation techniques, the team worked with frontline staff and security experts in the Department of Work and Pensions to identify new forms of secure data sharing needed to support service delivery

Methods: Social network analysis, applying and developing anomaly detection techniques at the technical asset cluster level and integrating interpretive cartography with informational cartography.

Funders: GCHQ, EPSRC

Find out more: https://www.ncsc.gov.uk/blog-post/origin-stories

Games and Abstraction

Dates: January 2013 – June 2016

Lead researchers: Professor Chris Hankin, *Imperial College London*; Professor Pasquale Malacaria, *QMUL*; and Professor Carlos Cid, *Royal Holloway*

Overview: This project aimed to develop new techniques to support human decision making and enable well-founded security design decisions to be made. In particular, it supported professionals and systems administrators who are designing secure systems to optimise the use of their limited resources in defending systems against commodity style attacks. The system is designed to assume no technical knowledge of cyber security on the part of the user, but rather asks them to supply information about their organisation and its requirements and preferences. It enabled a precise analysis to provide a more robust decision support tool than pre-existing work.

A prototype web tool that gives advice to users about the implementation of their cyber defences was developed during this project. The web tool is being developed further in a subsequent EPSRC-funded project (see below).

Policy implications: The research team have engaged with companies to explore possible commercialisation of the tools. The follow on project involves case studies of prototype tools initiated in this work, and this ongoing project is expected to produce a tool which could be commercialised. This may have relevance to NCSC programmes of work on supporting businesses to be secure.

Methods: Theoretical, interviews with local systems administrators.

Funders: EPSRC and NCSC

External collaborators: CESG (now part of NCSC).

Follow on work: EPSRC funded project EP/R002983/1 titled: Customized and Adaptive approach for Optimal Cybersecurity Investment (until August 2022). This research builds on the Games and Abstraction project to help organisations to make better cyber security investment decisions. For example, in a given organisation is it better to prioritise a policy of changing passwords over patching software regularly? And how frequently should passwords be changed? Should all employees scan for malware all USB sticks?

Productive Security – Improving Security Compliance and Productivity Through Measurement

Dates: October 2012 – June 2016

Lead researchers: Professor Angela Sasse, *Ruhr University Bochum*, Professor David Pym *UCL*

Overview: There has been a growing body of evidence that security policies and controls are not effective because employees either can't or won't comply. A key reason for non-compliance is the workload and complexity of security controls chosen - employees simply cannot cope with an ever-increasing number of long, complex passwords. Yet most security decision-makers do not factor the impact on employees, their tasks, and the company's business processes, into their decision about which security controls to put in place. Current attempts to 'educate' employees about the need for security are largely ineffective because they simply push more information on people who are already overworked. Even in organisations with a high security awareness, non-compliance can be observed because security policies cause excessive friction or are not agile enough to meet the needs of the business.

The project team worked primarily with two large companies to conduct empirical research on how security and security behaviours fit within the work day. This provided the companies with a catalogue of their security mechanisms and the employee effort associated with them, and a survey tool and set of organisation-specific scenarios for measuring their employees' security attitudes and likely behaviour.

The work improved employees' understanding of organisational risks, the role of security controls, and how their behaviour can prevent or facilitate security breaches. Engaging directly with employees to understand their perception of security in their jobs and the workplace resulted in a number of findings. These included indications that training should maintain relevance as the organisation changes and employees change roles, and that organisations should have a consistent approach to communicating security awareness.

Policy implications: The research findings were used by NCSC to promote the adoption of usable security policies and measures, and engaging staff in security. This included their 2015 Password Guidance: Simplifying Your Approach which guides system owners and service providers toward taking more responsibility for protecting accounts, rather than putting all workload on end-users. The new advice is: don't impose long passwords, complex rules or frequent changes on users. In 2018, the NCSC changed its Guidance on how to effectively combat phishing which also incorporated findings from the Productive Security project.

This project, alongside the CySeCa project and work by The Centre for Research and Evidence on Security Threats (Crest) on Security Dialogues informed the NCSC 'You Shape Security' guidance collection. https://www.ncsc.gov.uk/collection/you-shape-security.

Methods: Interviews and custom surveys to directly engage employees on policies where there are compliance issues. They developed methods and tools to measure the impact of security controls on employees and further determine how well they fit with business processes and employees' tasks.

Find out more: RISCS, Hewlett Packard Enterprise (HPE) and NCSC published a white paper encouraging organisations to engage employees in order to improve cyber security, co-authored by Productive Security researchers Professor Angela Sasse and Dr Simon Parkin. Available here: https://www.riscs.org.uk/wp-content/uploads/2015/12/Awareness-is-Only-the-First-Step.pdf

Funders: EPSRC

External collaborators: Hewlett Packard Enterprise (HPE)

Follow on work: The Cyber Readiness for Boards project builds on the outcomes of this work.