ANNUAL REPORT 2022/23

RISCS Research Institute for Sociotechnical Cyber Security

CONTENTS

FOREWORD

The Research Institute for Sociotechnical Cyber Security is the oldest of the NCSC's Research Institutes. Since its inception in 2012, it has acted as a trailblazer in building a community of experts to tackle some of the most challenging problems we face in making the UK one of the safest places in the world to live and do business online.

As such, RISCS has had a significant impact not only in reframing cyber security as essentially multidisciplinary in nature, but also as a template for the success of our other Research Institutes – VeTSS, RISE, and RITICS.

I am therefore delighted to welcome Professor Genevieve Liveley and the University Bristol as the new Director and host institution for RISCS. Their bid provided a vision and strategy which we believe will not only build on the legacy of RISCS but will continue to drive the development of sociotechnical thinking in cyber security.

Finally, I would like to place on record the NCSC's gratitude and appreciation for the work of University College London and all the previous Directors of RISCS, who have provided such a strong foundation for sociotechnical security.

Paul Waller
Head of Capability Research, NCSC

The Research Institute for Sociotechnical Cyber Security (RISCS) is funded by the National Cyber Security Centre (NCSC) and hosted at the University of Bristol.

RISCS is the UK's first academic research institute to focus on understanding the overall cyber security of organisations, including their constituent technologies, people, and processes.

RISCS takes an evidence-led and interdisciplinary approach to addressing these sociotechnical cyber security challenges. By providing a platform for the exchange of ideas, problems, and research solutions between academia, industry, and the policy community, RISCS promotes and supports world-leading, multidisciplinary, and scientifically robust research into sociotechnical approaches to cyber security.

INTRODUCTION

Having worked in the Sociotechnical and Risk Group within NCSC for the last three years, I have been lucky to work extensively with RISCS on a series of projects, primarily focused on economics and incentives.

This year, however, I have been privileged to take over as the NCSC Lead for RISCS and it has given me a greater appreciation of the breadth and depth of research and impact RISCS delivers as a truly multidisciplinary institute.

During this year, the RISCS Fellows have continued to produce fantastic outputs across the range of their themes.

To focus somewhat unfairly on just one of the Fellows, I have been fortunate enough to work directly with Dr Tim Stevens on the International Dimensions theme over the last few months. Tim’s excellent work and that of the other Fellows illustrates the benefits that this type of thinking can provide to the wider ecosystem of cyber security.

I am therefore delighted that RISCS will be continuing the Fellowships and is planning to expand these internationally.

At the same time, RISCS has continued to fund innovative sociotechnical projects focused on national priorities which will help keep the UK safe online. The current RUSI/Kent project on Cyber Insurance and Ransomware continues this tradition; helping to address important knowledge gaps identified as research priorities by the National Cyber Strategy in 2022.

This year has been one of transition for RISCS, with the institute moving from its original home at University College London to the University of Bristol.

I would like to acknowledge the hard work, dedication, and leadership of Dr Tristan Caulfield and his team at UCL, which has enabled RISCS to continue delivering through its Fellowships, Community, and Projects throughout this period.

At the same time, I am excited to be working with Professor Genevieve Liveley and Dr Louise Evans on RISCS in its new home at the University of Bristol.

They have bold and ambitious plans for RISCS to engage, influence, and collaborate with stakeholders across the cyber security landscape in domestic and international partnerships with academia, government, and industry. I am looking forward to helping them realise these plans in collaboration with all of you.

I would like to acknowledge the hard work, dedication, and leadership of Dr Tristan Caulfield and his team at UCL

I am particularly enthused by the focus on connecting RISCS with the general public and the NGO sector, as I am by the focus on involving early career researchers in academia with RISCS and identifying opportunities to work with NCSC's other Research Institutes: RITICS, RISE, VeTSS, and the Alan Turing Institute.

I believe that this is all in keeping with core RISCS strengths of innovation, collaboration, and a focus on nurturing the diverse ecosystem of skills, individuals, and backgrounds that will be critical to addressing the cyber security challenges of the future.

John W5,
Sociotechnical Research Lead,
Sociotechnical and Risk Group, NCSC

DIRECTOR'S MESSAGE

It's been both a pleasure and a privilege to have been part of the RISCS family for the past three years as a Fellow, and so I'm absolutely delighted to be following in the footsteps of former RISCS Directors Tristan Caulfield, Madeline Carr, and Angela Sasse, as I now step into this role. As the University of Bristol becomes the new home of RISCS, I want to mark this new tenure by paying my warmest tribute to the extraordinary contribution to the cyber security ecosystem made by each of these Directors and their teams: UCL is going to be a tough act to follow!

In this new phase for RISCS we want to continue and to build on the excellent work that UCL has already delivered. The Bristol vision for RISCS is to further grow this vibrant interdisciplinary hub providing thought-leadership and practical support for a diverse, dynamic, and world-leading community, drawing together experts from academia, industry, and policy with shared expertise and interest in the human-centred understanding of cyber security (yes – this means you!).

Our approach is based upon the understanding that world-leading and scientifically robust research into the unfolding interactions between people, processes, and technology in cyber security demands an integrated, multidisciplinary dialogue.

In this context, we see researchers in the arts and humanities as particularly important interlocutors to bring into the conversation, as these disciplines study what it means to be human and so provide key insights into the sociotechnical dynamics that allow our security interventions to succeed or falter.

Our commitment to deep interdisciplinarity extends beyond academia and we see the 'real world' expertise of industry and community groups as foundational to the success of the RISCS research programme. We will be using the talent represented by our Fellows alongside wider business, community, and policy stakeholders to debate critical questions on the sociotechnical conditions of cyber security as we work to shape the future research agenda in this space.

> “
>
> **Our commitment to deep interdisciplinarity extends beyond academia and we see the 'real world' expertise of industry and community groups as foundational to the success of the RISCS research programme.**

Through our activities and engagements over the next three years, then, we are aiming to develop a rich intellectual synthesis that can be used to identify new capabilities, emerging points of intervention, and pathways to impact. Our core methodology for this next phase in the lifecycle of RISCS is accordingly supported by four pillars:

1. growing national capability and expertise in sociotechnical cyber security (across academia and industry);
2. uniting, developing and nurturing the community of researchers involved in this area (including early career researchers and industry stakeholders);
3. framing the core research questions and future strategies for this area (in collaboration with key stakeholders, including local communities);
4. shaping the future of human-centred research and policy-development in cyber security (with NCSC and policy makers).

I am very much looking forward to this exciting new phase for RISCS and to working with you all.

Genevieve Liveley, *RISCS Director*

We see RISCS as a driver for the ESRC's five types of change:

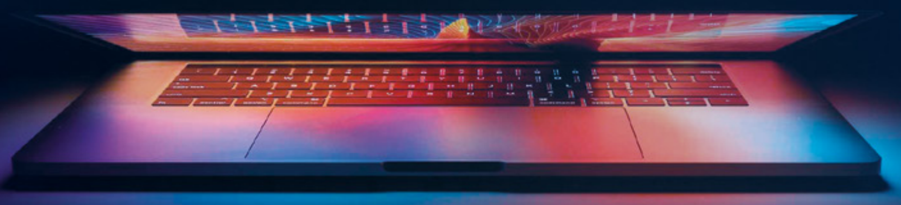
INSTRUMENTAL
changes to plans, decisions, behaviours, practices, actions, policies

CONCEPTUAL
changes to knowledge, awareness, attitudes, or emotions

CAPACITY
changes to skills and expertise

CULTURAL/ATTITUDINAL
towards knowledge exchange and research itself

CONNECTIVITY
changes to the number and quality of relationships and trust



NCSC'S SOCIOTECHNICAL AND RISK GROUP (StRG)

While there have been exciting changes at RISCS over the last few months, welcoming our new Director, Professor Genevieve Liveley at the University of Bristol, at NCSC we have also been going through some changes of our own.

Many of you will likely have got to know us over the last few years, either through our collaboration with RISCS or other avenues such as the Sociotechnical Security Group (StSG) – a multi-disciplinary team in NCSC developing sociotechnical approaches for cyber security.

While StSG has delivered some great outcomes as part of NCSC's mission to make the UK the safest place to live and work online, we decided late last year there was an opportunity for greater impact in the future by combining risk more visibly with our sociotechnical expertise.

Sociotechnical and risk are certainly two distinct disciplines (and cyber risk management as a skillset and profession is well established across teams in NCSC), but there is a real synergy between the two.

How to improve current cyber risk management practices to ensure we are able to manage effectively the complex risk picture in cyber security has long been an established part of the work of StSG and also RISCS, through research themes such as Cyber Risk Quantification and Leadership and Culture.

As such, this is very much an evolution of the shape and identity of the team rather than a dramatic change. However, bringing together some of our NCSC risk consultants (with their deep cyber risk expertise and experience of working closely with a broad range of critical customers and sectors) with our sociotechnical specialists gives us the opportunity to collaborate as individuals, as a team, and across disciplines.

This is very much an evolution of the shape and identity of the team rather than a dramatic change.

It also offers us the opportunity to be more effective in solving the challenges we face in cyber security now and in the future. And so, the new Sociotechnical and Risk Group was formed!

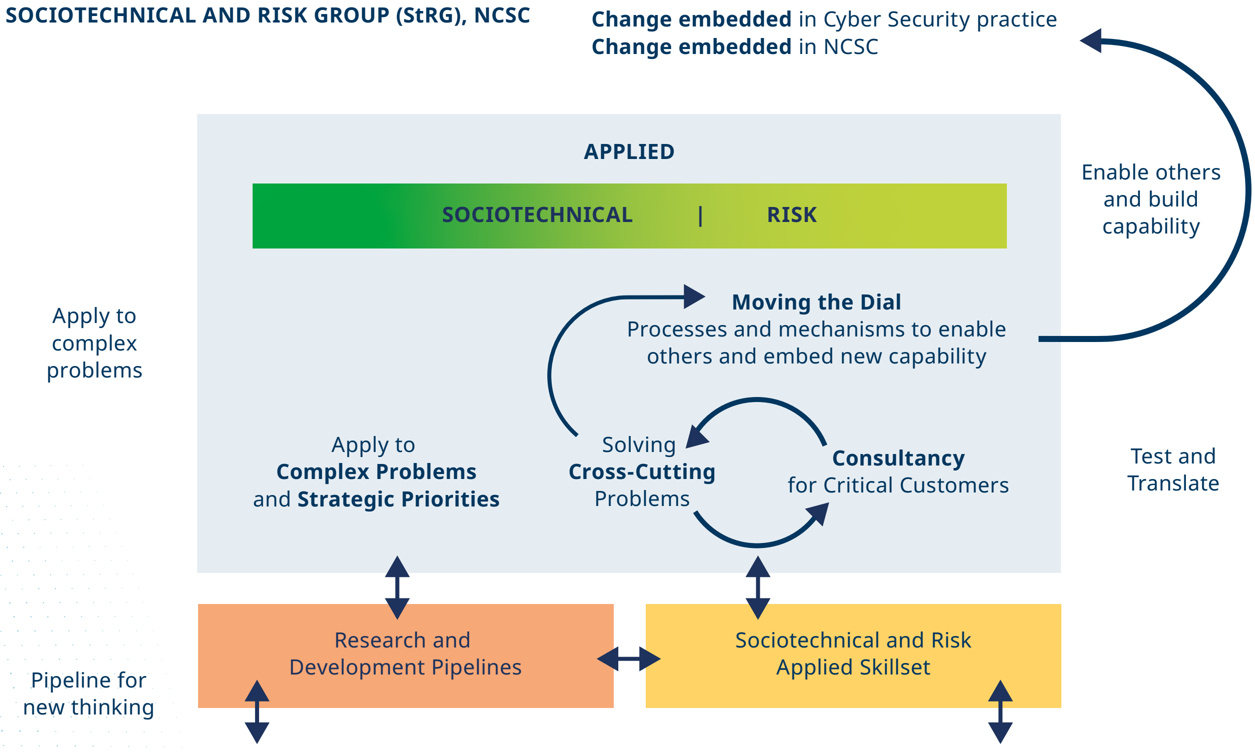
While we are still in the early stages of evolving into the Sociotechnical and Risk Group, there are a range of ways we work and engage with stakeholders, projects, and challenges across NCSC and further afield.

We work with critical customers to provide sociotechnical and risk expertise and consultancy. Our aim is to use this experience and engagement to identify and find ways of solving cross-cutting problems that show up across customers, sectors, and areas of cyber security so that, as well as engaging one-to-one with customers, we can test out new approaches to solving problems for the many wherever possible. When we have developed new approaches or thinking to tackle novel and complex problems, we seek to enable others and build sociotechnical and risk capability in sustainable and scalable ways.

And it is equally true for us now as the newly-formed Sociotechnical and Risk Group as it was for StSG that we cannot achieve our aims alone. Our relationship with RISCS and the opportunity to collaborate with colleagues from academia, industry, and government, to bring together a diversity of minds, expertise, and cutting-edge thinking, is critical.

So, as we welcome Genevieve as the new Director of RISCS, on behalf of the Sociotechnical and Risk Group (or StRG – it may take a while to adjust to our new acronym!) I look forward to exploring the opportunities of a closer alignment between risk and sociotechnical and am excited to collaborate on delivering even greater impact in the future.

Anna G,
Head of Sociotechnical and Risk, NCSC


SOCIOTECHNICAL AND RISK GROUP (StRG), NCSC
Change embedded in Cyber Security practice
Change embedded in NCSC
APPLIED
SOCIOTECHNICAL | RISK
Enable others and build capability
Moving the Dial
Processes and mechanisms to enable others and embed new capability
Apply to complex problems
Apply to **Complex Problems** and **Strategic Priorities**
Solving **Cross-Cutting** Problems
Consultancy for Critical Customers
Test and Translate
Research and Development Pipelines
Sociotechnical and Risk Applied Skillset
Pipeline for new thinking

ADVISORY BOARD MESSAGE

Co-chaired by Dr Jason Nurse and Dr Emma Moreton, the new RISCS Advisory Board and Peer Review College consists of members from key stakeholder groups in industry, government, and academia.

The core mission of the Advisory Board is to advise on the strategic priorities of the Institute, as well as to support the activities of the RISCS research community and to maximise the impact of our work. The Institute's commitment to deep interdisciplinarity sees the 'real world' expertise of industry and community groups as foundational to its research programme.

Accordingly, the Advisory Board and Peer Review College members will be asked to advise on:

1. growing national capability and expertise in sociotechnical cyber security
2. supporting the community of researchers involved in this area
3. framing core research questions and future strategic priorities in policy for this area
4. reviewing and providing 'critical friend' feedback on research activity

LOOKING AHEAD

We will never have an equation for the human feeling of security. There are certainly mathematical and technical aspects of the discipline. We would be lost trying to do cryptography without the mathematical advances of the last 50 years (since Diffie Hellman and DES). The specific work the CHERI project is doing to reduce exploitability is likely going to change the game.

But we still have to grapple with human beings who write code. And as the RISCS 'Motivating Jenny' project illuminated, there are opportunities to think about personal motivation and a culture of security.

And even if human beings write less code *(note: don't miss Matt Welch's provocative 'End of Programming' in the January Communications of the ACM https://tinyurl.com/EndOfProgramming)* they will still be specifying requirements, checking systems, dealing with the edge cases, and otherwise creating systems.

We will never have an equation for the human feeling of security.

We are going to see new specialties emerge. I have already seen the phrase 'professional prompt engineer' used to refer to people who are skilled at asking ChatGPT or DALL-E good questions. To be direct: calling that 'engineering' or a 'profession' prompted some strong reactions from me, but our editor has taken them out.

Thinking about the future of the field led me to ask: 'What should every engineer know about security?'

The practice of security reviewers hoping to stop a moving production line is not working, and that means we need to start building security in. That will require more security engineers, and more security knowledge from non-specialist engineers.

Awais Rashid and company have done useful work in the CyBoK project and, in a similar way, I have recently released a book, *Threats: What Every Engineer Should Learn From Star Wars*, which is the result of a hypothesis that threats – the things we worry about – are essential to how we conceptualize security, and that a good grounding in threats will be tremendously helpful to every engineer.

It is a serious book in a silly Trojan horse. But the wrapping, drawing readers in, is an essential part of what writers do.

We do it in ways that signal our audience. I name mine on the cover and using LaTeX signals in a different way.

I want to go back to the Trojan horse analogy, which I do not use in the book – not even when discussing the Millennium Falcon being brought into the Death Star.

Stories are a part of how we learn, as are analogies. And so, we can augment the technical lessons about security with human stories – including classical ones.

In my case, I aim to draw in engineers because there is competition for their attention. If we make it more accessible and fun to learn about security, we are more likely to succeed. Lizzie Coles-Kemp has demonstrated a similar point using Lego Bricks.

And so, developing a sociotechnical science of security will enable us to build the systems that underlie a future we want to live in. I am excited to be a part of the next phase.

Adam Shostack,
RISCS Advisory Board Member

POLICY FOCUS

In 2021, the UK Government published its National Cyber Strategy, which sets out how, with over £2.6 billion of funding, the UK will cement its position as a responsible and democratic cyber power, able to protect and promote its interests in and through cyberspace.
The Strategy was designed to be adaptive and responsive to a fast-changing digital environment.

Whilst we may have a good understanding of how cyber threats manifest in the UK economy now, we will not have the same quality of understanding in the future unless we are prepared to keep measuring, monitoring, and analysing the changing landscape.

Developing the evidence base for cyber interventions is a key part of the Department for Science, Innovation and Technology's work. Without the right evidence base, the Government cannot ensure its policy interventions are the right ones or assess their impact.

Our research and analytical work includes understanding how cyber attacks affect companies through the *Cyber Breaches Survey* and looking at the shortage of cyber skills through the *Cyber Security Skills in the UK Labour Market Survey.* We also have a dedicated team that works across Government, academia, and external experts to anticipate and assess technology developments most vital to our cyber power.

> **Whilst we may have a good understanding of how cyber threats manifest in the UK economy now, we will not have the same quality of understanding in the future unless we are prepared to keep measuring, monitoring, and analysing the changing landscape.**

What RISCS is doing will be crucial to meeting the ambitions laid out in the National Cyber Strategy. Novel and high quality research, and bringing together a broad range of unique stakeholders, will be critical in making the UK the safest place to be online, in enabling us to capitalise on the opportunities, and in solving the challenges of cyber security. I look forward to the research the individuals at RISCS will be working on in the coming year.

Irfan Hermani,
Department for Science, Innovation and Technology, and RISCS Advisory Board Member

RISCS COLLABORATIONS

The RISCS community has always thrived upon its collaborations. In the coming year, we will be identifying new synergies with NCSC's other Research Institutes – RITICS, RISE, and VeTSS. We will also be pursuing opportunities to work more closely with the Alan Turing Institute, REPHRAIN, SPRITE+, the Centre for Sociodigital Futures (CenSoF), and the new Institute for Digital Security and Behaviour.

In this context, we are looking forward to supporting The National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online (REPHRAIN) in their campaign to promote a 'capability approach' to protecting citizens online.

Our commitment to deep interdisciplinarity extends beyond academia and we see the 'real world' expertise of industry and community groups as foundational to the success of the RISCS research programme. We will be using the talent represented by our Fellows alongside wider business, community, and policy stakeholders to debate critical questions on the sociotechnical conditions of cyber security as we work to shape the future research agenda in this space.

As researchers and practitioners in cyber security, we have a moral obligation to design and develop protection mechanisms for everyone – irrespective of their personal, social, economic and political realities.

People differ in their health, ability, and education – and can also be in vulnerable situations, displaced from their homes, or living under oppressive regimes. This lived reality negatively affects marginalized and vulnerable individuals in their ability to engage with digital systems and to protect themselves from the exploitation that data collection and aggregation can facilitate.

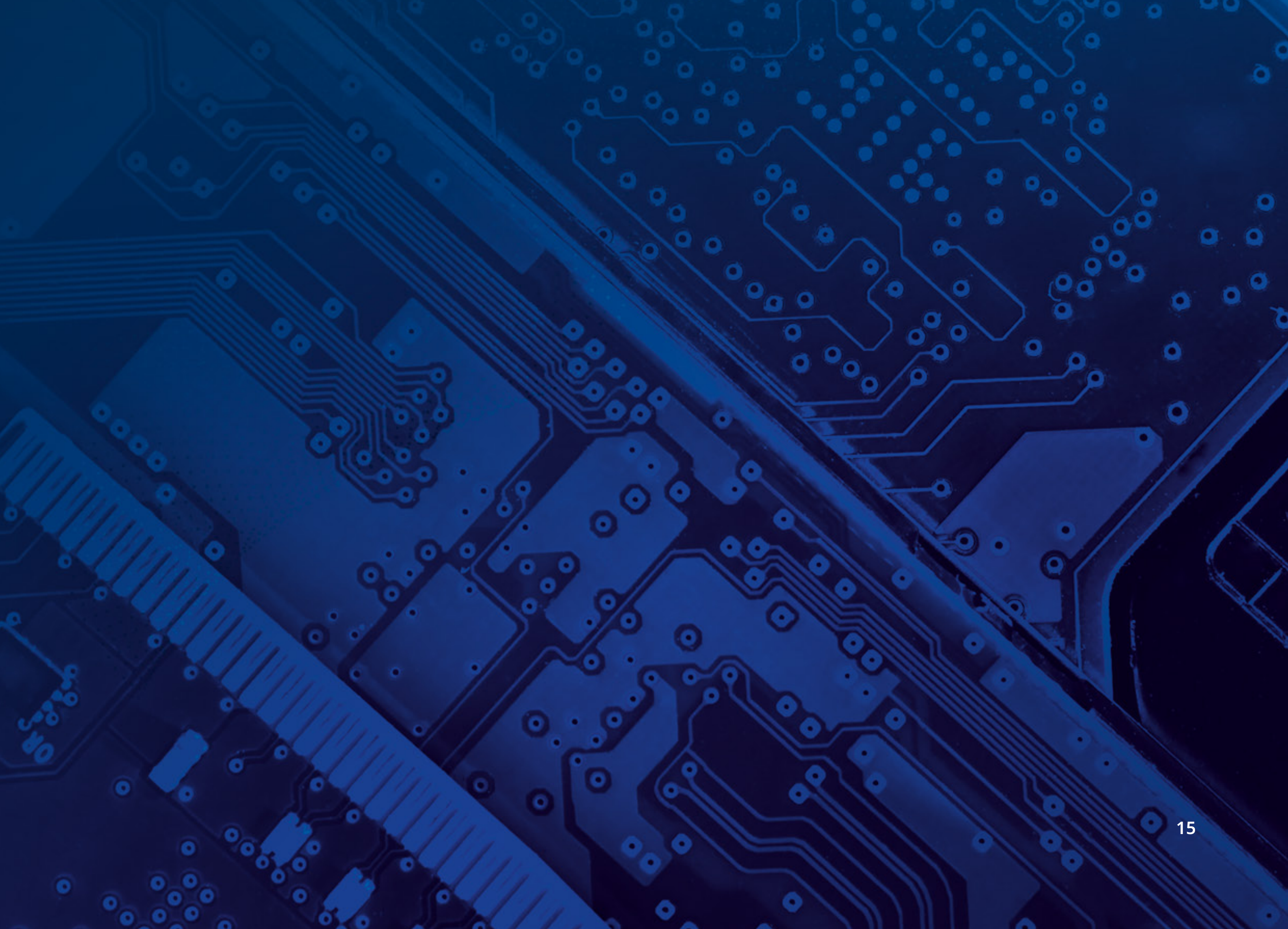
As researchers and practitioners in cyber security, we have a moral obligation to design and develop protection mechanisms for everyone – irrespective of their personal, social, economic and political realities. Socioeconomically disadvantaged groups and individuals in vulnerable situations too often find it difficult to make use of technologies to their advantage and can end up becoming victims of a pervasive digital push.

The usable security community has made a strong case for putting humans at the heart of systems design. REPHRAIN asks us all to consider a wider question – *‘What opportunities do people have to use and adopt protection mechanisms?’* Addressing this question entails moving beyond issues of the usability of protection mechanisms.

It requires us to build a deeper understanding of the personal, social, economic, and political circumstances of those individuals we intend to protect. This calls for a paradigm shift in the way we understand humans at the other end of technology. And by use of the term ‘humans’ we propose to go beyond the narrow formulations of ‘user’ – recognising that there are also involuntary participants, bystanders, and implicated actors in the digital world. We propose the adoption of a ‘capability approach’ as a foundation to develop protection mechanisms for citizens in a digital first society.

Partha Das Chowdhury, *REPHRAIN*

Read the REPHRAIN Manifesto in full: https://tinyurl.com/REPHRAIN-Manifesto



RISCS PRINCIPAL AND SENIOR FELLOWSHIPS FOR 2023

The RISCS Principal and Senior Fellowships for 2023 will be focused on the following five themes:

1. Digital Responsibility

This overarching theme is fundamental to the success of cyber security: unless we consider digital security as a reciprocal arrangement where the needs of all parties are supported, security responsibilities can become one-sided, leading to an erosion of trust in technology and diminishing the benefits and take-up of technological approaches. Our focus on Digital Responsibility will help us to build a more positive and healthy relationship with digital technology and advise on ways to use it that minimise harm and help to increase the benefits for all. As we digitise and connect more of our products and services, we need to be as digitally inclusive and equitable as possible – with the goal that no member or section of society is left behind. As we work to ensure that everyone becomes more cyber secure, we will be asking: Under what conditions can security technologies effectively support the discharge and ascription of digital responsibilities? How can we ensure reciprocity and inclusivity, and raise the bar for responsible cyber security across the UK?

Lizzie Coles-Kemp
Royal Holloway, University of London, RISCS Principal Fellow

2. Cybercrime

Understanding how people behave, both individually and in groups, and across different parts of the cyber security ecosystem, is a priority for the cyber security research community. This includes understanding people whose intentions are non-malicious and who simply want to do a good job, as well as the intentions, drivers, and behaviours of those who have more malicious aspirations, and those who inadvertently find themselves acting as 'accidental insiders'. This research theme will help to guide the RISCS community towards new insights into understanding both the perpetrator and the victim, exploring topics such as insider threat, online harms, and supporting victims of cybercrime.

Maria Bada
Queen Mary University of London, RISCS Senior Fellow

3. Futures Literacy

In a world characterised by high levels of volatility, uncertainty, complexity, and ambiguity, it is more important than ever that we equip ourselves with robust strategies to help the cyber security community understand as well as communicate risk and resilience. Whether it is assessing the risk of moving proprietary data to the Cloud, considering the potential impacts of emerging technology on current and future industry, or designing trusted automated products, it is critical that cyber security is informed by rigorous futures thinking. ‘Futures Literacy’ is the practical capability that enables us to do this kind of thinking well, and to use strategic foresight to take informed action in the present. By supporting the RISCS community to become futures literate, this theme will help us all to make more effective decisions as we assess risk and prepare for a range of possible futures.

Will Slocombe
University of Liverpool, RISCS Senior Fellow

4. International Relations

Most of the cyber security challenges we face, as well as the opportunities we have to address those challenges, have important international dimensions. States compete for power and influence in cyberspace through diverse economic, military, and intelligence means. They seek advantage through direct strategic competition and by exploiting the opportunities of international diplomacy and trade. Companies are integrated into complex transnational supply chains and a global cyber security market that thrives on innovation but struggles to keep pace with dynamic and agile cyber threats. Considerations of how to balance national priorities against a complex international cybersecurity landscape, while still keeping human beings at the centre of decision-making, is a major challenge which this theme will help to address.

Tim Stevens
King’s College London, RISCS Senior Fellow

5. Quantification and Cyber Risk

The body of knowledge around cyber risk quantification has been growing in recent years as people seek methods to introduce more repeatability and objectivity to their risk management processes and to frame cyber risk in terms that stakeholders care about. Yet there are barriers to the wider adoption of quantification in cyber security: misconceptions about what cyber risk quantification is; lack of accessible tools and resources; lack of knowledge of good practice and how best to integrate quantification into a wider risk management process; and the risk of poor implementation of quantification driving perverse behaviours. As we work to increase understanding of cyber risk quantification, we will be asking: How do we enable the cyber security community to use quantification to best effect in understanding cyber risk and enabling effective cyber security decision-making? Can quantification play a role in bridging the gap between cyber risk and other areas of risk such as safety?

Anna Cartwright
Oxford Brookes University, RISCS Senior Fellow

RISCS PROJECT IMPACT & ENGAGEMENT TRACKER

Selected recent highlights from the impact and engagement activities carried out under the auspices of RISCS and by RISCS Fellows include:

Jamie MacColl participated in a panel on ransomware at the Home Office Security and Policing Conference

Jason Nurse spoke at the Ransomware Resilience Summit Europe in 2022: *https://tinyurl.com/RRS-2022*

Maria Bada spoke about *'How to protect societies from ransomware cyberattacks'* as part of a panel presentation at the Chatham House *'Strengthening Cyber Resilience Conference'*

Will Slocombe and **Genevieve Liveley** presented on *'Securing the Future(s): Creative Futuring for UK Defence and Security'* to an international audience of academics, policymakers, and strategic foresight experts as part of the 2022 Anticipation Conference.

Anna Cartwright held two policy workshops: the first on '*Optimising the use of UK Government survey data on cyber security'; the second 'Informing policy with cyber security data: Optimising use of UK government survey data on cyber security'*

Under the auspices of the Digital Responsibilities theme, **Lizzie Coles-Kemp** published a paper on *'Protecting the Vulnerable: Dimensions of Assisted Digital Access'* Coles-Kemp, L, Robinson, N & Heath, CPR 2022, Protecting the Vulnerable: Dimensions of Assisted Digital Access. in Proceedings of the Human-Computer Interaction Conference. ACM. *https://doi.org/10.1145/3555647*

DIGITAL RESPONSIBILITY THEME UPDATE

This report sets out the findings of the first phase of the RISCS digital responsibility research programme. Led by Lizzie Coles-Kemp, RISCS Research Fellow for Digital Responsibility, the first phase of this research programme sought to set out what digital responsibility is, to explore its relationship to both cyber and digital security, and to sketch a framework that further supports the establishment of digital responsibility.

We started the fellowship by undertaking two consultation activities: a four-week reading group and a townhall meeting. The consultation activities enabled us to identify what digital responsibility is and what the main barriers are to achieving it. The four-week reading group programme enabled participants to take part in a weekly discussion about an academic paper on a key aspect of digital responsibility.

Digital technology disrupts and reforms the sense of obligation and duty that the state, organisations, and individuals have towards each other.

The economics markets underpinning digital product and services have a strong influence in determining digital responsibility.

The second activity was a townhall-style workshop focused on the practice of digital responsibility. The discussions from the reading group highlighted that digital responsibilities are subject to constant negotiation and that digital technology disrupts and reforms the sense of obligation and duty that the state, organisations, and individuals have towards each other.

The discussions also tentatively concluded that digital technology is designed in such a way that such duties and obligations are typically pushed onto the end user of a technology – the point at which responsibility pushback is least effective.

The townhall consultation revealed the breadth and the complexity of digital responsibility, showing that the establishment, assignment, and discharge of obligations and duties takes place in both the design of digital technologies and in their use – and that the economics markets underpinning digital product and services have a strong influence in determining digital responsibility.

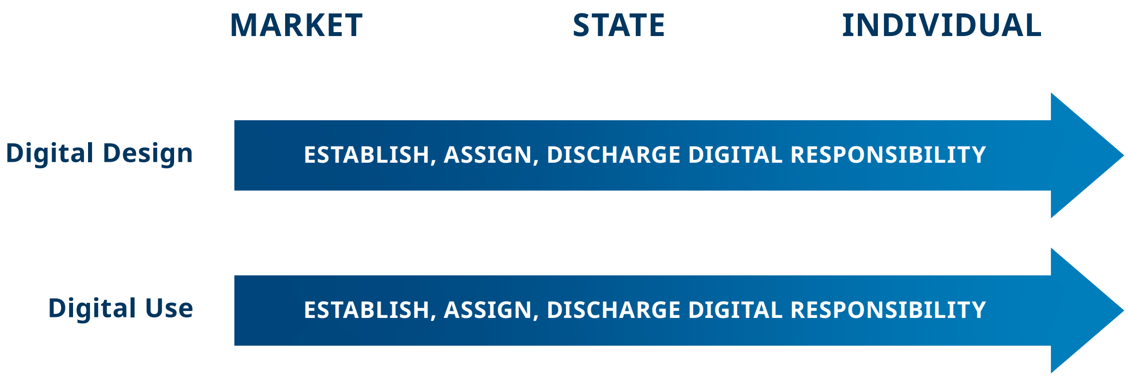

MARKET
STATE
INDIVIDUAL
Digital Design
ESTABLISH, ASSIGN, DISCHARGE DIGITAL RESPONSIBILITY
Digital Use
ESTABLISH, ASSIGN, DISCHARGE DIGITAL RESPONSIBILITY

Figure: A simple schema of digital responsibility

Our diagram illustrates two realms, digital technology design and digital use, as two areas of activity where digital responsibilities are determined. This determination can be broken down into the following three phases: established, assigned, and discharged.

Our research shows that in the UK the markets/technology companies, the state, and the individual are the main parties involved in the determination of digital responsibility. To study the roles of these parties in more detail we have produced three pieces of analysis that reflect on the ways that digital responsibilities can be shaped through interaction between the markets, the state, and the individual. In this work we have looked at what happens when collaboration between the parties breaks down or is ineffective.

We have also examined how digital responsibilities cannot be fully established without engagement both from the institutions designing and implementing digital products and from the individuals and communities using them.

Our research shows that in the UK the markets/technology companies, the state, and the individual are the main parties involved in the determination of digital responsibility.

In our first piece of analysis, we use the prism of the UK government debate about online harms to examine how the markets, state, and individuals interact in the establishment, assignation, and discharge of digital responsibilities.

In the second piece of analysis, we look at digital responsibility through the example of how one part of the Kurdish diaspora engaged with the UK census where response was digital by default. In this work, we look at the roles that individuals and communities play in the establishment of digital responsibilities and how political systems shape such establishment.

> **Digital responsibilities cannot be fully established without engagement both from the institutions designing and implementing digital products and from the individuals and communities using them.**

In the third piece of analysis, we look at digital inclusion as a digital responsibility and examine how third sector organisations discharge their duties and obligations surrounding digital inclusion as part of their humanitarian support for refugees.

Combined, these analyses reveal the constellations of interest in digital responsibility, the realms of activity in which digital responsibility is primarily discharged, and how these two aspects of digital responsibility interact.

In Phase two of RISCS's Digital Responsibility Programme, we shall model the relationships between the three main parties involved in the determination of digital responsibilities and use the models to evaluate how and under what conditions these parties might more closely collaborate in the determination of digital responsibilities.

Professor Lizzie Coles-Kemp,
RISCS Principal Fellow

INTERNATIONAL RELATIONS THEME UPDATE

The International Relations theme will continue to bring together academic, industry, and practitioners to discuss key dimensions of international cyber security, particularly as they relate to the UK and its partners. In 2022, we published the outcomes of a high-level workshop on the implications of European Union cyber policy for the UK. In 2023, we plan to address the role of offensive cyber operations in UK defence and security, in order to inform government decision-making in this important area of national strategy.

We will also continue to raise awareness of international cyber security as a critical field of research, policy, and practice.

Dr Tim Stevens,
RISCS Senior Fellow

FUTURES LITERACY THEME UPDATE

The aim of the Futures Literacy theme is to improve the RISCS community's understanding of the relationship between futures thinking, risk, and cyber security.

Resilient cyber security frameworks demand the capacity to anticipate the probability of future threats (in terms of both their nature and potential impact) so as to successfully develop mitigation and defense strategies.

In 2022, Will Slocombe (Co-Director of the Olaf Stapledon Centre for Speculative Futures at the University of Liverpool) joined the team for this theme and collaborated with dstl for a joint presentation at the biennial 'Anticipation' conference, to discuss ways of 'Securing the Future(s): Creative Futuring for UK Defence and Security' with an international audience of academics, policymakers, and strategic foresight experts.

Will now takes over from Genevieve as Senior Fellow for this theme, and, as the Sociotechnical Security Group at NCSC evolves into the Sociotechnical and Risk Group (StRG), he will continue to investigate the best future tools and approaches needed to understand and to communicate risk.

Over the course of 2023 this theme will work to further develop expertise in this exciting research area, to map best practice, and to build both capacity and community among those interested and involved in strategic futures and security.

Dr Will Slocombe,
RISCS Senior Fellow

QUANTIFICATION AND CYBER RISK THEME UPDATE

The Quantification and Cyber Risk theme has three broad objectives to explore:

How do we integrate quantification into a wider risk management process?

How do we overcome the challenges and enable the cyber security community to use quantification to best effect in understanding cyber risk and enabling effective cyber security decision-making?

Can quantification play a role in bridging the gap between cyber risk and other areas of risk such as safety?

To speak to the objectives of the theme, we undertook two complementary strands of work:

- Optimising the use of UK Government survey data on cyber security
- Cyber risk management in UK businesses

Optimising the use of UK Government survey data on cyber security

There is a wealth of UK Government survey data on cyber security. In this stand of work, we encouraged research that uses this data through a series of activities, including two workshops and an innovative prize competition for early career researchers. This allowed us to identify existing research and the barriers in using and accessing data on cyber security, and to explore ways of facilitating and making more efficient collaborations between policy makers, academics, and practitioners.

Cyber risk management in organisations

One project focused on micro and small organisations and the role that local IT companies can play in cascading cyber security best practices. This project involved econometric analysis of the Cyber Security Breaches Survey data alongside focus groups/interviews with experts in the field. Our findings are summarised in a paper, ‘Cascading information on best practice: cyber security risk management in micro and small businesses and the role of IT companies’, submitted for publication.

A second project focused on medium and large organisations and explored the divergence in attitudes between security-focused executives, e.g. CISOs, and business executives, e.g. CEOs. We first conducted an analysis of Cyber Security Breaches Survey data and found evidence that CEOs were significantly less likely than CISOs to say their business had been attacked in the last 12 months. To explore this issue in more detail we commissioned a survey of around 200 medium and large organisations in the UK. The results are being written up for publication in an academic journal.

Vision for 'Quantification and Cyber Risk' theme in 2023

Key priorities we would like to address in the future for this theme are:

How can we obtain accurate and reliable data so that we can quantify cyber risk? How can we quantify risk in different types of organisations, ranging from micro businesses, large businesses, charities, public sector organisations, and critical infrastructure?

How do businesses quantify cyber risk (if at all)? How can we utilise data to improve cyber risk management practices in organisations?

How can we enable sharing and accurate analysis of that data?

We will continue two strands of work: one on 'Optimising the use of UK Government survey data on cyber security' and a second on 'Cyber risk management in organisations'. An ambition going forwards is to join these strands of work together and analyse how we can improve the linkages between data on cyber security and risk management behaviour in organisations.

We plan to organise a workshop, bringing together policy makers, law enforcement, academics, and businesses, to discuss the evidence and practice of cyber risk management in UK organisations. We will also conduct and encourage further research using existing UK government data, particularly providing support to early career researchers across disciplines.

Dr Anna Cartwright,
RISCS Senior Fellow

Find out more about Anna's work on Quantification and Cyber Risk:
Cartwright, A., Cartwright, E., Xue, L. and Hernandez-Castro, J. (2022), *'An investigation of individual willingness to pay ransomware'*, Journal of Financial Crime.
https://tinyurl.com/Anna-Cartwright-1

Cartwright, A., Cartwright, E., MacColl, J., Mott, G., Turner, S., Sullivan, J. and Nurse, J.R.C. (2023) *'How Cyber-Insurance Influences the Ransomware Payment Decision: Theory and Evidence'*, The Geneva Papers on Risk and Insurance, forthcoming.

Cartwright, A. and Cartwright, E. (2023) *'The economics of ransomware attacks on integrated supply chain networks'*, ACM Digital Threats: Research and Practice, forthcoming.
https://tinyurl.com/Anna-Cartwright-2

CYBERCRIME THEME UPDATE

The aim of the RISCS fellowship on cybercrime is to:

1. Explore the impact of cybercrime in the UK from the victim's perspective, understanding the societal harms of cyber-attacks such as ransomware, including long-lasting physical, reputational, and psychological consequences on targets and victims. When cyber-attacks target national critical infrastructure, the disruption caused can have long-term consequences on the way society functions. That disruption can undermine trust in legitimate processes.
2. Explore the latest developments on emerging technologies with a particular focus on artificial intelligence and how it is being used to fight cybercrime as well as to conduct criminal activity. This aspect can shed light onto the emerging risks for victims and help understand the societal harms of cyber-attacks.

Looking to the future, work for the coming year will focus on:

- Identifying the best methods for collecting and sharing data for conducting research on cybercrime. To achieve this goal, engagement with stakeholders of all sectors is paramount.
- Understanding the needs of vulnerable groups and current practices that might lead to their victimisation online. This will help in setting guidelines and policies to enhance resilience and minimise the potential harms that can be experienced online.
- Understanding how AI can extend the scale and sophistication of cybercrime.

Dr Maria Bada,
RISCS Senior Fellow

Find out more about Maria's work on cybercrime and specifically on enhancing resilience to cyber-attacks in her CDO-KPMG paper on *'Enhancing national resilience of ransomware.'* This project was published here: *https://tinyurl.com/resilience-to-ransomware*

The project focused on developing countries in Africa, Asia, and Latin America and provided a number of recommendations for developing economies in baseline policy-making in enhancing resilience to ransomware attacks. This policy paper will provide evidence to policy-makers on the existing gaps and needs to enhance resilience to cybercrime and reduce harm, and is expected to influence future cybersecurity capacity, building projects, and policy in this area.

RANSOMWARE: THE ROLE OF CYBER INSURANCE (RACI) – RISCS PROJECT UPDATE

Led by Dr Jason Nurse (University of Kent), RaCI is a multidisciplinary research project that brings together economics and sociotechnical cyber security academics with cyber policy researchers. The Kent Team is working in collaboration with the world-renowned think tank RUSI (Royal United Services Institute) and two other UK universities, De Montfort University and Oxford Brookes University.

Ransomware is arguably the most persistent cyber threat facing organisations, society, and UK national security. RaCI focuses on one of the most contentious aspects of the public policy debate around ransomware – the role of cyber insurance. It aims to provide an assessment of the argument that cyber insurance is fuelling the ransomware business model by incentivising victims to pay ransom payments, but also to identify ways in which cyber insurance can potentially disrupt some of the drivers and enablers of ransomware. **The project also explores the implications of current so-called 'hard' market conditions for the theory that cyber insurance can act as a form of cyber security governance.**

To explore these themes, the research team conducted an extensive literature review, 65 stakeholder interviews, and a workshop. Participants came from the insurance industry, UK government, UK and international law enforcement, incident response firms, law firms, and ransomware negotiation and payment firms.

The project team is currently in process of publishing at least one academic journal article and a RUSI policy report. The RUSI report includes a series of recommendations targeted at the insurance industry and UK government. To support the publication of the RUSI report and to ensure impact among relevant stakeholders, the research team will also conduct briefings across Whitehall and with industry bodies.

Jamie MacColl, *RUSI*

Project Outputs:

- 'How Cyber-Insurance Influences the Ransomware Payment Decision: Theory and Evidence', The Geneva Papers on Risk and Insurance (forthcoming)
- 'Cyber Insurance and the Ransomware Challenge', RUSI Occasional Paper (forthcoming)
- 'Between a rock and a hard(ening) place: Cyber insurance and organisational cyber resilience in the ransomware era' (forthcoming)

MANAGER’S MESSAGE

It is with some trepidation that we take on RISCS, with its existing excellent track record in the field, but also excitement, as our plans for the Institute with a ‘Bristol flavour’ unfold. My role is to support Genevieve, the Fellows, the Advisory Board, and the many other stakeholders in delivering our RISCS vision.

In particular, I see this being enacted through engagement and translational activities, leveraging our in-house expertise at Bristol (with help from PolicyBristol, and the Public Engagement and Industrial Liaison Office) and, importantly, through a direct link into Bristol Cyber Security Group.

At the heart of our plan to build and nurture an energetic and synergetic community of expertise in sociotechnical cyber security sits our RISCS Fellowship Programme.

Expanding upon the current RISCS model, we will be coordinating four types of Fellowship:

Senior Fellows	UK-wide academic thought-leaders in the human-centred understanding of cyber security
Associate Fellows	early career researchers and the ‘rising stars’ from the sociotechnical cyber security community
Honorary Fellows	representing business, industry, and policy stakeholders
International Fellows	representing global expertise in this space

Our Fellowship programme will provide the framework through which we coordinate our research strategy, helping to forge industry-university partnerships and garnering expert input on the shaping of new research programmes and funding calls. Each Fellow will be actively engaged in research in one or more problem areas identified as a priority for NCSC and will work closely with a dedicated NCSC lead.

Our Senior Fellows are already in place for 2023 and we will be recruiting across the wider programme in the coming year.

We will keep you up-to-date on the activities and findings of our Fellows through our new website. And you can also keep in touch with us via email: contact-riscs@bristol.ac.uk

I look forward to connecting with you all through RISCS and supporting you as our activities increase throughout the year.

Louise Evans, *RISCS Manager*

RISCS
Research Institute for
Sociotechnical Cyber Security