Institution:	University of Northumbria at Newcastle
Unit of Assessment:	11 - Computer Science and Informatics
Title of case study:	Cyber Security: Situational Awareness and Infrastructure Protection research changing policy and practice

1. Summary of the impact

Cyber security and situational awareness research has impacted organisations' strategy, policy and practice. Impact was delivered through nuWARP (Northumbria University Warning, Advice and Reporting Point) registered as part of the UK Government's Centre for the Protection of National Infrastructure. **International impact**: direct contribution to EU Cyber Security Strategy; improved practices at the Nigerian Economic and Financial Crimes Commission; redeveloped business model at Star Spreads (online gambling company) leading to safer practices for customers. **National impact**: contributed to improved business models and policies in SMEs (Washington Metalworks, Shared Interest, SRM Ltd), which have improved data security and online practice.

2. Underpinning research

An ongoing cyber security challenge is acquiring real-time situational awareness for monitoring network infrastructure state and maintaining optimal performance. Research in the UoA has been developed (particularly in an SME context) into protecting online infrastructure, such as web servers and networks, with a focus on sonification (the rendering of data as non-speech audio) to enhance situational awareness. (Laing, Badii, and Vickers, 2012).

During 2001-2003, Vickers et al explored the potential of non-speech audio as a monitoring medium for running processes. Their research demonstrated the efficacy of sonification for detecting and locating errors in programs. An experiment revealed that a structured musical language was successful in letting participants identify salient features within a computer program, leading to a set of sonification design guidelines (Vickers and Alty, 2002). A second experiment in which participants were tasked with finding bugs in eight programs showed that more bugs were located when program listings were supplemented with the sonification system, which did not add to the time taken to complete the tasks (Vickers and Alty 2003). The musical experience of participants in these two experiments had no effect on their ability to use the sonification technique. The results subsequently supported the case for using sonification in process monitoring and cyber security scenarios (Vickers, 2011).

Laing and Vickers subsequently conducted research (Aljawarneh, Laing, and Vickers, 2007 and 2008) into protecting web servers against tampering attacks on their content. Solutions already existed to protect static (fixed) content, but dynamic content (e.g. the contents of a shopping basket on an online store) remained vulnerable. The research provided a solution to this problem via a system that detected when tampering had taken place and restored the original safe content before transmission by the web server. Experiments in which participants launched 72 tampering attacks against the server showed the system detected all the attacks and with no reduction in server performance. This provides an important security feature for web-based networks.

In 2010 Laing and Vickers conducted a TSB-funded project (BK008B) with a consortium of SMEs (see section 4) to investigate the sonification of self-organised criticality in computer network traffic to spot patterns that could signal impending problems (a big data problem, one of David Willetts' "*Eight Great Technologies*"). The system was tested on data captured from consortium partners and showed how changes in network state (possible indicators of disruptions) could be monitored in real time. This led to a UK Patent Office filing in March, 2012 (GB1205564.6) and an R&D partnership was established with Security Risk Management Ltd to commercialise the idea. The project's SME links support the multi-partner RCUK/GCHQ Cyber Security Research Institute project "Choice Architecture for Information Security (EP/K006568/1)" which brings together academic partners (Northumbria and Newcastle) and SMEs (through the agency of nuWARP) to investigate and develop tools and techniques for a choice architecture tailored to information security.

Researchers and their positions:

- Dr Vickers (Northumbria University): Principal Lecturer 2001-2005, Reader in Computer Science 2005–present.
- Dr Laing (Northumbria University): Senior Lecturer 2003-2008, Learning and Teaching Fellow Computer Science 2008–present / nuWARP Project Director, 2010–present.

3. References to the research

Outputs marked with a * have been flagged to indicate a 2* quality threshold.

- *Vickers, P. and Alty, J.L. (2002) 'Musical Program Auralisation: A Structured Approach to Motif Design', *Interacting with Computers*, **14** (5) 457–485. http://dx.doi.org/10.1016/S0953-5438(02)00004-8.
- *Vickers, P. and Alty, J.L. (2003) 'Siren Songs and Swan Songs: Debugging with Music', *Communications of the ACM*, **46** (7), 86-92. http://dx.doi.org/10.1145/792704.792734.
- Aljawarneh, S., Laing, C. and Vickers, P. ''Security Policy Framework and Algorithms for Web Server Content Protection'', in Proc. ACSF 2007 2nd Conference on Advances in Computer Security and Forensics (J. Haggerty and M. Merabti, eds.), Liverpool John Moores University, June 2007. http://nrl.northumbria.ac.uk/id/eprint/917.
- *Aljawarneh, S., Laing, C. and Vickers, P. 'Design and Experimental Evaluation of a Web Content Verification and Recovery (WCVR) System: A survivable security system', in 3rd conference on Advances in Computer Security and Forensics (ACSF 2008) (J. Haggerty and M. Merabti, eds.), (Liverpool, UK), 10–11 July 2008. http://nrl.northumbria.ac.uk/id/eprint/2293.
- Vickers, P. (2011) 'Sonification for Process Monitoring', in The Sonification Handbook (T. Hermann, A. D. Hunt, and J. Neuhoff, eds.), pp. 455–492, Berlin: Logos Verlag. http://sonification.de/handbook/index.php/chapters/chapter18/.
- Laing, C., Badii, A. and Vickers, P. (eds.) Securing Critical Infrastructures and Industrial Control Systems: Approaches for Threat Protection. IGI Global, Dec 2012. http://dx.doi.org/10.4018/978-1-4666-2659-1.

Current and Previous Awards

- 20010-2012 HEIF4. 'The development of Northumbria University's Warning, Advice and Reporting Point (nuWARP)', (PI: Laing, C.) HEIF4, 03/2010, 04/2011 and 03/2012, £102,000.
- 2010–2011 TSB BK008B. 'Monitoring and Identification of Anomalies within Network Traffic Behaviour', (PI: Laing, C., and Vickers, P.), £136,982.
- 2012–2015 (EP/K006568/1). 'Choice Architecture for Information Security', Joint project with Newcastle and Northumbria Universities, EPSRC Research Institute in the Science of Cyber Security: (Laing as Co-I with Briggs, P and Coventry, L), £887,750.

Patent Applications

- Laing, C. and Vickers, P. 'A method and system for sonifying critical measurements in an environment', United Kingdom Patent Application No GB1205564.6, 29 Mar. 2012.

4. Details of the impact

The UoA's security research led us in 2010 to register a community shared service for SMEs, nuWARP (www.nuwarp.org.uk) a comprehensive SME Warning Action Reporting Point, within the UK Government Centre for Protection of the National Infrastructure (http://www.warp.gov.uk/). This service provides (i) a Filtered Warning Service, (ii) Trusted Sharing Service, and (iii) an Incident Response Service. The impacts described below were achieved through the agency of nuWARP which provides a link between the academic research and the commercial sector and which arose

from our Cyber Security research.

Influencing Strategy and Policy

ENISA (European Network and Information Security Agency) commissioned nuWARP to write a case study based on device and network security for its 2011 report on Emerging and Future Risks (downloaded more than 950 times to date – Source 1 below). The Senior Expert in Risk Management at ENISA said the case study was "*key*" to the successful completion of the report and its wide readership and that it: "*helped in the assessment of related risks."* This report forms a major part of the latest EU Cyber Security Directive's backbone: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (ec.europa.eu/digital-agenda) (Source 2). The Government Department for Business, Innovation, and Skills, as well as national bodies such as the British Computer Society, have also commissioned reports on cyber security and good practice from nuWARP.

Information Sharing for Changing Practice

A team from the Nigerian Economic and Financial Crimes Commission (EFCC) attended a nuWARP 12-day training course in digital forensic investigations (09/2010). This provided a mix of skills development and instilling a greater understanding of policies and procedures, in this case the development of best-practice digital forensics investigatory policies and procedures which will help the EFCC to do their jobs more effectively

Between April and August 2012 nuWARP worked with Star Spreads, a Dublin-based SME, providing guidance on online payment procedures, fraud detection, and vulnerability assessment culminating in nuWARP conducting a full penetration test. The work was concerned with securing an online gambling site, a type of business in which trust and privacy are essential elements. nuWARP assisted Star Spreads to develop their online payment security, policies and procedures leading to a redeveloped business model (Source 3). As a result, nuWARP was asked to review the mobile payments policies and procedures of Excelpoint, a software development SME, as well as the trust and privacy implications of moving to a cloud environment (Source 4).

Behavioural change is evidenced by the IT Coordinator for Washington Metalworks, who confirmed that attendance at a nuWARP workshop (04/2011) helped: "*raise awareness in the company of threats within the business and to take preventative measures*" (Source 4).

Shared Interest, a Newcastle-based financial service provider, asked nuWARP to undertake a network forensics investigation, from which nuWARP provided a series of half-day training programmes for senior management, normal business staff, and their overseas staff (December 2012). Consequently, Shared Interest updated its security policies and procedures; in particular they are implementing a social media policy and procedure, and with help from nuWARP they are reviewing their Bring Your Own Device (BYOD) policies, especially staff mobile phone usage when overseas (Source 5).

Directly resulting from being part of the TSB project consortium (RMT Accountants, PEM IT Services, Security Risk Management Ltd, and the International Association of Accountants Innovation and Technology Consultants), Security Risk Management Ltd, an information assurance firm (www.srm-solutions.com), "*have identified a number of potential opportunities surrounding situational awareness and sensory planes … The generation and maintenance of Situational Awareness is fundamental to our ability to operate effectively in what has become known as the Cyber Environment*" (Managing Director of SRM) (Source 6). SRM are now pursuing these opportunities in partnership with the University and are seeking to recruit specialists working in this field.

Public Engagement

Vickers provided advice (Dec 2012, Jan, May, June 2013) on sonification strategies and the technological solutions available to an independent freelance sound artist who subsequently secured Arts Council funding to build a sonified solar system model which was selected for exhibition at the British Science Festival 2013 (www.thesoniccosmos.com) (Source 7).

Also selected as part of the British Science Festival (originating from "*Securing Critical Infrastructures and Industrial Control Systems: Approaches for Threat Protection*" (Laing *et al*. 2012) was a public panel debate entitled "*Cyber Pearl Harbour; Fact or Fiction?*" (http://www.britishscienceassociation.org/british-science-festival/cyber-pearl-harbour-fact-or-fiction).

5. Sources to corroborate the impact

1. Christopher Laing, et al., 'Cyber-Bullying And Online Grooming: Helping To Protect Against The Risks', ENISA Emerging and Future Risks, 10/2011. (see http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/Cyber-Bullying%20and%20Online%20Grooming) – This report corroborates the impact on ENISA and the EU Cyber Security Directive.
2. Senior Expert: Risk Management, ENISA – This contact corroborates the impact the research had in shaping the EU Cyber Security directive.
3. Director, Star Spreads – This contact corroborates the impact on online payment policies and procedures at Star Spreads.
4. IT Manager, Washington Metalworks – This contact corroborates the behaviour and practice change in the organisation as a result of attendance at a nuWARP workshop.
5. Finance Director/HR Manager, Shared Interest – These contacts corroborate the impact on security policies and procedures at Shared Impact.
6. Letter from Managing Director, SRM Ltd, Dec 2012. – This details the new business opportunity in cyber situational awareness which resulted from SRM's links with UoA researchers through the TSB project.
7. www.thesoniccosmos.com – this website showcases the British Science Festival exhibit informed by sonification research carried out at Northumbria.