

### Catalogue Annexe

#### Contents

Cyber Readiness for Boards (CR4B)	2
Leveraging the Multi-Stakeholder Nature of Cyber Security	2
Cyber Protect: Protecting Businesses in the Eastern Region from the Risk of Cybercrime	3
Cyber Security Quirks: Personalised Interventions for Human Cyber Resilience	3
A Framework to Model and Incentivise Cyber Security Investment Decisions (MERIT)	3
Economic Metrics for Supporting Cyber Security Investment Decision-Making	4
Gamification Training to Protect Against Socially Engineered Cyber Attacks: An Evidence Based Design.	4
Incentivising Cyber Risk Management Behaviours: The Role of Cyber Insurance	4
Keeping the Internet of Things Secure: Investigating Incentives for Internet Service Providers and Individuals in the UK and Japan	4
Case by Case: Building a Database on Cybercriminal Business Models	4
Advanced Modelling of Cybercriminal Careers (AMOC): New Tech and Intelligence from Online Evidence Bases	4
Why Johnny doesn't write secure software: Secure software development by the Masses	4
Online Ties Taking Over (OTTO)?	5
Addressing Cybersecurity and Cybercrime Via a Co-Evolutionary Approach to Reducing Human-Related Risks (ACCEPT)	5
Cyber Security Across the Lifespan (CSALSA)	6
Evaluating Criminal Transactional Methods in Cyberspace as Understood in an International Context	6
Victims of Computer Misuse Crime	6
Connecting Delayed Pre-commitment with Cyber Awareness in Order to Address the Perception Gap and Present Bias	6
Motivating Jenny to Write Secure Software: Community and Culture of Coding	6
Economical, Psychological and Societal Impact of Ransomware (EMPHASIS)	7
Investigative Interviewing of Cybercrime Victims to Gain Best Evidence	7
Gentle Interventions for Security (GIFS)	7
ECSEPA: Evaluating Cyber Security Evidence for Policy Advice	7
Detecting and Preventing Mass Marketing Fraud (DAPM)	8
Supporting Data Security and Privacy in the Home	8
Developer Security Essentials – The Magid Project	8
Impact of Gamification on Developer-Centred Security	8
Visualising Access Control Policies	9
Choice Architecture for Information Security	9
Cyber Security Cartographies (CySeCa)	9
Games and abstraction	9
Productive Security – Improving Security Compliance and Productivity Through Measurement	10

This Annexe provides a list of academic publications relating to each project, listed in the same order as the catalogue. Please note that some of the newest projects do not yet have any academic publications as of March 2021.

If you have any questions or comments, please feel free to get in touch with the RISCS Team at [riscs.administrator@ucl.ac.uk](mailto:riscs.administrator@ucl.ac.uk)

### Cyber Readiness for Boards (CR4B)

No publications to date.

### Leveraging the Multi-Stakeholder Nature of Cyber Security

Bustince, H., Marco-Detchart, C., Fernández, J., Wagner, C., Garibaldi, J.M., 2020. Similarity between interval-valued fuzzy sets taking into account the width of the intervals and admissible orders. In *Fuzzy Sets and Systems 390*, (pp. 23-47)

Ellerby, Z., Miles, O., McCulloch, J. and Wagner, C., 2020, July. Insights from interval-valued ratings of consumer products—a DECSYS appraisal. In *2020 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)* (pp. 1-8). IEEE. Available at: [https://nottingham-repository.worktribe.com/preview/4326314/WCCI\\_food\\_ratings\\_revised.pdf](https://nottingham-repository.worktribe.com/preview/4326314/WCCI_food_ratings_revised.pdf)

Ellerby, Z., McCulloch, J., Wilson, M. and Wagner, C., 2019, September. Exploring how Component Factors and their Uncertainty Affect Judgements of Risk in Cyber-Security. In *International Conference on Critical Information Infrastructures Security* (pp. 31-42). Springer, Cham. Available at: <https://arxiv.org/pdf/1910.00703.pdf>

Ellerby, Z., McCulloch, J., Young, J. and Wagner, C., 2019, June. DECSYS–Discrete and Ellipse-based response Capture SYStem. In *2019 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)* (pp. 1-6). IEEE. Available at: [https://nottingham-repository.worktribe.com/preview/2185519/DECSYS\\_software\\_paper\\_FUZZ-IEEE.pdf](https://nottingham-repository.worktribe.com/preview/2185519/DECSYS_software_paper_FUZZ-IEEE.pdf)

Havens, T.C., Pinar, A.J., Anderson, D.T. and Wagner, C., 2018, July. SPFI: shape-preserving Choquet fuzzy integral for non-normal fuzzy set-valued evidence. In *2018 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)* (pp. 1-6). IEEE. Available at: <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8491555>

Havens, T.C., Wagner, C. and Anderson, D.T., 2017, July. Efficient modeling and representation of agreement in interval-valued data. In *2017 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)* (pp. 1-6). IEEE. Available at: <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8015466>

Kabir, S. and Wagner, C., 2020, June. A Bidirectional Subsethood Based Fuzzy Measure for Aggregation of Interval-Valued Data. In *18th International Conference on Information Processing and Management of Uncertainty in Knowledge-Based Systems (IPMU)* (pp. 603-617). Available at: <https://www.semanticscholar.org/paper/A-Bidirectional-Subsethood-Based-Fuzzy-Measure-for-Kabir-Wagner/772bb942adc7a55a11921adc062de433a770ea69>

Kabir, S., Wagner, C., Havens, T.C., and Anderson, D.T., 2020, March. A Similarity Measure Based on Bidirectional Subsethood for Intervals. In *IEEE Transactions on Fuzzy Systems*. IEEE. Available at: <https://ieeexplore.ieee.org/document/9019656>

Kabir, S., Wagner, C., Havens, T.C. and Anderson, D.T., 2019, June. Measuring Similarity between Discontinuous Intervals - Challenges and Solutions. In *International Conference on Fuzzy Systems (Fuzz-IEEE)* (pp. 1-6). IEEE. Available at: <https://ieeexplore.ieee.org/document/8858862>

Kabir, S., Wagner, C., Havens, T.C. and Anderson, D.T., 2018, July. A bidirectional subsethood based similarity measure for fuzzy sets. In *2018 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)* (pp. 1-7). IEEE. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8491669>

Kabir, S., Wagner, C., Havens, T.C., Anderson, D.T. and Aickelin, U., 2017, July. Novel similarity measure for interval-valued data based on overlapping ratio. In *2017 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)* (pp. 1-6). IEEE. Available at: <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8015623>

McCulloch, J., Ellerby, Z. and Wagner, C., 2020, July. Choosing Sample Sizes for Statistical Measures on Interval-Valued Data. In *2020 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)* (pp. 1-7). IEEE. Available at: [https://nottingham-repository.worktribe.com/preview/4370777/WCCI\\_MC\\_sample\\_size.pdf](https://nottingham-repository.worktribe.com/preview/4370777/WCCI_MC_sample_size.pdf)

McCulloch, J., Ellerby, Z. and Wagner, C., 2019, June. On Comparing and Selecting Approaches to Model Interval-Valued Data as Fuzzy Sets. In *2019 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)* (pp. 1-6). IEEE. Available at: <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8858993>

McCulloch, J., Ellerby, Z. and Wagner, C., 2019. On the Relationship between Similarity Measures and Thresholds of Statistical Significance in the Context of Comparing Fuzzy Sets. *IEEE Transactions on Fuzzy Systems*. Available at: <https://core.ac.uk/download/pdf/210990178.pdf>

McCulloch, J., 2018, July. SyFSeL: Generating Synthetic Fuzzy Sets Made Simple. In *2018 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)* (pp. 1-6). IEEE. Available at: <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8491549>

Pekaslan, D., Garibaldi, J.M. and Wagner, C., 2018, July. Exploring subsethood to determine firing strength in non-singleton fuzzy logic systems. In *2018 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)* (pp. 1-8). IEEE. Available at: <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8491614>

Pekaslan, D., Garibaldi, J.M., Wagner, C. and Kabir, S., 2017. Determining firing strengths through a novel similarity measure to enhance uncertainty handling in non-singleton fuzzy logic systems. Available at: [https://nottingham-repository.worktribe.com/preview/892629/IJCCI\\_Determining%20Firing%20Strengths.pdf](https://nottingham-repository.worktribe.com/preview/892629/IJCCI_Determining%20Firing%20Strengths.pdf)

Razak, T.R., Garibaldi, J.M., Wagner, C., Pourabdollah, A. and Soria, D., 2017, July. Interpretability indices for hierarchical fuzzy systems. In *2017 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)* (pp. 1-6). IEEE. Available at: <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8015616>

### Cyber Protect: Protecting Businesses in the Eastern Region from the Risk of Cybercrime

No publications to date.

### Cyber Security Quirks: Personalised Interventions for Human Cyber Resilience

No publications to date.

### A Framework to Model and Incentivise Cyber Security Investment Decisions (MERIT)

No publications to date.

### Economic Metrics for Supporting Cyber Security Investment Decision-Making

No publications to date.

### Gamification Training to Protect Against Socially Engineered Cyber Attacks: An Evidence Based Design.

No publications to date.

### Incentivising Cyber Risk Management Behaviours: The Role of Cyber Insurance

MacColl, J., Nurse, J.R.C., & Sullivan, J. (2021). Cyber insurance and the cyber security challenge. *RUSI Occasional Paper*.

Sullivan, J., & Nurse, J.R.C. (2021). Cyber Security Incentives and the Role of Cyber Insurance. *RUSI Emerging Insights Paper*.

### Keeping the Internet of Things Secure: Investigating Incentives for Internet Service Providers and Individuals in the UK and Japan

No publications to date.

### Case by Case: Building a Database on Cybercriminal Business Models

No publications to date.

### Advanced Modelling of Cybercriminal Careers (AMOC): New Tech and Intelligence from Online Evidence Bases

Ursani, Z., Peersman, C., Edwards, M., Chen, C., and Rashid, A., 2021. The Impact of Adverse Events in Darknet Markets: an Anomaly Detection Approach. *International Workshop on Attackers and Cyber-Crime Operations (WACCO)*.

Williams, E.J., Edwards, M., Peersman, C., Davidson, B., and Rashid, A., 2020. Understanding motivations and characteristics of cybercriminals: Revisiting theoretical approaches through the lens of contemporary practitioner experiences. Presentation at *Cybercrime (online) conference*.

### Why Johnny doesn't write secure software: Secure software development by the Masses

Chowdhury, P.D., Hallett, J., Patnaik, N., Tahaei, M., and Rashid, A., 2021. Developers Are Neither Enemies Nor Users: They Are Collaborators. *IEEE Secure Development Conference*.

Hallett, J., Patnaik, N., Shreeve, B. and Rashid, A., 2021, May. "Do this! Do that!, And nothing will happen" Do specifications lead to securely stored passwords? In *2021 IEEE/ACM 43rd International Conference on Software Engineering (ICSE)* (pp. 486-498). IEEE.

Mukisa, S.S. and Rashid, A., 2017, September. Challenges of privacy requirements modelling in V2X applications: A telematic insurance case study. In *2017 IEEE 25th International Requirements Engineering Conference Workshops (REW)* (pp. 97-103). IEEE.

Patnaik, N., Hallett, J., and Rashid, A., 2019. An Analysis of Developers' Struggle With Crypto Libraries In: *Proceedings of the Fifteenth Symposium on Usable Privacy and Security USENIX Association*.

Rashid, A., 2021. Developer-Centred Security. In *Encyclopedia of Cryptography, Security and Privacy*. Springer.

Rauf, I., Petre, M., Tun, T., Lopez, T., Lunn, P., Van der Linden, D., Towse, J., Sharp, H., Levine, M., Rashid, A. and Nuseibeh, B., 2021. The Case for Adaptive Security Interventions. *ACM Transactions on Software Engineering and Methodology (TOSEM)*, 31(1), pp.1-52.

Rauf, I., Van der Linden, D., Levine, M., Towse, J., Nuseibeh, B., and Rashid, A., 2020. Security but not for security's sake: The impact of social considerations on app developers' choices. In: *13th International Workshop on Cooperative and Human Aspects of Software Engineering (CHASE)*, Seoul, South Korea.

van der Linden, D., Williams, E., Hallett, J., and Rashid, A., 2020. The impact of surface features on choice of(in)secure answers by Stackoverflow readers. In: *IEEE Transactions on Software Engineering (TSE)*.

van der Linden, D., Anthonysamy, P., Nuseibeh, B., Tun, T.T., Petre, M., Levine, M., Towse, J. and Rashid, A., 2020. Schrödinger's Security: Opening the Box on App Developers' Security Rationale. In: *Proc. 42nd International Conference on Software Engineering (ICSE)*, Seoul, South Korea.

van der Linden, D., Hadar, I., Edwards, M., and Rashid, A., 2019. Data, data, everywhere: quantifying software developers' privacy attitudes. In: *Proc. 9th Int. Workshop on Socio-Technical Aspects of Security (STAST)*, Luxembourg, Luxembourg, 2019.

van der Linden, D. and Rashid, A., 2019. The effect of software warranties on cybersecurity. *ACM SIGSOFT Software Engineering Notes*, 43(4), pp.31-35.

van der Linden, D., Rashid, A., Williams, E., and Warinschi, B., 2018. Safe Cryptography for All: Towards Visual Metaphor Driven Cryptography Building Blocks. In *SEAD'18: SEAD'18:IEEE/ACM 1st International Workshop on Security Awareness from Design to Deployment*, May 27, 2018, Gothenburg, Sweden. ACM, New York, NY, USA, Article 4, 4 pages. <https://doi.org/10.1145/3194707.3194709>

Weir, C., Rashid, A., and Noble, J., 2017. I'd Like to Have an Argument, Please: Using Dialectic for Effective App Security. In *EuroUSEC 2017: the 2nd European Workshop on Usable Security*. Reston, VA: Internet Society.

Weir, C., Rashid, A., and Noble, J., 2017. Developer Essentials: Top Five Interventions to Support Secure Software Development. Lancaster: Lancaster University.

### Online Ties Taking Over (OTTO)?

No publications to date.

### Addressing Cybersecurity and Cybercrime Via a Co-Evolutionary Approach to Reducing Human-Related Risks (ACCEPT)

Becker, I., Posner, R., Islam, T., Ekblom, P.J., Borrion, H., McGuire, M., Li, S., 2021. 'Privacy in Transport? Exploring Location Privacy User Segments.' in *Proceedings of the 54th Hawaii International Conference on System Sciences (HICSS 2021)*, pp. 5347-5356, University of Hawai'i at Mānoa, 2021 (Best Paper Award of Location Intelligence Invited Track)

Sağlam, R.B., Aslan, C.B., Li, S., Dickson L., Pogrebna, G., 2020. 'A Data-Driven Analysis of Blockchain Systems' Public Online Communications on GDPR.' In: *Proceedings of 2020 IEEE International Conference on Decentralized Applications and Infrastructures (IEEE DAPPS 2020)*, pp. 22-31. IEEE

Hernández-Castro, C.J., Li, S., R-Moreno, M.D., 2020. 'All About Uncertainties and Traps: Statistical Oracle-based Attacks on a New CAPTCHA Protection Against Oracle Attacks.' *Computers and Security*, vol. 92, Article No. 101758. Elsevier

Islam, T., Becker, I., Posner, R., Ekblom, P., McGuire, M., Borrion, H., Li, S., 2019. 'A Sociotechnical and Co-evolutionary Framework for Reducing Human- Related Risks in Cyber Security and Cybercrime Ecosystems.' In: Wang G., Bhuiyan M., De Capitani di Vimercati S., Ren Y.(eds) *Dependability in Sensor, Cloud, and Big Data Systems and Applications. DependSys 2019. Communications in Computer and Information Science, vol 1123.* Springer, Singapore

Mahaini, M.I., Li, S., Sağlam, R.B., 2019. 'Building Taxonomies based on Human-Machine Teaming: Cyber Security as an Example.' In: *Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES 2019)*, Article No. 30. ACM

Morris J, Becker I, Parkin S., 2019. 'In Control with no Control: Perceptions and Reality of Windows 10 Home Edition Update Features.' In: *Proceedings of 2019 Workshop on Usable Security (USEC). Internet Society*

Ng, I. and Wakenshaw, S., 2018. Service ecosystems: a timely worldview for a connected, digital and data-driven economy. *The Sage Handbook of Service-Dominant Logic, Sage, London*, pp.199-213.

Pogrebna, G., Renaud K, Taratine, B. (2019). 'The many faces of active cyber.' *Network Security, 2019(2)*, pp. 20.

Pogrebna, G., Skilton M. (2019). *Navigating New Cyber Risks: How Businesses Can Plan, Build and Manage Safe Spaces in the Digital Age.* (1st edition). Springer Nature Switzerland AG: Palgrave Macmillan

### Cyber Security Across the Lifespan (CSALSA)

Muir, K. and Joinson, A., 2020. An Exploratory Study into the Negotiation of Cyber-Security within the Family Home. *Frontiers in Psychology: Human-Media Interaction, vol. 11*, 424. <https://doi.org/10.3389/fpsyg.2020.00424>, <https://doi.org/10.3389/fpsyg.2020.00424>

### Evaluating Criminal Transactional Methods in Cyberspace as Understood in an International Context

No publications to date.

### Victims of Computer Misuse Crime

Button, M., Blackburn, D., Sugiura, L., Shepherd, D., Kapend, R., & Wang, V. (2021). From feeling like rape to a minor inconvenience: Victims' accounts of the impact of computer misuse crime in the United Kingdom. *Telematics and Informatics, 64*, 101675.

Button, M., Blackburn, D., Sugiura, L., Shepherd, D., Kapend, R., & Wang, V. (2021). Victims of Cybercrime: Understanding the Impact Through Accounts. In *Cybercrime in Context: The Human Factor in Victimization, Offending, and Policing* (pp. 137-156). Springer.

Button, M., Sugiura, L., Blackburn, D., Shepherd, D.W.J., Wang, V. and Kapend, R., 2020. *Victims of Computer Misuse: Main Findings.* Available at: [https://researchportal.port.ac.uk/portal/files/20818559/Victims\\_of\\_Computer\\_Misuse\\_Main\\_Findings.pdf](https://researchportal.port.ac.uk/portal/files/20818559/Victims_of_Computer_Misuse_Main_Findings.pdf)

Button, M., Sugiura, L., Shepherd, D.W.J., Blackburn, D., Wang, V. and Kapend, R., 2020. *Victims of Computer Misuse: Executive Summary.* Available at: [https://researchportal.port.ac.uk/portal/files/20818541/Victims\\_of\\_Computer\\_Misuse\\_Executive\\_Summary.pdf](https://researchportal.port.ac.uk/portal/files/20818541/Victims_of_Computer_Misuse_Executive_Summary.pdf)

### Connecting Delayed Pre-commitment with Cyber Awareness in Order to Address the Perception Gap and Present Bias

No publications to date.

### Motivating Jenny to Write Secure Software: Community and Culture of Coding

Lopez, T., Weir, C., Tun, T., Cooper, H., Bandara, A., Levine, M., Nuseibeh, B. and Sharp, H. (2020) 'Security in the World', *figshare [Online]*. DOI: 10.21954/ou.rd.12205712

Lopez, T., Weir, C., Tun, T., Cooper, H., Bandara, A., Levine, M., Nuseibeh, B. and Sharp, H. (2020) 'Security in the Community', *figshare [Online]*. DOI: 10.21954/ou.rd.12213113

Lopez, T., Weir, C., Tun, T., Cooper, H., Bandara, A., Levine, M., Nuseibeh, B. and Sharp, H. (2020) 'Security and Me', *figshare [Online]*. DOI: 10.21954/ou.rd.12213137

Lopez, T., Weir, C., Tun, T., Cooper, H., Bandara, A., Levine, M., Nuseibeh, B. and Sharp, H. (2020) 'Security Between Us', *figshare [Online]*. DOI: 10.21954/ou.rd.12213146

Lopez, T., Tun, T.T, Bandara, A., Levine, M., Nuseibeh, B. and Sharp, H. 2020. Taking the Middle Path: Learning about Security Through Online Social Interaction. *IEEE Software*, vol. 37, no. 1, pp. 25-30, Jan.-Feb. 2020.

Lopez, T., Tun, T.T, Bandara, A., Levine, M., Nuseibeh, B. and Sharp, H. 2019. An Anatomy of Security Conversations in Stack Overflow. *Software Engineering in Society, International Conference of Software Engineering, 2019*. Montréal, Canada, May 25 - June 1, 2019.

Lopez, T., Sharp, H., Tun, T.T., Bandara, A., Levine, M., and Nuseibeh, B. 2019. 'Hopefully We Are Mostly Secure': Views on Secure Code in Professional Practice', *12th International Workshop on Cooperative and Human Aspects of Software Engineering (CHASE), International Conference of Software Engineering, 2019*. Montréal, Canada, May 27, 2019.

Lopez, T., Sharp, H., Tun, T.T., Bandara, A., Levine, M., and Nuseibeh, B. 2019. Talking about security with professional developers, *7th International Workshop Series on Conducting Empirical Studies in Industry (CESSER-IP), International Conference of Software Engineering, 2019*. Montréal, Canada, May 28, 2019.

Lopez, T., Tun, T.T., Bandara, A., Levine, M., Nuseibeh, B. and Sharp, H. 2018. An Investigation of Security Conversations in Stack Overflow: Perceptions of Security and Community Involvement. *1st International Workshop on Security Awareness from Design to Deployment, International Conference of Software Engineering, 2018*. Gothenburg, Sweden, 27 May, 2018.

### Economical, Psychological and Societal Impact of Ransomware (EMPHASIS)

Connolly, L.Y., Lang, M. and Wall, D.S., 2019. Information Security Behavior: A Cross-Cultural Comparison of Irish and US Employees. *Information Systems Management*, 36(4), pp.306-322. DOI <https://www.tandfonline.com/doi/full/10.1080/10580530.2019.1651113>

de Balthasar T., Hernandez-Castro J. (2017) An Analysis of Bitcoin Laundry Services. In: *Lipmaa H., Mitrokotsa A., Matulevičius R. (eds) Secure IT Systems. NordSec 2017. Lecture Notes in Computer Science, vol 10674*. Springer, Cham. [https://doi.org/10.1007/978-3-319-70290-2\\_18](https://doi.org/10.1007/978-3-319-70290-2_18)

Goldsmith, A. and Wall, D.S., 2019. The seductions of cybercrime: Adolescence and the thrills of digital transgression. *European Journal of Criminology*, p.1477370819887305.

Hernandez-Castro, J., Cartwright, E. and Stepanova, A., 2017. Economic analysis of ransomware. Available at: <https://arxiv.org/pdf/1703.06660.pdf>

Wall, D.S., 2018. How big data feeds big crime. *Current History*, 117(795), pp.29-34.

Wall, D. S. and Boiten, E. (2017) NHS caught out by WannaCry - now scrambling to catch up. *Public Sector Focus*, 13, pp. 24-25.

Wall, David S., Crime, Security and Information Communication Technologies: The Changing Cybersecurity Threat Landscape and Its Implications for Regulation and Policing (July 20, 2017). <http://dx.doi.org/10.2139/ssrn.3005872>

Warren S., Oxburgh G., Briggs P., Wall D., 2017. How Might Crime-Scripts Be Used to Support the Understanding and Policing of Cloud Crime?. In: Tryfonas T. (eds) *Human Aspects of Information Security, Privacy and Trust. HAS 2017. Lecture Notes in Computer Science, vol 10292*. Springer, Cham. [https://doi.org/10.1007/978-3-319-58460-7\\_38](https://doi.org/10.1007/978-3-319-58460-7_38)

### Investigative Interviewing of Cybercrime Victims to Gain Best Evidence

No publications to date.

### Gentle Interventions for Security (GIFS)

No publications to date.

### Evaluating Cyber Security Evidence for Policy Advice (ECSEPA)

Chung A, Dawda S, Hussain A, Shaikh S and Carr M. (2018). 'Cybersecurity: Policy', *Encyclopedia of Security and Emergency Management, LR Shapiro and MH Maras eds*. Springer Nature. Available at: <https://link.springer.com/referencework/10.1007/978-3-319-69891-5>

Hussain A, Shaikh S, Chung A, Dawda S and Carr M. (2018). 'An Evidence Quality Assessment Model for Cybersecurity Policymaking'. *Critical Infrastructure Protection XII, IFIP*. Available at: <https://pureportal.coventry.ac.uk/en/publications/an-evidence-quality-assessment-model-for-cybersecurity-policymaki>

### Detecting and Preventing Mass Marketing Fraud (DAPM)

Edwards, M., Suarez-Tangil, G., Peersman, C., Stringhini, G., Rashid, A. and Whitty, M., 2018, May. The geography of online dating fraud. In *Workshop on Technology and Consumer Protection (ConPro). IEEE, San Francisco (Vol. 7)*. Available at: [https://kclpure.kcl.ac.uk/portal/files/96714575/2018conpro\\_geoscammy.pdf](https://kclpure.kcl.ac.uk/portal/files/96714575/2018conpro_geoscammy.pdf)

Sorell, T., Whitty, M., 2019. Online romance scams and victimhood. *Secur J* 32, 342-361. <https://doi.org/10.1057/s41284-019-00166-w>

Sorell, T., 2019. Scambaiting on the Spectrum of Digilantism. *Criminal Justice Ethics*, 38(3), pp.153-175.

Suarez-Tangil, G., Edwards, M., Peersman, C., Stringhini, G., Rashid, A. and Whitty, M., 2019. Automatically dismantling online dating fraud. *IEEE Transactions on Information Forensics and Security*, 15, pp.1128-1137.

Whitty, M.T., 2019. "Predicting susceptibility to cyber-fraud victimhood", *Journal of Financial Crime*, Vol. 26 No. 1, pp. 277-292. <https://doi.org/10.1108/JFC-10-2017-0095>

Whitty, M.T., 2018. Do you love me? Psychological characteristics of romance scam victims. *Cyberpsychology, behavior, and social networking*, 21(2), pp.105-109. Available at: <https://www.liebertpub.com/doi/pdfplus/10.1089/cyber.2016.0729>

Whitty, M., Edwards, M., Levi, M., Peersman, C., Rashid, A., Sasse, A., Sorell, T. and Stringhini, G., 2017, April. Ethical and Social Challenges with developing Automated Methods to Detect and Warn potential victims of Mass-marketing Fraud (MMF). In *Proceedings of the 26th International Conference on World Wide Web Companion* (pp. 1311-1314).



## Supporting Data Security and Privacy in the Home

Nthala, N. and Flechais, I., 2018. Informal support networks: an investigation into home data security practices. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS) 2018* (pp. 63-82).

## Developer Security Essentials – The Magid Project

Weir, C., Becker, I., Noble, J., Blair, L., Sasse, M. A. and Rashid, A. 2020. In: *Software - Practice and Experience*. 37 p. Interventions for Software Security: Creating a Lightweight Program of Assurance Techniques for Developers.

Weir, C., Blair, L., Becker, I., Noble, J., Sasse, A. and Rashid, A., 25/05/2019, *Proceedings of the 41st International Conference on Software Engineering: Software Engineering in Practice Track*. Sharpe, H. and Whalen, M. (eds.). IEEE.

## Impact of Gamification on Developer-Centred Security

Maarek, M., Louchart, S., McGregor, L. and McMenemy, R., 2018, December. Co-created Design of a Serious Game Investigation into Developer-Centred Security. In *International Conference on Games and Learning Alliance* (pp. 221-231). Springer, Cham. [https://doi.org/10.1007/978-3-030-11548-7\\_21](https://doi.org/10.1007/978-3-030-11548-7_21)

Maarek, M., McGregor, L., Louchart, S. and McMenemy, R., 2019, June. How could serious games support secure programming? Designing a study replication and intervention. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 139-148). IEEE. <https://doi.org/10.1109/EuroSPW.2019.00022>

## Visualising Access Control Policies

Morisset, C. and Sanchez, D., 2018. VisABAC: A Tool for Visualising ABAC Policies. In *ICISSP* (pp. 117-126). Available at: <https://www.scitepress.org/papers/2018/66474/66474.pdf>

Morisset, C. and Sanchez, D., 2018, January. On building a visualisation tool for access control policies. In *International Conference on Information Systems Security and Privacy* (pp. 215-239). Springer, Cham.

## Choice Architecture for Information Security

Briggs, D.J.L.C.P. and van Moorsel, A., 2014. Nudging whom how: IT proficiency, impulse control and secure behaviour. *Networks*, 49, p.18.

Coventry L., Briggs P., Jeske D., and van Moorsel A., 2014. SCENE: A Structured Means for Creating and Evaluating Behavioural Nudges in a Cyber Security Environment: [https://link.springer.com/chapter/10.1007%2F978-3-319-07668-3\\_23](https://link.springer.com/chapter/10.1007%2F978-3-319-07668-3_23)

Coventry, L., Jeske, D. and Briggs, P., 2014. Perceptions and actions: Combining privacy and risk perceptions to better understand user behaviour. <http://cups.cs.cmu.edu/soups/2014/workshops/privacy/s2p3.pdf>

Jeske, D., Coventry, L. and Briggs, P., 2014, July. Decision justifications for wireless network selection. In *2014 Workshop on Socio-Technical Aspects in Security and Trust* (pp. 1-7). IEEE.

Morisset, C., Yevseyeva, I., Gross, T. and van Moorsel, A., 2014, September. A formal model for soft enforcement: influencing the decision-maker. In *International Workshop on Security and Trust Management* (pp. 113-128). Springer, Cham.

Morisset, C., Gross, T., van Moorsel, A. and Yevseyeva, I., 2014, June. Nudging for quantitative access control systems. In *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 340-351). Springer, Cham.

Yevseyeva, I., Morisset, C., Gross, T. and van Moorsel, A., 2014, September. A decision making model of influencing behavior in information security. In *European Workshop on Performance Engineering* (pp. 194-208). Springer, Cham.

Yevseyeva, I., Morisset, C., Turland, J., Coventry, L., Gross, T., Laing, C. and van Moorsel, A., 2014. Consumerisation of IT: Mitigating risky user actions and improving productivity with nudging. *Procedia Technology*, 16, pp.508-517.

### Cyber Security Cartographies (CySeCa)

Burdon, M. and Coles-Kemp, L., 2019. The significance of securing as a critical component of information security: An Australian narrative in *Computers & Security*, 87, p.101601.

Burdon M., 2016. The regulatory challenges of Australian information security practice in *Computer Law & Security Review*

Coles-Kemp, L., 2014. Digital Enlightenment Yearbook 2014: Social Networks and Social Machines, Surveillance and Empowerment.

Lewis, M., 2014. A Tactile Visual Library To Support User Experience Storytelling in *Proceedings of NordDesign 2014*. Design Society, 2014.

### Games and abstraction

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C. and Smeraldi, F., 2016. Decision support approaches for cyber security investment. *Decision support systems*, 86, pp.13-23.

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C. and Smeraldi, F., 2014, June. Game theory meets information security management. In *IFIP International Information Security Conference* (pp. 15-29). Springer, Berlin, Heidelberg.

Hankin, C. and Malacaria, P., 2013. Payoffs, intensionality and abstraction in games. In *Computation, Logic, Games, and Quantum Foundations. The Many Facets of Samson Abramsky* (pp. 69-82). Springer, Berlin, Heidelberg.. [https://doi.org/10.1007/978-3-642-38164-5\\_6](https://doi.org/10.1007/978-3-642-38164-5_6)

Khouzani, M.H.R., Malacaria, P., Hankin, C., Fielder, A. and Smeraldi, F., 2016, September. Efficient numerical frameworks for multi-objective cyber security planning. In *European Symposium on Research in Computer Security* (pp. 179-197). Springer, Cham.

Panaousis, E., Fielder, A., Malacaria, P., Hankin, C. and Smeraldi, F., 2014, November. Cybersecurity games and investments: A decision support approach. In *International Conference on Decision and Game Theory for Security* (pp. 266-286). Springer, Cham.

### Productive Security – Improving Security Compliance and Productivity Through Measurement

Abu-Salma, R., Krol, K., Parkin, S., Koh, V., Kwan, K., Mahboob, J., Traboulsi, Z. and Sasse, M.A., 2017, April. The security blanket of the chat world: An analytic evaluation and a user study of telegram. *Internet Society*.

Beautement, A., Becker, I., Parkin, S., Krol, K. and Sasse, A., 2016. Productive security: A scalable methodology for analysing employee security behaviours. In *Twelfth Symposium on Usable Privacy and Security (SOUPS) 2016* (pp. 253-270).

- Becker, I. F., Parkin, S., and Sasse, M. A., 2016. "Combining Qualitative Coding and Sentiment Analysis: Deconstructing Perceptions of Usable Security in Organisations". In: *The LASER Workshop: Learning from Authoritative Security Experiment Results*. IEEE, 2016.
- Becker, I., Parkin, S. and Sasse, M.A., 2017a. Finding security champions in blends of organisational culture. *Proc. USEC*, 11.
- Becker, I., Parkin, S. and Sasse, M.A., 2017b. Measuring the Success of Context-Aware Security Behaviour Surveys. In *The {LASER} Workshop: Learning from Authoritative Security Experiment Results ({LASER} 2017)* (pp. 77-86).
- Beyer, M., Ahmed, S., Doerlemann, K., Arnell, S., Parkin, S., Sasse, A. and Passingham, N., 2016. Awareness is only the first step: A framework for progressive engagement of staff in cyber security. *Business white paper: Hewlett Packard*. Available at: <http://www.riscs.org.uk/wpcontent/uploads/2015/12/Awareness-is-Only-the-First-Step.pdf>
- Caputo, D.D., Pfleeger, S.L., Sasse, M.A., Ammann, P., Offutt, J. and Deng, L., 2016. Barriers to usable security? Three organizational case studies. *IEEE Security & Privacy*, 14(5), pp.22-32.
- Caulfield, T., Ioannidis, C. and Pym, D., 2016, February. Discrete Choice, Social Interaction, and Policy in Encryption Technology Adoption (Short Paper). In *International Conference on Financial Cryptography and Data Security* (pp. 271-279). Springer, Berlin, Heidelberg.
- Caulfield, T., Ioannidis, C. and Pym, D., 2016, November. On the adoption of privacy-enhancing technologies. In *International Conference on Decision and Game Theory for Security* (pp. 175-194). Springer, Cham.
- Caulfield, T. and Fielder, A., 2015. Optimizing time allocation for network defence. *Journal of Cybersecurity*, 1(1), pp.37-51.
- Caulfield, T. and Pym, D., 2015. Improving security policy decisions with models. *IEEE Security & Privacy*, 13(5), pp.34-41.
- Caulfield, T., Baddeley, M. and Pym, D., Social Learning in *Systems Security Modelling constructions*, 14(15), p.3.
- Caulfield, T., Pym, D. and Williams, J., 2014, June. Compositional security modelling. In *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 233-245). Springer, Cham.
- Collinson, M., McDonald, K. and Pym, D., 2014. A substructural logic for layered graphs. *Journal of Logic and Computation*, 24(4), pp.953-988. <https://doi.org/10.1093/logcom/exu002>
- Dodier-Lazaro, S., Abu-Salma, R., Becker, I. and Sasse, M.A., 2017, May. From paternalistic to user-centred security: Putting users first with value-sensitive design. In *CHI 2017 Workshop on Values in Computing. Values In Computing*.
- Dodier-Lazaro, S., Becker, I., Krinke, J. and Sasse, M.A., 2017, July. No Good Reason to Remove Features. In *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 25-44). Springer, Cham.
- Ioannidis, C., Pym, D., Williams, J. and Gheyas, I., 2019. Resilience in information stewardship. *European Journal of Operational Research*, 274(2), pp.638-653.
- Kenyon B., 2014. UCISA Information Security Management Toolkit Edition 1.0 Volume 1. Available at: <https://www.ucisa.ac.uk/ismt>
- Kirlappos, I., Parkin, S. and Sasse, M.A., 2015. "Shadow Security" as a tool for the learning organization. *ACM SIGCAS Computers and Society*, 45(1), pp.29-37.

- Kirlappos, I. and Sasse, M.A., 2015, February. Fixing Security Together: Leveraging trust relationships to improve security in organizations. *Internet Society*.
- Kirlappos, I., Parkin, S. and Sasse, M.A., 2014. Learning from "Shadow Security": Why understanding non-compliance provides the basis for effective security.
- Kirlappos I., Sasse M.A., 2014. What Usable Security Really Means: Trusting and Engaging Users. In: Tryfonas T., Askoxylakis I. (eds) *Human Aspects of Information Security, Privacy, and Trust. HAS 2014. Lecture Notes in Computer Science, vol 8533*. Springer, Cham. [https://doi.org/10.1007/978-3-319-07620-1\\_7](https://doi.org/10.1007/978-3-319-07620-1_7)
- Kirlappos, I., Beautement, A. and Sasse, M.A., 2013, April. "Comply or Die" Is Dead: Long live security-aware principal agents. In *International Conference on Financial Cryptography and Data Security (pp. 70-82)*. Springer, Berlin, Heidelberg.
- Krol, K., Spring, J.M., Parkin, S. and Sasse, M.A., 2016. Towards robust experimental design for user studies in security and privacy. In *The {LASER} Workshop: Learning from Authoritative Security Experiment Results ({LASER} 2016) (pp. 21-31)*.
- Krol, K., Parkin, S. and Sasse, M.A., 2016a. Better the devil you know: A user study of two CAPTCHAs and a possible replacement technology. In *NDSS Workshop on Usable Security (USEC) (Vol. 10)*.
- Krol, K., Parkin, S. and Sasse, M.A., 2016b. "I don't like putting my face on the Internet!": An acceptance study of face biometrics as a CAPTCHA replacement. In *2016 IEEE International Conference on Identity, Security and Behavior Analysis (ISBA) (pp. 1-7)*. IEEE.
- Murdoch, S.J., Becker, I., Abu-Salma, R., Anderson, R., Bohm, N., Hutchings, A., Stringhini, G. (2017). Are payment card contracts unfair? (Short paper). Abu-Salma, R., Sasse, M.A., Bonneau, J., Danilova, A., Naiakshina, A., Smith, M. (2017). *Obstacles to the Adoption of Secure Communication Tools*.
- Parkin, S., Krol, K., Becker, I. and Sasse, M.A., 2016. Applying cognitive control modes to identify security fatigue hotspots. In *Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016)*.
- Parkin, S. and Epili, S., 2015, July. A technique for using employee perception of security to support usability diagnostics. In *2015 Workshop on Socio-Technical Aspects in Security and Trust (pp. 1-8)*. IEEE.
- Parkin, S., Driss, S., Krol, K. and Sasse, M.A., 2015, December. Assessing the user experience of password reset policies in a university. In *International Conference on Passwords (pp. 21-38)*. Springer, Cham.
- Parkin, S. and Krol, K., 2015. Appropriation of security technologies in the workplace. Experiences of Technology Appropriation: Unanticipated Users, Usage, Circumstances, and Design, Oslo, Norway.
- Sasse, A., 2015. Scaring and bullying people into security won't work. *IEEE Security & Privacy*, 13(3), pp.80-83.
- Sasse, M.A., Steves, M., Krol, K. and Chisnell, D., 2014, June. The great authentication fatigue—and how to overcome it. In *International Conference on Cross-Cultural Design (pp. 228-239)*. Springer, Cham.
- Sasse, M.A. and Kirlappos, I., 2014. Design for Trusted and Trustworthy Services: Why We Must Do Better. *Trust, Computing, and Society*, pp.229-249.

Sasse, M.A., 2013, August. "Technology Should Be Smarter Than This!": A Vision for Overcoming the Great Authentication Fatigue. In *Workshop on Secure Data Management* (pp. 33-36). Springer, Cham.