CURRICULUM VITAE AND RESEARCH MEMO

Dr. TSOHOU AGGELIKI

Assistant Professor in Information Systems Security and Privacy

Department of Informatics, Ionian University

Corfu, October 2019

Table of Contents

A. CURRICULUM VITAE

A.1 PERSONAL INFORMATION

Name and Surname:	**Tsohou Aggeliki**
Parents names	George and Maria
Birth Date:	October 6, 1980
E-mail Address:	atsohou@ionio.gr
Phone (Work):	+30 - 2261087705
URL:	http://di.ionio.gr
Google Scholar:	https://scholar.google.com/citations?user=etn5eNkAAAAJ&hl=en

A.2 EDUCATION

ISO 27001 Lead Auditor (2016), Information Security Management Systems (ISMS) Auditor/Lead Auditor (In accordance with ISO 27001:2013), TUV NORD, IRCA Certified Training Course

Postdoctoral Researcher (2013-2014), University of Jyväskylä, Department of Computer Science and Information Systems, Finland

Postdoctoral Researcher (2011-2013), Brunel Business School, Brunel University West London, UK

PhD Diploma (Excellent), Department of Information and Communications Systems Engineering, University of the Aegean, Greece (2010) (Thesis: *Information Security Awareness in Information Systems Security Management*)

M.Sc. in Information Systems (Excellent), Department of Informatics, Athens University of Economics and Business, Greece (2002-2004)

B.Sc. in Informatics (Very Good), Department of Informatics, Athens University of Economics and Business, Greece (1998-2002)

A.3 RESEARCH INTERESTS

- Information Security and Privacy Policies, Risk Perceptions and User Awareness
- Information Security Risk Assessment and Management
- Data Protection Impact Assessment
- Security Policies for Acceptable Internet Use
- Privacy Enhancing Tools
- Privacy Protection in Information Systems
- Information Security and Privacy Standards

A.4 CURRENT EMPLOYMENT

September 2016 – now: **Assistant Professor** in Internet Information Security and Privacy, Ionian University, Department of Informatics, Greece

A.5 SYNOPSIS OF WORK EXPERIENCE

A.5.1 **September 2014 – September 2016**: Lecturer in Internet Information Security and Privacy, Ionian University, Department of Informatics, Greece

A.5.2 **July 2013 – August 2014:** Post-Doctoral Researcher, University of Jyväskylä, Department of Computer Science and Information Systems, Finland

A.5.3 **July 2012 - June 2013**: Senior Research Fellow in Information Security and Privacy for Cloud e-Government Services, Brunel University West London, UK.

A.5.4 **June 2011 – June 2012**: Senior Research Fellow, Marie Curie – FP7/People in e-Government Process Engineering, Brunel University West London, UK.

A.5.5 **December 2009 – June 2011**: Fellow, Special Secretary for Administrative Reform and eGovernment, Greek Ministry of the Interior, Decentralization and E-Government, Greece

A.5.6 **September 2010 – July 2011**: Visiting Lecturer, Department of Digital Systems, University of Piraeus, Greece

A.5.7 **February 2010 – July 2010:** Research Fellow, Department of Digital Systems, University of Piraeus, Greece

A.5.8 **March 2005 – September 2009**: Participation in research and development projects through University of the Aegean and Athens University of Economics and Business, Greece.

A.6 AWARDS AND GRANTS

A.6.1 **Outstanding Reviewer 2012** for the Scientific Journal Information Management and Computer Security, Emerald Literati Network Awards for Excellence 2012 (http://www.emeraldinsight.com/authors/literati/reviewer_2012.htm)

A.6.2 **Outstanding Reviewer 2013** for the Scientific Journal Transforming Government: People, Process and Policy, Emerald Literati Network Awards for Excellence 2013 (http://www.emeraldinsight.com/authors/literati/reviewer_2013.htm)

A.6.3 **Maria Curie Fellowship 2011** as part of the EU funded Project CEES

A.6.4 The article Tsohou A., Kokolakis S., Karyda M., Kiountouzis E., "Process-Variance Models in Information Security Awareness Research", *Information Management and Computer Security*, Vol.16, No. 3, pp. 271 – 287, 2008 was chosen from Emerald Publisher as a **Highly Commended Award Winner for Outstanding Paper at the Emerald Literati Network Awards for Excellence** 2009 and from Information Management and Computer Security Journal as a **Sample Article** (http://www.emeraldinsight.com/authors/literati/awards.htm?year=2009&journal=imcs)

A.6.5 **Fellowship**, M.Sc. program in Information Systems, Department of Informatics, Athens University of Economics and Business, Greece (2002-2004)

A.7 WORK EXPERIENCE

A.7.1 TEACHING EXPERIENCE

Postgraduate (MSc) Programs

A.7.1.1 **Course Instructor**, "*Internet Security and Privacy Policies*" module (Spring Semester, 2019), M.Sc. Program in Digital Services and Innovation, Department in Informatics, Ionian University

A.7.1.2 **Course Instructor**, "*Information Security Management*" module (Spring Semester, 2018), M.Sc. Program in Technologies and Management of Information and Communication Systems, University of the Aegean

A.7.1.3 **Course Instructor**, "*Special Topics in Internet Security and Privacy*" module (Fall Semester, 2015; Fall Semester 2016; Fall Semester 2017), M.Sc. Program in Informatics, Department in Informatics, Ionian University

A.7.1.4 **Course Instructor**, "*Information Systems and Network Security*" module (Spring Semester, 2016; 2017; 2018) M.Sc. Program in Informatics, Department in Informatics, Ionian University

A.7.1.5 **Course Instructor**, "*Information Systems*" module (Fall Semester, 2016), M.Sc. Program in Technologies and Management of Information and Communication Systems, University of the Aegean

A.7.1.6 **Course Instructor**, "*Information Systems Security and Privacy Enhancing Technologies*" module (Fall Semester, 2016), M.Sc. Program in Technologies and Management of Information and Communication Systems, University of the Aegean

A.7.1.7 **Visiting Lecturer**, invited lectures on the "*Programming Languages and Biological Databases*" module (Fall Semester, 2016), M.Sc. Program in Bioinformatics and Neuroinformatics, Department in Informatics, Ionian University

A.7.1.8 **Visiting Lecturer**, invited lectures on the "*Information Systems Security and Privacy Enhancing Technologies*" module (Fall Semester, 2015), M.Sc. Program in Technologies and Management of Information and Communication Systems, University of the Aegean

A.7.1.9 **Visiting Lecturer**, invited lectures on the "*Information Security Management*" module (Spring Semester, 2015), M.Sc. Program in Technologies and Management of Information and Communication Systems, University of the Aegean

A.7.1.10 **Post-Doctoral Researcher**, "*Information Security Management*" course (Spring Semester, 2014), in collaboration with Prof. Siponen Mikko, M.Sc. Program in Service Innovation and Management, Department of Computer Science and Information Systems, University of Jyväskylä, Finland

A.7.1.11 **Visiting Lecturer,** "*Information Security Management and Policies*" module (Spring Semester, 2011), M.Sc. "Techno-economical Management and Digital Systems Security", Department of Digital Systems, University of Piraeus, Greece

A.7.1.12 **Visiting Lecturer**, "*Information Security Management and Policies*" module (Spring Semester, 2010), M.Sc. course "Techno-economical Management and Digital Systems Security", Department of Digital Systems, University of Piraeus, Greece.

Undergraduate Programs

A.7.1.13 **Course Instructor**, "*Information Security and Privacy Technologies and Policies*" module (Fall Semester, 2014; 2015; 2016; 2017; 2019; 2019), Undergraduate Program, Department of Informatics, Ionian University

A.7.1.14 **Course Instructor**, "*Special Topics on Information Security*" module (Spring Semester, 2016; 2017; 2018; 2019), Undergraduate Program, Department of Informatics, Ionian University

A.7.1.15 **Course Instructor**, "*Information Systems Security Management*" module (Spring Semester, 2015; 2016; 2017; 2018; 2019), Undergraduate Program, Department of Informatics, Ionian University

A.7.1.16 **Course Instructor**, "Mathematical Programming" module (Fall Semester, 2014; 2015; 2016; 2017; 2018; 2019), Undergraduate Program, Department of Informatics, Ionian University

A.7.1.17 **Course Instructor**, "Decision Support Systems" module (Spring Semester, 2015), Undergraduate Program, Department of Informatics, Ionian University

A.7.1.18 **Visiting Lecturer**, "Information Systems Security" course (Spring Semester, 2011), Department of Digital Systems, University of Piraeus, Greece.

A.7.1.19 **Visiting Lecturer,** "Information Security Management and Policies" course (Fall Semester, 2010), Department of Digital Systems, University of Piraeus, Greece.

A.7.1.20 **Visiting Lecturer**, "Information Systems Security" course (Spring Semester, 2010), Department of Digital Systems, University of Piraeus, Greece.

Other Training Courses and Programs

A.7.1.21 **Invited Lecturer,** Lecture on Information Systems Security and Digital Privacy, National Centre for Public Administration and Local Government, Athens, Greece (2.2010-4.2010)

A.7.1.22 **Invited Lecturer**, Lecture on Information Security Management and International Standards, European Intensive Programme on Information and Communication Technologies Security (**IPICS 2009, 2010, 2011, 2012, 2013, 2015, 2017, 2018**)

A.7.2 PH.D. SUPERVISION AND EXTERNAL PH.D. REVIEWS

B.7.2.1 **Supervisor** on the Ph.D. research by *Rena Lavranou*, "Artificial Intelligence and Internet Users' Information Privacy Awareness Enhancement" Ionian University, In progress

B.7.2.2 **Supervisor** on the Ph.D. research by *Ioannis Paspatis*, "De-anonymization of Mobile Application Data and Privacy Risks", Ionian University, In progress

B.7.2.3 **Supervisor** on the Ph.D. research by *Aikaterini Soumelidou*, "Privacy Policy Visualization and Information Privacy Awareness", Ionian University, In progress

B.7.2.4 **Supervisor** on the Ph.D. research by *Thanos Papaioannou*, "Digital Identity and Privacy Perceptions", Ionian University, In progress

B.7.2.5 **Member of the Supervising Committee** for the Ph.D. research by *Andreas Skalkos*, "Information Privacy and Human Behaviour", University of the Aegean, In progress

B.7.2.6 **Member of the Review Committee** for the doctoral thesis by *Giannakas Filipos*, "Utilization of games in mobile devices for enhancing security and privacy awareness of primary education Internet users", University of the Aegean, September 2018

B.7.2.7 **Member of the Review Committee** for the doctoral thesis by *Georgiou Dimitra*, "Security Policies for Cloud Computing", University of Piraeus, December 2017

B.7.2.8 **Member of the Review Committee** for the doctoral thesis by *Alexandra Michota*, "Privacy in Online Social Networks", University of Piraeus, December 2017

B.7.2.9 **Member of the Review Committee** for the doctoral thesis by *Simou Stavros*, "Designing Cloud Forensic-Enabled System, University of the Aegean, June 2017

B.7.2.10**External Reviewer** on the doctoral thesis of *Saud Alotaibi*, titled "Transparent User Authentication for Mobile Applications", University of Plymouth, January 2019.

B.7.2.11**External Reviewer** on the doctoral thesis of *Jouko Selkälä,* titled "Chief Information Officer Decision making: Issues and a Process View", Department of Computer Science and Information Systems, University of Jyvaskyla, November 2015.

B.7.2.12**External Reviewer** on the doctoral thesis of *Ana Nieto Jiménez*, titled "Design of Mechanisms for Development of Secure Systems trading-off Quality of Service", University of Malaga, May 2015.

A.7.3 MSc THESIS SUPERVISION

A.7.3.1 **Supervisor** on six MSc Theses for the M.Sc. Program in Informatics, Department in Informatics, Ionian University

A.7.3.2 **Member of the Advisory Committee** on four MSc. Theses for the M.Sc. Program in Informatics, Department in Informatics, Ionian University

A.7.3.3 **Member of the Advisory Committee** on four MSc. Theses, M.Sc. Programs, University of the Aegean

A.7.4 BSc THESIS SUPERVISION

A.7.4.1 **Supervisor** on eight completed BSc Thesis for the B.Sc. Program, Ionian University

A.7.3.4 **Member of the Advisory Committee** on seven completed BSc Thesis for the B.Sc. Program, Ionian University

A.7.3.5 **Member of the Advisory Committee** on one BSc Thesis for the B.Sc. Program, University of Piraeus

A.7.5 WORK EXPERIENCE IN RESEARCH AND DEVELOPMENT PROJECTS

Scientific Coordinator in International Research Projects

A.7.4.1 **Scientific Coordinator**, EU Programme H2020, Project Reference DS-08-2017: 787068, "*Data Governance for Supporting GDPR (DEFeND)*", Ionian University, (07.2018-Today)

A.7.4.2 **Scientific Coordinator**, Cooperation Programme Interreg V/A Greece-Italy (EL-IT) 2014-2020: 5003441, "Open City TechNology Enabler (OCTaNe)", Ionian University, (05.2018-Today)

Researcher in International Research Projects

A.7.4.3 **Information Security Awareness Expert**, Expert Services related to the European Cyber Security Month (ECSM) in 2019, ENISA (09.2019-12.2019)

A.7.4.4 **Information Security Awareness Expert**, Expert Services related to the European Cyber Security Month (ECSM) in 2017, ENISA (11.2016-11.2017)

A.7.4.5 **Process Engineer**, EU Programme FP7/Marie Curie People Project Reference IAPP-2008-230658: "*CEES - Citizen oriented Evaluation of E-Government Systems*", Brunel University, (07.2011-04.2013).

A.7.4.6 **Information systems evaluation**, EU Programme FP7/Project Reference INFSO-ICT-248010: "*UbiPOL- Ubiquitous Participation Platform for Policy Making*", Brunel University, (08.2011-04.2013).

A.7.4.7 **Information Privacy Manager**, EU Programme FP7/Project Reference CIP-ICT-PSP-2011-5: "*Openly Accessible Services and Interacting Society*", Brunel University, (02.2012-06.2013).

Scientific Coordinator National Research and Development Projects

A.7.4.8 **Scientific Manager**, "*ioniAn Pdmfc Partnership (APPly)*", Ionian University, PDM &FC (04.2017 – Today)

A.7.4.9 **Scientific Manager**, IPICS 2017 European Intensive Programme on Information and Communication Technologies Security, Ionian University (03.2017 – 08.2017)

Researcher in National Research and Development Projects

A.7.4.10 **Information Privacy Expert**, "Compliance of Ionian University with the General Data Protection Regulation 2016/679 - GDPR)" (09.2018 – 12.2018)

A.7.4.11 **Information Privacy Expert**, "Compliance of the Pasteur Institute with the General Data Protection Regulation 2016/679 - GDPR)" (11.2018 – 02.2019)

A.7.4.12 **Information Privacy Expert**, "Compliance of University of the Piraeus with the General Data Protection Regulation 2016/679 - GDPR)" (08.2018 – 12.2018)

A.7.4.13**Information Privacy Expert**, “Compliance of University of the Aegean with the General Data Protection Regulation 2016/679 - GDPR)” (General Data Protection Regulation - GDPR)» (03.2018 – 08.2018)

A.7.4.14 **Information Privacy Expert**, “Compliance of GRNet with the General Data Protection Regulation 2016/679 - GDPR)” (06.2018 – 10.2018)

A.7.4.15 **Information Security Risk Analyst**, “*Training on Information Security Risk Assessment for Executives of the Information Technology Services Department for the Ministry of Finance*”, PLANET A.E., 2016.

A.7.4.16**Information Security Risk Analyst**, “Study, Design and Evaluation of a Comprehensive Security Plan for the GIS of the Greek Prefectural Administrations”, TREK Consulting SA and University of the Aegean, Greece, 2008-2009.

A.7.4.17**Research Fellow**, Development of teaching material for the course entitled: “Information Security in e-Government Systems for the project training and certification of local government employees on basic skills at ICT use”, PLANET SA, Greece, 2009.

A.7.4.18**Information Security Risk Analyst**, “Study, Design and Evaluation of a Comprehensive Security Plan for the National Observatory for SMEs web portal of the Hellenic Organization of Small and Medium Sized Enterprises and Handicraft (EOMMEX) S.A”, TREK Consulting SA - University of the Aegean, Greece, 2008-2009.

A.7.4.19**Information Security Risk Analyst**, “Study, Design and Evaluation of a Comprehensive Security Plan for the back-office information system for the Greek Prefectural Administrations”, National Technical University of Athens, Information Society SA, University of the Aegean, Greece, 2008-2009.

A.7.4.20**Information Security Risk Analyst**, “Study, Design and Evaluation of a Comprehensive Security Plan for the Development Directorate information system and the web portal of the Greek Prefectural Administrations”, KANTOR Management & Consultants SA, and University of the Aegean, Greece, 2007-2008.

A.7.4.21**Information Security Risk Analyst,** “Security study for the information system and web portal for the General Secretariat for Information Systems”, Greek Ministry of Economy & Finance, University of the Aegean, 2007-2008.

A.7.4.22**Information Security Risk Analyst**, “Security study for the Greek one-stop-shop eGovernment services (Portal ERMIS)”, InfoQuest SA - Decision Systems Integration SA, Greek Ministry of Interior, and University of the Aegean, 2007-2008.

A.7.4.23**Information Security Risk Analyst,** “Study, Design and Evaluation of a Comprehensive Security Plan for the Directorate of Commerce information system and web portal for the Greek Prefectural Administrations”, Siemens SA - Quality & Reliability SA, Information Society SA, Athens University of Economics and Business, 2006.

A.7.4.24**Information Security Risk Analyst**, “Study, Design and Evaluation of a Comprehensive Security Plan for the Town-Planning And Town-Planning Applications Directorate integrated information system and web portal for the Greek Prefectural Administrations", Singular Integrators SA – UniSystems SA, Information Society SA, Athens University of Economics and Business, 2006.

A.7.4.25**Information Security Risk Analyst**, "Security study for the Country Signing Certification Authority and Document Signer Certificate Authority applications for Electronic Passports of the National Passport Center", D.S. Technologies SA, Hellenic Police, Athens University of Economics and Business, 2006.

A.7.4.26**Information Security Risk Analyst**, "Study, Design and Evaluation of a Comprehensive Security Plan for the clinical information system for the management of regional health services of Ionian Islands", Remaco SA, Information Society SA, Athens University of Economics and Business, 2006.

A.7.4.27**Information Security Risk Analyst**, "Study, Design and Evaluation of a Comprehensive Security Plan for the Hellenic Fire Department information system and web portal", Quality and Reliability SA, Hellenic Fire Service, University of the Aegean, 2006.

A.7.4.28**Research Fellow,** ISO/IEC 27001:2005 conformity assessment for the ECDL Hellas, CheckPoint LtD, ECDL Hellas SA, 2006.

A.7.4.29**Information Security Risk Analyst**, "Security study of the integrated clinical information system for the General Hospital in Korinthos", Korinthos General Hospital, University of the Aegean, 2006.

A.7.4.30**Information Security Risk Analyst**, "Study and technical specifications for a modular system that will support the administrative functions of Greek universities (e-University)", Information Society SA, University of the Aegean, 2005-2006.

A.7.4.31**Research Fellow**, "Study for the development of the web security seal of the Hellenic Organization for Standardization", Hellenic Organization for Standardization, Athens University of Economics and Business, 2005.

A.7.5 OTHER WORK EXPERIENCE

Expert Consultant, Special Secretary for Administrative Reform and eGovernment, Greek Ministry of the Interior, Decentralization and E-Government (**12.2009-06.2011)**

A.8 PUBLICATIONS

A.8.1 PUBLICATIONS IN PEER-REVIEW SCIENTIFIC JOURNALS

(Exhibitors per article indicate the total number of citations from non-authors)

J.22 Soumelidou, A. and Tsohou, A. (2019), Effects of privacy policy visualization on users' information privacy awareness level, *Information Technology & People*, Accepted, Emerald, ISI impact factor for 2017: 2.138

J.21 Tsohou, A., Siponen, M. and Newman, M. (2019), How Does IT-Based Service Degradation Influence Consumers' Use of Services? An IT-Based Service Degradation Decision Theory, *Journal of Information Technology*, ISI impact factor for 2017: 4.435, Accepted.

J.20 Lavranou, E. and Tsohou, A. (2019), Developing and Validating a Common Body of Knowledge for Information Privacy, *Information & Computer Security*, Accepted.

J.19 Paspatis, I. Tsohou, A. and Kokolakis, S. (2019), AppAware: A Policy Visualization Model for Mobile Applications, *extended article from MCIS 2018, Information & Computer Security*, Accepted.

J. 18 [11] Siponen, M. and Tsohou, A. (2018), Demystifying the influential IS legends of "positivism", *Journal of the Association for Information Systems*, Vol. 19, No, 7, pp. 600-617 ISI impact factor for 2017: 2.839

J.17 [4] Tsohou, A. and Holtkamp, P. (2018), Are users competent to comply with information security policies? An analysis of professional competence models, *Information Technology & People*, Vol. 31 Issue: 5, pp.1047-1068, https://doi.org/10.1108/ITP-02-2017-0052, Emerald, ISI impact factor for 2017: 2.138

J. 16 [8] Lee, H., Tsohou A. and Choi, Y. (2017), Embedding persuasive features into policy issues: Implications to designing public participation processes, Government Information Quarterly, Accepted, ISI impact factor for 2017: 4.009

J. 15 [3] Tsohou, A. and Kosta, E. (2017), Enabling valid informed consent for location tracking through privacy awareness of users: A process theory, *Computer Law & Security Review: The International Journal of Technology Law and Practice*, Vol. 33, No. 4, pp. 434-457, ISI impact factor for 2017: 0.867

J.14 [73] Tsohou A., Karyda M., Kokolakis S., (2015) Analyzing the role of Cognitive and Cultural Biases in the Internalization of Information Security Policies: Recommendations for Information Security Awareness Programs, *Computers & Security*, 52, 128-141 ISI impact factor for 2017: 2.650

J.13 Moon J.O., Lee H., Kim J.W., Aktas E., Tsohou A., Choi Y. (2015), Customer Satisfaction from Open Source Software Services in the Presence of Commercially Licensed Software, *Asia Pacific Journal of Information Systems*, Vol. 25, No. 3, pp. 473-499

J.12 [69] Tsohou A., Karyda M., Kokolakis S., Kiountouzis E., (2014) Managing the Introduction of Information Security Awareness Programs in Organisations, *European Journal of Information Systems*, 24, pp. 38-58, ISI impact factor for 2016: 2.819

J.11 [15] Tsohou A., Lee H., Irani A., (2014), Innovative Public Governance Through Cloud Computing: Information Privacy, Business Models and Performance Measurement Challenges, *Transforming Government: People, Process and Policy*, Vol. 8, No. 2, pp.251 – 282, Emerald.

J.10 [24] Tsohou A., Lee H., Irani Z., Weerakkody V., Osman I., and Anouze A., (2013), Proposing a Reference Process Model for the Citizen-Centric Evaluation of E-Government Services, *Transforming Government: People, Process and Policy*, Vol. 7, No. 2, pp. 240-255, Emerald

J.09 [6] Tsohou A., Lee H., Al-Yafi K., Weerakkody V., El-Haddadeh R., Irani Z., Ko A., Medeni T., Campos L., (2012), Supporting Public Policy Making Processes with Workflow Technology: Lessons Learned From Cases in Four European Countries, *International Journal of Electronic Government Research*, Vol. 8, No. 3, pp.63-77, IGI Global

J.08 [52] Tsohou A., Karyda M., Kokolakis S., Kiountouzis E., (2012), Analyzing Trajectories of Information Security Awareness, *Information Technology & People*, Vol. 25, Issue 3, 2012, Emerald, ISI impact factor for 2016: 1.339

J.07 [40] Tsohou A., Kokolakis S., Lambrinoudakis C., Gritzalis S., (2010), A security standards' framework to facilitate best practices' awareness and conformity, *Information & Computer Security*, Vol. 18, No. 5, pp. 350-365, Emerald

J.06 [4] Tsohou A., Lambrinoudakis C., Kokolakis S., Gritzalis S., The Importance of Context Dependant Privacy Requirements and Perceptions to the Design of Privacy Aware Systems, *The European Journal of the Informatics Professional (UPGrade*), Vol. XI, Issue 1, pp. 32-37.

J.05 [5] Tsohou A., Karyda M., Kokolakis S., Kiountouzis E., (2010), Aligning Security Awareness with Information Systems Security Management, *Journal of Information System Security*, Vol. 6, No. 1, pp. 36-54.

J.04 Tsohou A., Rizomiliotis P., Lambrinoudakis C., Gritzalis S., (2009), Security and Privacy Issues in Bipolar Disorder Research, *The Journal on Information Technology in Healthcare*, Vo. 7, No. 4, pp. 244-250

J.03 [73] Tsohou A., Kokolakis S., Karyda M., Kiountouzis E., (2008), Investigating information security awareness: research and practice gaps, *Information Security Journal: A Global Perspective*, Vol.17, No. 5-6, pp. 207-227, Taylor and Francis

J.02 [33] Tsohou A., Kokolakis S., Karyda M., Kiountouzis E., (2008), Process-Variance Models in Information Security Awareness Research, *Information Management and Computer Security*, Vol.16, No. 3, pp. 271 – 287, 2008, Emerald (Chosen as a Highly Commended Award Winner for Outstanding Paper at the Emerald Literati Network Awards for Excellence 2009).

J.01 [69] Tsohou A., Karyda M., Kokolakis S., Kiountouzis E., (2006), Formulating Information Systems Risk Management Strategies through Cultural Theory, *Information Management and Computer Security*, Vol. 14, No. 3, pp. 198-217, Emerald

A.8.2 PUBLICATIONS IN PEER-REVIEW CONFERENCE PROCEEDINGS

(Exhibitors per article indicate the total number of citations from non-authors)

C.25 Diamantopoulou, V., Tsohou, A., and Karyda, M. (2019) General Data Protection Regulation and ISO/IEC 27001:2013: Synergies of activities towards organizations' compliance, In *Proceedings of the TrustBus 2019 International Conference on Trust, Privacy & Security in Digital Business*, August 2019, Linz, Austria, Lecture Notes in Computer Science LNCS, Springer

C.24 Jiang, H., Siponen, M., and Tsohou, A. (2019), A Field Experiment for Understanding the Unintended Impact of Internet Monitoring on Employees: Policy Satisfaction, Organizational Citizenship Behavior and Work Motivation, In Proceedings of *the 27th European Conference on Information Systems (ECIS)*, Stockholm & Uppsala, Sweden, June 8-14, 2019, Association for Information Systems (AIS).

C.23 Paspatis, I. Tsohou, A. and Kokolakis, S. (2018) AppAware: A Model for Privacy Policy Visualization for Mobile Applications, In Proceedings of *the 12th Mediterranean Conference on Information Systems,* Corfu, Greece, September 2018, Association for Information Systems (AIS).

C. 22 [1] Gritzalis, A., Tsohou A. and Lambrinoudakis C. (2017) Transparency Enabling Systems for Open Governance: Their Impact on Citizens' Trust and the Role of Information Privacy, In the Proceedings of the *7th International Conference on eDemocracy, Privacy-Preserving, Secure, Intelligent eGovernment Services*, 14 – 15 December 2017, Athens - Greece

C. 21 Kosyfaki, C., Angelova N., Tsohou A. and Magkos, M. (2017) The Privacy Paradox in the Context of Online Health Data Disclosure by Users, *In (Themistocleous M., Morabito V., eds.) Proceedings of the 14th European, Mediterranean and Middle Eastern Conference on Information Systems (EMCIS 2017),* Coimbra, Portugal, September 2017, Lecture Notes in Business Information Processing, Springer, Vol., 299, pp. 421-428.

C. 20 [1] Paspatis, I., Tsohou A. and Kokolakis S. (2017), Mobile Application Privacy Risks: Viber Users' De-Anonymization Using Public Data, *In the Proceedings of the 11th Mediterranean Conference on Information Systems,* Genova, Italy, September 2017, Association for Information Systems (AIS).

C. 19 Skalkos A., Tsohou A., Karyda M. and Kokolakis S. (2017) Investigating the Values that Drive the Adoption if Anonymity Tools: A Laddering Approach, Research In progress, *The 11th Mediterranean Conference on Information Systems,* Genova, Italy, September 2017

C.18 Diamantopoulou V., Tsohou A., Loukis E. and Gritzalis S. (2017) Does the Development of Information Systems Resources Lead to the Development of Information Security Resources? An Empirical Investigation, *In the Proceedings of the 23rd Americas Conference on Information Systems (AMCIS 2017),* Boston, USA, August 2017

C.17 [1] Karavaras E., Magkos E. and Tsohou A. (2016) Low User Awareness Against Social Malware: an Empirical Study and Design of a Security Application, *In Proceedings of the 13th European, Mediterranean and Middle Eastern Conference on Information Systems (EMCIS 2016)*, Krakow, Poland, June 2016

C.16 [1] Jiang H. and Tsohou A. (2015), The same Antecedents do not fit all activities: an Activity-Specific Model of Personal Internet Use in Workplace, (Research in Progress), *In Proceedings of the 23nd European Conference on Information Systems (ECIS 2015),* May 2015, Mursten, Germany, Association for Information Systems (AIS)

C.15 [7] Koufi V., Tsohou A., Malamateniou F. and Vassilacopoulos G., (2014), A Framework for Privacy-Preserving Access Control to Cloud Process-based PHR Systems, *In Proceedings of the 25th European Medical Informatics Conference*, August 2014, Istanbul, Turkey.

C.14 [1] Jiang H. and Tsohou A. (2014), Expressive Or Instrumental: A Dual-Perspective Model Of Personal Web Usage At Workplace (Research in Progress) *In Proceedings of the 22nd European Conference on Information Systems (ECIS 2014),* June 2014, Tel Aviv, Israel, Association for Information Systems (AIS)

C.13 [5] Jiang H. and Tsohou A. (2014), The Dual Nature of Personal Web Usage At Workplace: Impacts, Antecedents And Regulating Policies, *In Proceedings of the 22nd European Conference on Information Systems (ECIS 2014),* June 2014, Tel Aviv, Israel, Association for Information Systems

(AIS)

C.12 Oh J., Lee H. and Tsohou A. (2013) Relational Versus Structural Embeddedness in IT Outsourcing Networks: The Role Of Requirement Unpredictability And Measurement Difficulty, *In Proceedings of the 17th Pacific Asia Conference on Information Systems (PACIS)*, June 2013, Jeju Island, Korea, Association for Information Systems (AIS)

C.11 [2] Tsohou A., Al-Yafi K., Lee H., (2012), Evaluating M-Government Applications: An Elaboration Likelihood Model Framework, *Proceedings of the European, Mediterranean & Middle Eastern Conference on Information Systems (EMCIS)*, (Eds. Ghoneim A., Klischewski R., Schrödl H., Muhammed K.), 7-8 June, Munich, Germany

C.10 Tsohou A., Lee H., Zahir I., Weerakkody V., Osman I., Latif A., Medeni T., (2012), Evaluating E-Government Services From A Citizens' Perspective: A Reference Process Model, *Proceedings of the European, Mediterranean & Middle Eastern Conference on Information Systems (EMCIS)*, (Eds. Ghoneim A., Klischewski R., Schrödl H., Muhammed K.), 7-8 June, 2012, Munich, Germany

C.09 [12] El-Haddadeh R., Tsohou A., Karyda M., (2012), Implementation Challenges for information Security Awareness initiatives in E-government, *Proceedings of the ECIS 2012 20th European Conference on Information Systems,* (Eds. Janssen M, Weerakkody V, Dwivedi Y), June 2012, Barcelona, Spain, Association for Information Systems (AIS)

C.08 [2] Tsohou A., Karyda M., Kokolakis S., Kiountouzis E., (2010), Analyzing Information Security Awareness through Networks of Association, *Proceedings of the TrustBus 2010 7th International Conference on Trust, Privacy & Security in Digital Business*, pp. 227-237, September 2010, Bilbao, Spain, Lecture Notes in Computer Science LNCS, Springer

C.07 [13] Evans R., Tsohou A., Tryfonas T., Morgan T., (2010), Architecting Secure Systems with the ISO standards 26702 and 27001, *Proceedings of the SoSE 2010 5th IEEE International Conference on Systems of Systems Engineering*, pp. 1-6, June 2010, Loughborough, UK, IEEE Computer Society Press

C.06 [11] Vrakas N., Kalloniatis C., Tsohou A., Lambrinoudakis C., (2010), Privacy Requirements Engineering for Trustworthy e-Government Services, *Proceedings of the TRUST 2010 3rd International Conference on Trust and Trustworthy Computing*, pp. 298-307, June 2010, Berlin, Germany, Lecture Notes in Computer Science LNCS, Springer

C.05 [3] Tsohou A., Kokolakis S., Lambrinoudakis C., Gritzalis S., (2010), Unifying ISO Security Standards Practices into a Single Security Framework, *Proceedings of the 12th Annual IFIP Workshop on Information Security Management*, pp. 188-203, May 2010, Port Elizabeth, South Africa

C.04 [17] Tsohou A., Karyda M., Kokolakis S., Kiountouzis E., (2009), Aligning Security Awareness with Information Systems Security Management, *Proceedings of the MCIS 2009 4th Mediterranean Conference on Information Systems*, pp. 866- 878, September 2009, Athens, Greece, Association for Information Systems (AIS)

C.03 [9] Tsohou A., Kokolakis S., Lambrinoudakis C., Gritzalis S., (2009), Information Systems Security Management: A review and a classification of the ISO standards, *Proceedings of the e-Democracy 2009 Next Generation Society: Technological and Legal Issues*, pp. 220-235, Athens, Greece, 2009, Lecture Notes of the ICSSIT Institute for Computer Sciences, Social Informatics, and Telecommunications Engineering LNICST 26, Springer

C.02 Tsohou A., Rizomiliotis P., Lambrinoudakis C., Gritzalis S., (2009), Security and Privacy Issues in Bipolar Disorder Research, *Proceedings of the ICICTH 7th International Conference on Information and Communication Technologies in Health*, July 2009, Samos, Greece, INEAG

C.01 [11] Tsohou A., Theoharidou M., Kokolakis S., Gritzalis D., (2007), Addressing Cultural Dissimilarity in the Information Security Management Outsourcing Relationship, *Proceedings of the TRUSTBUS'07 4th International Conference on Trust, Privacy and Security in Digital Business*, pp.24-33, Regensburg, Germany, September 2007, Lecture Notes in Computer Science LNCS, Springer

A.8.3 PUBLICATIONS IN WORKSHOPS, POSTERS AND ABSTRACTS IN PEER-REVIEW CONFERENCE PROCEEDINGS

W.10 Diamantopoulou V., Tsohou A. and Karyda M. (2019), From ISO/IEC 27002:2013 Information Security Controls to Personal Data Protection Controls: Guidelines for GDPR Compliance, 3rd International Workshop on SECurity and Privacy Requirements Engineering (SECPRE 2019), Luxemburg, September 2019.

W.09 Papaioannou T., Tsohou A. and Karyda M. (2019), Shaping Digital Identities in Social Networks: Data Elements and the Role of Privacy Concerns, 3rd International Workshop on SECurity and Privacy Requirements Engineering (SECPRE 2019), Luxemburg, September 2019.

W.08 Tsohou A., Magkos M., Mouratidis H., Chrysoloras G., Piras L., Pavlidis M., Debussche J., Rotoloni

M. and Gallego-Nicasio Crespo B., Privacy, Security, Legal and Technology Acceptance Requirements for a GDPR Compliance Platform, 3rd International Workshop on SECurity and Privacy Requirements Engineering (SECPRE 2019), Luxemburg, September 2019.

W.07 Grammenos, P., Syreggela, N.A., Magkos E. and Tsohou A. (2016), Internet Addiction of Young Greek Adults: Psychological Aspects and Information Privacy, In Proceedings of the 2nd World Congress in Genetics, Geriatrics and Neurodegenerative Diseases Research, Springer, Sparta, Greece, October 2016

W.06 Papaioanou A. and Tsohou A. (2016), Social Networks as Education Tools: Aspects of Use and Privacy, In Proceedings of the 8th Conference on Informatics in Education, October 2016, Piraeus, Greece.

W.05 Lee H. and Tsohou A. (2014), Can information systems intervene into citizens cognitive process to facilitate public participation? An elaboration likelihood model approach, *pre-ECIS SIGeGov workshop* "Rethinking Information Systems in the Public Sector: Bridging Academia and Public Service", June 2014, Tel Aviv, Israel.

W.04 Tsohou A., Lee H., Weerakkody V., Irani Z., (2013), A Persuasive Information System for Policy Making: An Elaboration Likelihood Model Approach, *IT Management Worskhop*, 17th Pacific Asia Conference on Information Systems (PACIS), June 2013, Jeju Island, Korea

W.03 Tsohou A. (2013), Innovative governance through cloud computing in public sector (OASIS-Openly Accessible Services and Interacting Society), *4th Transforming Government Workshop*, London, UK, March 2013

W.02 Tsohou A., Lee H., and Barbos M., (2012), A location based persuasive information system for public consultation: An elaboration likelihood mode approach. *In the proceedings of 2nd international workshop on advanced service management*, Matsmoto, Japan, 29 – 30 Aug 2012

W.01 Tsohou A., Lee H., Rebahi Y., Khalil M. and Hohberg S. (2012), Ubiquitous Participation Platform for POLicy Making (UbiPOL): Security and Identity Management Considerations, **Poster and Abstract** *In Proceedings of 9th Trust, Privacy and Security in Digital Business Conference (TrustBus 2012)*, (Eds. Fischer-Hübner S., Katsikas S. and Quirchmayr G.), Lecture Notes in Computer Science, Springer Berlin Heidelberg, Vol. 7449, p.p. 236-237, September, 2012, Vienna, Austria

A.8.4 THESES

T.02 Tsohou A., "*Information Security Awareness in Information Systems Security Management*", PhD Thesis, Department of Information and Communication Systems Engineering, University of the Aegean, Greece, February 2010.

T.01 Tsohou A., "Risk Perceptions in Information Systems Security Management: Theoretical approaches and influential factors", M.Sc. Thesis, M.Sc. in Information Systems, Department of Informatics, Athens University of Economics and Business, February 2004 .

A.9 INVITED SPEAKER ACTIVITIES

A.9.1 KEYNOTE SPEAKER

A.9.1.1 GDPR – A researcher's view**, Executive Breakfast: GDPR - Security Solutions and Compliance**, 5th April 2017, PDMFC, IBM, Lisbon, Portugal

A.9.2 INVITED SPEAKER

A.9.2.1 "The role of employees and personal data subjects for GDPR application", **Workshop GDPR the next day**, 30th May 2018, University of Piraeus, Greece

A.9.2.2 "Human behaviour change as a success factor for Internet information security", **3rd Business Continuity Management Forum**, 15th December 2016, Netweek, Fidel & Fortis Ltd. Athens, Greece

A.9.2.3 "Information privacy policies and Internet users' privacy awareness" **ECSM Cyber Awareness Event**, 21st October 2016, ENISA, Piraeus, Greece

A.10 ORGANIZATION OF INTERNATIONAL CONFERENCES, WORKSHOPS AND SUMMER SCHOOLS

A.9.1 ORGANIZATION OF INTERNATIONAL SUMMER SCHOOLS

A.9.7.1 **Organization of Summer School,** IPICS 2017 European Intensive Programme on Information and Communication Technologies Security, Organized by Ionian University Department of Informatics, Organizing Committee: Tsohou A., Magkos M., Chrissikopoulos V., Kastabolidou K., (Corfu: Greece), June-July 2017

A.9.7.2 **Member of Organizing Committee**, IPICS 2010 European Intensive Programme on Information and Communication Technologies Security, Samos, Greece, 17-27 July 2010

A.9.2 ORGANIZATION OF INTERNATIONAL CONFERENCES AND WORKSHOPS

A.9.7.1 **Member of Organizing Committee,** *STM 2010 6t^h International Workshop on Security and Trust Management*, in conjunction with EuroPKI 2010 and CRITIS 2010, Athens, Greece, September 2010, Lecture Notes in Computer Science LNCS, Springer

A.11 SYNTACTIC ACTIVITIES

A.11.1 MEMBER OF EDITORIAL TEAM IN INTERNATIONAL JOURNALS

A.11.1.1 *Internet Research, Emerald* (Editorial Board Member) (Enrolment in 2011)

A.11.1.2 *Information Management and Computer Security, Emerald* (Editorial Advisory Board Member) (Enrolment in 2011)

A.11.1.3 *Transforming Government: People, Process and Policy, Emerald* (Editorial Advisory Board Member) (Enrolment in 2015)

A.11.2 ASSOCIATE EDITOR IN INTERNATIONAL JOURNALS

A.11.2.1 *Human-centric Computing and Information Sciences*, Springer, Science Citation Index Expanded (Enrolment in 2018)

A.11.3 MEMBER OF EDITORIAL TEAM IN SPECIAL ISSUES

A.11.3.1 *Algorithms-SI 2016* Special Issue "Humanistic Data Processing" Algorithms Journal

A.11.3.2 *CaEE-SI 2016* New Trends in Humanistic Informatics: Implementations and Applications, Computers & Electrical Engineering Journal

A.11.3.3 *JoWUA 2013*, Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications Journal

A.11.4 INTERNATIONAL CONFERENCES TRACK CHAIR

A.11.5.1 *EMCIS 2019, 16th European Mediterranean & Middle Eastern Conference on Information Systems,* 9-10 December 2019, Dubai, Track: **Information Systems Security and Information Privacy Protection**, Track Chair: Aggeliki Tsohou

A.11.5.2 *MCIS 2018, 12th European Mediterranean & Middle Eastern Conference on Information Systems, Corfu, Greece, 28-30* September 2018, Track: **Security and Privacy**, Track Chairs: Javier Lopez, Maria Karyda, Aggeliki Tsohou

A.11.5.3 *EMCIS 2018, 15th European Mediterranean & Middle Eastern Conference on Information Systems,* 7-8 September 2017, 4-5 October, Limassol, Cyprus, Track: **Information Systems Security and Information Privacy Protection**, Track Chair: Aggeliki Tsohou

A.11.5.4 *MCIS 2017, 11th European Mediterranean & Middle Eastern Conference on Information Systems*, 5-6 September 2017, Genova, Italy, Track: **Trust, Security and Privacy**, Track Chairs: Maria Karyda and Aggeliki Tsohou

A.11.5.5 *EMCIS 2017, 14th European Mediterranean & Middle Eastern Conference on Information Systems*, 7-8 September 2017, Coimbra, Portugal, Track: **Security and Privacy Protection for Information Systems and Digital services,** Track Chairs: Aggeliki Tsohou, Theo Tryfonas, Hemin Jiang

A.11.5.6 *EMCIS 2016, 12th European Mediterranean & Middle Eastern Conference on Information Systems*, 1-2 June, Krakow, Poland, Track: **Security and Privacy Protection for Information Systems and Digital services,** Track Chairs: Aggeliki Tsohou, Ella Kolkowska

A.11.5.7 *EMCIS 2015, 11th European Mediterranean & Middle Eastern Conference on Information Systems*, 1-2 June, Athens, Greece, Track: **Security and Privacy Protection for Information Systems and Digital services,** Track Chairs: Aggeliki Tsohou

A.11.5.8 *EMCIS 2013, 10th European, Mediterranean & Middle Eastern Conference on Information Systems*, 17 – 18 October, Windsor, United Kingdom, **Track: Security and Privacy Protection for Information Systems**, Track Chairs: Aggeliki Tsohou, Costas Lambrinoudakis

A.11.5.9 *AMCIS 2011, 18th Americas Conference on Information Systems*, Seattle, Washington August 9-11, 2012, **Mini-track: E-Government Trust and Information Security Issues and Concerns,** Mini-Track Chairs: Ramzi El-Haddadeh, Aggeliki Tsohou

A.11.4 INTERNATIONAL CONFERENCES PROGRAM COMMITTEE MEMBER

A.11.3.1 *E-Democracy 2019,* 9th International Conference on e-Democracy, Athens, Greece, December 2019

A.11.3.2 *HAISA 2019, 14h* International Symposium on Human Aspects of Information Security & Assurance, Nicosia, Cyprus, July 2019

A.11.3.3 *ESORICS 2019* 24th European Symposium on Research in Computer Security, Luxemburg, Luxemburg, September 2019

A.11.3.4 *HAISA 2018, 13h* International Symposium on Human Aspects of Information Security & Assurance, Dundee, Scotland, August 2018

A.11.3.5 *PCI 2018,* 22nd Panhellenic Conference on Informatics, Athens, Greece, November 2018

A.11.3.6 *ESORICS 2018* 23rd European Symposium on Research in Computer Security, Barcelona, Spain, September, 2018

A.11.3.7 *HAISA 2017, 12th* International Symposium on Human Aspects of Information Security & Assurance, Adelaide, Australia, November 2017

A.11.3.8 *TrustBus 2017,* 14th International Conference on Trust, Privacy and Security in Digital Business, Lyon, France, August 2017

A.11.3.9 *E-Democracy 2017* 7th International Conference on e-Democracy, Athens, Greece, December 2017

A.11.3.10 *COLLABORATECOM 2017* 3rd International Conference on Collaborative Computing: Networking, Applications and Worksharing, Guangzhou, China, November 2017

A.11.3.11 *ESORICS 2017* 22nd European Symposium on Research in Computer Security, Oslo, Norway, September 2017

A.11.3.12 *PCI 2016,* 20th Panhellenic Conference on Informatics, Patra, Greece, November 2016

A.11.3.13 *TrustBus 2016,* 13th International Conference on Trust, Privacy and Security in Digital Business, Porto, Portugal, September 2016

A.11.3.14 *ESORICS 2016*, 21st European Symposium On Research In Computer Security, Crete, Greece, September 2016

A.11.3.15 *SECRYPT 2016*, 13th International Conference on Security and Cryptography, Lisbon, Portugal, July 2016

A.11.3.16 *E-Democracy 2015,* 7th International Conference on e-Democracy, Athens, Greece, December 2015

A.11.3.17 *ARES 2015*, 10th International Conference on Trust, Privacy and Security in Digital Business, Toulouse, France, September 2015

A.11.3.18 *TrustBus 2015* 12th International Conference on Trust, Privacy and Security in Digital Business, València, Spain, September 2015

A.11.3.19 *PCI 2015*, 19th Panhellenic Conference on Informatics, Athens, Greece, October 2015

A.11.3.20 *TrustBus 2014,* 11th International Conference on Trust, Privacy and Security in Digital Business, Munich, Germany, September, 2014

A.11.3.21 *PCI 2014*, 18th Panhellenic Conference on Informatics, Athens, Greece, October 2014

A.11.3.22 *ARES 2014,* 9th International Conference on Trust, Privacy and Security in Digital Business, Fribourg, Switzerland, September 2014

A.11.3.23 *IADIS 2014*, 7th International Conference on Information Systems, Madrid, Spain, March 2014

A.11.3.24 *ARES 2013,* 8th International Conference on Availability, Reliability and Security Regensburg, Germany, September 2013

A.11.3.25 *TrustBus 2013,* 10th International Conference on Trust, Privacy and Security in Digital Business, Prague, Czech Republic, August 2013

A.11.3.26 *IADIS 2013*, 7th International Conference on Information Systems, Lisbon, Portugal, March 2013

A.11.3.27 *TrustBus 2012,* 9th International Conference on Trust, Privacy and Security in Digital Business, Vienna, Austria, September 2012

A.11.3.28 *IEEE CloudCom 2011*, 3rd IEEE International Conference on Cloud Computing Technology and Science, Greece, Athens, December 2011

A.11.3.29 *TrustBus 2011*, 8th International Conference on Trust, Privacy and Security in Digital Business, Toulouse, France, August, 2011

A.11.3.30 *SECRYPT 2010*, 7th International Conference on Security and Cryptography, Athens, Greece, July 2010

A.11.3.31 *OTM IS 2010*, 5th International Symposium on Information Security, Crete, Greece, October 2010

A.11.5 REVIEWER OF RESEARCH WORK IN SCIENTIFIC JOURNALS

A.11.4.1 *International Journal of Information Security*, Springer

A.11.4.2 *Information & Management*, Elsevier

A.11.4.3 *Communications of the Association for Information Systems*, Association for Information Systems

A.11.4.4 *Behaviour & Information Technology*, Taylor & Francis

A.11.4.5 *Information Technology & People*, Emerald

A.11.4.6 *Computers and Security*, Elsevier.

A.11.4.7 *Information Security Journal: A Global Perspective* (Previously published as: *Information Systems Security*), Taylor & Francis.

A.11.4.8 *International Journal of Information Security*, Springer.

A.11.4.9 *Transforming Government: People, Process and Policy*, Emerald.

A.11.4.10 *Journal of Enterprise Information Management*, Emerald.

A.11.4.11 *Asia Pacific Journal of Information Systems, Korea Society of Management Information Systems*

A.11.4.12 *European Journal of Information Systems*, Palgrave

A.11.4.13 *Journal of the Association of Information Systems*, Association for Information Systems

A.11.4.14 *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, Innovative Information Science & Technology Research Group

A.11.4.15 *International. Journal of Electronic Governance*, Inderscience Publishers

A.11.4.16 *International Journal of Critical Infrastructure Protection*, Elsevier

A.11.5. REVIEWER OF RESEARCH WORK IN INTERNATIONAL CONFERENCES

A.11.6.1 *ICIS 2019*, International Conference on Information Systems, Munich, Germany, December 2019

A.11.6.2 *PACIS 2019*, 23rd Pacific Asia Conference on Information Systems, Xi'an, China, July 2019

A.11.6.3 *ICEGOV 2019*, 12th International Conference on Theory and Practice of Electronic Governance, Melbourne, Australia, April 2019

A.11.6.4 *DBSec 2019*, Annual IFIP WG 11.3 Conference on Data and Applications Security and Privacy, Charleston, SC, USA, July 2019

A.11.6.5 *DPM 2018*, 13th International Workshop on Data Privacy Management, Barcelona, Spain, September 2018

A.11.6.6 *ISSA 2017* 16th International Information Security South Africa Conference, Sandton, South Africa, August 2017

A.11.6.7 *DPM 2016*, 11th International Workshop on Data Privacy Management, Heraklion, Crete, September 2016

A.11.6.8 *ISSA 2016* 15th International Information Security South Africa Conference, Johannesburg, South Africa, August 2016

A.11.6.9 *ECIS 2016*, 24th European Conference of Information Systems, Istanbul, Turkey, June 2016

A.11.6.10 *IFIP SEC 2016*, 31th International Information Security and Privacy Conference (IFIP TC-11 SEC), Ghent, Belgium, June 2016

A.11.6.11 *SITIS 2015*, 11th International Conference on Signal Image Technology & Internet Based Systems, Bangkok, Tailand, November 2015

A.11.6.12 *IFIPTM 2015*, 9th International Conference on Trust Management (IFIP), Hamburg, Germany, May 2015

A.11.6.13 *ISPEC 2015*, 11th International Conference on Information Security Practice and Experience, Beijing, China, May 2015

A.11.6.14 *PCI 2015*, 19th Panhellenic Conference on Informatics, Athens, Greece, October 2015

A.11.6.15 *E-Democracy 2015*, 6th International Conference on e-Democracy, Athens, Greece, December 2015

A.11.6.16 *CRITIS 2015*, 10th International Workshop on Critical Information Infrastructures Security, Berlin, Germany, October 2015

A.11.6.17 *ECIS 2015*, 23rd European Conference of Information Systems, Münster, Germany, May 2015

A.11.6.18 *RCIS 2015, 9th International Conference on Research Challenges in Information Science,* Athens, Greece, May 2015

A.11.6.19 *ECIS 2014*, 22nd European Conference on Information Systems, Tel Aviv, Israel, June 2014

A.11.6.20 *CRITIS 2014*, 9th International Workshop on Critical Information Infrastructures Security, Limassol, Cyprus, October 2014

A.11.6.21 *IFIPTM 2014*, 8th International Conference on Trust Management (IFIP WG 11.11), Singapore, July 2014

A.11.6.22 *ICIS 2014*, 22nd International Conference on Information Systems, Auckland, New Zealand, December 2014

A.11.6.23 *SEC 2014*, 29th International Information Security and Privacy Conference (IFIP TC-11 SEC), Marrakech, Morocco, June 2014

A.11.6.24 *PACIS 2014* 18th Pacific Asia Conference on Information Systems, Chengdu, China, June 2014

A.11.6.25 *PCI 2014*, 18th Panhellenic Conference on Informatics, Athens, Greece, October 2014

A.11.6.26 *PACIS 2013*, 17th Pacific Asia Conference on Information Systems, Jeju Island, Korea, June 2013

A.11.6.27 *ECIS 2013,* 21st European Conference on Information Systems, Utrecht, The Netherlands, June 2013

A.11.6.28 *IEEE GLOBECOM ManSec-CC 2012,* 1rst International workshop on Management and Security technologies for Cloud Computing, California, USA, December 2012

A.11.6.29 *EMCIS 2012,* 9th European, Mediterranean and Middle Eastern Conference on Information Systems, Munich, Germany, June 2012

A.11.6.30 *CAiSE 2011,* 23rd International Conference on Advanced Information Systems Engineering, London, UK, June 2011

A.11.6.31 *WISTP 2011,* 5th Workshop in Information Security Theory and Practice, Heraclion, Greece, June 2011

A.11.6.32 *IFIP SEC 2011, 26th International Information Security Conference (IFIP TC-11),* Luzern, Switzerland, June 2011

A.11.6.33 *WMSCI 2010,* 14th World Multi-Conference on Systemics, Cybernetics and Informatics, Orlando, Florida, USA, June 2010

A.11.6.34 *CRITIS 2010,* 5th International Conference on Critical Information Infrastructure Security, Athens, Greece, September 2010

A.11.6.35 *EGOVIS 2010,* 1st International Conference on Electronic Government and the Information Systems Perspective, Bilbao, Spain, September 2010.

A.11.6.36 *ECIS 2010,* 18th European Conference on Information Systems, University of Pretoria, South Africa, June 2010

A.11.6.37 *HAISA 2009,* 3rd International Symposium on Human Aspects of Information Security & Assurance, Athens, Greece, June 2009

A.11.6.38 *ISSA 2009* Information Security Conference, Johannesburg, South Africa, July 2009

A.11.6.39 *ESORICS 2008,* 13th European Symposium on Research in Computer Security, Malaga, Spain, October 2008

A.11.6.40 *ISC 2008,* 11th Information Security Conference, Taipei, Taiwan, September 2008.

A.11.6.41 *ICIS 2007,* 15th International Conference on Information Systems, Montréal, Québec, Canada, December 2007.

A.11.6.42 *IADIS e-Commerce 2007,* 6th International Conference on e-Commerce, Algarve, Portugal, December 2007.

A.12 ADMINISTRATIVE ACTIVITIES

A.12.1 Coordinator

A.12.7.1 PhD Studies Coordinator (2018- Today)

A.12.7.2 Erasmus Representative for the Department of Informatics (2017-Today)

A.12.7.3 Coordinator of the undergraduate and postgraduate studies timetable (2014 - Today)

A.12.7.4 Coordinator of the undergraduate and postgraduate exams timetable (2015 - Today)

A.12.1 PARTICIPATION IN COMMITTEES

A.12.7.1 Member of the Coordination Committee for the Msc Studies Program “Digital Services and Innovation”, (2018 - Today)

A.12.7.2 Member of the Committee for the ‘Strategy of Buildings and Infrastructure Usage’ for the Department (2015)

A.12.7.3 Member of the Committee for the Department’s Website Content analysis (2015)

A.12.7.4 Member of the Committee for the Coordination of the M.Sc. in Informatics (2015 – Today)

A.12.7.5 Coordination of the Ceremony for the Honorary Doctorate Dr. Bernd Wegner from the Department of Informatics, Ionian University

A.12.7.6 Coordination of the Ceremony for the Honorary Doctorate Dr. Georgios Paxinos from the Department of Informatics, Ionian University

A.12.7.7 Member of the Committee for the preparation of Ionian University for External Auditing by the Hellenic Quality Assurance & Accreditation Agency (HQA)

B. RESEARCH MEMO FOR PUBLICATIONS

B.1 PUBLICATIONS IN PEER-REVIEW SCIENTIFIC JOURNALS—

J.22 Soumelidou, A. and Tsohou, A. (2019), Effects of privacy policy visualization on users' information privacy awareness level, *Information Technology & People*, Accepted, Emerald, ISI impact factor for 2017: 2.138

The purpose of this paper is to propose visualization techniques as a new representation for privacy policies instead of traditional textual representation, and to examine empirically their effects on users' information privacy awareness level. We selected as a case the privacy policy of Instagram and conducted two empirical investigations, each one with three interventions, each representing a different version of the Instagram privacy policy to users. Through a pre and a post questionnaire we examined the effects that each representation technique had on users' privacy awareness level.The paper finds that visualized privacy policies lead to higher privacy awareness levels than conventional textual ones, especially when icons are included. This study provides evidence that the visualization techniques are superior to the conventional privacy policy regarding the enhancement of privacy awareness. Moreover, we implemented two new representation techniques offering beneficial guidelines for designing more attractive privacy policy representations. However, our sample is rather limited for generalization to the wide population; nonetheless they are significant to demonstrate the effect of visualized techniques. The results and the methodology of the paper, could guide practitioners for the representation of a privacy policy, given that we provide systematic and concrete steps. This paper examines the value of privacy policy visualization as a new approach for enabling user privacy awareness, as well as implements two visualization techniques for a given privacy policy. The paper and its findings should be useful for researchers, as well as for practitioners.

J.21 Tsohou, A., Siponen, M. and Newman, M. (2019), How Does IT-Based Service Degradation Influence Consumers' Use of Services? An IT-Based Service Degradation Decision Theory, *Journal of Information Technology*, ISI impact factor for 2017: 4.435, Accepted.

Information technology is crucial for modern services. Service delivery may include a complex mix of information technology and telecommunication providers, global networks and customers' information technology devices. This research focuses on service failures that are caused by information technology problems, which we conceptualize as information technology-based service degradation (ITSD). When information technology-based service degradation occurs in a modern service, the information technology problem may originate from the service provider, another partner or any information technology equipment involved. But the customer may not be able to pinpoint the source of the problem immediately. We argue that existing research can only partially explain customers' behavior following information technology-based service degradation; current research cannot account for the way in which information technology characteristics in information technology-based service degradation influence customers' decisions to continue using or rejecting the service. To fulfill this gap, we interviewed information technology-based services' customers. Our interviews suggest that the reasons affecting customers' behavior may change and have differing importance during the information technology-based service degradation experience. We theorized the information technology-based service degradation experience into five stages: blaming, bypassing, tolerating, abandoning and overcoming. The first two stages contain stage-specific factors influencing the progression of service usage, and the final three stages contain stage-specific factors that matter in the decision to use or quit the service. As a new contribution, we propose a stage theory for explaining customers' behavior following information technology-based service degradation. Our results outline new research directions in information technology-based service degradation, including further testing and refinement of our proposed theory in the case of different services. For service providers, our findings provide new information for improving service recovery strategies to keep customers engaged.

J.20 Lavranou, E. and Tsohou, A. (2019), Developing and Validating a Common Body of Knowledge for Information Privacy, *Information & Computer Security*, Accepted.

This paper aims to present a common body of knowledge (CBK) for the field of information privacy, titled InfoPrivacy CBK. The purpose of the proposed CBK is to guide internet users to better understand the concept of information privacy and associate information privacy-related concepts. The InfoPrivacy CBK was created with an educational orientation to provide the basis for designing privacy awareness and training programs and organizing relevant educational material. The proposed CBK for information privacy was developed conceptually and includes five domains and four levels of analysis. It is illustrated with conceptual maps. The authors identified a variety of concepts related to information privacy and created a set of categories to categorize the concepts. They used, as inclusion criteria, both theoretical and practical information privacy aspects, so that the developed CBK can address the challenges of modern technologies for preserving information privacy. To validate and refine the conceptually developed CBK, the authors conducted an empirical research, in which seven information privacy experts participated. The experts commented largely positively for the structure and content of InfoPrivacy CBK, as well as for the extent to which it achieves the intended educational goals. The proposed InfoPrivacy CBK was validated by a limited number of information privacy experts, mainly due to the lengthy and in-depth participation that was required.

The InfoPrivacy CBK can be used primarily by privacy awareness and training programs developers, such as organizations, data protection officers, the state, educational policy makers and teachers. Internet users will benefit from InfoPrivacy CBK by acquiring knowledge and skills from theoretically grounded training programs, which can enhance their awareness and critical thinking on issues related to the protection of their information privacy. This will lead to more privacy-aware online societies, communities, networks, etc. This work intends to bridge the existing gap in the literature through the creation of a novel CBK for information privacy; information privacy is a field for which no such research effort has been recorded. This paper offers important knowledge in the field of information privacy, which could be useful to both technological education designers and learners (students, employees, etc.).

J. 19 Paspatis, I. Tsohou, A. and Kokolakis, S. (2019), AppAware: A Policy Visualization Model for Mobile Applications, *extended article from MCIS 2018, Information & Computer Security*, Accepted.

J. 18 *Siponen, M. and Tsohou, A. (2017), Demystifying the influential IS legends of "positivism", Journal of the Association for Information Systems, Accepted, ISI impact factor for 2016: 2.109*

Positivism has been used to establish a standard that IS research must meet to be scientific. According to such positivistic beliefs in IS, scientific research should: 1) be generalizable; 2) focus on stable independent variables; 3) have certain ontological assumptions; and 4) use surveys rather than qualitative methods. We argue that logical positivist philosophers required none of these. On the contrary, logical positivist philosophers regarded philosophizing in general and ontological considerations in particular as nonsense. Moreover, the positivists' preferred empirical research method was not a survey, but rather a qualitative observation recorded by field notes. In addition, positivist philosophers neither required statistical nor non-statistical generalizability. Many positivist philosophers also acknowledged the study of singular cases as being scientific.

Many research orientations (e.g., single-setting research, examination of change, qualitative research) that are deemed as unscientific in IS seem to be (in principle) "scientific" according to logical positivism. In turn, what has been justified as scientific by positivism in IS (e.g., requirements of statistical or non-statistical generalizability, surveys, focus on fixed things, ontological views) either were not required by logical positivists or were regarded as nonsensical by logical positivists. Furthermore, given that positivism is sometimes associated (or confused) with logical empiricism in IS, we also briefly discuss logical empiricism. Finally, realizing that certain influential, taken-for-granted assumptions that underlie IS research are unwarranted, could have ground-breaking implications for future IS research.

J.17 Tsohou, A. and Holtkamp, P. (2018), Are users competent to comply with information security policies? An analysis of professional competence models, *Information Technology & People*, Vol. 31 Issue: 5, pp.1047-1068, https://doi.org/10.1108/ITP-02-2017-0052, Emerald, ISI impact factor for 2017: 2.138

Information security policies (ISPs) are used by organizations to communicate rules on the use of information systems (IS). Research studies show that compliance with the ISPs is not a straightforward issue and that several factors influence individual behavior toward ISP compliance, such as security awareness or individual perception of security threats. The purpose of this paper is to investigate the competencies associated with users' ISP compliance behavior. In order to reveal the competencies that are associated with the users' ISP compliance behavior, the authors systematically analyze the ISP compliance literature and the authors develop an ISP compliance competency model. The authors then target to explore if IS users are equipped with these competencies; to do so, the authors analyze professional competence models from various industry sectors and compare the competencies that they include with the developed ISP compliance competencies. The authors identify the competencies associated with ISP compliance and the authors provide evidence on the lack of attention in information security responsibilities demonstrated in professional competence frameworks. ISP compliance research has focused on identifying the antecedents of ISP compliance behavior. The authors offer an ISP compliance competency model and guide researchers in investigating the issue further by focusing on the professional competencies that are necessary for IS users. The findings offer new contributions to practitioners by highlighting the lack of attention on the information security responsibilities demonstrated in professional competence frameworks. The paper also provides implications for the design of information security awareness programs and information security management systems in organizations. To the best of the authors' knowledge, the paper is the first study that addresses ISP compliance behavior from a professional competence perspective.

Lee, H., Tsohou A. and Choi, Y. (2017), Embedding persuasive features into policy issues: Implications to designing public participation processes, Government Information Quarterly, Accepted, ISI impact factor for 2016: 4.090

J.16 Lee, H., Tsohou A. and Choi, Y. (2017), Embedding persuasive features into policy issues: Implications to designing public participation processes, Government Information Quarterly, Volume 34, Issue 4, December 2017, pp. 591-600, ISI impact factor for 2016: 4.090

Public participation is one of the most important tasks for policy making processes, and public authorities are lacking ideas on designing public participation processes facilitating active citizen participation. Based on a persuasion theory, this paper examines if policy issues embedded with persuasive features draw more attention, longer elaboration time and more participation. Particularly preference matching, location matching, social proof and authority are identified as persuasive features in e-participation context and propositions on their impacts on citizens' participation processes are developed. A prototype mobile participation tool is developed to test the propositions and tested by 80 experiment participants in the UK and Turkey. The findings indicate that the mixture of central and peripheral features is most effective in drawing participation while single feature has limitations. This study also argues that the design of e-participation tools needs to consider the psychological aspects of citizens for motivating their participations.

J.15 *Tsohou, A. and Kosta, E. (2017), Enabling valid informed consent for location tracking through privacy awareness of users: A process theory, Computer Law & Security Review: The International Journal of Technology Law and Practice, Vol. 33, No. 4, pp. 434-457, ISI impact factor for 2016: 0.938*

People use mobile devices for an increasing variety of purposes in order to enjoy the vast possibilities; they check the local weather, road traffic, personalised local news, their personalised favourite social network etc. At the same time, application developers and market stores deploy mobile applications that collect vast amounts of information on mobile users, such as their age, gender, location or specific phone identifiers. Numerous studies illustrate that mobile applications collect valuable information about users and use it for profiling the users for their own purposes or sell this information for commercial interests. Therefore, the topic of consent to information processing becomes increasingly more interesting for researchers, legal experts and practitioners.

In this paper, the authors examine the issue of valid informed consent for location tracking by mobile phone users. They first analyse the legal premises for informed consent that represent requirements for mobile application developers and providers who request consent. However, the ones who give consent are the mobile users and therefore their understanding of consent is of paramount importance. Extensive literature is missing on empirical studies examining the topic from the users' perception perspective. For that reason, the authors conduct an empirical investigation with mobile users and present their findings in the form of a process theory. The process theory reveals how users' valid informed consent for location tracking can be obtained, starting from enhancing reading the privacy policy to stimulating privacy awareness and enabling informed consent. The paper includes a discussion section in which the authors describe the implications of the process theory for the different stakeholders and offer recommendations deriving from the empirical findings. The contribution is addressed to software and mobile application developers and providers, technology regulation researchers and policy makers, as well as security and privacy researchers.

J. 14 *Tsohou A., Karyda M., Kokolakis S., (2015) Analyzing the role of Cognitive and Cultural Biases in the Internalization of Information Security Policies: Recommendations for Information Security Awareness Programs, Computers & Security, Vol. 52, pp. 128–141*

Standards and best practices for information security awareness programs focus on the content and processes of the programs, without taking into consideration how individuals internalize security-related information and how individuals make security related decisions. Relevant literature, however has identified that individual perceptions, beliefs, and biases significantly influence security policy compliance behaviour. Security awareness programs need, therefore, to be aligned with the factors affecting the internalization of the communicated security objectives. This paper explores the role of cognitive and cultural biases in shaping information security perceptions and behaviors. We draw upon related literature from contiguous disciplines (namely behavioral economics and health and safety research) to develop a conceptual framework and analyze the role of cognitive and cultural biases in information security behaviour. We discuss the implications of biases for security awareness programs and provide a set of recommendations for planning and implementing awareness programs, and for designing the related material. This paper opens new avenues for information security awareness research with regard to security decision making and proposes practical recommendations for planning and delivering security awareness programs, so as to exploit and alleviate the effect of cognitive and cultural biases on shaping risk perceptions and security behaviour.

J.13 *Moon J.O., Lee H., Kim J.W., Aktas E., Tsohou A., Choi Y. (2015), Customer Satisfaction from Open Source Software Services in the Presence of Commercially Licensed Software, Asia Pacific Journal of Information Systems, Vol. 25, No. 3, pp. 473-499*

The limited literature on Open Source Software (OSS) customers' adoption does not provide explanations on how OSS services are adopted by customers in the presence of functionally superior commercially licensed software (CLS). This paper aims to uncover the process that shapes customer satisfaction of OSS services in comparison to CLS. Expectation Disconfirmation Theory (EDT) is adapted and integrated with pre implementation factor model that influences software customers' expectations including cost, reputation, and experience. The constructed research model is empirically validated using a field survey of OSS and CLS database management system (DBMS) customers in Korea. The theoretical contribution of the paper lies on the application of EDT to explain the wide adoption of OSS DBMS services in the presence of functionally superior CLS DBMSs. Furthermore, this paper integrates EDT with pre-implementation factors for customers' expectations, which has been considered a limitation of the theory. Among the practical contributions, this study draws attention to the substantive differences between OSS and CLS customers' expectations. Additionally, it offers initial explanations for the differences in customer behavior for OSS and CLS and the way that customers' expectations and actual performance are mingled together to form customer satisfaction.

J.12 *Tsohou A., Karyda M., Kokolakis S., Kiountouzis E., (2014) Managing the Introduction of Information Security Awareness Programs in Organisations, European Journal of Information Systems, 24, pp. 38-58*

Several studies explore information security awareness focusing on individual and/or organisational aspects. This paper argues that security awareness processes are associated with interrelated changes that occur at the organisational, the technological and the individual level. We introduce an integrated analytical framework that has been developed through action research in a public sector organisation, comprising actor-network theory, structuration theory and contextualism. We develop and use this framework to analyse and manage changes introduced by the implementation of a security awareness program in the research setting. The paper illustrates the limitations of each theory (actor-network theory, structuration theory and contextualism) to study multi-level changes when used individually, demonstrates the synergies of the three theories and proposes how they can be used to study and manage awareness related changes at the individual, organisational and technological level.

J.11 *Tsohou A., Lee H., Irani A., Innovative Public Governance Through Cloud Computing: Information Privacy, Business Models And Performance Measurement Challenges, Transforming Government: People, Process and Policy, Vol. 8, No. 2, Emerald.*

Purpose: Innovative technologies, such as federation of services and cloud computing, can greatly contribute to the provision of e-government services, through scalable and flexible systems. Furthermore, they can facilitate in reducing costs and overcoming public information segmentation. Nonetheless, when public agencies employ those technologies they encounter several associated organizational and technical changes, as well as significant challenges. The purpose of this paper is to identify and analyse such challenges and discuss proposed solutions.

Design/methodology/approach: We followed a multi-disciplinary perspective (social, behavioural, business and technical) and conducted a conceptual analysis for the analyzing the associated challenges. We realized focus groups interviews in two countries for evaluating the performance models that resulted from the conceptual analysis.

Findings: This study identifies and analyses several challenges that may emerge while adopting innovative technologies for public governance and e-government services. Furthermore, it presents suggested solutions deriving from the experience of designing a related platform for public governance including solutions for privacy requirements, proposed business models and KPIs for public services on cloud computing.

Research limitations: The challenges and solutions discussed are based on the experience gained by designing one platform. However, we rely on issues and challenges collected from four countries.

Practical implications: The identification of challenges for innovative design of e-government services through a central portal in Europe and using service federation is expected to inform practitioners in different roles about significant changes across multiple levels that are implied and may accelerate the challenges' resolution.

Originality/value: This is the first study that discusses from multiple perspectives and through empirical investigation the challenges to realise public governance through innovative technologies. The results emerge from an actual portal that will function at a European level.

J.10 *Tsohou A., Lee H., Irani Z., Weerakkody V., Osman I., and Anuze A. (2013), Proposing a Reference Process Model for the Citizen-Centric Evaluation of E-Government Services, Transforming Government: People, Process and Policy, Vol. 7, No. 2, pp. 240-255, Emerald*

Evaluating and optimizing e-government services is imperative for governments especially due to the capacity of e-services to transform public administrations and assist the interactions of governments with citizens, businesses and other government agencies. Existing widely applied evaluation approaches neglect to incorporate citizens' satisfaction measures. The purpose of this paper is twofold: to contribute to the understanding of citizen-centric e-government evaluation and unify existing key performance indicators (KPIs); and to propose a reference process model of a novel evaluation approach that uses the unified KPIs to facilitate the creation of a "know-how" repository.

The authors adopt a quantitative research approach for the evaluation of e-government services that is based on data envelope analysis (DEA). A survey was conducted for the empirical investigation and data were collected from 13 e-government services in Turkey. Based on the empirical application of the e-government evaluation method, a reference process model is designed. The proposed evaluation method was proved valid and able to provide assessment with richer explanations than traditional statistical measurements. DEA enabled the identification of insufficient e-government services and the provision of suggested improvements. The reference process model is constructed based on the experience gained by applying the method to a sole cultural setting;, i.e. e-government services in Turkey. The proposed evaluation method, in comparison to other user-oriented ones, provided assessments with richer explanations than traditional statistical measurements, such as structured equation modelling. The reference process model constructed based on the empirical research is expected to accelerate the citizen-oriented evaluation of e-government and promote impact-oriented indicators. This is the first application of DEA in the e-government field, although it has been widely applied for performance measurement in other fields, especially operations research. The novelty of DEA is that the assessment results provide suggestions for strategic improvement of the e-services.

J.9 *Tsohou A., Lee H., Al-Yafi K., Weerakkody V., El-Haddadeh R., Irani Z., Ko A., Medeni T.,* *Campos L., "Supporting Public Policy Making Processes with Workflow Technology: Lessons Learned From Cases in Four European Countries", International Journal of Electronic Government Research, Vol. 8, No. 3, 2012, IGI Global.*

Workflow technology has been proven an enabler of numerous benefits for the private and public organisations including cost reduction, efficiency savings in terms of time and cost, increased capability, faster processing, reductions in errors and work iterations, service quality and customer satisfaction. Public sector has endorsed these benefits by adopting workflow management systems to support administrative processes, such as human resources management or claims processing. However, this technology has not yet been used to support the formulation of policy making processes which would be expected to facilitate the participation of citizens in the policy making processes and increase their awareness on political issues. The purpose of this paper is to investigate the feasibility of adopting workflow tools for the support of the decision making processes that lead to public policies, despite the variant institutional settings. To do so, public policy making processes from four countries are introduced and analysed. The findings indicate that the policy formulation processes show commonalities among the stages although they belong to different policy domains and contexts leaving open the possibility to use workflow technology's benefits for the policy-making process.

J.8 *Tsohou A.,_Karyda M., Kokolakis S., Kiountouzis E., (2012) Analyzing Trajectories of Information Security Awareness, Information Technology & People, Vol. 25, Issue 3, Emerald*

Recent global security surveys indicate that security training and awareness programs are not working as well as they could be and that investments made by organizations are inadequate. The purpose of the paper is to increase our understanding of this phenomenon and illuminate the problems that organizations face when trying to establish an information security awareness program. Following an interpretive approach we apply a case study method and we employ Actor Network Theory (ANT) and the Due Process for analyzing our findings. The paper contributes to both understanding and managing security awareness programs in organizations, by providing a framework that enables the analysis of awareness activities and interactions with the various organizational processes and events. The application of ANT still remains a challenge for researchers since no practical method or guide exists. In this paper we enhance and practically present its application through the due process model extension. Our exploration highlights the fact that information security awareness initiatives involve different stakeholders, with often conflicting interests. Practitioners must acquire, additionally to technical skills, communication, negotiation and management skills in order to address the related organizational and managerial issues. Moreover, the results of our inquiry reveal that the role of artifacts used within the awareness process is not neutral but can actively affect it. This study is one of the first to examine information security awareness as a managerial and socio-technical process within an organizational context.

J.7 *Tsohou A., Kokolakis S., Lambrinoudakis C., Gritzalis S., "A Framework of Security Standards to Facilitate Best Practices' Awareness and Conformity", Information Management & Computer Security, Vol. 18, No. 5, 2010.*

Recent information security surveys indicate that both the acceptance of international standards and the relative certifications increase continuously. However, it is noted that still the majority of organizations does not know the dominant security standards or does not fully implement them. The aim of this paper is to facilitate the awareness of information security practitioners regarding globally known and accepted security standards, and thus, contribute to their adoption. The paper adopts a conceptual approach and results in a classification framework for categorizing available information security standards. The classification framework is built in four layers of abstraction, where the initial layer is founded in ISO/IEC 27001:2005 information security management system. The paper presents a framework for conceptualizing, categorizing and interconnecting available information security standards dynamically. The completeness of the information provided in the paper relies to the pace of standards' publications; thus the information security standards that have been classified in this paper need to be updated when new standards are published. However, the proposed framework can be utilized for this constant effort. Information security practitioners can benefit by the proposed framework for available security standards and effectively inquire the relevant standard each time. Guidelines for utilizing the proposed framework are presented through a case study. Although the practices proposed are not innovative by themselves, the originality of this work lies on the best practices' linkage into a coherent framework that can facilitate the standards diffusion and systematic adoption.

J.6 *Tsohou A., Lambrinoudakis C., Kokolakis S., Gritzalis S., "The Importance of Context Dependant Privacy Requirements and Perceptions to the Design of Privacy Aware Systems", The European Journal of the Informatics Professional (UPGrade), Vol. XI, Issue 1, February 2010, pp. 32-37.*

The issue of information privacy protection is ensured nowadays by European and national legislation. However, it is not possible to protect information system user privacy adequately without establishing privacy requirements and employing an appropriate privacy assessment process that can identify the required privacy level and the possible countermeasures for achieving it. In this paper we draw upon security management tasks in order to highlight the gaps that need to be explored regarding privacy management, so as to be able to justifiably select the privacy enhancing technologies that fit a system's privacy requirements.

J.5 *Tsohou A., Karyda M., Kokolakis S., Kiountouzis E., "Aligning Security Awareness with Information Systems Security Management", Journal of Information System Security – Vol. 6, No. 1, 2010, pp. 36-54. (Republication of C.4)*

This paper explores the way information security awareness connects to the overall information security management framework it serves. To date, the formulation of security awareness initiatives has tended to ignore the important relationship with the overall security management context, and vice versa. In this paper we show that the two processes can be aligned so as to ensure that awareness activities serve the security management strategy and that security management exploits the benefits of an effective awareness effort. To do so, we analyze the processes of security awareness and security management using a process analysis framework and we explore their interactions. The identification of these interactions results in making us able to place awareness in a security management framework instead of viewing it as an isolated security mechanism.

J.4 *Rizomiliotis P., Tsohou A., Lambrinoudakis C., Gritzalis S., "Security and Privacy Issues in Bipolar Disorder Research", The Journal on Information Technology in Healthcare, Vo. 7, No. 4, 2009, HL7 Ramius Corp. (Republication of C.2)*

Mental health diseases are common but research to further knowledge and understanding of them is hampered by data privacy and confidentiality regulations that apply to medical records. Centralised databases containing the relevant medical history of thousands of patients with an individual mental disease would be of great value for researchers, enabling techniques such as data mining to be applied. The major challenge in achieving this is anonymising the data to satisfy legal and ethical requirements without removing important clinical information. In this paper we propose a model that can be used to create a central repository of anonymised data for patients with bipolar disease. Knowledge obtained from the database is fed into an expert system which can guide clinicians in patient management. Security requirements are provided by access to the database being controlled by RBAC (Role Based Access Control).

J.3 *Tsohou A., Kokolakis S., Karyda M., Kiountouzis E., "Investigating information security awareness: research and practice gaps", Information Security Journal: A Global Perspective, Vol.17, No. 5-6, pp. 207-227, 2008, Taylor and Francis.*

The aim of this survey is largely exploratory, namely, to discover patterns and trends in the way that practitioners and academics alike tackle the security awareness issue and to have a better understanding of the reasons why security awareness practice remains an unsolved problem. Open coding analysis was performed on numerous publications (articles, surveys, standards, reports and books). A classification scheme of six categories of concern has emerged from the content analysis (e.g., terminology ambiguity), and the chosen publications were classified based on it. The paper identifies ambiguous aspects of current security awareness approaches and the proposed classification provides a guide to identify the range of options available to researchers and practitioners when they design their research and practice on information security awareness.

J.2 *Tsohou A., Kokolakis S., Karyda M., Kiountouzis E., "Process-Variance Models in Information Security Awareness Research", Information Management and Computer Security, Vol.16, No. 3, pp. 271 – 287, 2008, Emerald.*

The purpose of this paper is to study the way information systems (IS) security researchers approach information security awareness and examine whether these approaches are consistent with the organization theory and IS approaches for the study of organizational processes. Open coding analysis was performed on selected publications (articles, surveys, standards, and reports). The chosen publications were classified and the classification results are presented, based on a proposed typology. The proposed typology allows us to identify different types of research models followed by security researchers and practitioners, and to infer a set of practical implications, for the benefit of those interested in empirically studying information security awareness. The paper represents a pilot survey, performed in a selected number of publications. The paper helps researchers and practitioners to distinguish the research models that can be adopted for the study of information security awareness organizational process, by identifying the key dimensions along which they differ. The proposed typology provides a guide to identify the range of options available to researchers and practitioners when they design their work regarding the security awareness topic. Moreover, it can facilitate the communication between scholars in the field of security awareness.

J.1 *Tsohou A., Karyda M., Kokolakis S., Kiountouzis E., "Formulating Information Systems Risk Management Strategies through Cultural Theory", Information Management and Computer Security, Vol. 14, No. 3, pp. 198-217, 2006, Emerald.*

The purpose of this paper is to examine the potential of cultural theory as a tool for identifying patterns in the stakeholders' perception of risk and its effect on information system (IS) risk management. Risk management involves a number of human activities which are based on the way the various stakeholders perceive risk associated with IS assets. Cultural theory claims that risk perception within social groups and structures is predictable according to group and individual worldviews; therefore this paper examines the implications of cultural theory on IS risk management as a means for security experts to manage stakeholders perceptions. A basic theoretical element of cultural theory is the grid/group typology, where four cultural groups with differentiating worldviews are identified. This paper presents how these worldviews affect the process of IS risk management and suggests key issues to be considered in developing strategies of risk management according to the different perceptions cultural groups have. The findings of this research are based on theoretical analysis and are not supported by relevant empirical research. Further research is also required for incorporating the identified key issues into information security management systems (ISMS). IS security management overlooks stakeholders' risk perception; for example, there is no scheme developed to understand and manage the perception of IS stakeholders. This paper proposes some key issues that should be taken into account when developing strategies for addressing the issue of understanding and managing the perception of IS stakeholders.

B.2 PUBLICATIONS IN PEER-REVIEW CONFERENCE PROCEEDINGS

C.25 Diamantopoulou, V., Tsohou, A., and Karyda, M. (2019) General Data Protection Regulation and ISO/IEC 27001:2013: Synergies of activities towards organizations' compliance, In *Proceedings of the TrustBus 2019 International Conference on Trust, Privacy & Security in Digital Business,* August 2019, Linz, Austria, Lecture Notes in Computer Science LNCS, Springer

The General Data Protection Regulation that is already in effect for about a year now, provisions numerous adjustments and controls that need to be implemented by an organisation in order to be able to demonstrate that all the appropriate technical and organisational measures have been taken to ensure the protection of the personal data. Many of the requirements of the GDPR are also included in the \ISO27k" family of standards. Consequently, organisations that have applied ISO27k to develop an Information Security Management System (ISMS) are likely to have already accommodated many of the GDPR requirements. This work identifies synergies between the new Regulation and the well-established ISO/IEC 27001:2013 and proposes practices for their exploitation. The proposed alignment framework can be a solid basis for compliance, either for organisations that are already certified with ISO/IEC 27001:2013, or for others that pursue compliance with the Regulation and the ISO/IEC 27001:2013 to manage information security.

C.24 Jiang, H., Siponen, M., and Tsohou, A. (2019), A Field Experiment for Understanding the Unintended Impact of Internet Monitoring on Employees: Policy Satisfaction, Organizational Citizenship Behavior and Work Motivation, In Proceedings of *the 27th European Conference on Information Systems*

(ECIS), Stockholm & Uppsala, Sweden, June 8-14, 2019, Association for Information Systems (AIS).

Internet monitoring is widely deployed in organizations as an attempt to regulate employees' cyberloafing behavior, which is defined as employees' usage of Internet for non-work-related purposes. Although previous studies have examined the effectiveness of Internet monitoring in regulating employees' cyberloafing, the impact of Internet monitoring on employees' perceptions or behaviors other than cyberloafing has not been investigated. As a first step to address this research gap, we conduct a field experiment to study the impact of Internet monitoring on employees' policy satisfaction, organizational citizenship behavior (OCB) and work motivation. We found that Internet monitoring decreased employees' policy satisfaction and OCB. We also found that Internet monitoring decreased employees' intrinsic work motivation, although it slightly increased employees' extrinsic work motivation. Our study contributes to the literature by examining the unintended impact of Internet monitoring on employees. It also has implications for organizations to make appropriate decisions regarding whether to implement Internet monitoring.

C.23 Paspatis, I. Tsohou, A. and Kokolakis, S. (2018) AppAware: A Model for Privacy Policy Visualization for Mobile Applications, In Proceedings of *the 12th Mediterranean Conference on Information Systems*, Corfu, Greece, September 2018, Association for Information Systems (AIS).

Privacy policies emerged as the main mechanism to inform users on the way their information is managed by online service providers, and still remain the dominant approach for this purpose. Literature notes that users find difficulties in understanding privacy policies because they are usually written in technical or legal language even, although most users are unfamiliar with them. These difficulties have led most users to skip reading privacy policies and blindly accept them. In an effort to address this challenge this paper presents AppWare, a multiplatform tool that intends to improve the visualization of privacy policies for mobile applications. AppWare formulates a visualized report with the permission set of an application, which is easily understandable by a common user. AppWare aims to bridge the difficulty to read privacy policies and android's obscure permission set with a new privacy policy visualization model. To validate AppAware we conducted a survey through questionnaire aiming to evaluate AppAware in terms of installability, usability, and viability-purpose. The results demonstrate that AppAware is assessed above average by the users in all categories

C.22 Gritzalis, A., Tsohou A. and Lambrinoudakis C. Transparency Enabling Systems for Open Governance: Their Impact on Citizens' Trust and the Role of Information Privacy, In the Proceedings of the 7th International Conference on eDemocracy, Privacy-Preserving, Secure, Intelligent eGovernment Services, 14 – 15 December 2017, Athens - Greece

Several governments and citizens embrace information systems that are designed to enable transparency of public expenses and discourage corruption in the public sector. The objective of this paper is to examine the capacity and value of information systems designed to enhance transparency, from a citizens'/users' perspective. Our purpose is to address research questions associated with the actual impact of transparency-enabling systems and openness on citizens' trust and uncertainty towards the governmental policies and actions. We also explored the impact of privacy requirements and personal data protection regulations on the system and citizens' willingness to access public data. To the best of our knowledge, these are largely unexplored issues in the literature. Our study involves the design of a web survey and the execution of an empirical study with citizens who have used such a system in Greece. In particular, we focused our empirical study on the Greek system 'Diavgeia', which is the national transparency and anti-corruption system

C. 21 Kosyfaki, C., Angelova N., Tsohou A. and Magkos, M. (2017) The Privacy Paradox in the Context of Online Health Data Disclosure by Users, *In the Proceedings of the 14th European, Mediterranean and Middle Eastern Conference on Information Systems (EMCIS 2017),* Coimbra, Portugal, September 2017, Springer.

The privacy paradox phenomenon corresponds to the inconsistency between the privacy concerns and the actual behavior of online users [9]. The existence of the phenomenon has been studied in many fields, such as social networks and especially a great variety of forums and online communities [3, 6]. This paper, questions its existence in the context of sensitive data, and more specific in the health data area via a survey which took place in Greece. Given that health-related information are perceived as highly sensitive personal data and are often excluded from discussions and sharing, this research aims to unravel the paradox's existence that leads to the disclosure of health data information during the visit of related online forums and communities, by the users.

C. 20 *Paspatis, I., Tsohou A. and Kokolakis S. (2017), Mobile Application Privacy Risks: Viber Users' De-Anonymization Using Public Data, In the Proceedings of the 11th Mediterranean Conference on Information Systems, Genova, Italy, September 2017, Association for Information Systems (AIS).*

Mobile application developers define the terms of use for the applications they develop, which users may accept or declined during installation. Application developers on the one hand seek to gain access to as many user information as possible, while users on the other hand seem to lack awareness and comprehension of privacy policies. This allows application developers to store an enormous number of personal data, sometimes even irrelevant to the application's function. It's also common that users choose not to alter the default settings, even when such an option is provided. In combination, the above conditions jeopardize users' rights to privacy. In this research, we examined the Viber application to demonstrate how effortless it is to discover the identity of unknown Viber users. We chose a pseudorandom sample of 2000 cellular telephone numbers and examined if we could reveal their personal information. We designed an empirical study that compares the reported behavior with the actual behavior of Viber's users. The results of this study show that users' anonymity and privacy is easily deprived and information is exposed to a knowledgeable seeker. We provide guidelines addressed to both mobile application users and developers to increase privacy awareness and prevent privacy violations.

C. 19 Skalkos A., Tsohou A., Karyda M. and Kokolakis S. (2017) Investigating the Values that Drive the Adoption if Anonymity Tools: A Laddering Approach, Research In progress, *The 11th Mediterranean Conference on Information Systems*, Genova, Italy, September 2017

Concerns about privacy and frustration over censorship and content blocking are driving millions to use privacy enhancing products. This research-in-progress focuses on anonymity tools, as a Privacy Enhancing Technology (PET), investigating the values that drive the adoption of anonymity tools by users. We use means-end analysis, a methodology we consider to be appropriate for investigating users' conceptions and incentives for adopting anonymity tools. We also use the laddering technique, a qualitative method based on in-depth interviews, to reveal the chains of attribute-consequence-values of anonymity tools users and to construct a Hierarchical Value Map. The aim of our research is to provide insights and enhance understanding of anonymity tools users' behavior, which we expect to benefit both researchers and software engineers to design platforms that more closely fit users' need.

C.18 *Diamantopoulou V., Tsohou A., Loukis E. and Gritzalis S. (2017) Does the Development of Information Systems Resources Lead to the Development of Information Security Resources? An Empirical Investigation, In the Proceedings of the 23rd Americas Conference on Information Systems (AMCIS 2017), Boston, USA, August 2017*

Information Systems (IS) are nowadays considered the most important leverage for organizations to operate and gain a competitive advantage. Investments in IS technology, in the recruitment of high qualified IT personnel and the establishment of internal and external robust IT related partnerships are considered determinant factors for business success and continuity. As organizations increasingly rely on IS resources, they face more advanced IS security challenges. This paper explores the relationship between the development of IS resources and security resources; are organizations willing to invest more in IS security resources as they invest more on IS resources? The authors conduct an empirical investigation in organizations located in five Mediterranean countries. The sample includes responses from 61 CEOs, information security managers and IS managers. The results reveal that IS resources positively affect the IS security resources. The human capital plays the most important role for the adoption of IS security.

C.17 *Karavaras E., Magkos E. and Tsohou A. (2016) Low User Awareness Against Social Malware: an Empirical Study and Design of a Security Application, In the Proceedings of the 13th European, Mediterranean and Middle Eastern Conference on Information Systems, Krakow, Poland, June 2016*

During the past few years, in harmony with the fast growing rate of user population in Online Social Networks (OSNs),a trend for malware writers has been to take advantage of the social relationships of OSN users, in order to lure them into following malicious URLs that lead to malware infection. One reason for the success of such Social Engineering (SE)-based malware has been the low security awareness of OSN users. Indeed, it can be shown that, on the average, OSN users do not have sufficient knowledge of the malicious link threats they may come up against, and thus are easy victims of SE attacks. In this paper we conduct an empirical investigation which, on the one hand, demonstrates Facebook users' low awareness of malicious link threats, and on the other hand explores the views of OSN users on the desirable properties of a security application that protects them against social malware. Furthermore, we design and describe the architecture of a security application which intends to raise Facebook users' security awareness by informing them about (possibly) malicious posts on their walls before or after they get infected. Our application acts proactively by helping users to not get infected by malicious posts, and reactively by helping the users who got infected to gain an understanding of the threat and become more alerted towards identifying malware links.

C.16 *Jiang H. and Tsohou A. (2015), The same Antecedents do not fit all activities: an Activity-Specific Model of Personal Internet Use in Workplace, (Research in Progress), In Proceedings of the 23nd European Conference on Information Systems (ECIS 2015), May 2015, Mursten, Germany*

IT devices connected to Internet, such as computers, tablets and smartphones, are commonly used in organizations. At the same time, organizational employees increasingly perform non-work related activities at work by using the IT resources, which is defined as personal Internet use (PIU) in workplace. Multiple models have been developed by previous studies to investigate why employees perform PIU. These studies consider all PIU activities as a uniform behavior. However, literature suggests that there are different types of PIU activities. Therefore, it is with limitations to consider PIU behavior and its antecedents uniformly for all activities, given that PIU behavior may differ significantly when bounded with the different activities. As a first step to close the gap, we examine separately the antecedents of three types of PIU activities: non-work related emailing activities, browsing activities, and online financial activities, to validate our hypothesis that the same antecedent does not explain all PIU activities. Our study contributes to research by demonstrating the necessity to separately examine different types of PIU activities when investigating why employees perform PIU.

C.15 *Koufi V., Tsohou A., Malamateniou F. and Vassilacopoulos G., (2014), A Framework for Privacy-Preserving Access Control to Cloud Process-based EHR Systems, 25th European Medical Informatics Conference, August 2014, Istanbul, Turkey.*

Although personalized medicine is optimizing the discovery, development and application of therapeutic advances, its full impact on patient and population healthcare management has yet to be realized. Electronic health Records (EHRs), integrated with data from other sources, such as social care data, Personal Healthcare Record (PHR) data and genetic information, are envisaged as having a pivotal role in realizing this individualized approach to healthcare. Thus, a new generation of EHRs will emerge which, in addition to supporting healthcare professionals in making well-informed clinical decisions, shows potential for novel discovery of associations between disease and genetic, environmental or process measures. However, a broad range of ethical, legal and technical reasons may hinder the realization of future EHRs due to potential security and privacy breaches. This paper presents a HIPAA-compliant framework that enables privacy-preserving access to next-generation EHRs.

C.14 *Jiang H. and Tsohou A. Expressive Or Instrumental: A Dual-Perspective Model Of Personal Web Usage At Workplace (Research in Progress) In Proceedings of the 22nd European Conference on Information Systems (ECIS 2014), June 2014, Tel Aviv, Israel*

IT devices such as computers, tablets, smartphones as well as Internet are playing extremely important role in both work and non-work fields. Meanwhile, IT facilities also blurred the boundary between work and non-work. With the ubiquity of IT devices and Internet at workplace, organizational employees nowadays increasingly engage in online behaviors for personal activities, which are not related to work, during office hours using organizational IT resources, hereafter Personal Web Usage (PWU). Previous studies have identified multiple motivations behind employees' PWU behavior from different perspectives. By reviewing existing literature, we propose the dual nature of PWU with respect to its antecedents, namely expressive nature and instrumental nature. Accordingly, we develop a dual-perspective model of PWU, in which different types of antecedents as well as their interactions are explained. In specific, drawing from job demand-control model, we identify a new antecedent addressing expressive aspect of PWU, namely burnout. And perceived benefit is identified to be the antecedent addressing the instrumental nature of PWU in our model. The proposed model sheds new light on PWU research by proposing an important, yet not recognized previously, nature of PWU, and thus offering a framework to unify existing research and proposing directions for future research.

C.13 *Jiang H. and Tsohou A. The Dual Nature of Personal Web Usage At Workplace: Impacts, Antecedents And Regulating Policies, In Proceedings of the 22nd European Conference on Information Systems (ECIS 2014), June 2014, Tel Aviv, Israel*

IT facilities such as computers, tablets, smartphones as well as Internet are playing extremely important role in both work and non-work fields currently, and IT facilities also blurred the boundary between work and non-work. With the ubiquity of IT devices and Internet at workplace, organizational employees nowadays increasingly engage in online behaviors for personal activities, which are not related to work during working hours by using organization's IT resources, hereafter Personal Web Usage (PWU). Different even opposite opinions on the antecedents, impacts and regulating policies of PWU have been proposed in proliferating literature. It is our contention that discussing the nature of PWU behind these multiple viewpoints is a necessary step to enhance our understanding to PWU. By reviewing previous research, we propose the dual nature of PWU with respect to its antecedents, impacts and regulating policies. For antecedents, PWU is both an expressive means for employees to vent their negative affections toward organizations, and an instrumental means for employees to pursue various positive utilities by using Internet. For impacts, PWU might have positive impacts on organizations in some circumstances and it could also exert negative effects in other ones. For regulating policies, discriminative policies rather than universal policy should be proposed in different organizations. The dual nature of PWU offers new insight to research in two folds. First, it facilitates to unify the different even opposite viewpoints from previous studies that are conducted from different perspectives. Second, it provides guidance for future research by proposing multiple research questions based on the duality of PWU

C.12 *Oh J., Lee H. and Tsohou A. Relational Versus Structural Embeddedness in IT Outsourcing Networks: The Role Of Requirement Unpredictability And Measurement Difficulty, 17th Pacific Asia Conference on Information Systems (PACIS 2013), June 2013, Jeju Island, Korea*

Relational and structural embeddedness are reported to play an important role in the context of information technology outsourcing (ITO). However, we do not fully understand which of the two types of embeddedness is more appropriate in preventing opportunistic behaviour and improving long-term performance in the presence of uncertainty which is not uniform across a wide range of outsourced IT services and products. In order to address this question, a virtual ITO network is simulated where firms take the partner selection and control strategy based on relational or structural embeddedness. They also compete with each other to maximize their long-term profits. The simulation results show that the advantage of each type of embeddedness is different according to the levels of measurement difficulty and requirement unpredictability which coexist in the ITO business environments. Therefore, this study provides a better understanding of the conditional superiority of each type of embeddedness in the presence of the two uncertainties and offers ITO managers with a guideline for a choice between relational and structural embeddedness.

C.11 *Tsohou A., Al-Yafi K., Lee H., "Evaluating M-Government Applications: An Elaboration Likelihood Model Framework", Proceedings of the European, Mediterranean & Middle Eastern Conference on Information Systems (EMCIS), (Eds. Ghoneim A., Klischewski R., Schrödl H., Muhammed K.) 2012, 7-8 June, Munich, Germany*

Mobile government application and services refer to governmental functions that are available to mobile devices, such as smart phones or personal digital assistants, to the users anytime/anywhere. M-Government and m-Participation are emergent concepts used to represent the evolving field of public administration functions provided as mobile services and the provision of participation to public consultations via mobile devices accordingly. In this paper we present an evaluation framework for m-government tools. The evaluation approach is grounded on the assumption that m-government tools should not only provide access to governmental information and functions, but they should also motivate users to participate to public policy making processes. The evaluation approach is based on the Elaboration Likelihood Model. Its novelty lies on a) its ability to capture the actual performance of a system instead of the users' perceptions, and b) its capacity to assess the motivational and persuasive ability of a system.

C.10 *Tsohou A., Lee H., Zahir I., Weerakkody V., Osman I., Latif A., Medeni T., "Evaluating E-Government Services From A Citizens' Perspective: A Reference Process Model", Proceedings of the European, Mediterranean & Middle Eastern Conference on Information Systems (EMCIS), (Eds. Ghoneim A., Klischewski R., Schrödl H., Muhammed K.), 7-8 June, 2012, Munich, Germany*

Evaluating and optimizing e-government services is imperative for governments especially due to the capacity of e-services to transform public administrations and assist the interactions of governments with citizens, businesses and other government agencies. Existing widely applied evaluation approaches neglect to incorporate citizens' satisfaction measures. Several citizen satisfaction models and indicators have been suggested in academia; however a reference process model that can assist practitioners to apply these performance measures is missing. In this paper we draw upon the evaluation approach proposed by the EU funded project CEES and propose a reference process model that captures re-usable practices for e-government evaluation from a citizens' perspective. The novelty of the proposed approach is that using DEA for evaluating the e-services the assessment results in suggestions for strategic improvement of the e-services.

C.9 *El-Haddadeh R., Tsohou A., Karyda M., "Analyzing Implementation Challenges for information Security Awareness initiatives in E-government", Proceedings of the ECIS 2012 20th European Conference on Information Systems, (Eds. Janssen M, Weerakkody V, Dwivedi Y), June 2012, Barcelona, Spain.*

With the widespread adoption of electronic government services, there has been a need to ensure a seamless flow of information across public sector organizations, while at the same time, maintaining confidentiality, integrity and availability. Governments have put in place various initiatives and programs including information security awareness to provide the needed understanding on how public sector employees can maintain security and privacy. Nonetheless, the implementation of such initiatives often faces a number of challenges that impede further take-up of e-government services. This paper aims to provide a better understanding of the challenges contributing towards the success of information security awareness initiatives implementation in the context of e-government. Political, organizational, social as well as technological challenges have been utilized in a conceptual framework to signify such challenges in e-government projects. An empirical case study conducted in a public sector organization in Greece was exploited in this research to reflect on these challenges. While, the results from this empirical study confirm the role of the identified challenges for the implementation of security awareness programs in e-government, it has been noticed that awareness programmers often pursue different targets of preserving security and privacy, which sometimes results in adding more complexity to the organization.

C.8 *Tsohou A., Karyda M., Kokolakis S., Kiountouzis E., "Analyzing Information Security Awareness through Networks of Association", 7th International Conference on Trust, Privacy & Security in Digital Business (TrustBus 2010), September 2010, Bilbao, Spain*

Information security awareness is a continuous effort to raise attention to information security and its importance, in order to stimulate security-oriented behaviors. Despite the increasing interest of researchers on the topic and the continuous notifications of global security surveys for its significance, awareness remains a critical issue of information security. Related approaches propose techniques and methods for promoting security without theoretical grounding and separately from the overall information security management framework. The aim of this paper is to suggest a theoretical and methodological framework which facilitates the analysis and understanding of the issues that are intertwined with awareness activities, in order to support the organization's security management.

C.7 *Evans R., Tsohou A., Tryfonas T., Morgan T., "Architecting Secure Systems with the ISO standards 26702 and 27001", 5th IEEE International Conference on Systems of Systems Engineering (SoSE 2010), June 2010, Loughborough, UK, IEEE Computer Society Press*

System engineers are confronted with fast-paced technology developments, complicated contractual relationships, emerging threats and global security requirements, concerns for sustainability and viability of their ventures and a raft of other issues. In this environment, information technology-intensive systems in particular are exposed to risk and recent high-profile incidents have contributed to significant emphasis to be given to security. It is however impossible for systems engineers to become specialists in all areas of concern in order to be able to tackle effectively those issues and thus architecting systems needs to take into account good practice and existing relevant knowledge. When such knowledge is embodied into established and widely accepted standards, not only is there the opportunity to capitalise on their mature content but also to ripe the benefits of compliance, seamless integration and competitive advantage that standardisation provides. In this spirit we investigate in this paper the use of two popular and established standards, the ISO 27000 series and ISO/IEC 26702, as aids in the process of engineering secure systems.

C.6 *Vrakas N., Kalloniatis C., Tsohou A., Lambrinoudakis C., "Privacy Requirements Engineering for Trustworthy e-Government Services", 3rd International Conference on Trust and Trustworthy Computing (TRUST 2010), June 2010, Berlin, Germany, Lecture Notes in Computer Science LNCS, Springer.*

Several research studies have applied information systems acceptance theories in order to examine issues related to the acceptance of eservices by users. Their application in the e-government systems has revealed that trust is a prerequisite for their usage. Moreover, it has been proved that privacy concerns are a main antecedent of trust in e-government systems intention of use. Therefore, information systems that are not privacy aware are not trusted and thus not accepted by users. Currently there are many different attacks that can be realized by malicious users for compromising the confidentiality of private data and thus putting at stake the trustworthiness of the systems. The conventional way for preventing such attacks is mainly the employment of Privacy Enhancing Technologies (PETs). However, PETs are employed as ad hoc technical solutions that are independent from the organizational context in which the system will operate. We argue that we need
privacy requirements engineering methods for capturing the context dependent privacy requirements

and for selecting the appropriate technical, organizational and procedural countermeasures which will help building privacy aware systems that can offer electronic services which users can trust.

C.5 *Tsohou A., Kokolakis S., Lambrinoudakis C., Gritzalis S., "Unifying ISO Security Standards Practices into a Single Security Framework", 12th Annual IFIP Workshop on Information Security Management, N.Clarke, S. Furnell (Eds.), May 2010, Port Elizabeth, South Africa, Emerald*

Compliance to standards is quite important for numerous reasons, including interoperability, conformity assessment etc. However, even though recent surveys indicate that international security standards do gain acceptance and that a continuously increasing number of organizations adopt them, still the majority do not know them or do not fully implement them. In this paper we facilitate the awareness of security practitioners on ISO security standards and we propose a security framework that is based on them. In order to explain the different layers of the framework and illustrate its applicability we have used as a case study a Payroll and Pensioner Information System.

C.4 *Tsohou A., Karyda M., Kokolakis S., Kiountouzis E., "Aligning Security Awareness with Information Systems Security Management", 4th Mediterranean Conference on Information Systems, September 2009, Athens, Greece*

This paper explores the way information security awareness connects to the overall information security management framework it serves. To date, the formulation of security awareness initiatives has tended to ignore the important relationship with the overall security management context, and vice versa. In this paper we show that the two processes can be aligned so as to ensure that awareness activities serve the security management strategy and that security management exploits the benefits of an effective awareness effort. To do so, we analyze the processes of security awareness and security management using a process analysis framework and we explore their interactions. The identification of these interactions results in making us able to place awareness in a security management framework instead of viewing it as an isolated security mechanism.

C.3 *Tsohou A., Kokolakis S., Lambrinoudakis C., Gritzalis S., "Information Systems Security Management: A review and a classification of the ISO standards", In: Next Generation Society: Technological and Legal Issues, Springer Lecture Notes of the ICSSIT Institute for Computer Sciences, Social Informatics, and Telecommunications Engineering A. Sideridis and C. Patrikakis (Eds.), e-Democracy 2009, LNICST 26, pp. 220-235, 2010*

The need for common understanding and agreement of functional and non-functional requirements is well known and understood by information system designers. This is necessary for both: designing the "correct" system and achieving interoperability with other systems. Security is maybe the best example of this need. If the understanding of the security requirements is not the same for all involved parties and the security mechanisms that will be implemented do not comply with some globally accepted rules and practices, then the system that will be designed will not necessarily achieve the desired security level and it will be very difficult to securely interoperate with other systems. It is therefore clear that the role and contribution of international standards to the design and implementation of security mechanisms is dominant. In this paper we provide a state of the art review on information security management standards published by the International Organization for Standardization and the International Electrotechnical Commission. Such an analysis is meaningful to security practitioners for an efficient management of information security. Moreover, the classification of the standards in the clauses of ISO/IEC 27001:2005 that results from our analysis is expected to provide assistance in dealing with the plethora of security standards.

C.2 *Rizomiliotis P., Tsohou A., Lambrinoudakis C., Gritzalis S., "Security and Privacy Issues in Bipolar Disorder Research", ICICTH 7th International Conference on Information and Communication Technologies in Health, A. Hasman et al. (Eds.), July 2009, Samos, Greece, INEAG*

Mental health diseases are common but research to further knowledge and understanding of them is hampered by data privacy and confidentiality regulations that apply to medical records. Centralised databases containing the relevant medical history of thousands of patients with an individual mental disease would be of great value for researchers, enabling techniques such as data mining to be applied. The major challenge in achieving this is anonymising the data to satisfy legal and ethical requirements without removing important clinical information. In this paper we propose a model that can be used to create a central repository of anonymised data for patients with bipolar disease. Knowledge obtained from the database is fed into an expert system which can guide clinicians in patient management. Security requirements are provided by access to the database being controlled by RBAC (Role Based Access Control).

C.1 *Tsohou A., Theoharidou M., Kokolakis S., Gritzalis D.: "Addressing Cultural Dissimilarity in the Information Security Management Outsourcing Relationship", Proceedings of the TRUSTBUS'07, 4th International Conference on Trust, Privacy and Security in Digital Business, pp.24-33, Regensburg, Germany, September 2007, Lecture Notes in Computer Science LNCS, Springer.*

Organizational culture influences the way a) information security is perceived, b) security countermeasures are adopted, and c) the organization reacts to the cultural changes of a new security program. In Information Security Management Outsourcing (ISMO), cultural differences may arise between the organization and the provider, for example conflict between the countermeasures applied by the provider and the company’s internal policies. We propose a conceptual framework of security mechanisms in order organizations that choose ISMO to identify and manage cultural dissimilarity.