National Cyber Security Centre
a part of GCHQ

The Sociotechnical Security Group (StSG)

Cyber security research in practice

The StSG is a new cyber security research function within the National Cyber Security Centre, with the remit to tackle complex cyber security problems that combine aspects of **people**, **processes** and **technology**. We strive to develop a **holistic understanding of cyber security** that acknowledges all the perspectives of the many people involved in protecting information and systems.

Traditional approaches to security research have been focused on understanding *technology*. But it's only part of the picture and doesn't account for the *interaction* of technology with people, processes and organisations.

The Sociotechnical Security Group aims to address this shortcoming. With research primarily drawing on behavioural and social science, systems theory approaches and engineering, data analysis, and complexity science, we provide thought leadership to the NCSC through:

- **Academic research, sponsorship and engagement**
- **Masterclasses and workshops**
- **Customer engagement and consultancy**
- **Briefing, seminars and presentations**
- **Advice and guidance**
- **Review and development of cyber security tools, methods and frameworks**
- **Blogs on the NCSC website: www.ncsc.gov.uk/blog**

ENGINEERING PROCESSES & ASSURANCE

Development Processes and Emerging Methods Understanding the position of security in architectural/ developmental frameworks and processes and exploring novel combinations of existing processes for better effect.

Secure Systems Development Identifying security considerations and a toolbox of techniques and knowledge that can be signposted and applied within a development lifecycle.

Understanding Requirements Understanding how security requirements are elicited then traded against other business needs and risks, and how this dictates the effectiveness of the security solution.

Systems Modelling Researching ways in which modelling can be used to support cyber security decision making in an engineering/ architectural endeavour.

Resilience and Response Approaches Examining how resilience and response can be designed into the system.

RISK

Enterprise Risk Management Maintaining an understanding of existing ERM techniques and developing new ones.

Reductive Risk Assessment Methods Understanding strengths and weaknesses of current-practice risk management processes in order to guide practitioner application and identify gaps in our research direction.

Systems Theory of Risk and Design Understanding systems theoretic approaches to assessing risk during system design and analysis.

Standardisation Exploring organisational and field-level implications of standardising approaches to risk management.

Data-Driven Security Developing data analysis techniques applicable to commonly-available cyber security datasets.

Security Metrics Designing and implementing appropriate metrics to measure security problems and assess interventions.

Complex Systems Investigating the application of complex systems theory to cyber security.

PEOPLE-CENTRED SECURITY

Establishing Situational Awareness Understanding barriers to security and developing techniques for eliciting security information.

Understanding People Studying and modelling individual and group psychology in the context of security behaviour and decision making.

Shaping Behaviour Determining the most effective way of realising the right security behaviours.

Shaping the Environment Understanding how to structure systems, services and experiences in a way that is likely to result in people making the right security decisions.

StSG
Sociotechnical Security Group