HAISA 2017

Day One – Tuesday, 28th November 2017

9:00 – 9:30	**Conference Welcome**
9:30 – 10:30	**Keynote Address** **Sean Duca, Vice President, Palo Alto Networks Inc.** **'Don't Be That Guy/Girl'** Employees are fast becoming the weakest link in the defence against cybercriminals. Sometimes common sense can only go so far, as you need to make sure that best practices around security don't go in one ear and out the other. We will take a current look at some of the challenges organisations face, what we can do to raise the bar from a pure compliance driven to security awareness program and to "gamifying" cybersecurity education programs for employees. Making security part of the culture of a organisation is everyone's business.
10:30 – 11:00	Coffee Break
11:00 – 12:30	**Session 1** **Persuading End Users to Act Cautiously Online: Initial Findings of a Fear Appeals Study on Phishing** J. Jansen and P. van Schaik **Understanding Susceptibility to Phishing Emails: Assessing the Impact of Individual Differences and Culture** M. Butavicius, K. Parsons, M. Pattinson, A. McCormac, D. Calic and M. Lillie **Mapping the Anatomy of Social Engineering Attacks to the Systems Engineering Life Cycle** J. van de Merwe and F. Mouton
12:30 – 13:30	Lunch
13:30 – 14:30	**Session 2** **Phish Phinder: Gamified Approach to Enhance User Confidence in Mitigating Phishing Attacks** G. Misra, N. Arachchilage and S. Berkovsky **A Comprehensive Framework for Cultivating and Assessing Information Security Culture** A. Tolah, S. Furnell and M. Papadaki

14:30 – 15:15	**Industry Presentation** **Andrew Bissett, Head of Advisory Services, SAI Global** **'Solving the Compliance Conundrum: Creating and measuring the effectiveness of security awareness learning'** Together with Towards Maturity a UK based research firm, SAI Global has commissioned a report entitled 'Solving the Compliance Conundrum, essential data driven insights for ethics & compliance professionals'. This report addresses the conundrums faced by Ethics and Compliance Professionals working alongside those responsible for learning and development to develop an effective and compliant culture in the workplace. This presentation will discuss the experiences SAI Global has had in working with organisations to implement effective learning as well as an overview of the results of the 'Solving the Compliance Conundrum' report. A key aspect will be the year on year changes the report identifies in compliance & ethics learning since 2013 when the report was first commissioned.
15:15 – 15:45	Coffee Break
15:45 – 17:15	**Session 3** **The Influence of Data Protection Regulation on the Information Security Culture of an Organisation - A Case Study Comparing Legislation and Offices Across Jurisdictions** A. da Veiga **Understanding the Relationships Between Resilience, Work Stress and Information Security Awareness** A. McCormac, D. Calic, M. Butavicius, K. Parsons, M.Pattinson and M. Lillie **The Lemming Effect in Information Security** D. Snyman, H. Kruger and W. Kearney
18:00	**Evening Social Networking Event at Sammy's on the Marina, Holdfast Shores**

HAISA 2017

Day Two – Wednesday, 29th November 2017

8:45 – 9:45	**Session 4** **How Reliable are Experts' Assessments? A Case Study on UAV Security** A. Shoufan and E. Damiani **The Influence of Organizational Commitment on Information Security Policy Compliance** V. Hooper and J. Ophoff
9:45 – 10:30	**Industry Presentation** **James Turner, Advisor, Intelligent Business Research Services (IBRS)** **'Security Leadership: A Fresh Perspective of Cyber Risk Management in a Hyper-Connected World'** The IT industry has hit a breaking point where the artificial grouping of information security and IT has left many organisations vulnerable. Business units have viewed information security as an IT problem, and IT has abdicated responsibility for many aspects of operations that should be viewed as basic hygiene. There are many real circumstances why this happens: cut budgets, slashed headcount, and enormous market disruption. But when we allow circumstances to dominate our strategy, we also trick ourselves into thinking that there is only one way to respond. Cyber security is not merely an IT problem, it is a foreseeable business risk. When incidents are accepted as foreseeable, and viewed as business risk, cyber security can become an enabler because it provides assurance that an organisation has a viable platform to build from and is operating sustainably.
10:30 – 11:00	Coffee Break
11:00 – 12:30	**Session 5** **Identifying the Factors Affecting End-Users' Risk-Taking Behavior** M. Alohali, N. Clarke, F. Li and S. Furnell **Securing Mobile Devices: Evaluating the Relationship Between Risk Perception, Organisational Commitment and Information Security Awareness** A. Reeves, K. Parsons and D. Calic **Digital Wellness: Concepts of Cybersecurity Presented Visually for Children** S. von Solms and R.Fischer
12:30 – 13:15	Lunch (45 minutes)
13:15 – 14:15	**Session 6** **Employee Information Security Beliefs in the Home Environment** J. Omidosu and J. Ophoff **Involving Users in the Design of a Serious Game for Security Questions Education** N. Micallef and N. Arachchilage

14:15 – 15:00	**Industry Presentation** **Jodie Siganto, Partner, Ringrose Siganto** **'The Australian Cyber Security Skills Shortage: A Conundrum'** In this session, Dr Siganto will talk about her research into Australian the skills shortage and more recent analysis of advertised cyber security roles. She will highlight some of the issues raised by this research including why the majority of information security practitioners believe there is a shortage when the traditional indicators of labour shortage are not present. She will also look at current recruitment methods and our conception of the skills required for information security practitioners and ask whether they are fit for purpose. She will conclude with some analysis of whether the current initiatives to solve the skills 'crisis' are likely to be successful.
15:00 – 15:30	Coffee Break
15:30 – 16:30	**Session 7** **An Information Privacy Culture Index Framework and Instrument to Measure Privacy Perceptions Across Nations: Results of an Empirical Study** A. da Veiga **Privacy Enhancing Tools for Public Users: A Literature Review on End-User Role and Evaluation** A. Padyab and A. Ståhlbröst
17:00	**Bus departs Oaks Pier for Conference Dinner at Woodstock Wines**
18:00	**Conference dinner & wildlife experience commences**

HAISA 2017

Day Three – Thursday, 30th November 2017

8:45 – 9:45	**Session 8** **Factors Influencing the Use of Privacy Settings in Location-Based Social Networks** H. Oladimeji and J. Ophoff **Jurisdictional Issues in Cloud Forensics** M. James and P. Szewczyk
9:45 – 10:30	**Industry Presentation** **Phil Kernick, Chief Technology Officer, CQR** **'Social Engineering – the games we play'** In this session, Phil will discuss the practicalities and challenges CQR faces in performing a social engineering exercise against a client organisation and how to use the outcomes to reduce risk within the organisation against such attacks.
10:30 – 11:00	Coffee Break
11:00 – 12:30	**Session 9** **Why Open Government is Good for Cybersecurity and Public Trust** C. Culnane and V. Teague **What Do They Really Think? Overcoming Social Acceptability Bias in Information Security Research** D. Ashenden **Towards the Design of a Cybersecurity Module for Postgraduate Engineering Studies** S. von Solms and L. Futcher
12:30 – 13:30	Lunch
13:30 – 15:00	**Session 10** **An Analysis of Unauthorized Wireless Network Usage in Western Australia** P. Szewczyk, D. Blackman and K. Sansurooah **Secure Coding Practices in the Software Development Capstone Projects** V. Mdunyelwa, J. van Niekerk and L. Futcher **The Socio-Technical Impact on Security of the Healthcare Internet of Things in the Use of Personal Monitoring Devices (PMDs)** H. Pathirana and P. Williams
15:00 – 15:15	**HAISA2018 Call for papers** ***Closing Remarks***