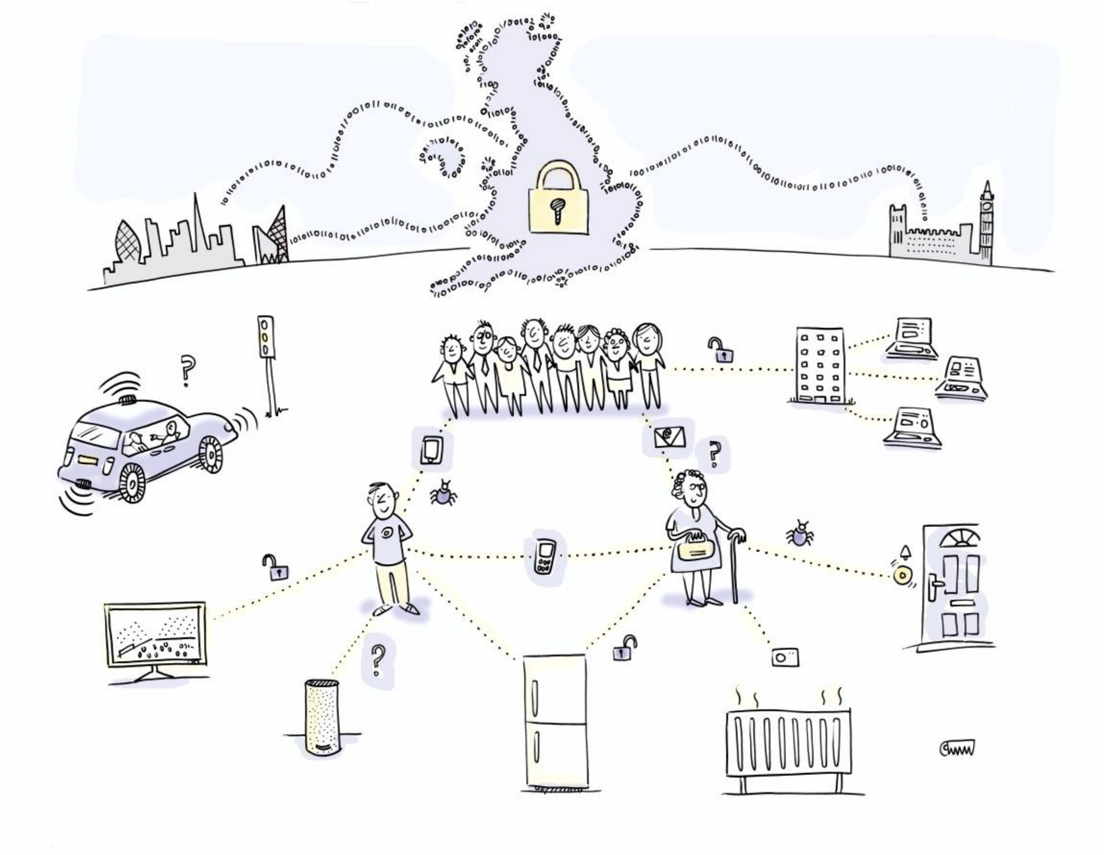
National Cyber Security Centre
a part of GCHQ

Sociotechnical Security Group

Sociotechnical Security Group Problem Book

An outline of the StSG's future research in cyber security



Author:

Helen L, Technical Director
Sociotechnical Security Group

Contents

Introduction

Managing security effectively requires an understanding of the whole system: people, data, process and technology. The Sociotechnical Security Group (StSG) is a multidisciplinary research team in the National Cyber Security Centre dedicated to understanding how to support people and organisations to make better cyber security decisions. This Problem Book describes the set of sociotechnical research questions that the StSG believes will enable the UK to continue to be the safest place to live and work online.

Our portfolio of research projects collectively contribute to these overarching challenges. The aim of this Problem Book is not to prescribe the solution, but to communicate a shared purpose and direction for sociotechnical research in cyber security. It seeks to encourage a diverse and multidisciplinary set of approaches that can be brought together to provide an outcome that is greater than the sum of its parts.

This Problem Book is designed for our current and future research partners across academia, industry and government, to enable them to work with us on the nine sociotechnical challenges that we have identified to help make the UK a safer place to live and work online.

About the Sociotechnical Security Group (StSG)

The StSG has three distinct yet interdependent areas of focus that draw from disciplines spanning across the social sciences, natural sciences, humanities and formal sciences:

- How people behave both individually and in groups;
- The interactions between people and technology and
- The security of whole systems.

We have three key objectives:

1. We generate and use research insights from a range of sociotechnical disciplines to inform our development of tools, techniques, advice and guidance to support the security of NCSC's customers.
2. We use our global relationships spanning governments, academia and industry to solve complex and seemingly intractable problems.
3. We develop our team's expertise and impact by balancing the need to develop solutions to today's problems with the need to build the subject matter expertise required to solve tomorrow's problems.

Our external partnerships with academia, industry and other parts of government provide a crucial extension to our capability. This set of problems articulates what we need more research in and why, in order to optimise collaboration with our partners. We invite discussion, contributions and ideas from our current and future partners on any of the research challenges described in this Problem Book. Please email helen.l@ncsc.gov.uk in the first instance.

Communicating cyber security risk

Problem #1: How can we incorporate Cyber Security into business decision making?

Summary

Organisations balance a wide range of risks in the course of managing their businesses. Cyber security should be an integral part of those risks, not a separate entity; but it is notoriously hard to articulate cyber security in consumable business terms.

How can we support organisations to incorporate cyber security into their wider risk picture in a way that positively impacts their business and reduces knowledge asymmetries?

Challenges arising from language and culture differences between people from diverse professional backgrounds and organisational responsibilities will need to be explored. Nurturing a dialogue around cyber security between practitioners, staff and senior decision makers that can bring relevance to an organisation's identity and growth is key. How this dialogue is affected by context and tempo should be investigated.

Improving how people reason about the future amid a landscape characterised by the increased levels of uncertainty and complexity that connected systems introduce is a central milestone to managing cyber risks more dynamically. A way of quantifying, visualising and reporting these risks to decision makers in a way that is meaningful, efficient, and measurably effective is yet to be established.

Importance to NCSC

There are few (if any) small businesses, organisations, and government departments in the UK whose business risk is not affected by cyber security. Yet the intangible and, often, insidious nature of cybercrime means that cyber security may not be considered as part of the usual business risk processes until it's too late.

Even then, businesses often turn to a compliance-led cyber security risk management process that exists in a separate place to other business risks. Answering this problem will move cyber security risk management towards critical thought and away from blind compliance.

Both industry and government look to the NCSC to provide advice and guidance on the analysis and communication of cyber security risk. Whilst meeting this need, the NCSC needs to balance diversity in risk thinking with the need to gain some consistency across the risk management profession. Security practitioners will need clear and authoritative guidance on how best to analyse and communicate cyber security risk to others within their organisation. Risk management that is less compliance-driven would enable UK organisations to use technology more confidently. Having a greater understanding of cyber security risks will support business decision making and enable innovation and growth.

Working with cyber security data

Problem #2: How do we gather, analyse and apply cyber security data to best effect?

Summary

Our technology systems can generate huge quantities of data that is relevant to security. Whilst there are high expectations of what these cyber security datasets can do, they are currently poorly understood and can easily be misrepresented or misinterpreted. A wide variety of commercial tools, some good and some poor, promise to use this data to solve a diverse set of cyber security problems, including supporting risk decisions, detecting cyber incidents and measuring the effectiveness of security interventions. But these tools are not always the answer and deriving meaning from the data can be difficult.

How do we identify and gather the right data, use it to our advantage, to gain insights into operating successfully and efficiently in the digital age? Raw data doesn't provide insights and meaning, so how can data analysis and visualisation optimise decision making? What is the value of new techniques such as machine learning? How can we provide guidance on the best kinds of cyber security datasets to collect, and generate actionable insights that use them effectively?

Importance to NCSC

As well as optimising the outputs of our Active Cyber Defence initiatives, the NCSC should be able to provide examples of quality datasets, their utility and limitations. We want to be able to answer questions like 'how can this data be used?', 'where does it meet my expectations and where doesn't it?' and 'how can I use it to make risk decisions?

Being able to bust 'big data' myths and naïve reliance on large data sets allows industry and government to be intelligent customers of the data analysis providers. The NCSC also wants encourage innovation, by engaging directly with the data analysis providers, and also supporting academia and start-ups (through the Cyber Accelerator) who may face challenges developing new ideas and products.

Improving resilience

Problem #3: How can an organisation survive a cyber breach more effectively?

The DCMS Cyber Security Breaches Survey 2020 found that almost half of businesses and a quarter of charities report having cyber security breaches or attacks in the last 12 months, up from 2019. These attacks are becoming more frequent, and the surface area across which they can take place is increasing. The cost to the business of a cyber breach can manifest itself in many different ways. Financial penalties, recovery times, reputational damage, additional and unwanted process leading to loss of staff morale are all significant penalties.

An organisation's resilience to cyber-attack depends on its ability to identify, adapt to and evolve with changing technologies and threats. Becoming more resilient may require innovations in technology, faster feedback loops, deception techniques or new organisational and governance practices. Simply adding more process, backup and redundancy does not provide lasting resilience; and returning to a previous state doesn't remove the vulnerabilities that had previously been exploited.

Genuine organisational resilience calls upon people and processes as well as technology. People are remarkably adaptive and resilient when they need to be. They are at the heart of business change and drive innovation when the situation asks for it. They can be an effective early warning system: spotting subtle differences or near misses that often get lost in the noise of purely technology-based monitoring systems.

The right augmentation of people and technology will enable organisations to recover effectively from the impacts of a cyber attack, whilst also learning and improving from them. Importantly, how an organisation is able to learn in the absence of an incident, by understanding what is working well, is a crucial evolution beyond established thinking in the business continuity and disaster recovery domains.

Possessing the ability to identify issues, learn lessons and adapt as a result of it will significantly reduce the harm organisations suffer from cyber attacks. This can also ensure that an organisation is able to take advantage of new opportunities without security standing in the way.

Importance to NCSC

With cyber breaches becoming more commonplace, the ability of a company to recover and adapt effectively from a cyber attack is an increasingly important factor of a vibrant UK economy.

Resilience, rather than prevention, and as opposed to 'afterthought' is a mindset that many organisations have not yet arrived at. Supporting businesses to become more resilient will simultaneously frustrate attacks, evolve the marketplace and require less direct support from government.

Developing culture

Problem #4: How can security contribute positively to an organisation's culture?

Summary

Positive organisational cultures, that are central to a business's identity and goals, are key to both a thriving work environment and to success in the marketplace.

Different parts of a business will all contribute to an organisation's culture and security should be part of this, not separate to it. A business that implements security successfully will minimise the friction introduced by it and maximise its positive contribution by aligning it as seamlessly as possible to existing work practices.

Supporting a business, whatever its size, to be able to identify what's *actually* happening in practice is fundamental to identifying how different parts of the business can work together to support a consistent culture. These feedback loops provide a lifeline of rich information to be able to find out how staff are interacting with security, identify what isn't working and enable a light to shine on alternative approaches that might work better.

A consistent dialogue between the business and its staff provides a barometer for the complex trust relationships that exist both within and with the business; and will establish a platform on which to strengthen trust and agility, the core of cyber resilience.

Any interventions need to respect the unique context of each organisation, and the people working within it. To have real impact, interventions will need to go further than awareness training, to include analysis and changes to processes, technologies, policies and governance, ensuring that people believe that the organisation is enabling security best practice. Supporting people to behave securely in line with their values and the culture of their environment will help mitigate risks and support more secure ways of working.

Importance to NCSC

There is a demand from NCSC's customer set to be provided with advice and support on how to develop positive security cultures. This needs to explain the various techniques currently available, and to demonstrate where novel capabilities need to be developed, whilst also making the case for the necessity of expending scarce resources on optimising security culture. This should help customers of security culture interventions to select the right approach, and to measure success in these interventions.

NCSC has the platform and expertise to provide leadership on this topic by seeding research and driving innovation. This will require NCSC to continue to develop thought leadership and practical capabilities in this space. These will ultimately contribute to the security of the UK, whilst driving economic prosperity.

Dealing with complexity

Problem #5: How can we understand security in complex interconnected systems?

Summary

Real sociotechnical systems are often too complex to fully imagine, describe, easily understand or accurately analyse within human cognitive abilities. Emergent properties and new risks that result from this increasing interconnectness and complexity of modern systems can potentially be missed, leading to hidden vulnerabilities.

Understanding people's cognitive ability to reason and appreciate complex sociotechnical systems and how they can be optimally augmented by tools and techniques is central to this problem. The ability to elicit and use both qualitative and quantitative data to build up a picture of a system is a key part of being able to support decision makers to reason about risk (threats and opportunities) in complex systems in an informed and productive way.

Different sociotechnical systems behave and react in different ways. The ability to gather feedback on the success of an intervention in a complex system is a challenging but crucial part of identifying and managing their inevitable emergent properties.

Importance to NCSC

Developing the application of risk management techniques and tools for understanding and managing complexity, and making these available to practitioners across industry and government, is a fundamental assurance task for NCSC.

These techniques may be used better understand potential scenarios for risk analysis or training purposes, for which there is considerable market demand. A particular focus exists on the interconnectedness and complexity inherent in the UK's Critical National Infrastructure.

Making security usable

Problem #6: How can we engineer systems with both security and usability in mind?

Summary

The burden of security has traditionally fallen heavily onto people, often resulting in insecure behaviours as they try to get the job done around technology that doesn't work for them. To rebalance this situation, engineers and practitioners need support and guidance in how to create systems with both security and usability in mind. How can we best design and create secure and usable systems? How do we gain assurance of engineering processes for the products and services that they are developing? How do these engineering processes align with other business processes in an organisation to maximise efficiency and cooperation?

To do this we need to understand the people using, building and maintaining these systems, including their capabilities, emotions, motivations and understanding.

The NCSC is encouraging better design of our sociotechnical systems and processes that allow people to behave securely by default and not to view security and usability as a trade-off: a system cannot be secure, unless it is usable. Developing systems with security and usability in mind allows organisations to take full advantage of new technologies, such as cross domain solutions, while still ensuring that the risks are understood and mitigated.

Importance to NCSC

NCSC is in a position to provide clear thought leadership around shifting the burden of responsibility for security from people to technology. They key is improving system design and maintenance to bring security and usability together. Answering this question will enable NCSC to provide general advice and guidance on secure and usable system design, in a way that developers and the people around them can relate to. It will enable NCSC to support the engineering profession to establish the fundamentals of cyber security into the things they are designing and building.

Managing uncertainty

Problem #7: How can we reason effectively about cyber risk in conditions of uncertainty?

The nature of the world we live in is characterised by increasing levels of volatility, uncertainty, complexity and ambiguity. The pace of technological change and the emergent way in which society uses these technologies, poses critical challenges for cyber security going forwards.

This impacts thinking about the future and decision-making across society and government. We need to make decisions and manage risks for these technologies in the face of conditions of discontinous change and high or even irreducible uncertainty. Security for Artificial Intelligence and intelligent, adaptable systems, in particular, need tools and approaches to risk and governance that are fit for purpose and able to anticipate, reason about and respond to emergent issues.

In light of this, how do we gain confidence in the decisions we take today on the design and security of complex, novel technologies? How can we trust intelligent technologies that are using their own, emergent, decision processes? How do we overcome our assumption that the future will be like the past so that we can reason effectively about the risks of digital systems and how society interacts with them both today and in the future?

New tools and ways of thinking about risk will be required that draw on the full range of human abilities and cognitive strategies for reasoning about the future. We need to equip ourselves with strategies, tools and mindsets that build in the practice of anticipation and are responsive to the condition of uncertainty, rather than ignoring or being paralysed by it.

Importance to NCSC

The NCSC is facing an increasing demand to offer guidance to organisations on cyber risk management and how to assure novel technologies and intelligent systems. Developing dynamic approaches to governance, assurance and risk management that are able to cope with future complexities in our digital systems and society’s use of them now and in the future is critical to keep the country safe in a digital age. Assuring the development of emerging technologies is also crucial to enable innovation and leadership in this space, contributing to the future prospectiy of the UK

Supporting the wider public

Problem #8: How can we support individuals to be secure in their daily digital lives?

Individuals interact with connected devices and carry out their lives online today more than ever before. Up until recently we have solely relied on people protecting themselves online, often with scarce resources and complex technical set ups to navigate, with limited success.

But as we move towards an age where people increasingly see their technology as extensions of their physical being and their online personas as a central part of their identity; appreciating the needs and wants behind the public's demand for connectivity becomes a more central part of how to make their lives safer and secure; by making security relevant and accessible.

Different parts of our society have different requirements and resources upon which they can draw to keep themselves safe and secure. How can we identify these to ensure that cyber security is inclusive and that we prevent the unintended security impact of digital exclusion?

We seek to support the NCSC, wider government, law enforcement, and industry to enable the citizen to be secure in their private digital lives. The context of this support needs to cover a variety of settings, from enabling secure everyday technology use to recovering from being a victim of cybercrime. Support to individuals needs to reach across communication and messaging aspects through to technological solutions. Understanding the connection between these aspects will be essential to correctly targeting our support.

Importance to NCSC

An individual's personal attack surface is broadening, and the ways in which the public are using technology constantly evolving. As a result, whilst the cyber threat to organisations is still very real, individuals are increasingly falling victim to cybercrime.

The NCSC has placed more emphasis on securing the wider public over the last year, to ensure that it is fully delivering the mission to help make the UK 'the safest place to live and do business online'. The hub of this work has been through the Cyber Aware campaign and the Suspicious Email Reporting Service, and the StSG has played a central part in its evidence-based approach.

The NCSC wishes to both further empower the public to protect themselves online and reduce the harm to them. This can be achieved through a spectrum of approaches: from the adoption of secure behaviours to making technology more secure by design to providing more support to the victims of cybercrime.

Optimising incentives

Problem #9. How can incentives and interventions be used effectively to improve cyber security?

Summary

People and organisations make decisions about cyber security every day and the decisions they make are unique to their context and values. The ecosystem in which decisions are made have a significant bearing on their choices; knowledge assymmetries, misaligned feedback loops and market failures can all affect the incentive to invest in cyber security.

A better understanding of the landscape in which decisions are being made, the people making the decisions (including adversaries), their governance and the communities and markets in which they sit is central to this problem. It will include consideration of the legislative and commercial compliance frameworks placed upon them, as well as the circumstances under which a decision is made.

Appreciating the way in which people and organisations make decisions is a key part of this problem. How can the design of a system can be optimised to incentivise making a choice with a better cyber security outcome?

Understanding the potential impact of different interventions, from a variety of perspectives, is also key. Poorly understood interventions may be ineffective, or even create new emergent problems. We must understand the impacts of the decisions we seek to change, and the impact of the interventions themselves.

Importance to NCSC

The NCSC and its wider government parters need to continue to build an understanding of how interventions and incentives can work most effectively for cyber security within the markets and legislative frameworks that organisations operate. Optimising the market in which cyber security operates is an important consideration of DCMS that this research can feed into.

In addition, organisations of all sizes look to us as thought leaders in how they can improve cyber security decision making within their organisation, and research in this area can help us continue to provide useful guidance on effective interventions.