RISCS

Annual Report 2020

Research Institute for Sociotechnical Cyber Security

Director’s Message

Professor Madeline Carr

Why RISCS matters more now than ever

2020 was certainly a year like no other. The implications of the kind of work we do at RISCS were amplified in some very tangible ways as governments raced to find technological solutions to the COVID-19 global pandemic. In a sobering display of the relevance of sociotechnical approaches, we observed how different political cultures responded to a range of ‘track and trace’ systems. In some places, there was a high level of compliance driven by a sense of social responsibility. In others, there were harsh penalties for non-compliance. Some systems generated big debates about privacy and the rights of individuals and others did not. Ultimately, the success of these systems depended only in part on engineering. Understanding how people and organisations would engage with a technological solution was really at the heart of the outcomes.

At the beginning of April 2020, a week after the first lockdown came into force, we launched five new 12-month research projects on the Economics and Incentives of Cybersecurity and five new RISCS Fellowships. We also had a newly expanded support team in place – some of whom are yet to meet one another in person. We immediately set about developing a strategy for addressing the COVID-related risks to these 10 initiatives. Not knowing what was to come or how things would unfold meant that we had to work in an extremely agile, collaborative, and creative way to ensure that everything stayed on track and that people were supported to do the great work they had signed up for. It’s important to me to take this opportunity to thank the incredible people behind what RISCS has achieved this year. This includes our management team, the leaders of the Economics and Incentives projects, the RISCS Fellows, our Advisory Board and our great colleagues in the NCSC. It was an incredibly challenging year but also a rewarding one punctuated with so much generosity, resilience, and good will. I expect everyone is looking forward to a more normal 2021 – but 2020 really showed us where our strengths lie.

There have been a lot of really exciting developments in RISCS this year that we feel situate us well for the future growth and evolution of the Institute. They include structuring our research around themes, introducing a RISCS Fellowship programme, funding work on the Economics and Incentives of Cybersecurity, restructuring our Advisory Board, and putting in place an enhanced support structure to alleviate the administrative and logistics burden on the academics who we engage with.

Structuring our work around Themes

Over the course of this year, we worked to structure our work around Research Themes which map onto the StSG Problem Book. This allows us to clearly identify where our research is making a contribution and where there are gaps that need to be addressed. We established themes for ‘Leadership and Culture’, ‘Cybercrime’, ‘Secure Development Practices’, and ‘Digital Responsibility’, to which we drew links from all of our past and existing projects. Early this year, we added a fifth research theme on ‘Anticipation and Prospection’ to help build out the emerging community of people who think to the future and try to bring structured thinking to issues of deep uncertainty – an area we explored in a workshop in 2019.

Fellowship Programme

An important element of RISCS growth and evolution has been our new Fellowship Programme. Through a competitive process, we appointed one RISCS Fellow to each of the five research themes. These people are leaders in these sub-communities and bring a depth of knowledge that will allow the themes to develop in a rigorous and innovative way. With a combination of financial and structural support from RISCS, the Fellows are building out the community interested in that particular area, they are supporting early career researchers to ensure that we have a robust succession pipeline, and they are shaping our research agenda with innovation and ambition to help us prioritise future funding calls.

Economics and Incentives Projects

Following on work we undertook in 2019 that highlighted the real imperative of bottoming out the financial drivers and impediments as well as the (dis)incentives for implementing sound cybersecurity, we held an open funding call for research that would progress this. Five projects were selected, and you can read about them in more depth in the Project Catalogue published alongside this report. Several of the research projects focused on small-medium enterprises (SMEs) and it became clear just how difficult it is to reach, engage with, and support this sector. Given the implications of SMEs for the global supply chain, how to support them to build cyber resilience is emerging as a major challenge.

Restructuring our Advisory Board

As RISCS approached the end of its five-year funding cycle, we took stock on how the Institute has changed and evolved over that period and where we feel it needs to head in the future. We've always been well supported by our Advisory Board and benefited greatly from their input and expertise. Over the course of 2020, it became apparent that harnessing that resource would be best facilitated by appointing an Advisory Board Chair. We were delighted that John Madelin agreed to take up the post and that long-time RISCS supporter and Advisory Board member, Larry Hirst, agreed to step in as Deputy Chair. John and Larry have worked extremely hard with the RISCS Manager, Esme Taylor, over the past few months, to bring in some new Advisory Board members, reshape our processes and practices and set in place an Advisory Board that will both support us and extend us through our next chapter.

Support Structures

Enabling great research that either helps to strengthen the foundations of our emerging field(s) or that produces usable findings for more immediate impact is key to RISCS purpose. Academics are increasingly asked to perform a lot of tasks that fall well outside of their area of expertise: marketing and promotions, event management, public engagement – and all of these take up time that would be more profitably spent on research and writing. To counter this in RISCS, we've worked hard this year to establish a supportive infrastructure that our research community can draw upon.

As promised last year, we've introduced a Policy Impact Officer. Flo Greatrix has made a significant difference to the extent and quality of our engagement with the UK policy community. In response to requests from the policy community, Flo has created a comprehensive Project Catalogue that documents every RISCS project, including findings, outputs and policy implications. This catalogue brings us right up to date and will now be maintained and recirculated periodically.

This comprehensive engagement with the policy community will be replicated with the business sector over 2021. In addition, we'll be focusing on developing international links so that RISCS work reaches a global audience and so that we also benefit from collaborations with like-minded colleagues around the world. There still remains so much to be done in terms of developing our understanding of the sociotechnical dimensions of cybersecurity. But if we learnt anything this year, it was that RISCS is an exceptional mechanism for bringing together the intellectual, policy and industrial resources needed to do this.

Contents

RISCS Research Themes

This year, RISCS has introduced five research themes into its sociotechnical portfolio. These hope to consolidate and embolden the scope and objectives of our work, and each have one of the RISCS Fellows as a leader. This year's Annual Report is therefore structured around the updates from each of the Fellows specific to their area of responsibility.

Theme 1: Leadership and Culture

How can an organisation position itself and what can it put in place to optimise cyber security behaviours and cyber risk decision making? What does an economics and incentives lens tell us about how organisations might be encouraged to raise their cyber security bar, and how they might go about this?

Theme 2: Cybercrime

To fully understand how we defend ourselves, we also need to understand how we might be attacked. Taking an economics and incentives lens to better understand the business models of the cybercrime ecosystem, and how cybercriminals and their victims are affected by them is an important aspect of this endeavour.

Theme 3: Secure Development

Whether it is a software system, a policy, or an organisational process that is being designed and developed, we aspire to have cyber security baked in earlier in the development process with the hope that people can build better systems in the first place and avoid repeating mistakes. But cyber security competes against many other business priorities and we do not currently have a compelling and evidence-based return on investment narrative about why investing in cyber security early is 'a good thing' for business (and not just a loss prevention exercise).

Theme 4: Digital Responsibility

As we digitise and connect more and more of our products and services, we need to be as digitally inclusive as possible so that no portion of society is left behind. We aspire to ensure that everyone becomes more cyber secure. What does an economics and incentives lens tell us from a citizen point of view? How can we ensure inclusiveness and raise the bar for cyber security across the UK?

Theme 5: Anticipation and Prospection

Anticipation is broadly defined as using the future to inform action in the present. It is the core discipline that deals with how we, as humans, reason about the future. Risk management uses reasoning about the future to inform actions and decisions in the present and, in our increasing technology and data-led society, we need to consider cyber risks amongst a complex and dynamic landscape. This theme will provide insights to improve cyber risk management going forward and draw upon the future-oriented insights generated from the fields of Psychology, Philosophy, Narratology, Anthropology, Political Science, Mathematics, the natural sciences and many others.

We have been working to extend the theme portfolio starting in April 2021. For now, we have recruited a researcher to lead on a 6th theme of International Cooperation. More information to follow shortly with other communications related to our plans for 2021/22.

RISCS Organisational Structure

RISCS Advisory Board
Chair: John Madelin
Deputy Chair: Larry Hirst

Leadership Team
Director: Madeline Carr
Technical Director: Helen L
Institute Manager: Esme Taylor

RISCS Community (Open)
Policy, Academia, Industry

Leadership & Culture
Fellow: Berta Pappenheim
NCSC Lead: Nico B

Secure Development Practices
Fellow: Shamal Faily
NCSC Lead: David K

Anticipation & Prospection
Fellow: Genevieve Liveley
NCSC Lead: Anna G

Cybercrime
Fellow: Maria Bada
NCSC Lead: Dylan L

Digital Responsibility
Fellow: Lizzie Coles-Kemp
NCSC Lead: Lee C4

International
Fellow: Tim Stevens

Policy Impact Officer
Florence Greatrix

Project Management and Events
Sarah Beech

Outreach and Engagement Officer
Patryk Wloch

Communications Update

Patryk Wloch, Outreach and Engagement Officer

For most of its existence, RISCS hasn’t been resourced to maintain high-quality outreach and engagement. The perception among the leadership team has been that this was a limiting factor. Eventually, the stars aligned, and I was recruited to lay foundations for the very first Communications Strategy of the Institute.

My time at RISCS – since I joined in June 2020 – has certainly been exciting. Indeed, my onboarding has taken place right after we have undergone a complete rebranding, including changing our name to better reflect the sociotechnical focus of our work.

New name and brand

The rebranding itself came about as part of a wider objective to strengthen our identity as an organisation. RISCS has been around for a while and is now firmly established within the broader cyber security environment. Reflecting upon who we are, and how we want to be seen, is essential for a maturing institution like us to keep moving forward.

The work undertaken at RISCS derives great value from our interdisciplinary – bringing together the *socio*- and -*technical* elements by fostering cooperation between researchers from diverse academic backgrounds. Following many conversations in early 2020, it was decided this fact was indeed central to our identity – and for every external observer to know this at first glance, we are now called **Research Institute for Sociotechnical Cyber Security**. With the new name, we have also updated our logo. While maintaining strong links to the past, this version is less *geometric* and more *organic*, which we also feel better reflects the human and organisational factors that so often run through our work.

New website

Following the rebranding, we have also worked on developing a new website. Our main objective has been to ensure information about our past and present work is easy to find and comprehensive, as well as to fully align the primary point of our online presence with the new RISCS brand. The new website also features a Research Directory, for which everyone is welcome to register – with all new entries moderated by the RISCS team to ensure high quality. The Directory is a place to look for collaborators and partners, and we are planning to work on further popularising it in the upcoming months.

The website is certainly a never-ending work in progress as we continue to improve it – please get in touch with us if there is anything you feel we could structure or present better.

Supporting the RISCS community

The primary focus of my work has been on supporting our researchers, including the PIs on our projects, as well as the first cohort of the RISCS Fellows, with whom I have worked particularly closely over recent months.

In particular, it is worth mentioning the fantastic events schedule our Fellows have run in Autumn 2020. Over just a few months, there have been more than 10 RISCS community events – from small book clubs and reading groups, to workshops, to high-profile showcases and engagements at international summits. It has been a complex task to ensure that these online events which (as everyone now knows) can get very tiring, remained engaging and appealing to the various audiences we were hoping to reach.

Every single event we have organised over the Autumn months has met and exceeded the target attendance, and the feedback we have received has been uniformly positive. You can read more about the specifics in each Fellow's respective update.

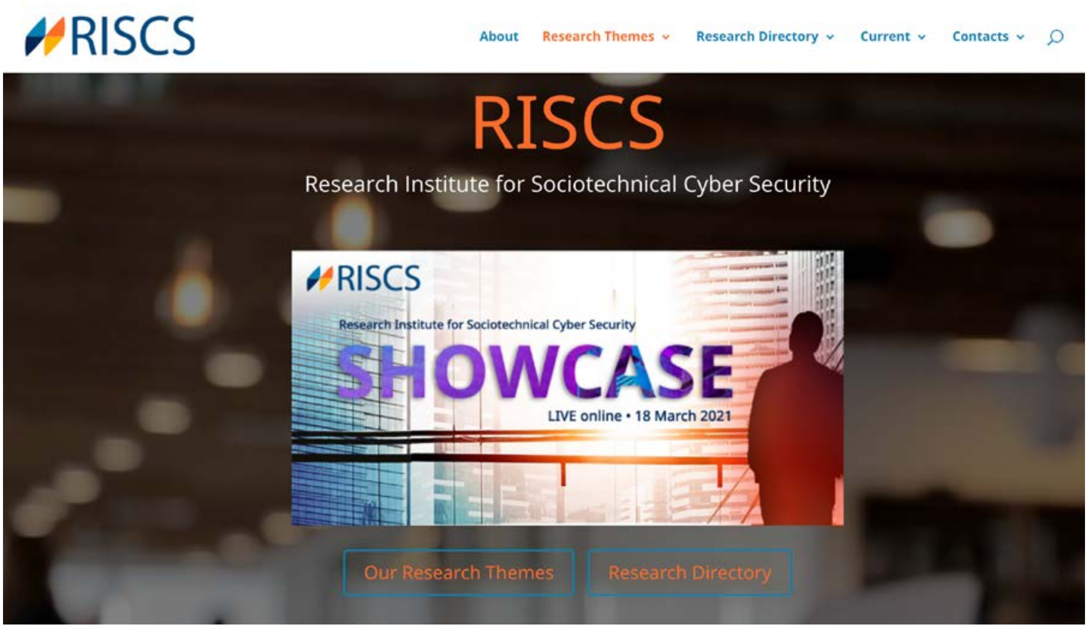
What's next?

It is clear that the new Communications support we were able to offer our community has been of value. It allowed our events and publications to reach the target audiences better; our updates to be communicated more regularly and more effectively; and finally – which is not always visible at first glance – it made a difference to how we work internally.

The next months will be particularly interesting from a Communications perspective, as the world recovers from the pandemic and slowly returns to (some of) the old ways. The key will be to utilise the opportunities we are getting back (like being able to meet in person), while remembering about what we have learned in adapting to the unprecedented circumstances we found ourselves in.

For example, we all clearly miss attending events which are not just highly elaborate Zoom calls. But it's important to note that, while challenging and fatiguing, holding events online has allowed for a wider range of participants to attend, limiting issues like the need for travel. This allowed for interactions and exchange of ideas between people who might have otherwise never found themselves in the same place, at the same time – which is what we felt was particularly valuable about this community work we did so much of. This balancing exercise will certainly be a key priority for me as I continue to improve the ways RISCS communicates with our community.

The new RISCS website


RISCS
About
Research Themes
Research Directory
Current
Contacts
RISCS
Research Institute for Sociotechnical Cyber Security
RISCS
Research Institute for Sociotechnical Cyber Security
SHOWCASE
LIVE online • 18 March 2021
Our Research Themes
Research Directory

Cybercrime Theme Report

Dr Maria Bada, RISCS Fellow

The focus of the RISCS fellowship on cybercrime over 2020 has been to:

- explore the impact of online cybercrime in the UK from the victims' perspective, and
- understand the role, challenges, and capacity of the police, the judiciary and other authorities in dealing with such crimes.

Particular attention is paid to the question of how and to what extent the current situation and needs of victims of online cybercrime differ from the situation and needs of victims of traditional offline crimes.

One of the main challenges in conducting research in the field of cybercrime is gaining access to data. Identifying the best methods for collecting and sharing data for such research is necessary, as well as the use of a broad range of research methodologies and tools. Establishing procedures to enable quicker and more straightforward access to datasets collected by the police, such as Action Fraud, complaint records from telecoms providers, or cases prosecuted under the Computer Misuse Act, could create a research mainstream. However, better and more targeted data collection from the authorities can also help conduct more targeted research and identify findings at a faster pace. Overall, cybercrime is being under-reported or not reported in a timely manner, which can also create a false picture of the current state around online victimisation and its impact.

In addition, we need to develop a better understanding of the barriers and factors that facilitate victims reporting an incident. Setting clear guidelines and maintaining accessible communication channels for those affected to contact the authorities need to be further explored as well. Individuals and businesses may not be willing to report they have been victimised for a number of reasons. An individual might not even be aware that they are a victim or not know where to seek help. An SME, for example, might be less willing to report due to fear of reputational damage. Victims require a response to what had happened (reactive response), whereas often law enforcement and other professionals appear to be focused on preventing crime (proactive response).

More and more findings show that computer misuse crime has an impact on victims in a similar way to that seen in fraud cases (which shouldn't come as a surprise, given that many such crimes are, indeed, committed with the aim of perpetrating fraud). The challenge is that law enforcement doesn't necessarily engage with online victims in the same ways. Understanding these behaviours can lead to bridging the gaps – not having the right skills, knowledge or resources – which lie at the root of the victim's inability to report.

Setting guidelines for training law enforcement and the judiciary on basic cybercrime related aspects and on the victims' needs is imperative. Another important question is how much of the burden of cyber safety should be placed on organisations rather than individuals, based on the impact such burden is going to have. In addition, shaping effective policy interventions in order to counter the psychological, emotional, behavioural, physical and financial impact of cybercrime on victims is necessary. Online victims will often avoid the Internet after their negative experience, therefore interventions to ensure victims are comfortable online again may be essential for their wellbeing.

Outreach and community building

During the fellowship, I have had the opportunity to engage with a variety of stakeholders from academia, private sector, policy, law enforcement and prosecution in the UK to explore this field further. Indeed, the fellowship included not only conducting research, but also engaging and building the wider community.

To date, in collaboration with RISCS and NCSC, I have conducted a number of interviews with stakeholders in the relevant sectors, as well as with the victims, in order to identify the current gaps and needs in the field. The research findings are currently being written up and will be published later this year.

As part of the outreach and community building, I spoke about the research conducted during my RISCS Fellowship at two events:

- the Annual Conference of the European Society of Criminology (ESC) and the American Society of Criminology's Division on Cybercrime organized on September 10th and 11th, 2020.
- the Virtual Roundtable event "Tackling Revenge Porn: Supporting Victims and Improving Criminal Justice Responses" on Thursday, October 29th, 2020, organised by the International Centre for Parliamentary Studies.

In addition, I assisted the Home Office and RISCS to organise the Cybercrime Showcase event which took place on 19th November 2020. The event included presentations from researchers focusing on the findings from their research projects funded by the Home Office specifically around the theme of victimisation. The projects explored the challenges in the field of online victimisation, the policy impact of current research on online victims, the evidence gaps and future research needed in the field. A large number of participants attended the event, which clearly illustrates the interest in – and the importance of – this type of research.

The COVID-19 pandemic has made it difficult to run a face-to-face workshop and engage with stakeholders and other researchers. However, organising the cybercrime showcase event and conducting interviews remotely allowed us to have appropriate findings to share with the community.

Cybercrime: Theme Stocktake

Research Streams

The projects conducted under the Cybercrime theme are still yet to finish and be published. The projects have focused on three main research streams:

1. **Understanding online offenders:** their careers, their business models as well as the factors that influence cyber offending behaviour such as peer effects. The projects under this research stream focused mainly on the risk factors for offending and offending pathways but also on exploring the potential value of interventions to prevent people becoming involved in cyber crime and divert those on an offending pathway.

   Impact of research projects: The projects looking at online offenders are aimed at building an understanding of offenders as well as the factors that influence cyber offending behaviour. The main aim of these projects is supporting law enforcement to identify vulnerabilities in organisational structures and to target disruptive interventions effectively. By identifying typologies of economic ecosystems and transaction types that cybercriminals use, or products and services that cybercriminals leverage to transact value, these markets can be better understood and effective preventative interventions can be developed.

2. **Understanding online victims:** their needs, current practices and procedures followed by law enforcement such as police interviews with victims as well as the support provided to victims. In addition, within this research stream, projects provided insights into the psychological and technical factors that lead to victim exploitation by poor decision-making through existing and prospective victims of fraud or ransomware attacks. These insights can be used to develop tools and techniques that can form the basis of practical interventions in tackling such incidents.

   Impact of research projects: looking at online victims at an individual but also an organisational level, focused on demonstrating the victims' experience as well as the harm that cybercrime victims experience, including financial, psychological and emotional, health related, and reputational harm. One of the projects delivered insights into the psychological and technical factors that lead to exploitation of victims by fraudsters. Findings from such work demonstrate that cybercrime can lead to serious harm for victims and can evidence the need for appropriate support for victims of such crimes preventing re-victimisation. By developing tools and techniques to form the basis of practical interventions in tackling fraud, as well as identifying interventions required to mitigate the impact of attacks, this research can help develop guidelines and practices that organisations themselves can implement or promote via self-regulation.

3. **Understanding different methods to build prevention measures:** especially for SMEs but also society. In this research stream projects explored the barriers that small organisations face in adopting cyber best practices and developing a cybersecurity culture. Furthermore, projects explored interventions which can increase the likelihood of organizations adopting best practices and especially reporting incidents.

   Impact of research projects: These projects aimed at contributing towards enhanced safety online and encouraging secure habits for many different kinds of users from different sectors, including the policy community, industry and the wider public.

Research methods

A variety of different qualitative and quantitative methods have been utilised. Across the RISCS cybercrime portfolio, a variety of different qualitative methods drawn from disciplines such as psychology, criminology and (socio)linguistics were used to form a detailed understanding of the characteristics of cyber offenders, their behavioural patterns, and their career progression in cybercrime. A wide variety of stakeholders have participated in interviews such as cyber protect officers, cyber-security experts, small business and charity owners and managers as well as online offenders and online victims. Also, more traditional methods such as surveys have been used for data collection.

Future strategic vision

The projects described above, explore different aspects related to cybercrime providing a holistic view of this topic and the associated risks. These findings can lead in shaping future developments at a national, local and international level in terms of preventing cyber-attacks, by developing innovative tools and interventions.

Digital Responsibility Theme Report

Professor Lizzie Coles-Kemp, RISCS Fellow

Digital responsibility is a routine topic in information security. For example, when designing security technologies there is often discussion about whether a product will be used if it places an additional burden on the person using the technology. The question of where the power and responsibility for security lies appears in discussions about regulation, technology design or the ways people use digital technology. Both practitioners and academics cite digital responsibility as important to the success of securing digital environments.

However, digital responsibility is hard to define and currently difficult to put into practice through policy or technology design. To respond to this challenge, RISCS has introduced a fellowship in digital responsibility. The goal of the fellowship is to develop a programme of work and research, the outcomes of which will help organisations build a positive and healthy relationships with digital technology, to ultimately minimise digital harms and increase the benefits of digital technologies for all.

One of the key questions is the extent to which security is a joint endeavour, a reciprocal arrangement where the well-being of all parties is considered. Without this reciprocity, security responsibilities can feel one-sided, leading to an erosion of trust in technology and diminishing the benefits and take-up of technological approaches.

A vision for the future

As an initial activity within the fellowship, we asked people across industry, government and the third sector to tell us what their challenges around digital responsibility were and what improvements could be realised if they were able to deploy digital responsibility principles in the future. Examples of these futures included:

- **A business that makes reciprocal responsibilities of all parties central to digital transformation.**

In this future, technologies and security controls are not designed solely by the security team and imposed blindly upon staff. Instead, staff are encouraged to participate in the co-design of security processes, controls, and tasks. Their inclusion allows security to be built in a way that supports the core mission of the organisation rather than hampers it. It allows for the mutual understanding of agreed security goals and an awareness of the benefits of security by all staff, who feel part of a wider security culture rather than on its periphery. This leads to greater adoption of security practices, less need to resort to insecure workarounds and a more positive perspective on security. It also raises a greater awareness of unintended consequences or harms that may arise and how these might be mitigated.

- **Local governments that need to keep citizens' information secure with limited resources, not only to continue to enable the delivery of essential services, but also to maintain the trust of those they serve.**

In this future, local government can apply security advice in a way that allows them to maintain the security of systems whilst continuing to deliver services to the diverse communities they serve. Adopting principles of digital responsibility and co-designing security with both practitioners and those responsible for service delivery enables security experts to calibrate their advice according to the context of the social, economic, political and technical constraints under which the local government organisation and its citizens operate. This leads to a more equitable distribution of security responsibilities between practitioners, the organisation and citizens. This enables more usable, accessible security that empowers rather than excludes vulnerable groups in society whilst satisfying security requirements for systems.

- **A third sector organisation that feels comfortable and confident in promoting security tools to vulnerable groups.**

Often, information security works against those marginalised in society whilst attempting to maintain security properties of a wider system. This happens by excluding them through unrealistic requirements or unintentionally enabling online harms to an individual. Using principles of digital responsibility provides the third sector organisation with a framework and a *common language*. This enables them to effectively share knowledge and concerns around the use of digital technologies with security practitioners and individuals. The third sector organisation can then share resources to help people build a secure digital society within which they have greater autonomy over their security and in which they feel more comfortable participating.

In all these futures, there is an emphasis on trust-building, a more equitable distribution of power in terms of controlling access to digital services and technologies, accessible and usable security technologies, and a sense of shared responsibility and co-operation towards digital transformation.

Realising these futures

The first phase of the fellowship is to build an academic community to help identify and consolidate the breadth of existing work which relates to digital responsibility. During November we ran a digital responsibility reading group and regularly had more than 25 people attend (including a few practitioners). In December we held a Townhall meeting where 40 participants from industry, government and academia attended to crystallise what we mean by digital responsibility and identify barriers to achieving it.

The scoping exercises from 2020 will be built upon with further workshops. Please get in touch if you would like to take part in our programme or share your views on digital responsibility.

Digital Responsibility: Theme Stocktake

There have been four RISCS-funded or affiliated projects exploring the topic of Digital Responsibility, although there is crossover with the ‘Leadership and Culture’ theme in most of these given their common interest in looking at security across organisations.

Cybersecurity Cartographies, led by the Digital Responsibility Fellow, Professor Lizzie Coles-Kemp, was a flagship RISCS Phase 1 project. Prior to this work, there was limited understanding around how a security manager selects the appropriate control combination for cyber security in organisations. 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. The comic strips approach offers ways in which different professional roles can work together to share understanding of complex topics such as information security.

The project *Cybersecurity across the Lifespan* found that people’s attitudes and behaviours towards cyber security and risk change across the course of their lives in sync with their goals and aspirations, cognitive abilities and knowledge and ability to control and adapt their cyber security behaviour. This work contributed to the understanding of how best to communicate cyber security findings to different groups, contributing to the digital responsibility agenda to be as digitally inclusive as possible so that no portion of society is left behind and people can have autonomy over their own cybersecurity.

The short project *Supporting Data Security and Privacy in the Home* also looked at how users take responsibility for their own cybersecurity, through looking at the role of social relationships in home data security using interviews. The work found that some people took responsibility for others' security and were more likely to offer unsolicited advice to family members than to friends.

Finally, as part of the new portfolio of projects exploring economics and incentives, a team at UCL are looking at the role of Internet Service Providers in protecting users from cyber security vulnerabilities and in helping them recover from them, which is often ambiguous. They are working with colleagues in Japan to determine which incentives and approaches might encourage Internet Service Providers and their customers to remediate compromised or vulnerable IoT devices. These findings, once available, will be very interesting to the digital responsibility community.

Leadership and Culture Theme Report

Berta Pappenheim, RISCS Fellow

Cyber security is central to the health and resilience of any organisation. Ensuring this is recognised and treated with due diligence at the highest management levels lies at the very heart of the Leadership and Culture Theme. For this reason, the work we undertake here is the more relevant, the more it is linked to the issues currently at the very top of the executive agendas.

When I joined RISCS in October 2020 to take over the Leadership and Culture Theme, I wanted to put my focus on something topical, something up to date, something relevant. And what has impacted upon the cyber security leaders, as well as the cyber security culture, more than the ongoing pandemic that has now been our reality for well over a year?

COVID-19 and Cyber Security

In the very beginning, we set out the very general questions that would then guide us as we progressed with our research: is COVID-19 changing the perceptions around cyber security? How are relevant stakeholders across various sectors – academic, industry, policy – going to take this issue forward?

Our hope has been to understand the implications of mass remote/hybrid working arrangements we all observe and partake in on a daily basis nowadays. In particular, our focus has been on the psychological contract between employees and leadership from the perspective of cyber risk. The formal research objectives have been devised as follows:

- To understand how different organisations adjusted to new forms of working while maintaining/reducing their cyber risk exposure.
- To explore strategies used by cyber security leaders to keep a positive cyber security culture front of mind.
- To gather best practices used for maintaining trust, nurturing teamwork, safeguarding mental health of team members (reducing insider risk / human error).

The first stage of evidence gathering was an extensive literature review we conducted - not only of very recent, strictly COVID-focused materials (which are scarce), but rather exploring a much broader range of resources which we felt were also of relevance. We looked at past events which, colloquially speaking, interrupted the ‘normal life’ somewhere and sometime - smaller, localised epidemics, as well as other past pandemics, being just one example.

In line with the very nature of RISCS, our research team has been highly interdisciplinary – consisting of myself, research assistants Amy Ertan and Georgia Crossland from Royal Holloway, as well as another small business owner Nadine Michaelides, all supported by Nico B from the Sociotechnical Security Group at the NCSC. We arrived at many interesting conclusions; even more interesting questions that arose on the way were left unanswered. We’re proud to say that the Literature Review has now been published, and is available at https://www.riscs.org.uk/remote-working-and-cyber-security-literature-review/.

Interviews with industry leaders

With the literature review serving as a more formalised basis for our topic of interest, we proceeded with the next stage of our research – expert interviews. Over the last two months, we have spoken to 18 CISOs from across a number of industries: from defence, manufacturing, and IT, to finance, banking, and consulting, to charity, legal, and government. The diverse range of the interviewees' backgrounds allowed us to validate one of our initial hypotheses: that the pandemic's impact on cyber security differed tremendously from sector to sector. We touched upon many dimensions – from gathering information on practicalities like how new employees are onboarded in the current circumstances, or how security awareness training is conducted, to attempting to better understand the more nuanced issues – like how these corporate efforts are received by the staff themselves.

We have now concluded the interviews and are currently at the stage of coding the data, as well as performing some preliminary analyses. Our results will be published in an upcoming White Paper directed at cybersecurity leaders and IT professionals. The publication will provide actionable advice based on what the best practice is at the moment – we hope to be able to share it with you very soon.

Next steps and the future

My background is somewhat different than the other Fellows in that it's strongly commercial, rather than purely academic – I run a cyberpsychology consultancy, and in my work interact with a wide range of companies, their staff and executives. Because of this, delivering insights which could be immediately utilised *on the ground* is a top priority for me.

Our next step is to prepare and publish the aforementioned White Paper. Then, its dissemination will be key. We need to take great strides to make sure it reaches those for whom it may be of immediate value, and I am looking forward to working with the RISCS Community and Advisory Board on this.

In the next year of the Fellowship, we are hoping to hold events with various groups of interest: industry leaders, boards, HR officials, in order to not only disseminate our findings, but also explore the many questions that will certainly be left unanswered after the literature review and interview stages. There are many avenues we are keen to pursue further – for example, it may be highly insightful to move away from the leadership, and instead speak to wider staff, whose opinions on the events of the past year, as well as the efforts undertaken to mitigate them, may be very different.

What's evident is that our research is essential precisely because it happens as its subject unfolds. The results we deliver will be unique, and different from other future work which, while certainly important, will inherently be looking at these unprecedented circumstances from a more remote, retrospective viewpoint.

Biographies

Georgia Crossland: is a doctoral student at Centre for Doctoral Training in Cyber Security, Royal Holloway University of London. Her thesis focuses on human factors and the psychology of the user in cyber security. Alongside her studies, Georgia has worked on a number of human factor projects for private organisations and government, generally concerning cyber security behaviours and awareness campaigns. Georgia has published government reports on cyber security behaviours, research in clinical psychologist journals, and selected articles on cyber security can be found on InfoSecurity magazine and her personal blog.

Amy Ertan (CISSP): is a predoctoral cybersecurity fellow at the Harvard Kennedy School's Belfer Center, a visiting researcher at the NATO Cooperative Cyber Defence Centre of Excellence, and information security doctoral candidate at Royal Holloway, University of London. Amy has published UK government reports on organisational cyber security behaviours and engaging C-Suite colleagues with cyber risk management, and selected articles on cyber security strategy may be found on Foreign Policy, InfoSecurity Magazine, and on her personal website.

Secure Development Practices Theme Report

Dr Shamal Faily, RISCS Fellow

In recent years, we have gleaned a better understanding of the role played by software developers and coding practices during the creation of secure and insecure software. For this knowledge to have impact, we need to consider the implications of this knowledge not only to software developers, but others with a stake in *building security into* technology products and services. To this end, we envisage broadening the Secure Development Practices theme to encompass the user and security research, as well as design activities that feed into secure software development. We also want to consider what can be done to shape the broader environment, such that secure design and development become dominant practices more generally.

For example, **what pedagogical challenges** do we face embedding Secure Development Practices knowledge into the higher education and professional training curricula? Similarly, **what are the barriers and opportunities** for growth in the market for secure development practices and services?

Building the community

We see community workshops as key to forming a UK hub around the Secure Development Practices theme.

Our first workshop, held on November 9th, 2020, was designed to attract those with an interest in areas tangential to Secure Development Practices. The first half of the workshop set the scene for the theme from a RISCS and HM Government's perspective. A panel of invited speakers from academia and industry then shared their experience on what currently works and what doesn't around Secure Development Practices. The second half of the workshop was dedicated to breakout discussions around barriers and opportunities in five chosen sub-themes. The workshop closed with a plenary session sharing key insights from these breakout groups, and possible roadmaps for developing the opportunities identified.

Succession planning and Early Career Researcher (ECR) development initiatives

Broadening the Secure Development Practices theme was one of two objectives of this fellowship. The other was to sustain the RISCS theme beyond the life of the fellowship project.

Using the community workshop as a platform to launch it, we created a RISCS managed online repository on MS Teams to share knowledge around SDP theme and sub-themes. The platform will be curated by the RISCS fellow, and attendees from the first community were invited to join it and use it for post-workshop collaboration on the breakout topics.

We plan to use virtual community workshops as a vehicle for reaching out to ECRs interested in this RISCS theme. For example, the 'call for scribes' to the ACE-CSRs led to interest from several ECRs; these ECRs were active participants during the breakout groups in the first workshop. To encourage further ECR participation in the theme, we're exploring how some funds set aside for physical workshops can be used as pump priming funding for ECRs wishing to progress work around SDP sub-themes.

Innovations

To date, we have developed a map of Secure Development Practice capability in UK Higher Education Industry. We are currently updating this map to indicate HEIs with undergraduate programmes that contain content in areas relevant to this RISCS theme.

We are developing a training package to facilitate knowledge exchange around human-centred threat modelling. This is designed to be used in conjunction with action research that evaluates the effectiveness of usability-driven approach to secure design and development. Although the COVID-19 pandemic has made it difficult to run the interventions planned, other work (in parallel with the RISCS fellowship) has allowed us to create online content suitable for remote delivery.

Vision for the future

As mentioned above, there are pedagogical challenges to embedding Secure Development Practices in curricula. For this, and many other reasons, the relevant knowledge and experience developers have varies widely. Despite this being fairly common knowledge, it is prevalent across academia and industry to make unwarranted assumptions about who developers are. A wide variety of professionals – psychologists, UX researchers, and others – are now involved in software development on a daily basis.

To date, most academic research within this theme has focused on sensitising developers to vulnerabilities and threats. These efforts have been quite successful, and the awareness level has increased substantially over the recent years. But because the backgrounds of those involved in software development are so different, the awareness itself doesn't readily translate into the ability to mitigate the deficiencies. The go-to solution for many is to look for answers on sites like Stack Overflow which, while certainly valuable, often feature incomplete or misleading information.

In our view, rather than cramming knowledge into people's heads, we should work on ensuring they – whether as individuals or teams – have access to the proper expertise required. The future research within our theme should attempt to find out how to ensure this access effectively and make strides to move the issue in question higher up on the policymakers' agenda.

Secure Development Practices: Theme Stocktake

To date, there have been four RISCS-funded or affiliated projects within the theme. All the projects fit in the category of 'Developer-Centred Security', but each focus on developers with different levels of experience: "Impact of Gamification on Developer-Centred Security" *(Games for DCS)* and the "Why Johnny doesn't write secure software?" *(Johnny)* projects focus on the masses; "Motivating Jenny to Write Secure Software" *(Jenny)* and "Developer Security Essentials" *(DSE)* projects focus on professional software developers. Nonetheless, there are consistent themes across all four projects that are relevant to Secure Development Practices and RISCS more generally.

Support developer decision making

Both *Johnny* and *Jenny* note the value of supporting developers when security decisions need to be made. *Johnny's* results found that developers only consider the active writing of code as security relevant, and a lack of domain knowledge and security knowledge make developers liable to certain biases where the trust placed on code developed by others is not warranted. *Jenny's* results found that, albeit infrequently, professional developers also need to be supported when facing secure coding decisions. The "Security in the Community" guide created by *Jenny* provides guidance on how to find well developed security advice on online forums; this guidance can be delivered via multiple forms of media to developers, irrespective of their level of expertise.

Sensitising developers

Johnny, *Jenny*, and *DSE* highlight the importance of sensitising developers to security. Results from *Johnny* indicate that developers should be encouraged to think about users and the consequences of insecurity for them. The outputs from *Jenny* and *DSE* help developers do just this. For example, *DSE* has produced a guide which highlights the relationship between design and code quality and software vulnerabilities; this can help developers identify security touchpoints in their everyday work. *Jenny*'s "Security Between Us" modelling workshop entails developers using Lego to build a physically tangible model, which can be annotated to help developers see where "security" is.

From developer-centred to design-centred security

While the outputs from all four projects sensitise developers to the implications of insecurity, they are less effective in sensitising them to the threats exploiting this insecurity. The outputs often rely on ideation to identify these threats, but this is unlikely to be successful without some level of security expertise, or threat intelligence – which also requires some level of security expertise to navigate. *Games for DCS* provides some visibility of threats that target insecurity, and how secure coding can address them, but threats can target intentionally or unintentionally insecure requirements and architectural design decisions. While these threats have not been considered, the projects outputs may just be extensible enough. For example, the workshop-based interventions in *Johnny* and *DSE* could incorporate threat modelling to consider the impact of design insecurity, and the outputs from these workshops could even be used to addressed them.

Inputs from other RISCS themes

These emerging themes suggest a broader need to look at inputs from "upstream" RISCS themes. For example, the biases developers have may appear to have a negative impact on secure coding, but play a more positive role in the broader context where developers operate. Fostering changes to practice, tools, or the operating environment may lead to latent conditions that become a source for other knowledge or skill-based errors. Exploring whether this could be the case non-disruptively could be a fruitful direction of work for the Anticipation and Prospection theme; work in risk management and shared narratives (within the Leadership and Culture theme) may also help better understand the norms and values that shape these biases. Finally, given the "wicked" nature of security design problems, working around responsible research and innovation (within the Digital Responsibility theme) may provide opportunities for evaluating the ethical import of different secure system design configurations.

Cyber Security Futures – Anticipation and Prospection Theme Report

Professor Genevieve Liveley, RISCS Fellow and Dr Anna G, NCSC Lead

Anticipating future threats, assessing their probability, imagining their possible harms, and identifying strategies to mitigate and defend against them, are core activities at the heart of cyber security. Cyber security requires particular expertise in thinking about the future, using "future-based information [and] acting in the present".

In recognition of this, in March 2020 RISCS introduced a dedicated research theme to its portfolio, and we began a study of "Anticipation and Prospection" in cyber security. The aim of the study is to explore new ways in which we might better understand the relationship between *futures thinking* and cyber security. In particular, to identify the key skills in *futures literacy* that we need to enable better and safer digital and cyber security.

> "The point of FL is to become more adept at inventing imaginary futures: to use these futures to discern system boundaries, relationships and emergence; to invent and detect changes in the conditions of change; to rethink the assumptions we use to understand the present."
>
> *Riel Miller, 2011. "Futures literacy: embracing complexity and using the future." Ethos, 10(10), 23-28*

In this context, we understand Futures Literacy as "the capacity to think about the future". Like Riel Miller, we see that the "point of Futures Literacy is to become more adept at inventing imaginary futures: to use these futures to discern system boundaries, relationships and emergence; to invent and detect changes in the conditions of change; to rethink the assumptions we use to understand the present."

This model of Futures Literacy serves to remind us that in cyber security we are not dealing with concrete certainties but with "present imaginaries of future situations" – that is, with future scenarios and strategies which are *narrative* fictions (Beckert, 2013, p. 325). When we imagine and explore the probabilities, costs, and risks of any kind of cyber risk we are dealing with a present imaginary of a future possible world – a fiction, a narrative.

Futurists and theorists have long argued that we understand and explore the future through narrative. Storytelling constitutes a human sense-making tool, and we make sense of the world "narratively". That is, we view narrative as a metaphor for life, and negotiate our lived experience – past, present, and future – as "storied". This has important implications for understanding how we think about the future – and narratology therefore has significant insights to offer into the narrative dynamics that frame our futures thinking. And this includes our understanding how we think about future risks in cyber security.

For, as Narratologist Gerard Prince puts it (1990, 1), "Narrative [...] does not merely reflect what happens; it discovers and invents what can happen." Our risk management strategies and plans for the future of cyber security, then, become stories which "discover and invent what can happen". Understanding the narrative dynamics which drive this futures sense-making process in cyber security will help to strengthen our futures literacy. And it will help us to imagine and develop better strategies for the future.

We have had a busy year launching this new theme. Our first aim was to scope and draw together the community of practice and expertise in this area across academia, government, and business, and we have already built up a Directory of Experts. They have been helping us to frame the priority research questions to be addressed under this theme. We have now run two virtual workshops with these experts. The first (in July 2020) set two exam questions for breakout groups to explore:

- What practical relevance and contribution could Anticipation and Futures Literacy bring to cyber security and how could it be embedded in your organisation?
- What outputs from the RISCS Anticipation project would you find most useful and valuable?

> "Narratology has made it clear that, while narrative can have any number of functions (entertaining, informing, persuading, diverting attention, etc.), there are some functions that it excels at or is unique in fulfilling. Narrative [is] … a particular mode of knowledge. It does not merely reflect what happens; it discovers and invents what can happen."
>
> *Prince, G. 1990. "On Narratology (Past, Present, Future)." French Literature Series, 17: 1-14.*

In response to the discussions from this summer workshop, the focus of our second event (in November 2020) was a Cyber Security Futures Book Club. By expanding our range – and types – of narratives about cyber security, we can start to equip ourselves for imagining and preparing for different possible futures for a digital society. We therefore invited our community of practitioners to introduce us to any books, stories, anecdotes, articles, films, TV, comics (anything at all – fiction or non-fiction) on the topic of "the future of cybersecurity". Among the numerous titles discussed were: Joanna Kavenna's ZED; Brian K Vaughan's Private Eye comics; William Gibson's Johnny Mnemonic (the story); Philip K. Dick's Minority Report (the film); Neal Stephenson's Fall: Or, Dodge in Hell; Cory Doctorow's Little Brother; and E.M. Forster's amazingly prescient The Machine Stops. We hope to continue the book club idea and welcome any further suggestions.

The book club was a real highlight of our year, with the second notable achievement the opportunity to represent the work of our RISCS theme at the UNESCO Futures Literacy Summit in December 2020. As well as our digital presence at the summit (expertly supported by the RISCS team at UCL), we hosted two virtual booths and a live webinar. Our special guests, Siân John MBE from Microsoft and Susan Halford from the Bristol Digital Futures Institute joined Madeline Carr and Helen L for a roundtable discussion on the topic of the futures of cyber security. We hope that the future of the "Anticipation and Prospection" theme continues to flourish next year.

Anticipation and Prospection: Partner Case Study

Lauren Katalinich, CyberSmart

More than anything, 2020 has demonstrated that the future is never certain. We can't predict what our industry is going to look like in ten years or even next year, but we can anticipate and prepare for the possible risks and opportunities that changes may bring. This year at CyberSmart, we decided to do just that.

We're a medium-sized startup on a mission to make cybersecurity accessible for SMEs. As with most rapidly growing businesses, our time is laser-focused on the now and how to best serve our customers' immediate challenges. But this year we set up an innovation function to engage in longer-term speculative thinking by considering how to apply futures methods usually used by much larger companies and governmental organisations.

Our framing was intentionally broad to lift our sights beyond our usual focus to consider: What is the future of trust in, and resilience of, the digital society? And what is CyberSmart's role within it? First, we turned to our colleagues. Through a formal horizon scanning exercise in the spring we explored events, trends and weak signals that might impact our exam question over the next two to five years. We collected a wide range of ideas, ranging form the political, economic, social, technological, environmental, legislative and organisational. But how to connect the dots and find coherence in many ideas?

We ran a few internal workshops in the early summer to interrogate cross-cutting themes to frame four scenarios. We created a map of the digital society, grouping ideas into subplots that we combined into four stories. These hovered above our map and brought it to life by helping us to distil the most provocative yet plausible narratives emerging in each scenario.

This process has provided a systematic approach to make sense of the noise in the world. A second outcome has been showing us how to root future thinking in evidence. Much of September was devoted to reading and digesting key articles, papers and reports to see whether there was evidence to support our ideas- or not. A third outcome has been demonstrating how storytelling can help formulate thought experiments to engage people and identify their assumptions about the future (irrespective of which future actually takes place). A workshop in the late summer with RISCS Fellow, Professor Genevieve Liveley, and her NCSC counterpart, Dr Anna G, helped to validate our approach and provide a sounding board that improved both the descriptions of our stories, as well as the analysis of our scenarios. This process was iterative; moving back and forth between the stories and scenarios meant that improvements in the former improved the latter, and vice versa.

We're grateful for Genevieve's and Anna's generous support and time. This project is just one example of the network of researchers we've been building around our innovation interests. We look forward to developing our collaborations with RISCS in the new year!

About CyberSmart: Despite a growing number of cyber attacks every year, most SMEs continue to operate without cyber protection because they see security as a complicated and costly process. CyberSmart's mission is to make security simple and accessible for every SME, with no expertise or big budget required.

For further information, contact Ben Koppelman Research and Innovation Lead at CyberSmart at ben@cybersmart.co.uk

Policy Update

Florence Greatrix, Policy Adviser

Since joining the team in January 2020, I have been amazed by the volume and quality of work going on in RISCS, and equally by the commitment from the policy community to the unique, cross-cutting and complex cyber security agenda.

I initially spent some time conducting desk research of the RISCS portfolio and the policy area, as well as engaging in valuable conversations with Advisory Board members from Government to identify what I could do to help them to best utilise RISCS. These actions allowed me to develop a strategic plan for our policy engagement activity, which underpinned most of my work in recent months. Below, I outline some of the highlights, as well as plans for the future.

I am delighted that our Project Catalogue has been published alongside this report. With RISCS maturing as an institution, I saw producing a succinct summary of completed and ongoing projects tailored to a policy audience as instrumental in strengthening our legacy– and my initial discussions with stakeholders confirmed the many practical advantages of having such a publication. While collating the policy relevant findings of RISCS projects has certainly been a sizeable task, I hope to keep the Catalogue regularly updated to maximise its usefulness and will be actively monitoring uptake and seeking feedback on this first iteration from our community.

Activity highlights

We produced and disseminated our first policy briefing on the 'Evaluating Cyber Security for Policy Advice' [ECSEPA] project in October. Through this briefing we hope to stimulate debate on how evidence is used in cybersecurity decision making and to build and strengthen relationships with policy colleagues. We raised a number of policy questions and received thoughtful comments and ideas back, which can inform future research.

My colleague Jenny Bird and I delivered an 'Introduction to Policy Engagement' session to researchers from RISCS, the UCL Cybersecurity CDT and the SPRITE+ Network in October. The training is for researchers and students who hold an interest in undertaking knowledge exchange with policy makers but have limited experience of doing so . It gave participants a sense of what's involved in effective policy engagement and hopefully the confidence to craft and execute a policy engagement strategy themselves. We were delighted to have Emma Green (DCMS) and Steve Bell (Home Office) with us as guest speakers and their contributions received particularly positive feedback from attendees.

I have also enjoyed working with our Fellows and current PIs to connect them with policy audiences and share relevant outputs throughout the year. I look forward to continuing and building on those collaborations in 2021.

Policy development

From the policy side, 2021 will be pivotal as it marks the final year of the current National Cyber Security Strategy. The UK's future approach and priorities will be shaped by the Integrated Review of Security, Defence, Development and Foreign Policy, of which for cyber security is a key component. I have attended (virtual) meetings of a cross Government 'evidence working group', to keep abreast of policy development and evidence needs, and to feed in RISCS updates and new project outputs. Strengthening our ongoing dialogue with policy colleagues is a key component of my role, and I am the initial point of contact for any policy queries – so do get in touch at any time!

Looking to the future

Early 2021 will be an exciting time, with many current RISCS projects – as well as the work programmes of the current RISCS Fellows – coming to an end. During this time, my focus will be on supporting our researchers with sharing their outputs with the policy community. The projects in our Economics and Incentives portfolio closely align with DCMS priorities, so I will be working to ensure that these findings feed through as much as possible.

I will be hoping to hold workshops with RISCS Fellows at the start of the next phase to facilitate collaborations on their new projects with policy stakeholders at the outset, and to maximise the potential for collaborations throughout their ambitious work programmes.

RISCS promotes an interdisciplinary approach to addressing cyber security challenges and acts as a platform for knowledge exchange between disciplines and sectors. I believe even small connections from an online meeting or an email introduction can go some way to building those bridges. It has been exciting to see the enthusiasm from our academic community and policy stakeholders alike in building connections and sharing expertise and ideas to date, and I look forward to supporting it and watching it grow further next year.

Closing Message: Reflections and hopes for the future

Helen L, Technical Director

I've been lucky enough to be the Technical Director for both the Sociotechnical Security Group (StSG) in the NCSC and RISCS for three years now. Working in this space has always been fascinating, but the last year has proven particularly exciting.

For many years we've been working hard to show that "if security doesn't work for people, it doesn't work". **For many years,** we have rhapsodised about the benefits of a multi-disciplinary approach to the complex problems of cyber security. And **for many years,** we have watched as sticky plasters get piled on, only to fall off in seemingly no time at all. But more recently people have begun to listen. Instead of only wanting to search where the light is shining, many now see the benefit of searching in the shadows too. COVID-19 has only sharpened the focus on how people and technology interact safely to get the job done.

Getting to this point is a huge achievement. Madeline and I are basking in the reflected glory earned by all those who have led and have been part of the RISCS community before us. Now we have the privilege to build the platform on which to tell our story and grow an engine of research and collaboration to meet the demand of all those that want to hear what we have to say. To this end, you'll notice that many of the changes this year are about putting in place the infrastructure we need. We've created posts that enable our experts to spend time on the things that they are gifted at (like defining the problem, building communities, seeding collaboration) and we've brought in expertise on the things that we need help on (like communication in all its forms, organising events and meetings, funding). We've picked five themes that we feel are really important to UK PLC right now and which we feel the diverse research community of RISCS can best add value to. These themes complement our StSG Problem Book and the NCSC Research Problem Book, and are each being led by a small team of people that span academia, NCSC, wider HMG and Industry.

What we've put in place is new and, in areas, different to how others are doing it. We're taking the approach of trying, learning and adapting… and our RISCS Advisory Board are an important part of that story. Part of our next phase will be to figure out how we can best leverage the wealth of knowledge and influence we have both in our Advisory Board and in our practitioner community; and work is already underway to address that. We also have a complex funding landscape to navigate at the moment. The UK government's pot of money ringfenced for cyber security (NCSP) comes to an end on 31 March 2021, with no guarantee on what succeeds it. The current economic climate brings with it a spectrum of priorities for Government, and no certainty on what funding will look like beyond the short term. **But what we all know is that cyber security will remain a high priority to ensure that UK remains the safest place to work and do business online through these times.**

For me, the key to our success going forward is not what funding we get, but how our story is told – by us, and others. The ground-breaking research that we do, that harnesses the spectrum of minds that join together under RISCS, and even more importantly, the narrative we weave together from it, will be the things that will enable a whole-scale paradigm shift in the way we approach security. We all have a role to play in that, but it's Madeline's and my job to build the stage.