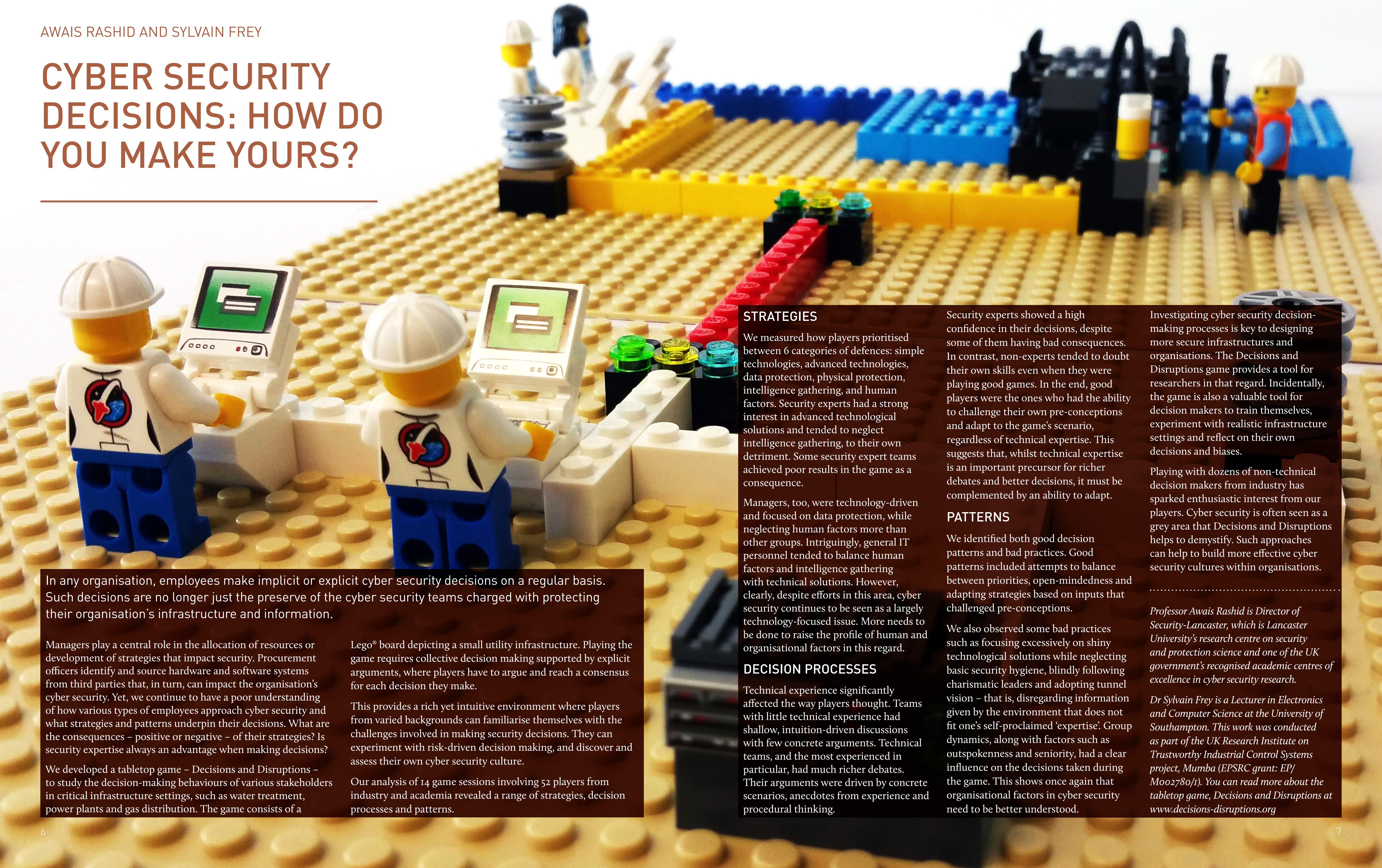
AWAIS RASHID AND SYLVAIN FREY

CYBER SECURITY DECISIONS: HOW DO YOU MAKE YOURS?



In any organisation, employees make implicit or explicit cyber security decisions on a regular basis. Such decisions are no longer just the preserve of the cyber security teams charged with protecting their organisation's infrastructure and information.

Managers play a central role in the allocation of resources or development of strategies that impact security. Procurement officers identify and source hardware and software systems from third parties that, in turn, can impact the organisation's cyber security. Yet, we continue to have a poor understanding of how various types of employees approach cyber security and what strategies and patterns underpin their decisions. What are the consequences – positive or negative – of their strategies? Is security expertise always an advantage when making decisions?

We developed a tabletop game – Decisions and Disruptions – to study the decision-making behaviours of various stakeholders in critical infrastructure settings, such as water treatment, power plants and gas distribution. The game consists of a Lego® board depicting a small utility infrastructure. Playing the game requires collective decision making supported by explicit arguments, where players have to argue and reach a consensus for each decision they make.

This provides a rich yet intuitive environment where players from varied backgrounds can familiarise themselves with the challenges involved in making security decisions. They can experiment with risk-driven decision making, and discover and assess their own cyber security culture.

Our analysis of 14 game sessions involving 52 players from industry and academia revealed a range of strategies, decision processes and patterns.

STRATEGIES

We measured how players prioritised between 6 categories of defences: simple technologies, advanced technologies, data protection, physical protection, intelligence gathering, and human factors. Security experts had a strong interest in advanced technological solutions and tended to neglect intelligence gathering, to their own detriment. Some security expert teams achieved poor results in the game as a consequence.

Managers, too, were technology-driven and focused on data protection, while neglecting human factors more than other groups. Intriguingly, general IT personnel tended to balance human factors and intelligence gathering with technical solutions. However, clearly, despite efforts in this area, cyber security continues to be seen as a largely technology-focused issue. More needs to be done to raise the profile of human and organisational factors in this regard.

DECISION PROCESSES

Technical experience significantly affected the way players thought. Teams with little technical experience had shallow, intuition-driven discussions with few concrete arguments. Technical teams, and the most experienced in particular, had much richer debates. Their arguments were driven by concrete scenarios, anecdotes from experience and procedural thinking.

Security experts showed a high confidence in their decisions, despite some of them having bad consequences. In contrast, non-experts tended to doubt their own skills even when they were playing good games. In the end, good players were the ones who had the ability to challenge their own pre-conceptions and adapt to the game's scenario, regardless of technical expertise. This suggests that, whilst technical expertise is an important precursor for richer debates and better decisions, it must be complemented by an ability to adapt.

PATTERNS

We identified both good decision patterns and bad practices. Good patterns included attempts to balance between priorities, open-mindedness and adapting strategies based on inputs that challenged pre-conceptions.

We also observed some bad practices such as focusing excessively on shiny technological solutions while neglecting basic security hygiene, blindly following charismatic leaders and adopting tunnel vision – that is, disregarding information given by the environment that does not fit one's self-proclaimed 'expertise'. Group dynamics, along with factors such as outspokenness and seniority, had a clear influence on the decisions taken during the game. This shows once again that organisational factors in cyber security need to be better understood.

Investigating cyber security decision-making processes is key to designing more secure infrastructures and organisations. The Decisions and Disruptions game provides a tool for researchers in that regard. Incidentally, the game is also a valuable tool for decision makers to train themselves, experiment with realistic infrastructure settings and reflect on their own decisions and biases.

Playing with dozens of non-technical decision makers from industry has sparked enthusiastic interest from our players. Cyber security is often seen as a grey area that Decisions and Disruptions helps to demystify. Such approaches can help to build more effective cyber security cultures within organisations.

Professor Awais Rashid is Director of Security-Lancaster, which is Lancaster University's research centre on security and protection science and one of the UK government's recognised academic centres of excellence in cyber security research.

Dr Sylvain Frey is a Lecturer in Electronics and Computer Science at the University of Southampton. This work was conducted as part of the UK Research Institute on Trustworthy Industrial Control Systems project, Mumba (EPSRC grant: EP/M002780/1). You can read more about the tabletop game, Decisions and Disruptions at www.decisions-disruptions.org