ΒΙΟΓΡΑΦΙΚΟ ΣΗΜΕΙΩΜΑ

ΑΝΑΛΥΤΙΚΟ ΥΠΟΜΝΗΜΑ ΕΠΙΣΤΗΜΟΝΙΚΩΝ ΕΡΓΑΣΙΩΝ

Δρ. ΤΣΩΧΟΥ ΑΓΓΕΛΙΚΗ

Επίκουρος Καθηγήτρια σε

Ιδιωτικότητα και Ασφάλεια σε Πληροφοριακά Συστήματα

Τμήμα Πληροφορικής

Ιόνιο Πανεπιστήμιο

Κέρκυρα, Οκτώβριος 2019

ΠΕΡΙΕΧΟΜΕΝΑ

Α. ΒΙΟΓΡΑΦΙΚΟ ΣΗΜΕΙΩΜΑ 3
Α.1 ΠΡΟΣΩΠΙΚΑ ΣΤΟΙΧΕΙΑ 3
Α.2 ΣΠΟΥΔΕΣ 3
Α.3 ΕΡΕΥΝΗΤΙΚΑ ΕΝΔΙΑΦΕΡΟΝΤΑ 3
Α.4 ΠΑΡΟΥΣΑ ΑΠΑΣΧΟΛΗΣΗ 4
Α.5 ΣΥΝΟΨΗ ΕΠΑΓΓΕΛΜΑΤΙΚΗΣ ΕΜΠΕΙΡΙΑΣ 4
Α.6 ΔΙΑΚΡΙΣΕΙΣ 4
Α.7 ΕΠΑΓΓΕΛΜΑΤΙΚΗ ΕΜΠΕΙΡΙΑ 5
Α.7.1 ΔΙΔΑΚΤΙΚΗ ΕΜΠΕΙΡΙΑ 5
Α.7.2ΕΠΙΒΛΕΨΗ ΥΠΟΨΗΦΙΩΝ ΔΙΔΑΚΤΟΡΩΝ ΚΑΙ ΣΥΜΜΕΤΟΧΗ ΣΕ ΕΞΕΤΑΣ
Α7.3 ΕΠΙΒΛΕΨΗ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΔΙΠΛΩΜΑΤΙΚΩΝ ΕΡΓΑΣΙΩΝ 8
Α.7.4 ΕΠΙΒΛΕΨΗ ΠΤΥΧΙΑΚΩΝ ΕΡΓΑΣΙΩΝ 8
Α.7.3 ΕΡΕΥΝΗΤΙΚΉ ΕΜΠΕΙΡΙΑ - ΕΡΓΑ ΕΡΕΥΝΑΣ 8
Α.7.4 ΛΟΙΠΗ ΕΠΑΓΓΕΛΜΑΤΙΚΗ ΕΜΠΕΙΡΙΑ 11
Α.8 ΔΗΜΟΣΙΕΥΜΕΝΟ ΕΡΓΟ 11
Α.8.1 ΔΗΜΟΣΙΕΥΣΕΙΣ ΣΕ ΕΠΙΣΤΗΜΟΝΙΚΑ ΠΕΡΙΟΔΙΚΑ ΜΕ ΣΥΣΤΗΜΑ ΚΡΙΤΩΝ 11
Α.8.2 ΔΗΜΟΣΙΕΥΣΕΙΣ ΣΕ ΠΡΑΚΤΙΚΑ ΔΙΕΘΝΩΝ ΣΥΝΕΔΡΙΩΝ ΜΕ ΚΡΙΣΗ ΠΛΗΡΟΥΣ ΚΕΙΜΕΝΟΥ 14
Α.8.3 ΔΗΜΟΣΙΕΥΣΕΙΣ ΣΕ WORKSHOPS, POSTERS ΚΑΙ ΠΕΡΙΛΗΨΕΙΣ ΣΕ ΔΙΕΘΝΗ ΣΥΝΕΔΡΙΑ ΜΕ ΚΡΙΣΗ 17
Α.8.4 ΔΙΑΤΡΙΒΕΣ 18
Α.9 ΠΡΟΣΚΕΚΛΗΜΕΝΕΣ ΟΜΙΛΙΕΣ 19
Α.9.1 ΚΕΝΤΡΙΚΗ ΟΜΙΛΗΤΡΙΑ 19
Α.9.2 ΟΜΙΛΗΤΡΙΑ 19
Α.10 ΔΙΟΡΓΑΝΩΣΗ ΔΙΕΘΝΩΝ ΣΥΝΕΔΡΙΩΝ ΚΑΙ ΣΕΜΙΝΑΡΙΩΝ 19
Α.10.1 ΔΙΟΡΓΑΝΩΣΗ ΘΕΡΙΝΩΝ ΣΧΟΛΕΙΩΝ 19
Α.10.2 ΔΙΟΡΓΑΝΩΣΗ ΣΥΝΕΔΡΙΩΝ ΚΑΙ WORKSHOPS 19
Α.11 ΣΥΝΤΑΚΤΙΚΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ 19
Α.11.1 ΜΕΛΟΣ ΣΥΝΤΑΚΤΙΚΗΣ ΕΠΙΤΡΟΠΗΣ ΕΠΙΣΤΗΜΟΝΙΚΩΝ ΠΕΡΙΟΔΙΚΩΝ 19
Α.11.2 ΜΕΛΟΣ ΣΥΝΤΑΚΤΙΚΗΣ ΕΠΙΤΡΟΠΗΣ ΕΠΙΣΤΗΜΟΝΙΚΩΝ ΠΕΡΙΟΔΙΚΩΝ – ΕΞΕΙΔΙΚΕΥΜΕΝΑ ΤΕΥΧΗ 20
Α.11.3 ΠΡΟΕΔΡΕΥΟΥΣΑ ΘΕΜΑΤΙΚΗΣ ΕΝΟΤΗΤΑΣ (TRACK CHAIR) ΣΕ ΔΙΕΘΝΗ ΣΥΝΕΔΡΙΑ 20
Α.11.4 ΜΕΛΟΣ ΕΠΙΣΤΗΜΟΝΙΚΗΣ ΕΠΙΤΡΟΠΗΣ ΠΡΟΓΡΑΜΜΑΤΟΣ (PROGRAM COMMITTEE MEMBER) ΣΕ ΔΙΕΘΝΗ ΣΥΝΕΔΡΙΑ 21
Α.11.5 ΚΡΙΤΗΣ (REVIEWER) ΕΡΕΥΝΗΤΙΚΩΝ ΕΡΓΑΣΙΩΝ ΣΕ ΕΠΙΣΤΗΜΟΝΙΚΑ ΠΕΡΙΟΔΙΚΑ 22

Α.11.6 ΚΡΙΤΗΣ (REVIEWER) ΕΡΕΥΝΗΤΙΚΩΝ ΕΡΓΑΣΙΩΝ ΣΕ ΔΙΕΘΝΗ ΣΥΝΕΔΡΙΑ 23
Α.12 ΔΙΟΙΚΗΤΙΚΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ 25
Α.12.1 ΣΥΜΜΕΤΟΧΗ ΣΕ ΟΜΑΔΕΣ ΕΡΓΑΣΙΑΣ 25
Β. ΑΝΑΛΥΤΙΚΟ ΥΠΟΜΝΗΜΑ ΓΙΑ ΤΙΣ ΥΠΟΒΑΛΛΟΜΕΝΕΣ ΕΠΙΣΤΗΜΟΝΙΚΕΣ ΔΗΜΟΣΙΕΥΣΕΙΣ **27**
Β.1 ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ 27
Β.2 ΕΡΕΥΝΗΤΙΚΕΣ ΕΡΓΑΣΙΕΣ ΔΗΜΟΣΙΕΥΜΕΝΕΣ ΣΕ ΔΙΕΘΝΗ ΕΠΙΣΤΗΜΟΝΙΚΑ ΠΕΡΙΟΔΙΚΑ 29
Β.3 ΕΡΕΥΝΗΤΙΚΕΣ ΕΡΓΑΣΙΕΣ ΔΗΜΟΣΙΕΥΜΕΝΕΣ ΣΕ ΠΡΑΚΤΙΚΑ ΔΙΕΘΝΩΝ ΕΠΙΣΤΗΜΟΝΙΚΩΝ ΣΥΝΕΔΡΙΩΝ ΜΕΤΑ ΑΠΟ ΚΡΙΣΗ ΠΛΗΡΟΥΣ ΚΕΙΜΕΝΟΥ 45

Α. ΒΙΟΓΡΑΦΙΚΟ ΣΗΜΕΙΩΜΑ

Α.1 ΠΡΟΣΩΠΙΚΑ ΣΤΟΙΧΕΙΑ

Ονοματεπώνυμο:	**Τσώχου Αγγελική**
Ονόματα γονέων:	Γεώργιος και Μαρία
Ημερομηνία γέννησης:	6 Οκτωβρίου 1980
Ηλεκτρονική Διεύθυνση:	atsohou@ionio.gr
Τηλέφωνο Εργασίας:	+30 - 2261087705
Διεύθυνση Ιστοσελίδας:	http://di.ionio.gr
Google Scholar:	https://scholar.google.com/citations?user=etn5eNkAAAAJ&hl=en

Α.2 ΣΠΟΥΔΕΣ

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

Μεταδιδακτορική Ερευνήτρια (Post-Doctoral Researcher) (2013-2014), University of Jyväskylä, Department of Computer Science and Information Systems, Φινλανδία

Μεταδιδακτορική Ερευνήτρια (Post-Doctoral Researcher) (2011-2013), Brunel University West London, Business School, Ηνωμένο Βασίλειο

Διδακτορικό Δίπλωμα (Άριστα), Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων, Πανεπιστήμιο Αιγαίου (2010), Τίτλος διδακτορικής διατριβής: *Η Ενημερότητα Ασφάλειας στα Πλαίσια της Διοίκησης Ασφάλειας Πληροφοριακών Συστημάτων*

Μεταπτυχιακό Δίπλωμα στα *Πληροφοριακά Συστήματα* (Άριστα), Τμήμα Πληροφορικής, Οικονομικό Πανεπιστήμιο Αθηνών (2002-2004)

Πτυχίο *Πληροφορικής* (Λίαν Καλώς), Τμήμα Πληροφορικής, Οικονομικό Πανεπιστήμιο Αθηνών (1998-2002)

Α.3 ΕΡΕΥΝΗΤΙΚΑ ΕΝΔΙΑΦΕΡΟΝΤΑ

- Πολιτικές Ασφάλειας και Ιδιωτικότητας, Αντιλήψεις Επικινδυνότητας και Ενημερότητα Χρηστών
- Ανάλυση Επικινδυνότητας και Διοίκηση Ασφάλειας Πληροφοριών
- Ανάλυση Αντικτύπου Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων
- Εργαλεία Ενίσχυσης της Ιδιωτικότητας
- Ιδιωτικότητα σε Πληροφοριακά Συστήματα
- Πρότυπα Ασφάλειας και Ιδιωτικότητας

Α.4 ΠΑΡΟΥΣΑ ΑΠΑΣΧΟΛΗΣΗ

Σεπτέμβριος 2016 - Σήμερα: **Επίκουρη Καθηγήτρια** σε Ασφάλεια και Ιδιωτικότητα στο Διαδίκτυο, Ιόνιο Πανεπιστήμιο, Τμήμα Πληροφορικής, Κέρκυρα, Ελλάδα

Α.5 ΣΥΝΟΨΗ ΕΠΑΓΓΕΛΜΑΤΙΚΗΣ ΕΜΠΕΙΡΙΑΣ

Α.5.1 **Σεπτέμβριος 2014 – Αύγουστος 2016**: **Λέκτορας** σε Ασφάλεια και Ιδιωτικότητα στο Διαδίκτυο, Ιόνιο Πανεπιστήμιο, Τμήμα Πληροφορικής, Κέρκυρα, Ελλάδα

Α.5.2 **Ιούλιος 2013 – Αύγουστος 2014:** Μεταδιδακτορική ερευνήτρια (Post-Doctoral Researcher), University of Jyväskylä, Department of Computer Science and Information Systems, Φινλανδία.

Α.5.3 **Ιούλιος 2012 - Ιούνιος 2013**: Ειδικευμένη ερευνήτρια (Senior Research Fellow) σε ασφάλεια και ιδιωτικότητα δημοσίων υπηρεσιών σε περιβάλλοντα νεφοϋπολογιστικής, Brunel University West London, Ηνωμένο Βασίλειο.

Α.5.4 **Ιούνιος 2011 – Ιούνιος 2012**: Ειδικευμένη ερευνήτρια (Senior Research Fellow, Marie Curie FP7 People) σε μηχανική επιχειρησιακών διαδικασιών (process engineering) σε περιβάλλοντα ηλεκτρονικής διακυβέρνησης, Brunel University West London, Ηνωμένο Βασίλειο.

Α.5.5 **Δεκέμβριος 12.2009 – Ιούνιος 2011**: Ειδική Συνεργάτης του Ειδικού Γραμματέα Επιχειρησιακού Προγράμματος «Διοικητική Μεταρρύθμιση 2007-2013» του Υπουργείου Εσωτερικών, Αποκέντρωσης και Ηλεκτρονικής Διακυβέρνησης, Ελλάδα

Α.5.6 **Σεπτέμβριος 2010 – Ιούλιος 2011**: Διδάσκουσα βάσει του Π.Δ. 407/80, Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Πειραιώς, Ελλάδα

Α.5.7 **Φεβρουάριος 2010 – Ιούλιος 2010:** Επιστημονικός Συνεργάτης, Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Πειραιώς, Ελλάδα

Α.5.8 **Μάρτιος 2005 – Σεπτέμβριος 2009**: Συμμετοχή σε ερευνητικά και αναπτυξιακά έργα μέσω των ερευνητικών ομάδων του Πανεπιστημίου Αιγαίου και του Οικονομικού Πανεπιστημίου Αθηνών, Ελλάδα

Α.6 ΔΙΑΚΡΙΣΕΙΣ

Α.6.1 **Outstanding Reviewer 2013** για το επιστημονικό Περιοδικό Transforming Government: People, Process and Policy, Emerald Literati Network Awards for Excellence 2013 (http://www.emeraldinsight.com/authors/literati/reviewer_2013.htm)

Α.6.2 **Outstanding Reviewer 2012** για το επιστημονικό Περιοδικό Journal Information Management and Computer Security, Emerald Literati Network Awards for Excellence 2012 (http://www.emeraldinsight.com/authors/literati/reviewer_2012.htm)

Α.6.3 **Υποτροφία Marie Curie 2011,** στο πλαίσιο Επιστημονικού Έργου υπό χρηματοδότηση από την Ευρωπαϊκή Επιτροπή

Α.6.4 **Highly Commended Award Winner for Outstanding Paper at the Emerald Literati Network Awards for Excellence 2009** για το άρθρο 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 (http://www.emeraldinsight.com/authors/literati/awards.htm?year=2009&journal=imcs)

A.6.5 **Πρότυπο Άρθρο (Sample Article)** για το περιοδικό Information Management and Computer Security 2009 για το άρθρο για το άρθρο 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

A.6.6 **Υποτροφία από το Μεταπτυχιακό Πρόγραμμα Σπουδών** στα *Πληροφοριακά Συστήματα* (Άριστα), Τμήμα Πληροφορικής, Οικονομικό Πανεπιστήμιο Αθηνών (2002-2004)

Α.7 ΕΠΑΓΓΕΛΜΑΤΙΚΗ ΕΜΠΕΙΡΙΑ

Α.7.1 ΔΙΔΑΚΤΙΚΗ ΕΜΠΕΙΡΙΑ

Μεταπτυχιακά Προγράμματα Σπουδών

A.7.1.1 **Διδάσκουσα**, αυτοδύναμη διδασκαλία ενοτήτων στο πλαίσιο του μαθήματος *Πολιτικές Ασφάλειας & Ιδιωτικότητας στο Διαδίκτυο* (Εαρινό εξάμηνο, 2019), Πρόγραμμα Μεταπτυχιακών Σπουδών σε Ψηφιακές Εφαρμογές & Καινοτομία, Τμήμα Πληροφορικής, Ιόνιο Πανεπιστήμιο

A.7.1.2 **Διδάσκουσα**, αυτοδύναμη διδασκαλία στο πλαίσιο του μαθήματος *Διοίκηση Πληροφοριακών Συστημάτων* (Εαρινό εξάμηνο, 2018), Πρόγραμμα Μεταπτυχιακών Σπουδών σε Τεχνολογίες και Διοίκηση Πληροφοριακών και Επικοινωνιακών Συστημάτων, Πανεπιστήμιο Αιγαίου

A.7.1.3 **Διδάσκουσα**, αυτοδύναμη διδασκαλία ενοτήτων στο πλαίσιο του μαθήματος *Ειδικά Θέματα Ασφάλειας και Ιδιωτικότητας στο Διαδίκτυο* (Χειμερινό εξάμηνο, 2015; Χειμερινό εξάμηνο, 2016; Χειμερινό εξάμηνο, 2017), Πρόγραμμα Μεταπτυχιακών Σπουδών σε Πληροφορική, Τμήμα Πληροφορικής, Ιόνιο Πανεπιστήμιο

A.7.1.4 **Διδάσκουσα**, αυτοδύναμη διδασκαλία ενοτήτων στο πλαίσιο του μαθήματος *Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων* (Εαρινό εξάμηνο, 2016; Εαρινό εξάμηνο 2017; Εαρινό εξάμηνο 2018), Πρόγραμμα Μεταπτυχιακών Σπουδών σε Πληροφορική, Τμήμα Πληροφορικής, Ιόνιο Πανεπιστήμιο

A.7.1.5 **Διδάσκουσα**, αυτοδύναμη διδασκαλία του μαθήματος *Ασφάλεια Πληροφοριακών Συστημάτων και Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας* (Χειμερινό Εξάμηνο, 2016), Τεχνολογίες και Διοίκηση Πληροφοριακών και Επικοινωνιακών Συστημάτων, Πανεπιστήμιο Αιγαίου

A.7.1.6 **Διδάσκουσα**, αυτοδύναμη διδασκαλία του μαθήματος *Πληροφοριακά Συστήματα* (Χειμερινό Εξάμηνο, 2016), Τεχνολογίες και Διοίκηση Πληροφοριακών και Επικοινωνιακών Συστημάτων, Πανεπιστήμιο Αιγαίου

A.7.1.7 **Προσκεκλημένη Εισηγήτρια**, αυτοδύναμη διδασκαλία ενοτήτων του μαθήματος *Γλώσσες Προγραμματισμού και Βιολογικές Βάσεις Δεδομένων* (Χειμερινό εξάμηνο, 2016), Πρόγραμμα Μεταπτυχιακών Σπουδών Βιοπληροφορική και Νευροπληροφορική, Τμήμα Πληροφορικής, Ιόνιο Πανεπιστήμιο

A.7.1.8 **Προσκεκλημένη Εισηγήτρια**, αυτοδύναμη διδασκαλία ενοτήτων του μαθήματος *Ασφάλεια Πληροφοριακών Συστημάτων και Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας* (Χειμερινό εξάμηνο,

2015), Πρόγραμμα Μεταπτυχιακών Σπουδών σε Τεχνολογίες και Διοίκηση Πληροφοριακών και Επικοινωνιακών Συστημάτων, Πανεπιστήμιο Αιγαίου

Α.7.1.9 **Προσκεκλημένη Εισηγήτρια**, αυτοδύναμη διδασκαλία ενοτήτων του μαθήματος *Διοίκηση Πληροφοριακών Συστημάτων* (Εαρινό εξάμηνο, 2015), Πρόγραμμα Μεταπτυχιακών Σπουδών σε Τεχνολογίες και Διοίκηση Πληροφοριακών και Επικοινωνιακών Συστημάτων, Πανεπιστήμιο Αιγαίου

Α.7.1.10 **Διδάσκουσα βάσει του Π.Δ. 407/80**, αυτοδύναμη διδασκαλία ενοτήτων στο πλαίσιο του μαθήματος *Πολιτικές και Διαχείριση Ασφάλειας* (Εαρινό Εξάμηνο 2011), Πρόγραμμα Μεταπτυχιακών Σπουδών, Μεταπτυχιακό Δίπλωμα Ειδίκευσης «Τεχνοοικονομική Διοίκηση και Ασφάλεια Ψηφιακών Συστημάτων», Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Πειραιώς

Α.7.1.11 **Επιστημονικός Συνεργάτης**, διαμόρφωση και διδασκαλία της ύλης δύο διαλέξεων του μαθήματος: *Πολιτικές και Διαχείριση Ασφάλειας* (Εαρινό Εξάμηνο 2010), Πρόγραμμα Μεταπτυχιακών Σπουδών, Μεταπτυχιακό Δίπλωμα Ειδίκευσης «Τεχνοοικονομική Διοίκηση και Ασφάλεια Ψηφιακών Συστημάτων», Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Πειραιώς.

Προπτυχιακά Προγράμματα Σπουδών

Α.7.1.1 **Διδάσκουσα**, αυτοδύναμη διδασκαλία του μαθήματος *Πολιτικές και Τεχνολογίες Ασφάλειας και Ιδιωτικότητας* (Χειμερινό Εξάμηνο, 2014; Χειμερινό Εξάμηνο, 2015; Χειμερινό Εξάμηνο, 2016; Χειμερινό Εξάμηνο, 2017; Χειμερινό Εξάμηνο, 2018; Χειμερινό Εξάμηνο, 2019), Πρόγραμμα Προπτυχιακών Σπουδών, Τμήμα Πληροφορικής, Ιόνιο Πανεπιστήμιο

Α.7.1.2 **Διδάσκουσα**, αυτοδύναμη διδασκαλία του μαθήματος *Διοίκηση Ασφάλειας Πληροφοριακών Συστημάτων* (Εαρινό Εξάμηνο, 2015; Εαρινό Εξάμηνο, 2016; Εαρινό Εξάμηνο, 2017; Εαρινό Εξάμηνο, 2018; Εαρινό Εξάμηνο, 2019), Πρόγραμμα Προπτυχιακών Σπουδών, Τμήμα Πληροφορικής, Ιόνιο Πανεπιστήμιο

Α.7.1.3 **Διδάσκουσα**, συνδιδασκαλία του μαθήματος *Ειδικά Θέματα Ασφάλειας Πληροφοριών* (Εαρινό Εξάμηνο, 2016; Εαρινό Εξάμηνο, 2017; Εαρινό Εξάμηνο, 2018; Εαρινό Εξάμηνο, 2019), Πρόγραμμα Προπτυχιακών Σπουδών, Τμήμα Πληροφορικής, Ιόνιο Πανεπιστήμιο

Α.7.1.4 **Διδάσκουσα**, αυτοδύναμη διδασκαλία του μαθήματος *Μαθηματικός Προγραμματισμός* (Χειμερινό Εξάμηνο, 2014; Χειμερινό Εξάμηνο, 2015; Χειμερινό Εξάμηνο, 2016; Χειμερινό Εξάμηνο, 2017; Χειμερινό Εξάμηνο, 2018), Πρόγραμμα Προπτυχιακών Σπουδών, Τμήμα Πληροφορικής, Ιόνιο Πανεπιστήμιο

Α.7.1.5 **Διδάσκουσα**, συνδιδασκαλία του μαθήματος *Μαθηματικός Προγραμματισμός* (Χειμερινό Εξάμηνο, 2019), Πρόγραμμα Προπτυχιακών Σπουδών, Τμήμα Πληροφορικής, Ιόνιο Πανεπιστήμιο

Α.7.1.6 **Διδάσκουσα**, αυτοδύναμη διδασκαλία του μαθήματος *Συστήματα Υποστήριξης Αποφάσεων* (Εαρινό Εξάμηνο, 2015), Πρόγραμμα Προπτυχιακών Σπουδών, Τμήμα Πληροφορικής, Ιόνιο Πανεπιστήμιο

Α.7.1.7 **Ειδικευμένη Ερευνήτρια,** Διδασκαλία στα πλαίσια μεταδιδακτορικής έρευνας, συνδιδασκαλία του μαθήματος "Information Security Management" (Εαρινό εξάμηνο, 2014), σε συνεργασία με τον Καθ. Siponen Mikko, Τμήμα Επιστήμης Υπολογιστών και Πληροφοριακών Συστημάτων, University of Jyväskylä, Finland

Α.7.1.8 **Διδάσκουσα βάσει του Π.Δ. 407/80**, αυτοδύναμη διδασκαλία του μαθήματος *Πολιτικές και Διαχείριση Ασφάλειας* (Χειμερινό εξάμηνο 2010) Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Πειραιώς.

Α.7.1.9 **Διδάσκουσα βάσει του Π.Δ. 407/80**, αυτοδύναμη διδασκαλία του μαθήματος *Ασφάλεια Πληροφοριακών Συστημάτων* (Εαρινό Εξάμηνο, 2011) Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Πειραιώς.

Α.7.1.10 **Επιστημονικός Συνεργάτης**, αυτοδύναμη διδασκαλία, διαμόρφωση και διδασκαλία της ύλης του μαθήματος: *Ασφάλεια Πληροφοριακών Συστημάτων* (Εαρινό Εξάμηνο 2010), Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Πειραιώς.

Προγράμματα Κατάρτισης και Επιμόρφωσης

Α.7.1.11 Εισηγήτρια θεμάτων ασφάλειας πληροφοριακών συστημάτων, **Εθνικό Κέντρο Δημόσιας Διοίκησης και Αυτοδιοίκησης** (2.2010-4.2010)

Α.7.1.12 Εισηγήτρια στο θερινό σχολείο **European Intensive Programme on Information and Communication Technologies Security** (IPICS 2009, 2010, 2011, 2012, 2013, 2015, 2017, 2018)

Α.7.2 ΕΠΙΒΛΕΨΗ ΥΠΟΨΗΦΙΩΝ ΔΙΔΑΚΤΟΡΩΝ ΚΑΙ ΣΥΜΜΕΤΟΧΗ ΣΕ ΕΞΕΤΑΣΤΙΚΕΣ ΕΠΙΤΡΟΠΕΣ ΔΙΔΑΚΤΟΡΙΚΩΝ ΔΙΑΤΡΙΒΩΝ

Α.7.2.1 **Επιβλέπουσα** διδακτορικής διατριβής της Ρένας Λαβράνου, «Εκπαίδευση χρηστών Διαδικτύου και χρήση τεχνικών μηχανικής μάθησης με στόχο την ενίσχυση της ενημερότητας για την πληροφοριακή ιδιωτικότητα», Ιόνιο Πανεπιστήμιο, σε εξέλιξη

Α.7.2.2 **Επιβλέπουσα** διδακτορικής διατριβής του Ιωάννη Πασπάτη, «Από-ανωνυμοποίηση δεδομένων εφαρμογών κινητών τηλεφώνων και κίνδυνοι ιδιωτικότητας», Ιόνιο Πανεπιστήμιο, σε εξέλιξη

Α.7.2.3 **Επιβλέπουσα** διδακτορικής διατριβής της Αικατερίνης Σουμελίδου, «Οπτικοποίηση Πολιτικών Ιδιωτικότητας και Ενημερότητα Ιδιωτικότητας», Ιόνιο Πανεπιστήμιο, σε εξέλιξη

Α.7.2.4 **Επιβλέπουσα** διδακτορικής διατριβής του Θάνου Παπαϊωάννου, «Ψηφιακή Ταυτότητα και Αντίληψη της Ιδιωτικότητας», Ιόνιο Πανεπιστήμιο, σε εξέλιξη

Α.7.2.5 **Μέλος της Τριμελούς Συμβουλευτικής Επιτροπής** της διδακτορικής διατριβής του Ανδρέα Σκάλκου, «Πληροφοριακή Ιδιωτικότητα και Ανθρώπινη Συμπεριφορά», Πανεπιστήμιο Αιγαίου, σε εξέλιξη

Α.7.2.6 **Μέλος της Επταμελούς Εξεταστικής Επιτροπής** της διδακτορικής διατριβής του Γιαννακά Φιλίππου με τίτλο "Αξιοποίηση παιγνίων σε κινητές συσκευές για την ενίσχυση της ευαισθητοποίησης των μαθητών της πρωτοβάθμιας και πρώιμης δευτεροβάθμιας εκπαίδευσης σε ζητήματα ασφάλειας και ιδιωτικότητας στο Διαδίκτυο", Πανεπιστήμιο Αιγαίου, Σεπτέμβριος 2018

Α.7.2.7 **Μέλος της Επταμελούς Εξεταστικής Επιτροπής** της διδακτορικής διατριβής της Γεωργίου Δήμητρας με τίτλο "Security Policies for Cloud Computing", Πανεπιστήμιο Πειραιώς, Δεκέμβριος 2017

Α.7.2.8 **Μέλος της Επταμελούς Εξεταστικής Επιτροπής** της διδακτορικής διατριβής της Μιχώτα Αλεξάνδρας με τίτλο "Privacy in Online Social Networks", Πανεπιστήμιο Πειραιώς, Δεκέμβριος 2017

Α.7.2.9 **Μέλος της Επταμελούς Εξεταστικής Επιτροπής** της διδακτορικής διατριβής του *Σίμου Σταύρου* με τίτλο "Designing Cloud Forensic-Enabled System", Πανεπιστήμιο Αιγαίου, Ιούνιο 2017

Α.7.2.10 **Εξωτερική κριτής** διδακτορικής διατριβής του *Saud Alotaibi*, για τη διδακτορική διατριβή με τίτλο "Transparent User Authentication for Mobile Applications", University of Plymouth, Ιανουάριος 2019.

Α.7.2.11 **Εξωτερική κριτής** διδακτορικής διατριβής του *Jouko Selkälä*, για τη διδακτορική διατριβή με τίτλο "Chief Information Officer decision making: Issues and a Process View", Department of Computer Science and Information Systems, University of Jyvaskyla, Νοέμβριος 2015.

Α.7.2.12 **Εξωτερική κριτής** διδακτορικής διατριβής της *Ana Nieto Jiménez*, για τη διδακτορική διατριβή με τίτλο "Design of Mechanisms for Development of Secure Systems trading-off Quality of Service", University of Malaga, Μάϊος 2015.

Α7.3 ΕΠΙΒΛΕΨΗ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΔΙΠΛΩΜΑΤΙΚΩΝ ΕΡΓΑΣΙΩΝ

Α.7.3.1 **Επιβλέπουσα** σε έξι μεταπτυχιακές διπλωματικές εργασίες του Μεταπτυχιακού Προγράμματος Πληροφορική, Ιόνιο Πανεπιστήμιο (2016-Σήμερα)

Α.7.3.2 **Μέλος της συμβουλευτικής και εξεταστικής επιτροπής** σε τέσσερις μεταπτυχιακές διπλωματικές εργασίες του Μεταπτυχιακού Προγράμματος Πληροφορική, Ιόνιο Πανεπιστήμιο (2016-Σήμερα)

Α.7.3.3 **Μέλος της συμβουλευτικής και εξεταστικής επιτροπής** σε τέσσερις μεταπτυχιακές διπλωματικές εργασίες του Μεταπτυχιακού Προγράμματος Πληροφορική, Ιόνιο Πανεπιστήμιο (2016-Σήμερα)

Α.7.4 ΕΠΙΒΛΕΨΗ ΠΤΥΧΙΑΚΩΝ ΕΡΓΑΣΙΩΝ

Α.7.3.4 **Επιβλέπουσα** σε οκτώ ολοκληρωμένες πτυχιακές εργασίες του Προπτυχιακού Προγράμματος Σπουδών Πληροφορική, Ιόνιο Πανεπιστήμιο

Α.7.4.1 **Μέλος της συμβουλευτικής και εξεταστικής επιτροπής** σε επτά ολοκληρωμένες πτυχιακές εργασίες του Προπτυχιακού Προγράμματος Σπουδών Πληροφορική, Ιόνιο Πανεπιστήμιο

Α.7.4.2 **Μέλος της συμβουλευτικής και εξεταστικής επιτροπής** σε μία πτυχιακή εργασία του Προπτυχιακού Προγράμματος Σπουδών Ψηφιακών Συστημάτων, Πανεπιστήμιο Πειραιώς

Α.7.3 ΕΡΕΥΝΗΤΙΚΉ ΕΜΠΕΙΡΙΑ - ΕΡΓΑ ΕΡΕΥΝΑΣ

Επιστημονική Υπεύθυνη σε Διεθνή Ερευνητικά Έργα

Α.7.3.1 **Επιστημονική Υπεύθυνη Έργου**, EU Programme H2020, Project Reference DS-08-2017: 787068, "*Data Governance for Supporting GDPR (DEFeND)*", για το Ιόνιο Πανεπιστήμιο, (07.2018-Σήμερα)

Α.7.3.2 **Επιστημονική Υπεύθυνη Έργου**, Cooperation Programme Interreg V/A Greece-Italy (EL-IT) 2014-2020: 5003441, "Open City TechNology Enabler (OCTaNe)", για το Ιόνιο Πανεπιστήμιο, (05.2018-Σήμερα)

Ερευνήτρια σε Διεθνή Ερευνητικά Έργα

Α.7.3.3 **Εξειδικευμένος Σύμβουλος σε Ενημερότητα Ασφάλειας Πληροφοριών**, Expert Services related to the European Cyber Security Month (ECSM) in 2017, ENISA (11.2016-08.2017)

Α.7.3.4 **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).

Α.7.3.5 **Information Systems Evaluation**, EU Programme FP7/Project Reference INFSO-ICT-248010: "UbiPOL- Ubiquitous Participation Platform for Policy Making", Brunel University, (08.2011-04.2013).

Α.7.3.6 **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).

Επιστημονική Υπεύθυνη σε Μελετητικά και Αναπτυξιακά Έργα Εθνικής Εμβέλειας

Α.7.3.7 **Επιστημονική Υπεύθυνη Έργου**, "*ioniAn Pdmfc Partnership (APPly)*", Ιόνιο Πανεπιστήμιο, PDM&FC (04.2017 - Σήμερα)

Α.7.3.8 **Επιστημονική Υπεύθυνη Έργου**, Διοργάνωση του Θερινού Σχολείου Εντατικό Πρόγραμμα σε Ασφάλεια Πληροφοριών και Επικοινωνιακών Συστημάτων (03.2017 – 08.2017)

Ερευνήτρια σε Μελετητικά και Αναπτυξιακά Έργα Εθνικής Εμβέλειας

Α.7.3.9 **Ερευνήτρια**, Έργο «Συμμόρφωση του Ιονίου Πανεπιστημίου με τον Γενικό Ευρωπαϊκό Κανονισμό για την Προστασία Δεδομένων 2016/679 (General Data Protection Regulation - GDPR)» (09.2018 – 12.2018)

Α.7.3.10 **Ερευνήτρια**, Έργο «Συμμόρφωση του Ινστιτούτου Παστέρ με τον Γενικό Κανονισμό για την Προστασία Δεδομένων (General Data Protection Regulation - GDPR)» (11.2018 – 02.2019)

Α.7.3.11 **Ερευνήτρια**, Έργο «Συμμόρφωση του Πανεπιστημίου Πειραιώς με τον Γενικό Κανονισμό για την Προστασία Δεδομένων (General Data Protection Regulation - GDPR)» (08.2018 – 12.2018)

Α.7.3.12 **Ερευνήτρια**, Έργο «Συμμόρφωση του Πανεπιστημίου Αιγαίου με τον Γενικό Κανονισμό για την Προστασία Δεδομένων (General Data Protection Regulation - GDPR)» (03.2018 – 08.2018)

Α.7.3.13 **Ερευνήτρια**, Έργο «Παροχή Υπηρεσιών υποστήριξης για τη συμμόρφωση πληροφοριακών συστημάτων της ΕΔΕΤ Α.Ε. με τον Νέο Γενικό Κανονισμό Προστασίας Δεδομένων Προσωπικού Χαρακτήρα 2016/679 (General Data Protection Regulation - GDPR)», (06.2018 – 10.2018)

Α.7.3.14 **Αναλύτρια Επικινδυνότητας**, Έργο "*Εκπαίδευση Λειτουργών Α' Τμήμα Υπηρεσιών Πληροφορικής - Πρότυπο 904 Διαχείριση Κινδύνων*", PLANET A.E., 2016.

Α.7.3.15 **Αναλύτρια Επικινδυνότητας**, Έργο "*Μελέτη Ασφάλειας για τα Γεωγραφικά Συστήματα Πληροφοριών (Ηλεκτρονική Πολεοδομία) για τις Νομαρχιακές Αυτοδιοικήσεις της Χώρας*", TREK Consulting - Πανεπιστήμιο Αιγαίου, 2009.

Α.7.3.16 **Ερευνήτρια**, «Παραγωγή εκπαιδευτικού υλικού με θεματική ενότητα "ασφάλεια πληροφοριακών συστημάτων σε περιβάλλοντα ηλεκτρονικής διακυβέρνησης" για το έργο κατάρτιση και πιστοποίηση σε βασικές δεξιότητες και κατάρτιση σε προηγμένες δεξιότητες στη χρήση ΤΠΕ εργαζομένων στην τοπική αυτοδιοίκηση», PLANET Α.Ε., 2009.

Α.7.3.17 **Αναλύτρια Επικινδυνότητας**, Έργο «*Μελέτη Ασφάλειας για το Ολοκληρωμένο Πληροφοριακό Σύστημα και τη Διαδικτυακή Πύλη επικοινωνίας του Εθνικού Παρατηρητηρίου για τις ΜΜΕ*», TREK Consulting - ΕΟΜΜΕΧ - Πανεπιστήμιο Αιγαίου, 2008-09.

Α.7.3.18 **Αναλύτρια Επικινδυνότητας,** Έργο "*Μελέτη Ασφάλειας των Ολοκληρωμένων Πληροφοριακών Συστημάτων και εγκαταστάσεων για τις υποστηρικτικές λειτουργίες των Νομαρχιακών Αυτοδιοικήσεων*", ΕΠΙΣΕΥ/ΕΜΠ - Πανεπιστήμιο Αιγαίου, (11.2007 – 04.2008).

Α.7.3.19**Αναλύτρια Επικινδυνότητας**, Έργο "*Μελέτη Ασφάλειας του Πληροφοριακού Συστήματος Λειτουργικής Περιοχή Βιομηχανίας και Ορυκτού Πλούτου των Νομαρχιακών Αυτοδιοικήσεων και εγκαταστάσεων των Νομαρχιακών Αυτοδιοικήσεων*", KANTOR AE - Πανεπιστήμιο Αιγαίου, (04.2008 – 07.2008)

Α.7.3.20 **Αναλύτρια Επικινδυνότητας**, Έργο "*Μελέτη Ασφάλειας του Πληροφοριακού Συστήματος Ενημέρωσης και Εξυπηρέτησης Συνταξιούχων της Γενικής Γραμματείας Πληροφοριακών Συστημάτων*", Quality and Reliability A.E. - INTRACOM – Πανεπιστήμιο Αιγαίου, (11.2007-02.2008).

Α.7.3.21 **Αναλύτρια Επικινδυνότητας**, Έργο "*Μελέτη Αποτίμησης Επικινδυνότητας & Σχεδίου Ασφαλείας της Κεντρικής Κυβερνητικής Διαδικτυακής Πύλης της Δημόσιας Διοίκησης για την Πληροφόρηση & Ασφαλή Διεκπεραίωση Ηλεκτρονικών Συναλλαγών των Πολιτών/Επιχειρήσεων*", Info-Quest - Decision Systems Integration – Πανεπιστήμιο Αιγαίου, (09.2007-02.2008).

Α.7.3.22 **Αναλύτρια Επικινδυνότητας**, Έργο "*Μελέτη Ασφάλειας Πληροφοριακού Συστήματος Εμπορίου και Ανωνύμων Εταιρειών*", Siemens - Quality & Reliability – Οικονομικό Πανεπιστήμιο Αθηνών, 2006.

Α.7.3.23 **Αναλύτρια Επικινδυνότητας**, Έργο "*Μελέτη Ασφάλειας Πληροφοριακού Συστήματος Ηλεκτρονικής Πολεοδομίας*", Singular Integrators – UniSystems – Οικονομικό Πανεπιστήμιο Αθηνών, 2006.

Α.7.3.24 **Αναλύτρια Επικινδυνότητας**, Έργο "*Σχεδιασμός και υλοποίηση ελληνικής Αρχής Πιστοποίησης για την έκδοση ηλεκτρονικών διαβατηρίων*", D.S. Technologies - Οικονομικό Πανεπιστήμιο Αθηνών, 2006.

Α.7.3.25 **Αναλύτρια Επικινδυνότητας**, Έργο "*Μελέτη Ασφάλειας Ολοκληρωμένου Πληροφοριακού Συστήματος Υγείας ΔΥΠε Ιονίων Νήσων*", Κοινωνία της Πληροφορίας ΑΕ – Remaco ΑΕ – Οικονομικό Πανεπιστήμιο Αθηνών, 2006.

Α.7.3.26**Αναλύτρια Επικινδυνότητας**, Έργο "*Μελέτη Ασφάλειας Πληροφοριακού Συστήματος Πυροσβεστικού Σώματος*", Quality and Reliability A.E. – Πανεπιστήμιο Αιγαίου, (1.2006 – 1.2007).

Α.7.3.27 **Ερευνήτρια**, Έργο, "*Έλεγχος Συμβατότητας της Εταιρείας «ECDL Ελλάς» με το Πρότυπο ISO/IEC 27001*", CheckPoint, ECDL Hellas, 2006.

Α.7.3.28 **Αναλύτρια Επικινδυνότητας**, Έργο "*Μελέτη Σχεδίου Ασφάλειας του Γενικού Νοσοκομείου Κορίνθου για τη λειτουργία αρχείων με ευαίσθητα δεδομένα*", ΓΝ Κορίνθου – Πανεπιστήμιο Αιγαίου, (11.2005 – 12.2005).

Α.7.3.29 **Ερευνήτρια,** Έργο e-UNIVERSITY: "*Μελέτη, Καθορισμός Τεχνικών Προδιαγραφών-Τευχών Διαγωνισμών & Επίβλεψη Αναδόχου Υλοποίησης του Συστήματος Δημοσιεύσεων, Πληροφόρησης και Συναλλαγών του Πολίτη σε θέματα Διοικητικών Υποθέσεων και της Προμήθειας και Εγκατάστασης Δικτυακού και Υπολογιστικού Εξοπλισμού*", Κοινωνία της Πληροφορίας Α.Ε. – Πανεπιστήμιο Αιγαίου, (6.2005 – 12.2006).

Α.7.3.30 **Ερευνήτρια**, Έργο "*Υλοποίηση του ελληνικού σήματος συμμόρφωσης/ποιότητας υπηρεσιών/δικτύων του ΕΛΟΤ*", ΕΛΟΤ – Οικονομικό Πανεπιστήμιο Αθηνών, 2005.

Α.7.4 ΛΟΙΠΗ ΕΠΑΓΓΕΛΜΑΤΙΚΗ ΕΜΠΕΙΡΙΑ

Ειδική Συνεργάτης του Ειδικού Γραμματέα Επιχειρησιακού Προγράμματος «Διοικητική Μεταρρύθμιση 2007-2013» του Υπουργείου Εσωτερικών, Αποκέντρωσης και Ηλεκτρονικής Διακυβέρνησης (12.2009-06.2011)

Α.8 ΔΗΜΟΣΙΕΥΜΕΝΟ ΕΡΓΟ

Α.8.1 ΔΗΜΟΣΙΕΥΣΕΙΣ ΣΕ ΕΠΙΣΤΗΜΟΝΙΚΑ ΠΕΡΙΟΔΙΚΑ ΜΕ ΣΥΣΤΗΜΑ ΚΡΙΤΩΝ

(Οι εκθέτες ανά άρθρο υποδηλώνουν τον αριθμό των ετεροαναφορών από μη συν-συγγραφείς)

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

Α.8.2 ΔΗΜΟΣΙΕΥΣΕΙΣ ΣΕ ΠΡΑΚΤΙΚΑ ΔΙΕΘΝΩΝ ΣΥΝΕΔΡΙΩΝ ΜΕ ΚΡΙΣΗ ΠΛΗΡΟΥΣ ΚΕΙΜΕΝΟΥ

(Οι εκθέτες ανά άρθρο υποδηλώνουν τον αριθμό των ετεροαναφορών από μη συν-συγγραφείς)

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

Α.8.3 ΔΗΜΟΣΙΕΥΣΕΙΣ ΣΕ WORKSHOPS, POSTERS ΚΑΙ ΠΕΡΙΛΗΨΕΙΣ ΣΕ ΔΙΕΘΝΗ ΣΥΝΕΔΡΙΑ ΜΕ ΚΡΙΣΗ

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, Association for Information Systems (AIS).

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, Association for Information Systems (AIS)

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

Α.8.4 ΔΙΑΤΡΙΒΕΣ

Τ.02 Τσώχου Α., *Η Ενημερότητα Ασφάλειας στα Πλαίσια της Διοίκησης Ασφάλειας Πληροφοριακών Συστημάτων*, Διδακτορική Διατριβή, Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων, Πανεπιστήμιο Αιγαίου, Φεβρουάριος 2010

Τ.01 Τσώχου Α., *Αντιλήψεις επικινδυνότητας στη Διαχείριση Ασφάλειας Πληροφοριακών Συστημάτων: Θεωρητικές προσεγγίσεις και παράγοντες διαμόρφωσης*, Μεταπτυχιακή Διατριβή, Μεταπτυχιακό σε Πληροφοριακά Συστήματα, Τμήμα Πληροφορικής, Οικονομικό Πανεπιστήμιο Αθηνών, Φεβρουάριος 2004

Α.9 ΠΡΟΣΚΕΚΛΗΜΕΝΕΣ ΟΜΙΛΙΕΣ

Α.9.1 ΚΕΝΤΡΙΚΗ ΟΜΙΛΗΤΡΙΑ

A.10.2.1 GDPR – A researcher's view**, Executive Breakfast: GDPR - Security Solutions and Compliance**, 5th April 2017, PDMFC, IBM, Lisbon, Portugal

Α.9.2 ΟΜΙΛΗΤΡΙΑ

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

Α.10 ΔΙΟΡΓΑΝΩΣΗ ΔΙΕΘΝΩΝ ΣΥΝΕΔΡΙΩΝ ΚΑΙ ΣΕΜΙΝΑΡΙΩΝ

Α.10.1 ΔΙΟΡΓΑΝΩΣΗ ΘΕΡΙΝΩΝ ΣΧΟΛΕΙΩΝ

A.10.1.1 **Διοργάνωση Θερινού Σχολείου**, Εντατικό Πρόγραμμα σε Ασφάλεια Πληροφοριών και Επικοινωνιακών Συστημάτων IPICS 2017, 28 Ιουνίου – 7 Ιουλίου 2017, Τμήμα Πληροφορικής, Κέρκυρα

A.10.1.2 **Μέλος Οργανωτικής Επιτροπής,** Εντατικό Πρόγραμμα σε Ασφάλεια Πληροφοριών και Επικοινωνιακών Συστημάτων IPICS 2010, 17 Ιουλίου – 27 Ιουλίου 2010, Σάμος, Ελλάδα

Α.10.2 ΔΙΟΡΓΑΝΩΣΗ ΣΥΝΕΔΡΙΩΝ ΚΑΙ WORKSHOPS

A.10.2.1 **Μέλος Οργανωτικής Επιτροπής**, *STM 2010*, 6th International Workshop on Security and Trust Management, in conjunction with EuroPKI 2010 and CRITIS 2010, Athens, Greece, September 2010

Α.11 ΣΥΝΤΑΚΤΙΚΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ

Α.11.1 ΜΕΛΟΣ ΣΥΝΤΑΚΤΙΚΗΣ ΕΠΙΤΡΟΠΗΣ ΕΠΙΣΤΗΜΟΝΙΚΩΝ ΠΕΡΙΟΔΙΚΩΝ

A.11.1.1 *Human-centric Computing and Information Sciences*, Springer, Science Citation Index Expanded (Associate Editor) (Enrolment in 2018)

A.11.1.2 *Internet Research*, *Emerald* (Editorial Board Member) (Έτος ένταξης 2011)

A.11.1.3 *Information Management and Computer Security*, *Emerald* (Editorial Advisory Board Member) (Έτος ένταξης 2011)

A.11.1.4 *Transforming Government: People, Process and Policy*, *Emerald* (Editorial Advisory Board Member) (Ετος ένταξης 2015)

Α.11.2 ΜΕΛΟΣ ΣΥΝΤΑΚΤΙΚΗΣ ΕΠΙΤΡΟΠΗΣ ΕΠΙΣΤΗΜΟΝΙΚΩΝ ΠΕΡΙΟΔΙΚΩΝ – ΕΞΕΙΔΙΚΕΥΜΕΝΑ ΤΕΥΧΗ

A.11.2.1 *Algorithms-SI 2016* Special Issue "Humanistic Data Processing" Algorithms Journal

A.11.2.2 *CaEE-SI 2016* New Trends in Humanistic Informatics: Implementations and Applications, Computers & Electrical Engineering Journal

A.11.2.3 *JoWUA 2013*, Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications Journal

Α.11.3 ΠΡΟΕΔΡΕΥΟΥΣΑ ΘΕΜΑΤΙΚΗΣ ΕΝΟΤΗΤΑΣ (TRACK CHAIR) ΣΕ ΔΙΕΘΝΗ ΣΥΝΕΔΡΙΑ

A.11.3.1 *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.11.3.2 *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.11.3.3 *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.11.3.4 *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.11.3.5 *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.11.3.6 *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.11.3.7 *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.11.3.8 *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.11.3.9 *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

Α.11.4 ΜΕΛΟΣ ΕΠΙΣΤΗΜΟΝΙΚΗΣ ΕΠΙΤΡΟΠΗΣ ΠΡΟΓΡΑΜΜΑΤΟΣ (PROGRAM COMMITTEE MEMBER) ΣΕ ΔΙΕΘΝΗ ΣΥΝΕΔΡΙΑ

A.11.4.1 *E-Democracy 2019*, 9th International Conference on e-Democracy, Athens, Greece, December 2019

A.11.4.2 *HAISA 2019, 14h* International Symposium on Human Aspects of Information Security & Assurance, Nicosia, Cyprus, July 2019

A.11.4.3 *ESORICS 2019* 24th European Symposium on Research in Computer Security, Luxemburg, Luxemburg, September 2019

A.11.4.4 *HAISA 2018, 13h* International Symposium on Human Aspects of Information Security & Assurance, Dundee, Scotland, August 2018

A.11.4.5 *ESORICS 2018* 23rd European Symposium on Research in Computer Security, Barcelona, Spain, September, 2018

A.11.4.6 *HAISA 2017, 12th* International Symposium on Human Aspects of Information Security & Assurance, Adelaide, Australia, November 2017

A.11.4.7 *TrustBus 2017*, 14th International Conference on Trust, Privacy and Security in Digital Business, Lyon, France, August 2017

A.11.4.8 *E-Democracy 2017*, 7th International Conference on e-Democracy, Athens, Greece, December 2017

A.11.4.9 *COLLABORATECOM 2017* 3rd International Conference on Collaborative Computing: Networking, Applications and Worksharing, Guangzhou, China, November 2017

A.11.4.10 *ESORICS 2017* 22nd European Symposium on Research in Computer Security, Oslo, Norway, September 2017

A.11.4.11 *PCI 2016*, 20th Panhellenic Conference on Informatics, Patra, Greece, November 2016

A.11.4.12 *TrustBus 2016*, 13th International Conference on Trust, Privacy and Security in Digital Business, Porto, Portugal, September 2016

A.11.4.13 *ESORICS 2016*, 21st European Symposium On Research In Computer Security, Crete, Greece, September 2016

A.11.4.14 *SECRYPT 2016*, 13th International Conference on Security and Cryptography, Lisbon, Portugal, July 2016

A.11.4.15 *E-Democracy 2015*, 7th International Conference on e-Democracy, Athens, Greece, December 2015

A.11.4.16 *ARES 2015*, 10th International Conference on Trust, Privacy and Security in Digital Business, Toulouse, France, September 2015

A.11.4.17 *TrustBus 2015* 12th International Conference on Trust, Privacy and Security in Digital Business, València, Spain, September 2015

A.11.4.18 *PCI 2015*, 19th Panhellenic Conference on Informatics, Athens, Greece, October 2015

A.11.4.19 *TrustBus 2014*, 11th International Conference on Trust, Privacy and Security in Digital Business, Munich, Germany, September, 2014

A.11.4.20 *PCI 2014*, 18th Panhellenic Conference on Informatics, Athens, Greece, October 2014

A.11.4.21 *ARES 2014*, 9th International Conference on Trust, Privacy and Security in Digital Business, Fribourg, Switzerland, September 2014

A.11.4.22 *IADIS 2014*, 7th International Conference on Information Systems, Madrid, Spain, March 2014

A.11.4.23 *ARES 2013*, 8th International Conference on Availability, Reliability and Security Regensburg, Germany, September 2013

A.11.4.24 *TrustBus 2013*, 10th International Conference on Trust, Privacy and Security in Digital Business, Prague, Czech Republic, August 2013

A.11.4.25 *IADIS 2013*, 7th International Conference on Information Systems, Lisbon, Portugal, March 2013

A.11.4.26 *TrustBus 2012*, 9th International Conference on Trust, Privacy and Security in Digital Business, Vienna, Austria, September 2012

A.11.4.27 *IEEE CloudCom 2011*, 3rd IEEE International Conference on Cloud Computing Technology and Science, Greece, Athens, December 2011

A.11.4.28 *TrustBus 2011*, 8th International Conference on Trust, Privacy and Security in Digital Business, Toulouse, France, August, 2011

A.11.4.29 *SECRYPT 2010*, 7th International Conference on Security and Cryptography, Athens, Greece, July 2010

A.11.4.30 *OTM IS 2010*, 5th International Symposium on Information Security, Crete, Greece, October 2010

Α.11.5 ΚΡΙΤΗΣ (REVIEWER) ΕΡΕΥΝΗΤΙΚΩΝ ΕΡΓΑΣΙΩΝ ΣΕ ΕΠΙΣΤΗΜΟΝΙΚΑ ΠΕΡΙΟΔΙΚΑ

A.11.5.1 *International Journal of Information Security*, Springer

A.11.5.2 *Information & Management*, Elsevier

A.11.5.3 *Communications of the Association for Information Systems*, Association for Information Systems

A.11.5.4 *Behaviour & Information Technology*, Taylor & Francis

A.11.5.5 *Information Technology & People*, Emerald

A.11.5.6 *Computers and Security*, Elsevier.

A.11.5.7 *Information Security Journal: A Global Perspective* (Previously published as: *Information Systems Security*), Taylor & Francis.

A.11.5.8 *International Journal of Information Security*, Springer.

A.11.5.9 *Transforming Government: People, Process and Policy*, Emerald.

A.11.5.10 *Journal of Enterprise Information Management*, Emerald.

A.11.5.11 *Asia Pacific Journal of Information Systems, Korea Society of Management Information Systems*

A.11.5.12 *European Journal of Information Systems*, Palgrave

A.11.5.13 *Journal of the Association of Information Systems*, Association for Information Systems

A.11.5.14 *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, Innovative Information Science & Technology Research Group

A.11.5.15 *International. Journal of Electronic Governance*, Inderscience Publishers

Α.11.6 ΚΡΙΤΗΣ (REVIEWER) ΕΡΕΥΝΗΤΙΚΩΝ ΕΡΓΑΣΙΩΝ ΣΕ ΔΙΕΘΝΗ ΣΥΝΕΔΡΙΑ

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, 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 IFIP International Conference on Trust Management, 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.

Α.12 ΔΙΟΙΚΗΤΙΚΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ

Α.12.1 ΣΥΜΜΕΤΟΧΗ ΣΕ ΟΜΑΔΕΣ ΕΡΓΑΣΙΑΣ

Α. 12.1.1 Μέλος της **Συντονιστικής Επιτροπής** του Μεταπτυχιακού Προγράμματος «Ψηφιακές Εφαρμογές και Καινοτομία» (2018 - Σήμερα)

Α. 12.1.2 Συντονίστρια **Erasmus** του Τμήματος (2017- Σήμερα)

Α. 12.1.3 Συντονίστρια **Προγράμματος Διδακτορικών Σπουδών** (2018- Σήμερα)

Α. 12.1.4 Υπεύθυνη Σχεδιασμού του **Ωρολογίου Προγράμματος** Διαλέξεων και Εξεταστικής Προπτυχιακών Σπουδών (2014 - Σήμερα)

Α. 12.1.5 Υπεύθυνη Σχεδιασμού του **Ωρολογίου Προγράμματος** Διαλέξεων και Εξεταστικής Μεταπτυχιακών Σπουδών (2015 - Σήμερα)

Α. 12.1.6 Συμμετοχή στην Ομάδα Εργασίας **Ανασχεδιασμού της Χρήσης Κτιριακών χώρων και Υποδομών** του Τμήματος (2015)

Α. 12.1.7 Υπεύθυνη της Ομάδας Εργασίας για την **Επικαιροποίηση του Ιστοτόπου του Τμήματος** (2015 - Σήμερα)

Α. 12.1.8 Συμμετοχή στην Ομάδα Εργασίας **συντονισμού του Μεταπτυχιακού Προγράμματος Σπουδών** Πληροφορική (2015 – Σήμερα)

Α. 12.1.9 Συντονισμός της Ομάδα Εργασίας για τη **διοργάνωση Τελετής Αναγόρευσης** του Dr. Bernd Wegner σε επίτιμο διδάκτορα του Τμήματος Πληροφορικής του Ιονίου Πανεπιστημίου

Α. 12.1.10 Συμμετοχή στην Ομάδα Εργασίας για την προετοιμασία **Εξωτερικής Αξιολόγησης** του Ιονίου Πανεπιστημίου από την Αρχή Διασφάλισης και Πιστοποίησης της Ποιότητας στην Ανώτατη Εκπαίδευση (ΑΔΙΠ)

Β. ΑΝΑΛΥΤΙΚΟ ΥΠΟΜΝΗΜΑ ΓΙΑ ΤΙΣ ΥΠΟΒΑΛΛΟΜΕΝΕΣ ΕΠΙΣΤΗΜΟΝΙΚΕΣ ΔΗΜΟΣΙΕΥΣΕΙΣ

Β.1 ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

Η ασφάλεια πληροφοριακών συστημάτων (Π.Σ.) προϋποθέτει την υλοποίηση τεχνικών αντιμέτρων, αλλά και την εφαρμογή οργανωτικών και διαδικαστικών μέτρων ασφάλειας. Όμως, όπως δείχνει η δημοσιευμένη έρευνα, ενώ η έρευνα των τεχνικών ζητημάτων έχει ήδη αποδώσει σε ένα μεγάλο πλήθος αποτελεσματικών εργαλείων και τεχνικών, ο άνθρωπος παραμένει ως ο "αδύναμος κρίκος" της αλυσίδας της ασφάλειας. Η συμμόρφωση με τους κανόνες, τις πολιτικές και τα μέτρα ασφάλειας δεν είναι εφικτή χωρίς τη διευθέτηση των ανθρωπίνων ζητημάτων της ασφάλειας. Μια από τις βασικές πρακτικές που προτείνονται για αυτό το σκοπό είναι οι πρωτοβουλίες ενημερότητας, κατάρτισης και εκπαίδευσης ασφάλειας Π.Σ. Οι σύγχρονες τεχνικές μελέτες για την ασφάλεια Π.Σ. αναγνωρίζουν την *ενημερότητα* ως ένα κρίσιμο παράγοντα στον οποίο πρέπει να εστιάσουν οι οργανώσεις για την αποτελεσματικότερη διοίκηση ασφάλειας Π.Σ.

Παρά το γεγονός ότι η σημασία της ενημερότητας ασφάλειας Π.Σ. αναγνωρίζεται από τους περισσότερους ερευνητές και οργανισμούς, η ενημερότητα παραμένει ένα από τα κρισιμότερα ζητήματα των τελευταίων πέντε ετών σε σχέση με την ασφάλεια. Μάλιστα, η σπουδαιότητα της ενημερότητας ασφάλειας επισημαίνεται από το γεγονός ότι αναγνωρίζεται πως μπορεί να συνεισφέρει στην ενσωμάτωση της διοίκησης ασφάλειας Π.Σ. στη λειτουργία του οργανισμού. Παρά τον υψηλό βαθμό προτεραιότητας που της αποδίδεται οι οργανισμοί είναι διστακτικοί να αποδώσουν σημαντικές δαπάνες για σχετικές πρωτοβουλίες, ενώ συνηθίζεται να υλοποιούνται αποκομμένα από το ευρύτερο πλαίσιο διοίκησης ασφάλειας Π.Σ. Η διαπίστωση, λοιπόν, της αποσπασματικής ανάπτυξης και εφαρμογής πρωτοβουλιών ενημερότητας ασφάλειας και η αποκομμένη από τη διοίκηση ασφάλειας Π.Σ. αντιμετώπισή της από τους ερευνητές, αποτέλεσαν αφορμή για την έρευνα που παρουσιάζει η παρούσα διατριβή.

Το αντικείμενο της έρευνας που παρουσιάζει η διατριβή, είναι *η διαδικασία διαμόρφωσης και ενσωμάτωσης στρατηγικών ενημερότητας ασφάλειας σε μία οργάνωση*. Στόχος της διατριβής είναι η δημιουργία ενός εννοιολογικού και μεθοδολογικού πλαισίου που θα συνεισφέρει στην ανάλυση και κατανόηση των ενεργειών που λαμβάνουν χώρα κατά τη διαμόρφωση και υλοποίηση δραστηριοτήτων ενημερότητας ασφάλειας Π.Σ. και την εν συνεχεία ενσωμάτωσή τους στις λοιπές δραστηριότητες της διοίκησης ασφάλειας Π.Σ. Βασικά ερωτήματα στα οποία απαντά η έρευνα, είναι:

> "Πώς γίνεται αποδεκτή και ενσωματώνεται μία δραστηριότητα ενημερότητας ασφάλειας πληροφοριακών συστημάτων σε ένα οργανωσιακό περιβάλλον;"
>
> "Τι είδους αλλαγές επιδιώκει μια πρωτοβουλία ενημερότητας ασφάλειας;"

Η διατριβή ξεκινά με τη *μελέτη και κριτική ανάλυση της δημοσιευμένης έρευνας* και *πρακτικής* σχετικά με την ενημερότητα ασφάλειας πληροφοριακών συστημάτων που οδηγεί στην αναγνώριση α) των ανοικτών ζητημάτων στο χώρο της ενημερότητας ασφάλειας, και β) των προσεγγίσεων αναφορικά με τα μοντέλα έρευνας που εφαρμόζονται (θεωρίες μεταβλητότητας, θεωρίες διεργασιών,

υβριδικά μοντέλα). Η κριτική ανάλυση της βιβλιογραφίας, αναδεικνύει την απουσία κατάλληλου θεωρητικού υπόβαθρου και μεθοδολογικού πλαισίου των περισσότερων ερευνών ενημερότητας ασφάλειας Π.Σ.

Η *εμπειρική έρευνα* της διατριβής στηρίζεται σε μία σε βάθος μελέτη περίπτωσης, όπου διαμορφώνεται και υλοποιείται μία πρωτοβουλία ενημερότητας ασφάλειας σε πραγματικό οργανωσιακό περιβάλλον. Το *θεωρητικό πλαίσιο* για την ανάλυση και ερμηνεία των δεδομένων της έρευνας περιλαμβάνει τη θεωρία δικτύων σύμπραξης (actor network theory) για την ανάλυση σε μικρο-επίπεδο, τη θεωρία της δομοποίησης (structuration theory) για την ανάλυση σε μακρο-επίπεδο και τη θεωρία του συγκειμενισμού (contextualism) για τη σύνδεση της ανάλυσης σε μακρο-επίπεδο και μικρο-επίπεδο.

Η *θεωρία της δομοποίησης* εφαρμόζεται στο πεδίο των Π.Σ., με στόχο κυρίως τη μελέτη του ρόλου της τεχνολογίας στους οργανισμούς και τις δομές τους ή τη μελέτη φαινομένων στα οποία εμπλέκεται η τεχνολογία και επηρεάζει την ανθρώπινη δράση. Η εφαρμογή της θεωρίας της δομοποίησης επιτρέπει να μελετηθούν οι ενέργειες των εμπλεκομένων μέσα στο πλαίσιο στο οποίο συμβαίνουν και να ερμηνευθεί η αλλαγή στα πλαίσια μίας οργάνωσης. Η *θεωρία του συγκειμενισμού* επιτρέπει την ανίχνευση της δυναμικής αλληλεπίδρασης των διαδικασιών αλλαγής και του εσωτερικού και εξωτερικού πλαισίου αναφοράς (συγκείμενο) με το περιεχόμενο της αλλαγής. Με αυτό τον τρόπο επιτρέπει την επεξήγηση του τρόπου με τον οποίο διαμορφώνεται το περιεχόμενο των αλλαγών από τις διαδικασίες αλλαγής λαμβάνοντας υπόψη τις συνθήκες του συγκεκριμένου περιβάλλοντος. Η *θεωρία δικτύων σύμπραξης* διερευνά τον τρόπο με τον οποίο οι άνθρωποι και τα τεχνουργήματα συνθέτουν ένα κοινωνικο-τεχνικό δίκτυο, μέσα από τη δράση ενός εστιακού δρώντος (focal actor). Επομένως, αναδεικνύει τον τρόπο με τον οποίο ανθρώπινα και μη ανθρώπινα στοιχεία συνεργάζονται και ενώνονται, διαμορφώνοντας ένα δίκτυο σύμπραξης. Η θεωρία δικτύων σύμπραξης, λοιπόν, παρέχει τη δυνατότητα ανάλυσης και ερμηνείας της διαδικασίας αλλαγής στο πλαίσιο μίας οργάνωσης ως μία διαδικασία διαπραγματεύσεων μεταξύ των συμμετεχόντων λαμβάνοντας υπόψη τις αντιλήψεις τους, τα συμφέροντά τους και το ρόλο που κατέχει στις διαπραγματεύσεις αυτές η τεχνολογία. Παράλληλα, η χρήση της *απαιτούμενης διαδικασίας* (due process) δίνει τη δυνατότητα παρακολούθησης της δυναμικής διαμόρφωσης του δικτύου αναδεικνύοντας τα κρίσιμα γεγονότα και οι οπτικές των συμμετεχόντων που καθορίζουν τη διαμόρφωση του δικτύου εστιάζοντας σε μεγαλύτερο βαθμό ανάλυσης.

Στα πλαίσια της διατριβής, λοιπόν, αναπτύσσεται *εννοιολογικό και μεθοδολογικό πλαίσιο* για την κατανόηση του τρόπου με τον οποίο διαμορφώνονται και ενσωματώνονται οι δράσεις ενημερότητας ασφάλειας Π.Σ. στις οργανώσεις. Η εφαρμογή του πλαισίου αυτού στην εμπειρική έρευνα οδήγησε σε τεκμηριωμένα συμπεράσματα που απευθύνονται τόσο στους ερευνητές, όσο και ειδικούς του χώρου της ασφάλειας των Π.Σ. Η *συμβολή* της έρευνας έχει θεωρητική, μεθοδολογική και πρακτική διάσταση:

- ✓ Σε *θεωρητικό επίπεδο*, τα συμπεράσματα της έρευνας επισημαίνουν την καταλληλότητα της θεωρίας δικτύων σύμπραξης για τη δυναμική παρακολούθηση της διαμόρφωσης της ενημερότητας ασφάλειας Π.Σ. και τον κρίσιμο ρόλο των ικανοτήτων και δεξιοτήτων του εστιακού δρώντα να ‘ευθυγραμμίσει’ τα συμφέροντα των δυνητικών συμμάχων με τα

συμφέροντα του δικτύου. Ο συνδυασμός της θεωρίας δικτύων σύμπραξης με τη θεωρία δομοποίησης συνεισφέρει στην κατανόηση του τρόπου με τον οποίο ένας δρων που δραστηριοποιείται στο μικρο-επίπεδο μπορεί να συνεισφέρει στη δημιουργία ενός νέου δικτύου σύμπραξης σε υψηλότερο επίπεδο, ενώ η θεωρία του συγκειμενισμού μπορεί να συντελέσει στην κατανόηση των συνθηκών του ευρύτερου πλαισίου που επιδρούν στη διαμόρφωση των δικτύων σύμπραξης σε μικρο-επίπεδο και μακρο-επίπεδο.

- ✓ Σε *πρακτικό επίπεδο*, το εννοιολογικό και μεθοδολογικό πλαίσιο της διατριβής μπορεί να αξιοποιηθεί ως πλαίσιο αναφοράς από ειδικούς ασφάλειας Π.Σ. που σχεδιάζουν να αναπτύξουν πρωτοβουλίες ενημερότητας, ώστε να εντοπίσουν 'κρίσιμα' γεγονότα κατά τη διαρκή διαμόρφωση του δικτύου σύμπραξης καθώς και τα σημεία όπου το δίκτυο μπορεί να αποσταθεροποιηθεί και για ποιες αιτίες. Ακόμη, πληροφορεί τους ειδικούς ασφάλειας Π.Σ. αναφορικά με τις πρόσθετες δεξιότητες που αναδεικνύεται ότι απαιτούνται για την αποτελεσματική διαχείριση μίας τέτοιας δραστηριότητας, όπως επικοινωνιακές, διαπραγματευτικές και διοικητικές δεξιότητες. Τέλος, επισημαίνεται η μη ουδετερότητα των τεχνουργημάτων αναφορικά με την επιρροή τους σε τέτοιες πρωτοβουλίες.
- ✓ Σε *μεθοδολογικό επίπεδο*, αρχικά οι ερευνητές χώρου της ασφάλειας, αλλά και των Π.Σ. γενικότερα, μπορούν να επωφεληθούν από την εφαρμογή της τυπολογίας μοντέλων έρευνας, κατά το σχεδιασμό της έρευνάς τους. Ακόμη, τα συμπεράσματα της έρευνας αναδεικνύουν τη συμβατότητα και συμπληρωματικότητα των τριών θεωριών για την κατανόηση και ανάλυση της ενημερότητας ασφάλειας Π.Σ.

Β.2 ΕΡΕΥΝΗΤΙΚΕΣ ΕΡΓΑΣΙΕΣ ΔΗΜΟΣΙΕΥΜΕΝΕΣ ΣΕ ΔΙΕΘΝΗ ΕΠΙΣΤΗΜΟΝΙΚΑ ΠΕΡΙΟΔΙΚΑ

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

Η εργασία σκοπεύει να αναδείξει τις τεχνικές οπτικοποίησης ως μέσο για την παρουσίαση των πολιτικών ιδιωτικότητας έναντι των παραδοσιακών τεχνικών, καθώς επίσης να εξετάσει την επίδραση τέτοιων τεχνικών οπτικοποίησης στην ενημερότητα των χρηστών για την ιδιωτικότητα. Για την διεξαγωγή των συμπερασμάτων επιλέχθηκε ως μελέτη περίπτωσης το μέσο κοινωνικής δικτύωσης Instagram και πραγματοποιήθηκαν δύο εμπειρικές έρευνες, κάθε μία από τις οποίες περιλαμβάνει τρεις παρεμβάσεις. Ακολούθως, η κάθε παρέμβαση παρουσιάζει διαφορετική τεχνική οπτικοποίησης της πολιτικής ιδιωτικότητας στους χρήστες, δηλαδή την παραδοσιακή πολιτική και τις δύο οπτικοποιημένες πολιτικές ιδιωτικότητας που δημιουργήσαμε. Μέσω της χρήσης ενός πριν - και ενός μετά- ερωτηματολογίου, μελετήσαμε την επίδραση που είχε η κάθε τεχνική παρουσίασης στην ενημερότητα των χρηστών για την ιδιωτικότητα. Τα ευρήματα της έρευνας παρέχουν ισχυρές ενδείξεις πως οι οπτικοποιημένες πολιτικές ιδιωτικότητας οδηγούν σε υψηλότερο επίπεδο

ενημερότητας των χρηστών έναντι των παραδοσιακών τεχνικών, ειδικά όταν περιλαμβάνονται εικόνες. Οι ερευνητές παρουσιάζουν δύο νέες τεχνικές οπτικοποίησης, οι οποίες μπορούν να προσφέρουν σημαντικές πληροφορίες και κατευθύνσεις σχετικά με τον σχεδιασμό πιο ελκυστικών πολιτικών ιδιωτικότητας. Ωστόσο, ένας από τους βασικούς περιορισμούς της έρευνας είναι το μέγεθος του δείγματος, το οποίο όμως είναι ικανοποιητικό ώστε να οδηγήσει σε αξιόπιστα συμπεράσματα. Τα αποτελέσματα και η μεθοδολογία της έρευνας θα μπορούσαν να λειτουργήσουν ως πρακτικός οδηγός για την οπτικοποίηση μιας πολιτικής ιδιωτικότητας, καθώς οι συγγραφείς παρέχουν συστηματικά και συγκεκριμένα βήματα προς αυτή την κατεύθυνση. Το άρθρο αφενός εξετάζει την αξία της οπτικοποίησης μιας πολιτικής ιδιωτικότητας ως νέα προσέγγιση για την αύξηση της ενημερότητας των χρηστών σχετικά με την προστασία της ιδιωτικότητάς τους και αφετέρου εφαρμόζει δύο νέες τεχνικές απεικόνισης για τον σκοπό αυτό. Ως εκ τούτου, τα ευρήματα της έρευνας μπορούν να αποδειχθούν χρήσιμα τόσο για τους ερευνητές και τους σχεδιαστές τέτοιων πολιτικών, όσο και για την παρακίνηση των ίδιων των χρηστών, ώστε να είναι πιο προσεκτικοί αναφορικά με την ιδιωτικότητάς τους.

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.

Οι σύγχρονες υπηρεσίες στηρίζονται σε κρίσιμο βαθμό στις τεχνολογίες πληροφορικής. Η παροχή υπηρεσιών μπορείς να στηρίζεται σε πολύπλοκα σχήματα τεχνολογιών πληροφορικής και παρόχων τηλεπικοινωνιών, διεθνή δίκτυα αλλά και συσκευές πληροφορικής των πελατών. Αυτή η έρευνα εστιάζει στις αστοχίες παροχής υπηρεσιών που οφείλονται σε προβλήματα των τεχνολογιών πληροφορικής, τις οποίες ονομάζουμε υποβάθμιση υπηρεσιών λόγω προβλημάτων τεχνολογίας (ΥΥΤΠ). Όταν συμβαίνει ΥΥΤΠ σε μία σύγχρονη υπηρεσία, τα προβλήματα τεχνολογίας μπορεί να οφείλονται στον παρόχο της υπηρεσίας, ένα συνεργάτη του ή οποιοδήποτε άλλο εξοπλισμό πληροφορικής αποτελεί κομμάτι της παροχής υπηρεσίας. Για τον πελάτη όμως δεν είναι εφικτό να αναγνωρίσει την πηγή του υποβιβασμού άμεσα. Σε αυτή την έρευνα ισχυριζόμαστε ότι η υπάρχουσα βιβλιογραφία μπορεί να επεξηγήσει τη συμπεριφορά των πελατών κατά την παρουσία ΥΥΤΠ μόνο εν μέρει. Η βιβλιογραφία δε μπορεί να εξηγήσει τον τρόπο που οι τεχνολογικοί παράγοντες επιδρούν στη συμπεριφορά του πελάτη κατά τη διαδικασία που αποφασίζει αν θα συνεχίσει να χρησιμοποιεί την υπηρεσία ή θα τη διακόψει. Για να αντιμετωπίσουμε αυτό το ερευνητικό κενό πραγματοποιήσαμε μία εμπειρική έρευνα με πελάτες υπηρεσιών που στηρίζονται σε τεχνολογίες πληροφορικής. Τα ευρήματα δείχνουν ότι οι αιτίες που επιδρούν στη συμπεριφορά των πελατών αλλάζουν κατά τη διάρκεια της εμπειρίας ΥΥΤΠ. Δημιουργήσαμε μία θεωρία επεξήγησης της συμπεριφοράς των πελατών που περιλαμβάνει πέντε στάδια: κατηγορίας, παράκαμψης,

ανεκτικότητας, παραίτησης και υπέρβασης. Τα δύο πρώτα στάδια περιλαμβάνουν παράγοντες που αφορούν μόνο τα συγκεκριμένα στάδια και αφορούν την εξέλιξη της χρήσης της υπηρεσίας, ενώ τα τρία τελευταία στάδια περιλαμβάνουν παράγοντες που επιδρούν στην συνέχιση ή τη διακοπή χρήσης. Ως νέα συμβολή, προτείνουμε μια θεωρία σταδίων για να εξηγήσουμε τη συμπεριφορά των πελατών μετά από ΥΥΤΠ. Τα αποτελέσματά μας περιγράφουν νέες ερευνητικές κατευθύνσεις στην ΥΥΤΠ, συμπεριλαμβανομένης της περαιτέρω βελτίωσης και επικύρωσης της προτεινόμενης θεωρίας. Για τους παρόχους υπηρεσιών, τα ευρήματά μας παρέχουν νέες πληροφορίες για τη βελτίωση των στρατηγικών ανάκτησης υπηρεσιών για να διατηρήσουν την εμπιστοσύνη των πελατών.

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

Το παρόν άρθρο παρουσιάζει ένα Κοινό Σύνολο Γνώσης (ΚΣΓ) για τον τομέα της πληροφοριακής ιδιωτικότητας, που ονομάζεται InfoPrivacy CBK. Ο σκοπός του προτεινόμενου ΚΣΓ είναι να καθοδηγήσει τους χρήστες του Διαδικτύου, ώστε να κατανοήσουν καλύτερα την έννοια της πληροφοριακής ιδιωτικότητας και των σχετικών εννοιών. Το InfoPrivacy CBK δημιουργήθηκε με εκπαιδευτικό προσανατολισμό, με στόχο να παρέχει τη βάση για το σχεδιασμό προγραμμάτων ενημερότητας και κατάρτισης σε θέματα ιδιωτικότητας και την οργάνωση σχετικού εκπαιδευτικού υλικού. Το προτεινόμενο ΚΣΓ για την πληροφοριακή ιδιωτικότητα αναπτύχθηκε εννοιολογικά και περιλαμβάνει πέντε τομείς και τέσσερα επίπεδα ανάλυσης. Απεικονίζεται με τη βοήθεια εννοιολογικών χαρτών. Οι συγγραφείς προσδιόρισαν μια ποικιλία εννοιών που σχετίζονται με την πληροφοριακή ιδιωτικότητα και δημιούργησαν ένα σύνολο κατηγοριών για την κατηγοριοποίησή τους. Χρησιμοποίησαν ως κριτήρια ένταξης τόσο θεωρητικές όσο και πρακτικές πτυχές της πληροφοριακής ιδιωτικότητας, έτσι ώστε το ΚΣΓ που αναπτύχθηκε να μπορεί να αντιμετωπίσει τις προκλήσεις των σύγχρονων τεχνολογιών για την προστασία της ιδιωτικότητας των πληροφοριών. Για την αξιολόγηση και τη βελτιστοποίηση του εννοιολογικά ανεπτυγμένου ΚΣΓ, οι συγγραφείς διενήργησαν μια εμπειρική έρευνα, στην οποία συμμετείχαν επτά ειδικοί της πληροφοριακής ιδιωτικότητας. Οι ειδικοί αξιολόγησαν σε μεγάλο βαθμό θετικά τόσο τη δομή όσο και το περιεχόμενο του InfoPrivacy CBK, καθώς και τον βαθμό στον οποίο επιτυγχάνει τους επιδιωκόμενους εκπαιδευτικούς του στόχους. Το προτεινόμενο InfoPrivacy CBK αξιολογήθηκε από έναν περιορισμένο αριθμό ειδικών της πληροφοριακής ιδιωτικότητας, κυρίως λόγω της εκτενούς και εις βάθος συμμετοχής που απαιτήθηκε. Το InfoPrivacy CBK μπορεί να χρησιμοποιηθεί κυρίως από τους υπεύθυνους ανάπτυξης προγραμμάτων για την πληροφοριακή ενημερότητα και την κατάρτιση, όπως για παράδειγμα από οργανισμούς, υπεύθυνους προστασίας δεδομένων, την πολιτεία, υπεύθυνους χάραξης εκπαιδευτικής πολιτικής και εκπαιδευτικούς. Οι χρήστες του Διαδικτύου θα επωφεληθούν από το InfoPrivacy CBK με την απόκτηση γνώσεων και δεξιοτήτων από θεωρητικά τεκμηριωμένα

προγράμματα κατάρτισης, τα οποία μπορούν να ενισχύσουν την ενημερότητα και την κριτική τους σκέψη σε θέματα που σχετίζονται με την προστασία της πληροφοριακής τους ιδιωτικότητας. Αυτό θα οδηγήσει σε περισσότερο ενήμερες για την ιδιωτικότητα διαδικτυακές κοινωνίες, κοινότητες, δίκτυα κ.λπ. Η εργασία αποσκοπεί στη γεφύρωση του υπάρχοντος χάσματος στη βιβλιογραφία μέσω της δημιουργίας ενός νέου ΚΣΓ για την πληροφοριακή ιδιωτικότητα, σε έναν τομέα στον οποίο δεν έχει καταγραφεί ανάλογη ερευνητική προσπάθεια. Το παρόν έγγραφο προσφέρει σημαντικές γνώσεις στον τομέα της προστασίας της ιδιωτικότητας των πληροφοριών, οι οποίες θα μπορούσαν να φανούν χρήσιμες τόσο στους σχεδιαστές τεχνολογικής εκπαίδευσης όσο και στους εκπαιδευόμενους (μαθητές, φοιτητές, εργαζόμενους κ.λπ.).

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.

Οι πολιτικές ιδιωτικότητας έχουν αναδυθεί ως ο κύριος μηχανισμός για την ενημέρωση των χρηστών σχετικά με τον τρόπο που οι πάροχοι ηλεκτρονικών υπηρεσιών διαχειρίζονται τα προσωπικά τους δεδομένα. Η βιβλιογραφία αναφέρει ότι οι χρήστες συναντούν δυσκολίες στην κατανόηση των πολιτικών ιδιωτικότητας επειδή συνήθως εμπεριέχουν τεχνική ή νομική ορολογία. Αυτές οι δυσκολίες έχουν οδηγήσει τους περισσότερους χρήστες στην μη ανάγνωση των πολιτικών ιδιωτικότητας και την «τυφλή» αποδοχή των σχετικών όρων. Σε μία προσπάθεια υπέρβασης του ανωτέρω προβλήματος, το παρόν άρθρο παρουσιάζει το AppAware, μία πλατφόρμα που σκοπεύει στη βελτίωση της παρουσίασης των πολιτικών ιδιωτικότητας εφαρμογών κινητών συσκευών μέσω οπτικοποίησης. Το AppAware μορφοποιεί μία οπτικοποιημένη αναφορά που παρουσιάζει τις άδειες που παραχωρούνται σε μία εφαρμογή κινητής συσκευής, η οποία αναφορά είναι ευανάγνωστη στον απλό (μη τεχνικό) χρήστη. Το AppAware σκοπεύει να αντιμετωπίσει τη δυσκολία που έχουν οι χρήστες να κατανοήσουν τις πολιτικές ιδιωτικότητας και τις άδειες που παραχωρούν κατά την αποδοχή των όρων. Προτείνουμε επίσης τον AppAware parser ως επιπρόσθετο χαρακτηριστικό (add-on) που συμπληρώνει την πλατφόρμα AppAware και βοηθάει τους χρήστες να παρακολουθούν τις εφαρμογές που έχουν εγκαταστήσει στην κινητή συσκευή τους. Για την επικύρωση του AppAware σχεδιάσαμε και υλοποιήσαμε μία εμπειρική έρευνα με δημοσκόπηση ώστε να αξιολογήσουμε την ευκολία εγκατάστασης, τη χρηστικότητας και τη βιωσιμότητα του AppAware. Τα αποτελέσματα δείχνουν ότι το AppAware αξιολογήθηκε ως άνω του μετρίου από τους χρήστες σε όλες τις κατηγορίες αξιολόγησης. Η εργασία αυτή είναι η πρώτη που παρουσιάζει λογισμικό για την οπτικοποίηση των πολιτικών ιδιωτικότητας βασιζόμενη στις πραγματικές άδειες που παραχωρούνται έπειτα από τη συναίνεση του χρήστη.

J. 18 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

Ο θετικισμός έχει καθιερωθεί ως πρότυπη προσέγγιση για την επιστημονική έρευνα. Σύμφωνα με τον θετικισμό στα πληροφοριακά συστήματα (ΠΣ), η επιστημονική έρευνα πρέπει: 1) να είναι γενικεύσιμη 2) να περιλαμβάνει σταθερές ανεξάρτητες μεταβλητές, 3) να περιλαμβάνει οντολογικές υποθέσεις, και 4) να αξιοποιεί ποσοτική έρευνα έναντι της ποιοτικής. Υποστηρίζουμε ότι οι φιλόσοφοι που θεμελίωσαν το θετικισμό δεν απαιτούσαν τίποτε από αυτά. Αντίθετα, οι φιλόσοφοι που θεμελίωσαν το θετικισμό θεωρούσαν γενικότερα τις φιλοσοφικές και οντολογικές θεωρήσεις ως ανοησίες. Επιπλέον, η προτιμώμενη μέθοδος εμπειρικής έρευνας των θετικιστών δεν ήταν η δημοσκόπηση, αλλά η ποιοτική παρατήρηση με σημειώσεις πεδίου. Επιπλέον, οι θετικιστές φιλόσοφοι ούτε απαιτούσαν στατιστική ούτε μη στατιστική γενικευσιμότητα. Πολλοί θετικιστές φιλόσοφοι αναγνώρισαν επίσης τη μελέτη των μοναδικών περιπτώσεων ως επιστημονική έρευνα.

Πολλοί ερευνητικοί προσανατολισμοί που θεωρούνται ως μη επιστημονικοί στο πεδίο των ΠΣ φαίνονται (κατ 'αρχήν) «επιστημονικοί» σύμφωνα με τον θετικισμό. Αυτά που έχουν καταγραφεί στο χώρο των ΠΣ ως τεκμήρια επιστημονικότητας βάσει του θετικισμού (π.χ. στατιστική ή μη στατιστική γενικευσιμότητα, δημοσκοπήσεις, εστίαση σε σταθερές, οντολογικές απόψεις) είτε δεν απαιτούνταν από θετικιστές είτε θεωρήθηκαν ανόητα από αυτούς. Επιπλέον, δεδομένου ότι ο θετικισμός συνδέεται μερικές φορές (ή συγχέεται) με το λογικό εμπειρισμό στα ΠΣ, στο άρθρο αυτό αναλύομε εν συντομία και τον λογικό εμπειρισμό. Τέλος, αναδεικνύουμε τη σημαντικότητα να κατανοήσουμε ότι κάποιες υποθέσεις για το θετικισμό έχουν θεωρηθεί δεδομένες και είχαν τεράστια επιρροή στο πεδίο. Αυτές οι υποθέσεις όμως ενδέχεται τελικά να είναι μη επιθυμητές καθώς δεν έχουν τη ρίζα τους στο θετικισμό και είναι αδικαιολόγητες, γεγονός που θα μπορούσε να επιφέρει πρωτοποριακές επιπτώσεις για τη μελλοντική έρευνα στα ΠΣ.

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

Οι οργανισμοί χρησιμοποιούν πολιτικές ασφάλειας ώστε να γνωστοποιούν στους χρήστες

πληροφοριακών συστημάτων τους κανόνες ορθής χρήσης αυτών. Οι έρευνες δείχνουν ότι η συμμόρφωση των χρηστών με τις πολιτικές ιδιωτικότητας δεν είναι αυτονόητη και ότι πολλοί παράμετροι επηρεάζουν τη σχετική συμπεριφορά των χρηστών, όπως η ενημερότητα ασφάλειας και η ατομική αντίληψη απειλών ασφάλειας. Ο σκοπός αυτής της έρευνας είναι να διερευνήσει τις δεξιότητες που απαιτούν από τους χρήστες προκειμένου να συμμορφώνονται με τις πολιτικές ασφάλειας. Προκειμένου να ανακαλύψουμε αυτές τις δεξιότητες πραγματοποιήσαμε μία συστηματική μελέτη της βιβλιογραφίας που αποκαλύπτει ποιοι παράγοντες επιδρούν στη συμπεριφορά συμμόρφωσης των χρηστών με τις πολιτικές ασφάλειας και αναπτύξαμε ένα μοντέλο δεξιοτήτων. Στη συνέχεια, επιδιώξαμε να μελετήσουμε αν οι χρήστες πληροφοριακών συστημάτων στους σύγχρονους οργανισμούς διαφορετικών τομέων της βιομηχανίας έχουν αυτές τις δεξιότητες. Για να το κάνουμε αυτό αναλύσαμε μοντέλα δεξιοτήτων για τους τομείς αυτούς και παρέχουμε αποδείξεις ότι οι δεξιότητες συμμόρφωσης με τις πολιτικές ασφάλειας δεν εμπεριέχονται στις απαραίτητες δεξιότητες των υπαλλήλων. Η έρευνα στη συμμόρφωση με τις πολιτικές ασφάλειας έχει εστιάσει στην αναγνώριση των παραγόντων που επιδρούν στη συμπεριφορά των χρηστών. Η παρούσα έρευνα παρέχει ένα μοντέλο δεξιοτήτων και κατευθύνει τους ερευνητές να εστιάσουν όχι μόνο στους παράγοντες που επιδρούν στη συμπεριφορά των χρηστών αλλά και στις σχετικές απαραίτητες δεξιότητες. Η έρευνα παρέχει συνεισφορά και για τους επαγγελματίες παρέχοντας κατευθύνσεις για τη βελτίωση των μοντέλων δεξιοτήτων, αλλά και τη βελτίωση των προγραμμάτων ενημερότητας ασφάλειας.

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

Η συμμετοχή των πολιτών σε δημόσια ζητήματα αποτελεί ένα από τα σημαντικότερα καθήκοντα για διαδικασίες χάραξης πολιτικής αλλά οι δημόσιες αρχές στερούνται ιδέες για το σχεδιασμό διαδικασιών που ενισχύουν και διευκολύνουν την ενεργό συμμετοχή των πολιτών. Με βάση τη θεωρία της πειθούς, το παρόν άρθρο εξετάζει εάν τα θέματα πολιτικής που έχουν ενσωματωμένα χαρακτηριστικά πειθούς προσελκύουν περισσότερο την προσοχή των πολιτών, ενεργοποιούν μεγαλύτερο χρόνο επεξεργασίας και μεγαλύτερη συμμετοχή. Ιδιαίτερα η ευθυγράμμιση με προτιμήσεις, η ευθυγράμμιση με την τρέχουσα τοποθεσία, η κοινωνική αποδοχή και η εξουσία αναγνωρίζονται ως χαρακτηριστικά πειθούς στο πλαίσιο της ηλεκτρονικής συμμετοχής των πολιτών. Σε αυτή την έρευνα αναπτύσσεται ένα καινοτόμο εργαλείο λογισμικού κινητής συμμετοχής για να δοκιμάσει τις προτάσεις που ενσωματώνουν πειθώ και δοκιμάζεται από 80 συμμετέχοντες στο Ηνωμένο Βασίλειο και την Τουρκία. Τα ευρήματα δείχνουν ότι το μείγμα των χαρακτηριστικών είναι πιο αποτελεσματικό στην ενίσχυση της συμμετοχής, ενώ η ενσωμάτωση ενός χαρακτηριστικού έχει

περιορισμούς. Η μελέτη αυτή υποστηρίζει επίσης ότι ο σχεδιασμός των εργαλείων ηλεκτρονικής συμμετοχής πρέπει να εξετάσει τις ψυχολογικές πτυχές των πολιτών για να παρακινήσει τη συμμετοχή τους.

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*

Οι άνθρωποι χρησιμοποιούν κινητές συσκευές για διάφορους σκοπούς και δυνατότητες, όπως να ελέγχουν τον τοπικό καιρό, την οδική κυκλοφορία, τις εξατομικευμένες τοπικές ειδήσεις, το εξατομικευμένο αγαπημένο κοινωνικό τους δίκτυο κλπ. Ταυτόχρονα, οι προγραμματιστές εφαρμογών αναπτύσσουν εφαρμογές κινητής τηλεφωνίας που συλλέγουν τεράστιες ποσότητες προσωπικών πληροφοριών για τους χρήστες κινητής τηλεφωνίας, όπως ηλικία, τοποθεσία ή συγκεκριμένα αναγνωριστικά τηλεφώνου. Πολλές μελέτες καταδεικνύουν ότι οι εφαρμογές κινητής τηλεφωνίας συλλέγουν πολύτιμες πληροφορίες σχετικά με τους χρήστες και τις χρησιμοποιούν για τη δημιουργία προφίλ των χρηστών για δικούς τους σκοπούς ή για την πώληση αυτών των πληροφοριών για εμπορικά συμφέροντα. Ως εκ τούτου, το θέμα της συναίνεσης για την επεξεργασία προσωπικών πληροφοριών γίνεται όλο και πιο ενδιαφέρον για ερευνητές, νομικούς εμπειρογνώμονες και επαγγελματίες. Στην παρούσα εργασία εξετάζουμε το ζήτημα της έγκυρης συναίνεσης για την παρακολούθηση τοποθεσίας από χρήστες κινητών τηλεφώνων. Αρχικά αναλύουμε τη νομική βάση για την εγκαθίδρυση ενήμερης συγκατάθεσης που αντιπροσωπεύουν προδιαγραφές λογισμικού για προγραμματιστές και παρόχους κινητών εφαρμογών που ζητούν συγκατάθεση. Ωστόσο, αυτοί που πράγματι δίνουν τη συγκατάθεσή τους είναι οι χρήστες κινητών συσκευών και επομένως η κατανόηση της συγκατάθεσής τους είναι υψίστης σημασίας. Η βιβλιογραφία παρουσιάζει έλλειψη σε εμπειρικές μελέτες που εξετάζουν το θέμα από την άποψη της αντίληψης των χρηστών. Για το λόγο αυτό, η παρούσα έρευνα διενεργεί μια εμπειρική έρευνα με χρήστες κινητών εφαρμογών και παρουσιάζει τα ευρήματα με τη μορφή μιας θεωρίας διεργασίας. Η θεωρία διεργασίας αποκαλύπτει πώς μπορεί να αποκτηθεί έγκυρη συναίνεση των χρηστών για την παρακολούθηση της τοποθεσίας τους, ξεκινώντας από την ενίσχυση της ανάγνωσης της πολιτικής ιδιωτικότητας για την ενίσχυση της ευαισθητοποίησης της ιδιωτικότητας και την παροχή έγκυρης συναίνεσης. Το άρθρο περιλαμβάνει συζήτηση των επιπτώσεων της θεωρίας διεργασίας για τους διάφορους ενδιαφερόμενους και παρέχει συστάσεις που προκύπτουν από τα εμπειρικά ευρήματα. Η συμβολή της εργασίας απευθύνεται σε προγραμματιστές και παρόχους λογισμικού και κινητών εφαρμογών, ερευνητές τεχνολογικής ρύθμισης και φορείς χάραξης πολιτικής, καθώς και ερευνητές στον τομέα της ασφάλειας και της

ιδιωτικότητας.

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*

Τα πρότυπα και οι βέλτιστες πρακτικές που υπάρχουν για την καθοδήγηση στο σχεδιασμό και την υλοποίηση προγραμμάτων ενημερότητας ασφάλειας πληροφοριών εστιάζουν στο ποιο θα πρέπει να είναι το περιεχόμενο αυτών των προγραμμάτων, χωρίς να λαμβάνουν υπόψη τον τρόπο με τον οποίο τα άτομα λαμβάνουν και επεξεργάζονται αυτό το περιεχόμενο και πώς το αξιοποιούν για την καθημερινή λήψη των αποφάσεών τους στον εργασιακό χώρο. Η πρόσφατη βιβλιογραφία παρόλα αυτά έχει αποδείξει ότι η τελική συμμόρφωση των χρηστών στις πολιτικές ασφάλειας επηρεάζεται από τις αντιλήψεις του ατόμου για την επικινδυνότητα, τις πεποιθήσεις του και τις προδιαθέσεις του. Επομένως τα προγράμματα ενημερότητας θα πρέπει να ευθυγραμμιστούν με αυτούς τους παράγοντες που καθορίζουν τον τρόπο με τον οποίο οι χρήστες ενστερνίζονται τα μηνύματα ασφάλειας πληροφοριών που μεταδίδονται. Η εργασία αυτή μελετά το ρόλο των γνωστικών (cognitive) και πολιτισμικών (cultural) προδιαθέσεων στη διαμόρφωση των αντιλήψεων επικινδυνότητας και των συμπεριφορών σε σχέση με την ασφάλεια. Η εργασία αξιοποιεί βιβλιογραφία από διαφορετικά πεδία, όπως οικονομικά της συμπεριφοράς (behavioural economics) και προσωπική ασφάλεια (safety) προκειμένου να αναπτύξει ένα εννοιολογικό πλαίσιο για την ανάλυση του ρόλου των γνωστικών και πολιτισμικών προδιαθέσεων του ατόμου στην ασφάλεια πληροφοριών. Στο πλαίσιο της εργασίας αναλύονται οι επιπτώσεις αυτών των προδιαθέσεων για τα προγράμματα ενημερότητας και τελικά παρέχουμε ένα σύνολο από συστάσεις προς τους αρμόδιους σχεδιασμού και υλοποίησης προγραμμάτων ενημερότητας της ασφάλειας. Η εργασία αναδεικνύει νέες οδούς για την έρευνα στο πεδίο της ενημερότητας ασφάλειας και των αποφάσεων ασφάλειας πληροφοριών, ενώ προτείνει πρακτικές συστάσεις για την υλοποίηση προγραμμάτων ενημερότητας αξιοποιώντας το ρόλο των προδιαθέσεων στη διαμόρφωση των αντιλήψεων επικινδυνότητας και των συμπεριφορών των χρηστών σε σχέση με την ασφάλεια.

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

Η βιβλιογραφία που αφορά στην υιοθέτηση λογισμικού ανοικτού κώδικά είναι περιορισμένη και δεν παρέχει επεξηγήσεις για τον τρόπο με τον οποίο υιοθετούνται από τους καταναλωτές, στην περίπτωση που υπάρχει διαθέσιμο εμπορικό λογισμικό που υπερέχει λειτουργικά. Η εργασία αποσκοπεί στην αποκάλυψη της διαδικασίας με την οποία διαμορφώνεται η ικανοποίηση του καταναλωτή από λογισμικό ανοικτού κώδικα σε σχέση με το εμπορικό λογισμικό. Υιοθετούμε τη θεωρία διάψευσης προσδοκιών (Expectation Disconfirmation Theory) ενσωματώνοντας παράγοντες κόστους, φήμης και προσωπικής εμπειρίας. Το μοντέλο που σχεδιάστηκε στην εργασία επικυρώνεται με εμπειρικά δεδομένα από έρευνα πεδίου στην Κορέα μεταξύ ενός συστήματος διαχείρισης βάσεων δεδομένων ανοικτού κώδικα και αντίστοιχου συστήματος στην αγορά που υπερέχει λειτουργικά. Η θεωρητική συνεισφορά της εργασίας συνίσταται στην εφαρμογή της θεωρίας διάψευσης προσδοκιών για τη σύγκριση της υιοθέτησης των δύο συστημάτων. Επιπλέον, η εργασία ενσωματώνει παράγοντες σχετικούς με τις προσδοκίες των καταναλωτών, το οποίο είχε αναγνωριστεί στη βιβλιογραφία ως ερευνητικό κενό. Η πρακτική συνεισφορά της εργασίας συμπεριλαμβάνει την αναγνώριση των διαφορών ανάμεσα στις προσδοκίες των χρηστών από λογισμικό ανοικτού κώδικα και εμπορικό λογισμικό. Τέλος η εργασία παρέχει επεξηγήσεις για τον τρόπο με τον οποίο οι αρχικές προσδοκίες των καταναλωτών συνδυάζονται με την προσωπική τους εμπειρία από τη χρήση του λογισμικού προς τη διαμόρφωση του βαθμού ικανοποίησής τους.

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*

Η βιβλιογραφία περιλαμβάνει διάφορες εργασίες που διερευνούν το ζήτημα της ενημερότητας ασφάλειας πληροφοριών εστιάζοντας στο ατομικό ή/και το οργανωσιακό επίπεδο. Σε αυτή την εργασία ισχυριζόμαστε ότι οι διαδικασίες της ενημερότητας ασφάλειας πληροφοριών συσχετίζονται με αλληλεξαρτώμενες αλλαγές που συμβαίνουν τόσο στο ατομικό και το οργανωσιακό αλλά και το τεχνολογικό επίπεδο. Προτείνουμε ένα ολοκληρωμένο θεωρητικό πλαίσιο ανάλυσης το οποίο αναπτύχθηκε με χρήση έρευνας παρεμβάσεων (action research) σε ένα δημόσιο οργανισμό. Το πλαίσιο ενσωματώνει τη θεωρία δικτύων σύμπραξης, τη θεωρία δομοποίησης και τη θεωρία του συγκειμενισμού.

Στην εργασία αναπτύσσουμε και εφαρμόζουμε το πλαίσιο για την υλοποίηση ενός προγράμματος ενημερότητας ασφάλειας πληροφοριών και τη διαχείριση των αλλαγών που προκύπτουν στον φορέα οργανισμό. Η εργασία αναδεικνύει τις ελλείψεις που έχει η κάθε μία θεωρία εάν εφαρμοστεί μόνη της για την ανάλυση αλλαγών σε πολλαπλά επίπεδα (multi-level changes), ενώ καταδεικνύει τη συνέργεια που προκύπτει από το συνδυασμό τους. Η εργασία προτείνει πώς το πλαίσιο μπορεί να εφαρμοστεί για την μελέτη και ανάλυση αλλαγών που σχετίζονται με την ενημερότητα ασφάλειας πληροφοριών και προκύπτουν σε ατομικό, οργανωσιακό και τεχνολογικό επίπεδο.

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.*

Οι καινοτόμες τεχνολογίες, όπως η νεφοϋπολογιστική, φέρουν τη δυνατότητα να συνεισφέρουν στην παροχή υπηρεσιών ηλεκτρονικής διακυβέρνησης, μέσα από ευέλικτα και επεκτάσιμα συστήματα. Επιπλέον, μπορούν να ενισχύσουν την μείωση κόστους και να μειώσουν την κατάτμηση των δημόσιων πληροφοριών. Παρόλα αυτά, όταν οι δημόσιες υπηρεσίες αξιοποιούν αυτές τις τεχνολογίες αντιμετωπίζουν σημαντικά προβλήματα που σχετίζονται με τις συνοδευόμενες τεχνικές και οργανωσιακές αλλαγές, καθώς και άλλες προκλήσεις. Ο σκοπός αυτής της εργασίας είναι να αναγνωρίσει και να αναλύσει αυτές τις προκλήσεις και να συζητήσει προτεινόμενες λύσεις. Ακολουθήσαμε μία διεπιστημονική προσέγγιση, συμπεριλαμβάνοντας κοινωνικά, συμπεριφορικά, επιχειρησιακά και τεχνικά στοιχεία, και βιβλιογραφική ανάλυση των προκλήσεων. Πραγματοποιήσαμε συνεντεύξεις ομάδων εργασιών (focus group interviews) σε δύο χώρες για την αξιολόγηση της επίδοσης των μοντέλων που προέκυψαν ως αποτέλεσμα της βιβλιογραφικής ανάλυσης. Η εργασία αναγνωρίζει και αναλύσει διάφορες τις προκλήσεις που μπορεί να αναδυθούν κατά την υιοθέτηση καινοτόμων τεχνολογιών στη δημόσια διακυβέρνηση και τις υπηρεσίες ηλεκτρονικής διακυβέρνησης. Επιπλέον παρουσιάζει προτεινόμενες λύσεις οι οποίες έχουν εξαχθεί από την εμπειρία σχεδιασμού και υλοποίησης μία σχετικής πλατφόρμας δημόσιας διακυβέρνησης με χρήση τεχνολογιών νεφοϋπολογιστικής, συμπεριλαμβανομένων απαιτήσεων προστασίας της ιδιωτικότητας, επιχειρησιακά μοντέλα, μετρικές αποτίμησης απόδοσης για τις δημόσιες υπηρεσίες. Οι προκλήσεις και οι λύσεις που αναλύονται στο πλαίσιο της εργασίας βασίζονται στην εμπειρία σχεδιασμού και υλοποίησης μίας

πλατφόρμας. Παρόλα αυτά, θα πρέπει να σημειωθεί ότι η πλατφόρμα αυτή συμπεριέλαβε δημόσιες υπηρεσίες από 4 χώρες. Αυτή η εργασία αποτελεί την πρώτη μελέτη που συζητά τις προκλήσεις αξιοποίησης τεχνολογιών νεφοϋπολογιστικής για τη δημόσια διακυβέρνηση λαμβάνοντας υπόψη πολλαπλές οπτικές και μέσω εμπειρικής έρευνας. Η εμπειρική έρευνα αφορά σε υπηρεσίες που θα αξιοποιηθούν σε μία πλατφόρμα που θα λειτουργήσει σε Ευρωπαϊκό επίπεδο.

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*

Η αξιολόγηση και βελτιστοποίηση των υπηρεσιών ηλεκτρονικής διακυβέρνησης είναι απαραίτητη για τις κυβερνήσεις ειδικά δεδομένων των δυνατοτήτων των ηλεκτρονικών υπηρεσιών να μεταρρυθμίσουν τη δημόσια διοίκηση και να βοηθήσουν στην αλληλεπίδραση της Πολιτείας και των πολιτών, των επιχειρήσεων και των δημόσιων φορέων. Από τις υπάρχουσες προσεγγίσεις αξιολόγησης απουσιάζουν μετρικές μέτρησης της ικανοποίησης των πολιτών. Ο σκοπός αυτής της εργασίας είναι διττός: να συνεισφέρει στην κατανόηση της πολιτοκεντρικής αξιολόγησης των υπηρεσιών ηλεκτρονικής διακυβέρνησης ενσωματώνοντας υπάρχουσες μετρικές κλειδιά για την απόδοση, και να προτείνει ένα πρότυπο διεργασιακό μοντέλο για μία καινοτόμα προσέγγιση αξιολόγησης που εφαρμόζει τις μετρικές αυτές προκειμένου να διευκολύνει τη δημιουργία βάσης γνώσης. Υιοθετήσαμε μία ποσοτική ερευνητική προσέγγιση για την αξιολόγηση των υπηρσιών ηλεκτρονικής διακυβέρνησης βασισμένη στην τεχνική ανάλυσης φακέλου δεδομένων (Data Envelope Analysis). Για την εμπειρική έρευνα πραγματοποιήθηκε δημοσκόπηση και συλλέχθηκαν δεδομένα για 13 υπηρεσίες ηλεκτρονικής διακυβέρνησης στην Τουρκία. Με βάση την εμπειρική έρευνα σχεδιάστηκε το προτεινόμενο πρότυπο διεργασιακό μοντέλο. Η προτεινόμενη προσέγγιση αξιολόγησης αποδείχθηκε έγκυρη και ικανή να παρέχει αποτίμηση και επεξηγήσεις πλουσιότερες από τις παραδοσιακές στατιστικές μετρικές. Η τεχνικής ανάλυσης φακέλου δεδομένων ενεργοποίησε την αναγνώριση μη αποδοτικών υπηρεσιών ηλεκτρονικής διακυβέρνησης και την παροχή σχετικών προτάσεων διόρθωσης. Το πρότυπο διεργασιακό μοντέλο κατασκευάστηκε λαμβάνοντας υπόψη την εμπειρία από την εφαρμογή της μεθόδου σε ένα μόνο πολιτισμικό περιβάλλον (της Τουρκίας). Η προτεινόμενη μέθοδος αξιολόγησης παρείχε πιο πλούσιες αποτιμήσεις σε σχέση με άλλες ανθρωποκεντρικές και

στατιστικές μεθόδους. Το προτεινόμενο πρότυπο μοντέλο αναμένεται να επιταχύνει την εφαρμογή πολιτοκεντρικής αξιολόγησης υπηρεσιών ηλεκτρονικής διακυβέρνησης και να ενισχύσει την εφαρμογή μετρικών επιπτώσεων. Η εργασία αυτή αποτελεί την πρώτη εφαρμογή της τεχνικής ανάλυσης φακέλου δεδομένων στο πεδίο της ηλεκτρονικής διακυβέρνησης. Η καινοτομία της τεχνικής είναι ότι τα αποτελέσματα της αξιολόγησης παρέχουν προτάσεις για στρατηγικές βελτιώσεις των υπηρεσιών.

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.*

Τα συστήματα ροής εργασιών έχουν καταστήσει εφικτά πολλαπλά οφέλη για ιδιωτικούς και δημόσιους οργανισμούς, συμπεριλαμβανομένων μείωσης κόστους, αύξηση αποδοτικότητας, αύξηση ικανοτήτων, αύξηση ταχύτητας επεξεργασίας, μείωση λαθών, αύξηση ποιότητας υπηρεσιών και αύξηση ικανοποίησης πελατών. Ο δημόσιος τομέας έχει εκμεταλλευτεί αυτά τα πλεονεκτήματα εφαρμόζοντας συστήματα διοίκησης ροής εργασιών για την υποστήριξη των διοικητικών διαδικασιών, όπως διαχείριση ανθρώπινων πόρων. Παρόλα αυτά, η τεχνολογία αυτή δεν έχει ακόμη αξιοποιηθεί για την υποστήριξη των διαδικασιών σχεδιασμού πολιτικής, κάτι που θα αναμενόταν ότι να ενισχύσει τη συμμετοχή των πολιτών στις διαδικασίες σχεδιασμού δημόσιων πολιτικών και να ενισχύσει την ενημερότητά τους σε δημόσια ζητήματα. Ο στόχος αυτής της εργασίας είναι να διερευνήσει τη δυνατότητα υιοθέτησης εργαλείων αυτοματοποίησης ροών εργασίας για την υποστήριξης των διαδικασιών λήψης αποφάσεων στο πλαίσιο δημόσιων πολιτικών, ανεξάρτητα από το θεσμικό πλαίσιο. Για αυτό το σκοπό αναλύονται οι διαδικασίες σχεδιασμού δημόσιων πολιτικών σε τέσσερις χώρες. Τα ευρήματα υποδεικνύουν ότι οι διαδικασίες σχεδιασμού έχουν σημαντικά κοινά στοιχεία, ακόμη κι αν ανήκουν σε διαφορετικά πεδία πολιτικής και διαφορετικά θεσμικά πλαίσιο, γεγονός που αφήνει ανοικτή τη δυνατότητα αξιοποίησης των τεχνολογιών αυτοματοποίησης ροών εργασίας στην υποστήριξη των διαδικασιών σχεδιασμού δημόσιων πολιτικών.

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

Οι πρόσφατες διεθνείς έρευνες καταδεικνύουν ότι τα προγράμματα ενημερότητας και κατάρτισης δεν είναι όσο αποτελεσματικά θα μπορούσαν να είναι και ότι οι επενδύσεις των οργανισμών σε σχετικά προγράμματα δεν είναι κατάλληλες. Ο σκοπός της παρούσας εργασίας είναι να ενισχύσει την κατανόησή μας για αυτό το φαινόμενο και να αναδείξει τα προβλήματα που αντιμετωπίζουν οι οργανισμοί όταν επιχειρούν την υλοποίηση ενός προγράμματος ενημερότητας ασφάλειας πληροφοριών. Υιοθετούμε την ερμηνευτική προσέγγιση και υλοποιούμε μία περίπτωση μελέτης (case study) εφαρμόζοντας τη θεωρία των δικτύων σύμπραξης (Actor Network Theory) και την τεχνική της απαιτούμενης διαδικασίας (due process) προκειμένου να αναλύσουμε τα δεδομένα μας. Η εργασία αυτή συνεισφέρει τόσο μέσω της κατανόησης και διαχείρισης προγραμμάτων ενημερότητας ασφάλειας σε οργανισμούς όσο και μέσω της παροχής ενός πλαισίου για την ανάλυση της αλληλεπίδρασης μεταξύ των ενεργειών ενός προγράμματος ενημερότητας με τις διάφορες διαδικασίες και γεγονότα του οργανισμού φορέα.

Η εφαρμογή της θεωρίας δικτύων σύμπραξης είναι πρόκληση για τους ερευνητές καθώς δεν υπάρχει καμία μέθοδος πρακτικής εφαρμογής ή καθοδήγηση για την εφαρμογή της. Σε αυτή την εργασία διευκολύνουμε την εφαρμογή της θεωρίας και παρέχουμε πρακτική καθοδήγηση πώς μπορεί να εφαρμοστεί μέσω της επέκτασης με την τεχνικής της απαιτούμενης διαδικασίας. Η έρευνά μας αναδεικνύει το γεγονός ότι τα προγράμματα ενημερότητας ασφάλειας συμπεριλαμβάνουν πολλούς εμπλεκομένους, οι οποίο πολλές φορές έχουν αντικρουόμενα συμφέροντα. Οι επαγγελματίες ασφάλειας θα πρέπει να κατέχουν, πρόσθετα των τεχνικών γνώσεων και ικανοτήτων, και δεξιότητες επικοινωνίας, διαπραγμάτευσης και διοίκησης, προκειμένου να διευθετήσουν όλα τα σχετικά οργανωσιακά και διοικητικά ζητήματα. Επιπρόσθετα, τα αποτελέσματα της έρευνάς μας αποκαλύπτουν ότι ο ρόλος των τεχνουργημάτων σε ένα πρόγραμμα ενημερότητας ασφάλειας δεν είναι ουδέτερος αλλά αντίθετα μπορούν να επηρεάσουν ενεργά το πρόγραμμα. Αυτή η έρευνα είναι μία από τις πρώτες που εξετάζουν τα προγράμματα ενημερότητας ασφάλειας ως μια διοικητική και κοινωνικο-τεχνική διαδικασία σε ένα οργανωσιακό πλαίσιο.

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.*

Η ευρεία διάδοση και εφαρμογή προτύπων στο χώρο των πληροφοριακών συστημάτων έχει

πολλαπλή συνεισφορά καθώς συντελεί στη διαλειτουργικότητα ομοειδών πληροφοριακών συστημάτων, στη πιστοποίηση οργανισμών, διαδικασιών, υπηρεσιών, προϊόντων κτλ. Οι πρόσφατες επισκοπήσεις και τεχνικές αναφορές υποδεικνύουν ότι τόσο η αποδοχή διεθνών προτύπων ασφάλειας, όσο και η συμμόρφωση οργανισμών με αυτά, αυξάνεται διαρκώς. Παρόλα αυτά, η πλειοψηφία των οργανισμών εξακολουθεί να μη γνωρίζει τα κυριότερα πρότυπα ασφάλειας ή να μη τα εφαρμόζει στο σύνολό τους. Η παρούσα εργασία έχει ως σκοπό να διευκολύνει την ενημερότητα των επαγγελματιών ασφάλειας για τα διεθνή και ευρέως διαδεδομένα πρότυπα ασφάλειας, συντελώντας με αυτό τον τρόπο στην υιοθέτησή τους. Η συνεισφορά της εργασίας έγκειται στην πρόταση και αξιοποίηση ενός πλαισίου κατάταξης των προτύπων ασφάλειας, το οποίο περιλαμβάνει τέσσερα επίπεδα. Ο τρόπος με τον οποίο θα μπορούσαν οι επαγγελματίες ασφάλειας να αξιοποιήσουν το παρεχόμενο πλαίσιο προκειμένου να ενημερωθούν και να αναζητήσουν το κατάλληλο κάθε φορά πρότυπο ασφάλειας, παρουσιάζεται μέσα από μία μελέτη περίπτωσης ενός πληροφοριακού συστήματος μισθοδοσίας και συντάξεων.

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.*

Το ζήτημα της προστασίας της ιδιωτικότητας των πληροφοριών αντιμετωπίζεται θεσμικά σήμερα τόσο σε επίπεδο Ευρωπαϊκής όσο και Εθνικής νομοθεσίας. Παρόλα αυτά, δεν είναι δυνατό να επιτευχθεί ικανοποιητική προστασία της ιδιωτικότητας των χρηστών πληροφοριακών συστημάτων, χωρίς την ύπαρξη τεχνικών έκφρασης των απαιτήσεων ιδιωτικότητας και την εφαρμογή μεθόδων αποτίμησης ιδιωτικότητας που θα προσδιορίζουν τα απαιτούμενα επίπεδα ιδιωτικότητας και τα εναλλακτικά μέτρα ασφάλειας για την επίτευξη αυτών. Στην παρούσα εργασία αξιοποιούμε την υπάρχουσα γνώση από τη διοίκηση ασφάλειας με σκοπό να αναδειχθούν τα ζητήματα που πρέπει να διερευνηθούν προκειμένου να επιτευχθεί η διοίκηση της ιδιωτικότητας, ώστε να είναι εφικτό να επιλέγονται τεκμηριωμένα τεχνολογίες προστασίας της ιδιωτικότητας λαμβάνοντας υπόψη τις ιδιαιτερότητες και απαιτήσεις του συγκεκριμένου συστήματος και πλαισίου.

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)

Στην παρούσα εργασία διερευνάται ο τρόπος με τον οποίο η διαδικασία της ενημερότητας ασφάλειας συνδέεται με το ευρύτερο πλαίσιο διοίκησης ασφάλειας πληροφοριακών συστημάτων (ΠΣ) το οποίο εξυπηρετεί. Μέχρι σήμερα, η διαμόρφωση πρωτοβουλιών ενημερότητας ασφάλειας αγνοεί την ιδιαίτερα σημαντική συσχέτιση με το συνολικό πλαίσιο διοίκησης ασφάλειας, και αντίστροφα. Σε αυτή την εργασία τεκμηριώνεται πώς οι δύο διεργασίες μπορούν να ευθυγραμμιστούν, ώστε να διασφαλίζεται ότι οι δραστηριότητες ενημερότητας εξυπηρετούν τη στρατηγική διοίκησης ασφάλειας, αλλά και ότι η διοίκηση ασφάλειας αξιοποιεί τα οφέλη από τις ενέργειες ενημερότητας. Για αυτό το σκοπό πραγματοποιείται ανάλυση των δύο διεργασιών με χρήση ενός πλαισίου ανάλυσης οργανωσιακών διαδικασιών και στη συνέχεια με τη ανάλυση των αναδεικνυόμενων αλληλεπιδράσεων. Η αναγνώριση των αλληλεπιδράσεων αυτών έχει ως αποτέλεσμα να καθίσταται δυνατή η τοποθέτηση της ενημερότητας ασφάλειας στο ευρύτερο πλαίσιο διοίκησης ασφάλειας ΠΣ, σε αντίθεση με την αντιμετώπισή της ως έναν μεμονωμένο μηχανισμό ασφάλειας.

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)*

Παρά το γεγονός ότι υπάρχει ανάγκη έρευνας στο χώρο των ψυχικών ασθενειών, η σχετική έρευνα παρεμποδίζεται από τα ζητήματα εμπιστευτικότητας και προστασίας της ιδιωτικότητας που αφορούν τους ιατρικούς φακέλους. Η συγκέντρωση του ιατρικού ιστορικού ασθενών που πάσχουν από την ίδια ασθένεια σε κεντρικές βάσεις δεδομένων, όπου μπορούν να εφαρμοστούν προηγμένες τεχνικές εξόρυξης γνώσης θα ήταν ιδιαίτερα πολύτιμες για τους ερευνητές. Η μεγαλύτερη πρόκληση είναι η ανωνυμοποίηση των δεδομένων, ώστε να ικανοποιούνται οι νομικές και ηθικές απαιτήσεις, ενώ παράλληλα να διατηρούνται οι κρίσιμες ιατρικές πληροφορίες. Στην παρούσα εργασία προτείνεται ένα μοντέλο δημιουργίας κεντρικού αποθετηρίου ανωνυμοποιημένων δεδομένων ασθενών που πάσχουν από διπολική διαταραχή. Η γνώση αυτή τροφοδοτεί ένα ευφυές σύστημα που διευκολύνει και καθοδηγεί τους κλινικούς γιατρούς στη διαχείριση ασθενών. Οι απαιτήσεις ασφάλειας ικανοποιούνται από την εφαρμογή ελέγχου πρόσβασης με μηχανισμούς ελέγχου πρόσβασης βάσει ρόλων (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.*

Η εργασία αυτή παρέχει μία διερευνητική επισκόπηση που στοχεύει αφενός στην αναγνώριση πρότυπων και τάσεων στον τρόπο με τον οποίο η επαγγελματική και η ακαδημαϊκή κοινότητα προσεγγίζουν το ζήτημα της ενημερότητας ασφάλειας, και αφετέρου, στην κατανόηση των αιτιών για τις οποίες η πρακτική της ενημερότητας ασφάλειας παραμένει άλυτο πρόβλημα. Η μέθοδος που εφαρμόστηκε είναι ανάλυση επιλεγμένων δημοσιευμένων εργασιών (επιστημονικά άρθρα, επισκοπήσεις, πρότυπα και τεχνικές αναφορές) με ανοικτή κωδικοποίηση (open coding). Η ανάλυση αυτή οδήγησε σε ένα σχήμα ταξινόμησης έξι κατηγοριών ανοικτών θεμάτων (π.χ. σύγχυση ορολογίας) και οι επιλεγμένες εργασίες κατηγοριοποιηθήκαν σύμφωνα με αυτό το σχήμα. Η παρούσα εργασία οδηγεί στην ανάδειξη ασαφών ζητημάτων των υπαρχουσών προσεγγίσεων ενημερότητας ασφάλειας, ενώ η προτεινόμενη ταξινόμηση παρέχει ένα οδηγό προς τους ερευνητές και επαγγελματίες ασφάλειας για το σχεδιασμό και τη μελέτη ερευνητικών ή εφαρμοσμένων προσεγγίσεων ενημερότητας ασφάλειας πληροφοριακών συστημάτων.

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.*

Σκοπός της εργασίας είναι να μελετηθεί ο τρόπος με τον οποίο οι μελετητές ασφάλειας πληροφοριακών συστημάτων (ΠΣ) έχουν προσεγγίσει το ζήτημα της ενημερότητας ασφάλειας πληροφοριών και να εξεταστεί κατά πόσο οι προσεγγίσεις αυτές είναι συμβατές με την οργανωσιακή θεωρία και τις προσεγγίσεις μελέτης οργανωσιακών διεργασιών στο χώρο των ΠΣ. Για αυτό το σκοπό πραγματοποιήθηκε ανάλυση επιλεγμένων δημοσιευμένων εργασιών (επιστημονικά άρθρα, επισκοπήσεις, πρότυπα και τεχνικές αναφορές) με ανοικτή κωδικοποίηση (open coding). Η ανάλυση είχε ως αποτέλεσμα την κατηγοριοποίηση των επιλεγμένων δημοσιευμένων εργασιών σύμφωνα με προτεινόμενη τυπολογία. Τα αποτελέσματα της εργασίας διευκολύνουν τους ερευνητές και επαγγελματίες ασφάλειας ΠΣ ώστε να διακρίνουν και να εφαρμόζουν κατάλληλα μοντέλα έρευνας στο σχεδιασμό πρωτοβουλιών και τη μελέτη ζητημάτων ενημερότητας ασφάλειας ΠΣ.

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.*

Σκοπός της παρούσας εργασίας είναι η διερεύνηση της εφαρμογής του Πολιτισμικού Προτύπου ως εργαλείο αναγνώρισης προτύπων στις αντιλήψεις επικινδυνότητας των εμπλεκομένων στην ασφάλεια πληροφοριών και της επίδρασής τους στη διαχείριση επικινδυνότητας πληροφοριακών συστημάτων (ΠΣ). Σύμφωνα με το Πολιτισμικό Πρότυπο οι αντιλήψεις επικινδυνότητας μεταξύ κοινωνικών ομάδων και δομών είναι προβλέψιμη και συσχετίζεται με τον τύπο κοινωνικής οργάνωσης. Η διαχείριση επικινδυνότητας ΠΣ περιλαμβάνει ένα σημαντικό αριθμό δραστηριοτήτων που βασίζονται στον τρόπο με τον οποίο οι εμπλεκόμενοι αντιλαμβάνονται τον κίνδυνο σε σχέση με τα αγαθά του ΠΣ. Επομένως, στην παρούσα εργασία εξετάζονται οι επιπτώσεις της εφαρμογής του Πολιτισμικού Προτύπου στη διαχείριση ασφάλειας ΠΣ ως εργαλείο των ειδικών ασφάλειας για τη διαχείριση των αντιλήψεων επικινδυνότητας. Η εργασία παρουσιάζει πώς οι διαφορετικοί τύποι μορφών κοινωνικής οργάνωσης επηρεάζουν τη διαχείριση επικινδυνότητας και παρέχει κύρια σημεία που πρέπει να λαμβάνονται υπόψη κατά τη διαμόρφωση στρατηγικών διαχείρισης επικινδυνότητας.

Β.3 ΕΡΕΥΝΗΤΙΚΕΣ ΕΡΓΑΣΙΕΣ ΔΗΜΟΣΙΕΥΜΕΝΕΣ ΣΕ ΠΡΑΚΤΙΚΑ ΔΙΕΘΝΩΝ ΕΠΙΣΤΗΜΟΝΙΚΩΝ ΣΥΝΕΔΡΙΩΝ ΜΕΤΑ ΑΠΟ ΚΡΙΣΗ ΠΛΗΡΟΥΣ ΚΕΙΜΕΝΟΥ

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

Πολλές κυβερνήσεις και πολίτες υιοθετούν συστήματα πληροφοριών που έχουν σχεδιαστεί για να ενισχύουν τη διαφάνεια των δημόσιων δαπανών και την αποθάρρυνση της διαφθοράς στον δημόσιο τομέα. Στόχος του παρόντος άρθρου είναι να εξετάσει την ικανότητα και την αξία των πληροφοριακών συστημάτων που αποσκοπούν στην ενίσχυση της διαφάνειας, από την οπτική των πολιτών / χρηστών. Στόχος μας είναι να αντιμετωπίσουμε τα ερευνητικά ζητήματα που συνδέονται με τον πραγματικό αντίκτυπο αυτών των συστημάτων σχετικά με

την εμπιστοσύνη και την αβεβαιότητα των πολιτών έναντι των κυβερνητικών πολιτικών και δράσεων. Διερευνήσαμε επίσης τον αντίκτυπο των προδιαγραφών ιδιωτικότητας και των κανονισμών προστασίας προσωπικών δεδομένων στα συστήματα αυτά και την προθυμία των πολιτών να έχουν πρόσβαση στα δημόσια δεδομένα. Από όσο γνωρίζουμε, αυτά είναι σε μεγάλο βαθμό ανεξερεύνητα ζητήματα στη βιβλιογραφία. Η μελέτη μας περιλαμβάνει εμπειρική έρευνα με πολίτες που έχουν χρησιμοποιήσει ένα τέτοιο σύστημα στην Ελλάδα. Συγκεκριμένα, επικεντρώσαμε την εμπειρική μας μελέτη στο ελληνικό σύστημα «Diavgeia», το οποίο είναι το εθνικό σύστημα διαφάνειας και καταπολέμησης της διαφθοράς

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.

Το παράδοξο της ιδιωτικότητας αφορά στην ασυμφωνία μεταξύ των ανησυχιών περί ιδιωτικότητας και της πραγματικής συμπεριφοράς των χρηστών Διαδικτύου. Η ύπαρξη του φαινομένου έχει μελετηθεί σε πολλούς τομείς, όπως τα κοινωνικά δίκτυα και ιδιαίτερα μια μεγάλη ποικιλία φόρουμ και διαδικτυακών κοινοτήτων. Το παρόν άρθρο, αμφισβητεί την ύπαρξή του στο πλαίσιο ευαίσθητων δεδομένων και ειδικότερα στον τομέα των δεδομένων υγείας μέσω εμπειρικής έρευνας που πραγματοποιήθηκε στην Ελλάδα. Δεδομένου ότι οι πληροφορίες που σχετίζονται με την υγεία θεωρούνται ευαίσθητα προσωπικά δεδομένα και συχνά αποκλείονται από συζητήσεις και ανταλλαγές, η έρευνα αμφισβητεί την ύπαρξη του παράδοξου που οδηγεί στην αποκάλυψη πληροφοριών για τα δεδομένα υγείας κατά την επίσκεψη σχετικών σε απευθείας σύνδεση φόρουμ και κοινοτήτων, τους χρήστες.

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).*

Οι προγραμματιστές εφαρμογών για κινητές συσκευές καθορίζουν τους όρους χρήσης για τις εφαρμογές που αναπτύσσουν και οι χρήστες μπορούν να τους αποδεχθούν ή να απορρίψουν κατά την εγκατάσταση. Οι προγραμματιστές εφαρμογών επιδιώκουν, αφενός, να αποκτήσουν πρόσβαση σε όσο το δυνατόν περισσότερες πληροφορίες για τους χρήστες, ενώ οι χρήστες αφετέρου φαίνεται ότι στερούνται ευαισθητοποίησης και κατανόησης των πολιτικών απορρήτου. Αυτό επιτρέπει στους προγραμματιστές εφαρμογών να αποθηκεύουν ένα τεράστιο αριθμό προσωπικών δεδομένων, μερικές φορές ακόμη και δεδομένα που δε συσχετίζονται άμεσα με τη λειτουργία της εφαρμογής. Είναι επίσης

κοινό ότι οι χρήστες επιλέγουν να μην αλλάξουν τις προεπιλεγμένες ρυθμίσεις, ακόμη και όταν παρέχεται μια τέτοια επιλογή. Σε συνδυασμό, οι παραπάνω συνθήκες θέτουν σε κίνδυνο τα δικαιώματα των χρηστών στην ιδιωτική ζωή. Σε αυτήν την έρευνα, εξετάσαμε την εφαρμογή Viber για να δείξουμε πόσο εύκολο είναι να ανακαλύψουμε την ταυτότητα άγνωστων χρηστών Viber. Επιλέξαμε ένα ψευδοτυχαίο δείγμα 2000 αριθμών κινητής τηλεφωνίας και εξετάσαμε αν μπορούσαμε να αποκαλύψουμε τα προσωπικά τους δεδομένα. Σχεδιάσαμε μια εμπειρική μελέτη που συγκρίνει την αναφερόμενη συμπεριφορά με την πραγματική συμπεριφορά των χρηστών Viber. Τα αποτελέσματα αυτής της μελέτης δείχνουν ότι η ανωνυμία και η ιδιωτικότητα των χρηστών παραβιάζονται εύκολα. Παρέχουμε οδηγίες που απευθύνονται τόσο στους χρήστες κινητών εφαρμογών όσο και στους προγραμματιστές για να αυξήσουν την ευαισθητοποίηση σχετικά με την προστασία της ιδιωτικής ζωής και να αποτρέψουν παραβιάσεις ιδιωτικότητας.

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

Οι ανησυχίες σχετικά με την ιδιωτικότητα, τη λογοκρισία και την παρεμπόδιση περιεχομένου οδηγούν εκατομμύρια ανθρώπους να χρησιμοποιούν προϊόντα που βελτιώνουν την προστασία πληροφοριακής ιδιωτικότητας. Αυτή η έρευνα επικεντρώνεται στα εργαλεία ανωνυμίας, ως τεχνολογία ενίσχυσης της προστασίας της ιδιωτικότητας (PET) και διερευνά τις αξίες που οδηγούν στην υιοθέτηση εργαλείων ανωνυμίας από τους χρήστες. Χρησιμοποιούμε ανάλυση μέσων-στόχων, μια μεθοδολογία που θεωρούμε κατάλληλη για τη διερεύνηση των αντιλήψεων και των κινήτρων των χρηστών για την υιοθέτηση εργαλείων ανωνυμίας. Χρησιμοποιούμε επίσης την τεχνική σκάλας, μια ποιοτική μέθοδο βασισμένη σε συνεντεύξεις, για να αποκαλύψουμε τις αλυσίδες των ιδιοτήτων-παραγόντων-αξιών των χρηστών των εργαλείων ανωνυμίας και να κατασκευάσουμε έναν χάρτη ιεραρχικών αξιών. Στόχος της έρευνάς μας είναι να παράσχουμε ιδέες και να βελτιώσουμε την κατανόηση της συμπεριφοράς των χρηστών εργαλείων ανωνυμίας, τα οποία αναμένουμε να ωφελήσουν τόσο τους ερευνητές όσο και τους μηχανικούς λογισμικού που σχεδιάζουν πλατφόρμες ώστε να ταιριάζουν καλύτερα στις ανάγκες των χρηστών.

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*

Τα Πληροφοριακά Συστήματα θεωρούνται στη σημερινή εποχή ένα σημαντικό κεφάλαιο για

τους οργανισμούς προκειμένου να λειτουργούν και να διατηρούν τα στρατηγικά τους πλεονεκτήματα. Οι επενδύσεις στα πληροφορικά συστήματα, την πρόσληψη εξειδικευμένου προσωπικού πληροφορικής και η θέσπιση ισχυρών εσωτερικών και εξωτερικών συνεργασιών για την πληροφορική, θεωρούνται καθοριστικοί παράγοντες για την επιτυχία της επιχείρησης και τη συνέχιση λειτουργίας. Καθώς όμως οι οργανισμοί εξαρτώνται ολοένα και περισσότερο από τους πόρους πληροφοριακών συστημάτων αντιμετωπίζουν πιο προηγμένες απειλές ασφάλειας πληροφοριών. Το παρόν άρθρο διερευνάει τη σχέση ανάμεσα στην ανάπτυξη πόρων πληροφοριακών συστημάτων και πόρων για την προστασία της ασφάλειας πληροφοριών. Είναι οι οργανισμοί πρόθυμοι να επενδύσουν στην ασφάλεια πληροφοριών καθώς επενδύουν περισσότερο σε πόρους πληροφοριακών συστημάτων; Οι συγγραφείς πραγματοποιήσαν μία εμπειρική έρευνα σε οργανισμούς πέντε χώρες της Μεσογείου. Το δείγμα περιλαμβάνει απαντήσεις από 61 Διευθύνοντες Συμβούλους, υπεύθυνους ασφάλειας και διευθυντές πληροφορικής. Τα αποτελέσματα καταδεικνύουν ότι οι ανάπτυξη πόρων πληροφοριακών συστημάτων επηρεάζει θετικά την ανάπτυξη πόρων για την ασφάλεια πληροφοριών. Ανάμεσα στους σχετικούς πόρους, η ανάπτυξη ανθρώπινων πόρων είναι πλέον καθοριστικής σημασίας για την υιοθέτηση μέτρων ασφάλειας πληροφοριών.

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*

Τα τελευταία χρόνια, σε αρμονία με τον ταχύτατα αυξανόμενο ρυθμό του πληθυσμού των χρηστών στα Online Social Networks (OSN), μια τάση για τους δημιουργούς κακόβουλου λογισμικού είναι να επωφεληθούν από τις κοινωνικές σχέσεις των χρηστών OSN, προκειμένου να τους προσελκύσουν να ακολουθήσουν κακόβουλα URLs που οδηγούν σε μόλυνση από κακόβουλο λογισμικό. Ένας λόγος για την επιτυχία τέτοιου είδους κακόβουλής ενέργειας μέσω κοινωνικής μηχανικής είναι η χαμηλή επίγνωση ασφάλειας των χρηστών. Πράγματι, κατά μέσο όρο, οι χρήστες κοινωνικών δικτύων δεν έχουν επαρκείς γνώσεις για τις κακόβουλες απειλές μέσω URLs που ενδέχεται να αντιμετωπίσουν και, ως εκ τούτου, είναι εύκολο να πέσουν θύματα των αντίστοιχων επιθέσεων. Στο παρόν άρθρο διεξάγουμε μια εμπειρική έρευνα η οποία, αφενός, καταδεικνύει τη χαμηλή επίγνωση των χρηστών του Facebook για τις κακόβουλες απειλές μέσω URLs και, αφετέρου, διερευνά τις απόψεις των

χρηστών σχετικά με τις επιθυμητές ιδιότητες μιας εφαρμογής ασφάλειας που τους προστατεύει από τέτοιες κακόβουλες ενέργειες. Επιπλέον, σχεδιάζουμε και περιγράφουμε την αρχιτεκτονική μιας εφαρμογής η οποία προτίθεται να αυξήσει την ευαισθητοποίηση των χρηστών του Facebook, ενημερώνοντάς τους σχετικά με (ενδεχομένως) κακόβουλες δημοσιεύσεις στους τοίχους τους πριν ή μετά τη μόλυνση. Η εφαρμογή ενεργεί προνοητικά, βοηθώντας τους χρήστες να μην μολυνθούν από κακόβουλες δημοσιεύσεις. Επιπλέον βοηθάει χρήστες που έχουν μολυνθεί να κατανοήσουν την απειλή και να ενημερωθούν περισσότερο για τον εντοπισμό συνδέσμων κακόβουλου λογισμικού.

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*

Οι νέες τεχνολογίες με σύνδεση στο Διαδίκτυο, όπως προσωπικοί υπολογιστές, tablets και κινητά τηλέφωνα, χρησιμοποιούνται διαρκώς από τους οργανισμούς. Ταυτόχρονα, παρατηρείται αύξηση του φαινομένου χρήσης από τους υπαλλήλους ενός οργανισμού των νέων τεχνολογιών για προσωπικούς λόγους εν ώρα εργασίας. Η βιβλιογραφία παρουσιάζει διάφορα μοντέλα ανάλυσης των αιτιών για τους οποίους οι υπάλληλοι πράττουν κατάχρηση των πόρων με αυτό τον τρόπο. Οι έρευνες αυτές αντιμετωπίζουν τη χρήση των νεών τεχνολογιών για προσωπικούς λόγους ως μία ενιαία συμπεριφορά. Παρόλα αυτά υπάρχουν έρευνες που υπονοούν ότι υπάρχουν διάφοροι τύποι συμπεριφοράς που εντάσσονται σε αυτό το πεδίο. Επομένως, είναι περιοριστικό να μελετούμε ως ένα ενιαίο φαινόμενο το πρόβλημα αυτό και τις αιτίες του. Ως ένα πρώτο βήμα την αντιμετώπιση αυτού του ερευνητικού κενού, η εργασία αυτή διαχωρίζει τρεις κατηγορίες χρήσης των νέων τεχνολογιών για προσωπικούς λόγους: χρήση ηλεκτρονικού ταχυδρομείου, πλοήγηση στο Διαδίκτυο και οικονομικές συναλλαγές. Εξετάζουμε διαφορετικές αιτίες για κάθε μία από τις τρεις κατηγορίες. Η εργασία συνεισφέρει στην έρευνα αναδεικνύοντας την αναγκαιότητα να εξεταστεί σε βάθος το φαινόμενο διακρίνοντας διαφορετικούς τύπους χρήσης.

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.*

Παρά το γεγονός ότι η προσωποποιημένη ιατρική μπορεί να βελτιστοποιήσει την εύρεση,

ανάπτυξη και εφαρμογή θεραπευτικών δράσεων, δεν έχει πλήρως αξιοποιηθεί από τις υπηρεσίες υγείας προς ασθενείς. Όταν ο ηλεκτρονικός φάκελος υγείας ενσωματωθεί με δεδομένα από άλλες πηγές, όπως κοινωνική πρόνοια, προσωπικό φάκελο υγείας και γενικές πληροφορίες, μπορεί να αποκτήσει κεντρικό ρόλο στην προσωποποιημένη υγειονομική περίθαλψη. Επομένως, μία νέα γενιά ηλεκτρονικού φακέλου υγείας θα αναδυθεί η οποία όχι μόνο θα υποστηρίζει τους επαγγελματίες υγείας να λαμβάνουν κατάλληλα πληροφορημένες αποφάσεις, αλλά επίσης μπορεί να υποστηρίξει την καινοτόμα ανακάλυψη συσχετίσεων ανάμεσα σε γενετικά, κλιματολογικά, διαδικαστικά στοιχεία. Παρόλα, υπάρχει ένα πλήθος από νομικά, ηθικά και τεχνικά αίτια που παρεμποδίζουν την υλοποίηση αυτού του ηλεκτρονικού φακέλου υγείας, εξ' αιτίας των πιθανών παραβιάσεων ασφάλειας πληροφοριών και της ιδιωτικότητας. Σε αυτή την εργασία παρουσιάζουμε ένα μοντέλο συμβατό με τη HIPAA το οποίο ενεργοποιεί έλεγχο πρόσβασης στην επόμενη γενιά ηλεκτρονικού φακέλου υγείας διατηρώντας την ιδιωτικότητα.

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*

Η χρήση κινητών συσκευών, όπως κινητά τηλέφωνα και tablets, κατέχουν σήμερα εξαιρετικά σημαντικό ρόλο σε προσωπικούς και επαγγελματικούς τομείς. Εν τω μεταξύ, οι τεχνολογικές εξελίξεις καθιστούν ολοένα και πιο δύσκολη τη διάκριση ανάμεσα στις εργασιακές και τις μη εργασιακές δραστηριότητες. Καθώς οι κινητές συσκευές και το Διαδίκτυο εντάσσονται όλο και περισσότερο στον εργασιακό χώρο, οι υπάλληλα συχνά πραγματοποιούν ενέργειες στο Διαδίκτυο που αφορούν προσωπικές υποθέσεις, εν ώρα εργασίας και από τον εργασιακό χώρο, αξιοποιώντας μάλιστα τεχνολογικούς πόρους του οργανισμού. Οι έρευνες έχουν αναγνωρίσει πληθώρα από κίνητρα που εξηγούν αυτή τη συμπεριφορά, από διαφορετικές οπτικές. Μέσω ανάλυσης της βιβλιογραφίας, προτείνουμε ένα δυϊκό μοντέλο για τη συμπεριφορά αυτή και εξετάζουμε τους παράγοντες διαμόρφωσης, τους οποίους διακρίνουμε σε δύο κατηγορίες: τους παράγοντες έκφρασης και τους παράγοντες σκοπού. Στη συνέχεια, αναπτύσσουμε ένα δυϊκό ερευνητικό μοντέλο συνδυάζοντας τις δύο κατηγορίες και τις αλληλοεπιδράσεις τους. Συγκεκριμένα, αξιοποιώντας τη θεωρία ελέγχου-ζήτησης εργασίας (job demand-control theory) αναγνωρίζουμε ένα νέο παράγοντα διαμόρφωσης που εξηγεί την πλευρά έκφρασης της συμπεριφοράς, την επαγγελματική εξουθένωση. Επίσης,

αναγνωρίζουμε ένα νέο παράγοντα διαμόρφωσης που εξηγεί την πλευρά σκοπού της συμπεριφοράς, το εκτιμώμενο όφελος. Το μοντέλο δίνει νέα οπτική στην έρευνα γύρω από τη συμπεριφορά προσωπικής χρήσης του Διαδικτύου στον εργασιακό χώρο, μέσω της πρότασης αναγνώρισης της διττής φύσης της, δίνοντας μία ευκαιρία κατανόησης των διαφορετικών εναλλακτικών μοντέλων που υπάρχουν στη βιβλιογραφία και επιτρέποντας το συνδυασμό τους σε μελλοντική έρευνα.

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*

Η χρήση κινητών συσκευών, όπως κινητά τηλέφωνα και tablets, κατέχουν σήμερα εξαιρετικά σημαντικό ρόλο σε προσωπικούς και επαγγελματικούς τομείς. Εν τω μεταξύ, οι τεχνολογικές εξελίξεις καθιστούν ολοένα και πιο δύσκολη τη διάκριση ανάμεσα στις εργασιακές και τις μη εργασιακές δραστηριότητες. Υπάρχουν αντικρουόμενες απόψεις στη βιβλιογραφία σχετικά με τους παράγοντες διαμόρφωσης, τις επιπτώσεις και τις πολιτικές ασφάλειας που περιορίζουν της προσωπικής χρήσης του Διαδικτύου στον εργασιακό χώρο. Σε αυτή την εργασία ισχυριζόμαστε ότι για να κατανοήσουμε το φαινόμενο θα πρέπει να αναλύσουμε περισσότερο τη συμπεριφορά αυτή και να κατανοήσουμε τη φύση της. Μέσω ανάλυσης της σχετικής βιβλιογραφίας προτείνουμε ότι η συμπεριφορά αυτή έχει διττή φύση η οποία συνδέεται με διαφορετικούς παράγοντες διαμόρφωσης, επιπτώσεις και πολιτικές περιορισμού. Αναφορικά με τους παράγοντες διαμόρφωσης η συμπεριφορά αυτή αποτελεί ταυτόχρονα ένα μέσο για να εκφράσουν αρνητικά συναισθήματα σε σχέση με τον οργανισμό και ένα μέσο σκοπού για την επίτευξη θετικών λειτουργιών χρησιμοποιώντας το Διαδίκτυο. Σε σχέση με τις επιπτώσεις αναγνωρίζουμε ότι η συμπεριφορά αυτή μπορεί να επιφέρει τόσο θετικές επιπτώσεις στους οργανισμούς όσο και αρνητικές. Για τις πολιτικές ασφάλειας, διακρίνουμε ότι διαφορετικές πολιτικές είναι κατάλληλες ανάλογα τον οργανισμό. Αυτή η διττή φύση της συμπεριφορά προσωπικής χρήσης του Διαδικτύου στον εργασιακό χώρο προσφέρει νέα οπτική στο φαινόμενο για δύο λόγους. Πρώτον διευκολύνει την ενοποίηση των αντικρουόμενων ερευνών στη βιβλιογραφία και δεύτερον παρέχει καθοδήγηση για μελλοντική έρευνα.

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*

Η σχετική και η δομική ενσωμάτωση κατέχουν σημαντικό ρόλο στο πλαίσιο της ανάθεσης εργασιών πληροφοριακών συστημάτων σε τρίτους φορείς. Παρόλα αυτά, δεν υπάρχει σαφής καθοδήγηση για το ποιος από τους δύο τύπους ενσωμάτωσης είναι πλέον κατάλληλος προκειμένου να αποτραπούν συμπεριφορές κερδοσκοπίας και να επιτευχθεί μακροπρόθεσμη επίδοση όταν υπάρχει αβεβαιότητα και ένα μεγάλο εύρος ανάπτυξης προϊόντων και συστημάτων πληροφορικής που έχουν ανατεθεί σε τρίτους. Προκειμένου να απαντήσουμε σε αυτό το ερώτημα, δημιουργούμε ένα εικονικό περιβάλλον που προσομοιάζει το δίκτυο συνεργατών μία τρίτης ανάθεσης, όπου οι εταιρείες παίρνουν τον έλεγχο επιλογής συνεργατών με σχετική και με δομική ενσωμάτωση αντίστοιχα. Οι συνεργάτες ανταγωνίζονται μεταξύ τους με στόχο τη μεγιστοποίηση των μακροπρόθεσμων κερδών. Τα αποτελέσματα της προσομοίωσης δείχνουν τα πλεονεκτήματα του κάθε τύπου ενσωμάτωσης και ότι υπερέχουν κάθε ένας ανάλογα με τα επίπεδα αβεβαιότητας. Επομένως, η έρευνα παρέχει καλύτερη κατανόηση των συνθηκών υπεροχής του κάθε τύπου και παρέχει στην ανώτερη διοίκηση καθοδήγηση για να επιλέξει ανάμεσά τους.

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*

Οι εφαρμογές και υπηρεσίες κινητής διακυβέρνησης (m-government) αναφέρονται σε υπηρεσίες που είναι διαθέσιμες μέσω κινητών συσκευών συνδεδεμένων στο Διαδίκτυο και είναι προσπελάσιμες οποιαδήποτε ώρα και από οποιαδήποτε τοποθεσία. Η κινητή διακυβέρνηση και η κινητή συμμετοχή των πολιτών είναι νέες έννοιες ενός αναπτυσσόμενου πεδίου της δημόσιας διακυβέρνησης και παρέχεται μέσω ηλεκτρονικών υπηρεσιών προσβάσιμων από κινητές συσκευές. Σε αυτή την εργασία παρέχουμε ένα πλαίσιο αξιολόγησης των εργαλείων κινητής διακυβέρνησης. Το πλαίσιο αξιολόγησης βασίζεται στην υπόθεση ότι τα εργαλεία κινητής διακυβέρνησης δεν παρέχουν μόνο μία εναλλακτική μέθοδο πρόσβασης στις δημόσιες δράσεις, αλλά στοχεύει και στην παροχή κινήτρων στους πολίτες για την αύξηση της συμμετοχής τους στις διαδικασίες διαμόρφωσης δημόσιων πολιτικών. Η μέθοδος αξιολόγησης βασίζεται στο μοντέλο Elaboration Likelihood Model. Η καινοτομία της εργασίας συνίσταται α) στην ικανότητα της να αποτυπώνει την πραγματική χρήση των εργαλείων από τους χρήστες και όχι την πρόθεση χρήσης, β) στη δυνατότητα που φέρει να

αποτιμά τις ικανότητες κινητοποίησης και πειθούς του συστήματος.

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*

Η αξιολόγηση και βελτιστοποίηση των υπηρεσιών ηλεκτρονικής διακυβέρνησης είναι απαραίτητη για τις κυβερνήσεις, ιδιαίτερα λόγω της δυνατότητες που φέρουν για την μεταρρύθμιση της δημόσιας διοίκησης. Οι υπάρχουσες προσεγγίσεις αξιολόγησης δεν συμπεριλαμβάνουν μετρικές που αντανακλούν την ικανοποίηση των πολιτών. Η βιβλιογραφία από την άλλη μεριά περιλαμβάνει διάφορα μοντέλα και τεχνικές για την αξιολόγηση της ικανοποίησης των πολιτών. Παρόλα αυτά, η βιβλιογραφία στερείται ενός μοντέλου αναφοράς για την επανα-χρησιμοποίηση πρακτικών αξιολόγησης ηλεκτρονικών υπηρεσιών διακυβέρνησης με συμπερίληψη της ικανοποίησης των πολιτών. Σε αυτή την εργασία, αξιοποιούμε την προσέγγιση αξιολόγησης που αναπτύχθηκε στο πλαίσιο του Κοινοτικού Προγράμματος CEES και προτείνουμε ένα μοντέλο αναφοράς που ενσωματώνει τη δυνατότητα επανα-χρησιμοποίησης πρακτικών ηλεκτρονικής διακυβέρνησης με πολιτο-κεντρική προσέγγιση. Η καινοτομία της εργασίας έγκειται στη χρήση της τεχνικής ανάλυσης φακέλου δεδομένων για την αξιολόγηση των ηλεκτρονικών υπηρεσιών προς την αναγνώριση σημείων στρατηγικής βελτίωσης των υπηρεσιών.

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.*

Με την ευρεία υιοθέτηση υπηρεσιών ηλεκτρονικής διακυβέρνησης έχει δημιουργηθεί η ανάγκη αδιάκοπης ροής δεδομένων μεταξύ των φορέων του δημοσίου τομέα, διατηρώντας παράλληλα την ακεραιότητα, εμπιστευτικότητα και ακεραιότητα των δεδομένων αυτών. Οι κυβερνήσεις έχουν θέσει σε ισχύ διάφορα κίνητρα και προγραμμάτα, συμπεριλαμβανομένων προγραμμάτων ενημερότητας, με σκοπό την ενίσχυση της κατανόησης για την προστασία της ασφάλειας πληροφοριών και της ιδιωτικότητας από τους υπαλλήλους των δημοσίων φορέων. Παρόλα αυτά, η υλοποίηση τέτοιων δράσεων ενημερότητας είναι πολλές φορές συνυφασμένη

με ένα πλήθος από προκλήσεις. Η εργασία αυτή προσφέρει μία κατανόηση των προκλήσεων προς την επιτυχή υλοποίηση προγραμμάτων ενημερότητας ασφάλειας στον δημόσιο τομέα σε σχέση με τις ηλεκτρονικές υπηρεσίες. Το εννοιολογικό πλαίσιο που αναπτύσσεται περιλαμβάνει πολιτικές, κοινωνικές, οργανωσιακές και τεχνολογικές προκλήσεις. Η εργασία περιλαμβάνει εμπειρική έρευνα μέσω μελέτης περίπτωσης σε ένα δημόσιο οργανισμό στην Ελλάδα. Ενώ τα αποτελέσματα της εμπειρικής έρευνας επιβεβαιώνουν το ρόλο των προκλήσεων που αναγνωρίστηκαν, παράλληλα αναγνωρίζεται μέσω της έρευνας ότι οι συμμετέχοντες στο σχεδιασμό των προγραμμάτων ενημερότητας επιδιώκουν συχνά διαφορετικούς στόχους ασφάλειας και ιδιωτικότητας, το οποίο συντελεί σε αύξηση της πολυπλοκότητας στον οργανισμό.

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*

Η ενημερότητα ασφάλειας πληροφοριών είναι μία διαρκής προσπάθεια εστίασης του ενδιαφέροντος στην ασφάλεια πληροφοριών και τη σημασία της, με σκοπό την ενεργοποίηση συμπεριφορών που ωφελούν την ασφάλεια. Παρά το αυξημένο ενδιαφέρον των ερευνητών στο πεδίο της ενημερότητας ασφάλειας και τις διαρκείς προειδοποιήσεις των διεθνών επισκοπήσεων ασφάλειας για τη σημασία της, η ενημερότητα ασφάλειας παραμένει ως ένα κρίσιμο ζήτημα της ασφάλειας πληροφοριών. Οι υπάρχουσες προσεγγίσεις ενημερότητας ασφάλειας προτείνουν τεχνικές και μεθόδους προώθησης της ασφάλειας, χωρίς όμως να στηρίζονται σε κάποιο θεωρητικό πλαίσιο, και μάλιστα ανεξάρτητα από το συνολικό πλαίσιο διοίκησης ασφάλειας πληροφοριών. Ο σκοπός της παρούσας εργασίας είναι να προτείνει ένα θεωρητικό και μεθοδολογικό πλαίσιο που θα διευκολύνει την ανάλυση και κατανόηση των ζητημάτων που εμπλέκονται στις δραστηριότητες ενημερότητας ασφάλειας, ώστε να υποστηριχθεί η διοίκηση ασφάλειας ενός οργανισμού.

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*

Οι σχεδιαστές συστημάτων βρίσκονται αντιμέτωποι με τις ταχείς τεχνολογικές εξελίξεις, τις πολύπλοκες συμβατικές σχέσεις, τις αναδυόμενες απειλές και απαιτήσεις ασφάλειας, τις ανησυχίες για τη βιωσιμότητα των προγραμμάτων τους κτλ. Σε αυτό το πλαίσιο, τα

πληροφοριακά συστήματα εκτίθενται σε υψηλούς κινδύνους, ενώ τα πρόσφατα στοιχεία περιστατικών αποτυχίας συντελούν στην απαίτηση έμφασης στην ασφάλεια. Παρόλα αυτά είναι μη εφικτό οι προγραμματιστές συστημάτων να εξειδικευτούν σε όλα τα πεδία ενδιαφέροντος προκειμένου να αντιμετωπίσουν με επιτυχία τα ζητήματα αυτά. Επομένως, ο σχεδιασμός των συστημάτων είναι απαραίτητο να λαμβάνει υπόψη τις καλές πρακτικές και την υπάρχουσα σχετική γνώση. Όταν αυτή η γνώση ενσωματώνεται σε καθιερωμένα και ευρέως αποδεκτά πρότυπα, δημιουργείται όχι μόνο η ευκαιρία να αξιοποιηθεί το ώριμο περιεχόμενό τους, αλλά και να αξιοποιηθούν τα πλεονεκτήματα συμμόρφωσης, ολοκλήρωσης και ανταγωνιστικού πλεονεκτήματος που παρέχει η προτυποποίηση. Για αυτό το σκοπό, στην παρούσα εργασία διερευνάται η αξιοποίηση δύο ευρέως αποδεκτών προτύπων: η σειρά ISO 27000 και το ISO/IEC 26702, ως εργαλεία που θα βοηθήσουν το σχεδιασμό ασφαλών συστημάτων.

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.*

Πολλές έρευνες στο χώρο των πληροφοριακών συστημάτων έχουν εφαρμόσει θεωρίες αποδοχής για την εξέταση ζητημάτων αποδοχής ηλεκτρονικών υπηρεσιών από τους χρήστες πληροφοριακών συστημάτων. Η εφαρμογή αυτών των θεωριών στο πεδίο της ηλεκτρονικής διακυβέρνησης έχει δείξει ότι η εμπιστοσύνη αποτελεί προαπαιτούμενο για την αποδοχή και χρήση των συστημάτων ηλεκτρονικής διακυβέρνησης. Παράλληλα, τα ζητήματα και οι ανησυχίες ιδιωτικότητας αποτελούν την κύρια προϋπόθεση για τη πρόθεση χρήσης των συστημάτων ηλεκτρονικής διακυβέρνησης από τους χρήστες. Επομένως, πληροφοριακά συστήματα που δε διαφυλάσσουν την ιδιωτικότητα δεν γίνονται έμπιστα από τους χρήστες με αποτέλεσμα να μη τα αποδέχονται. Σήμερα υπάρχουν πολλές κακόβουλες επιθέσεις που μπορεί να παραβιάσουν την εμπιστευτικότητα προσωπικών δεδομένων και να διακυβευτεί η εμπιστοσύνη προς το σύστημα. Ο τυπικός τρόπος για την αποτροπή τέτοιων επιθέσεων είναι η εφαρμογή τεχνολογιών προστασίας της ιδιωτικότητας. Παρόλα, η εφαρμογή των τεχνολογιών ενίσχυσης της ιδιωτικότητας εφαρμόζονται σήμερα αυθαίρετα και μη λαμβάνοντας υπόψη τις απαιτήσεις του εκάστοτε οργανωσιακού πλαισίου στο οποίο λειτουργεί ή θα λειτουργεί το σύστημα. Στην παρούσα εργασία ισχυριζόμαστε ότι είναι απαραίτητο να αναπτυχθούν

μέθοδοι ανάλυσης και σχεδίασης απαιτήσεων ιδιωτικότητας προκειμένου να ανιχνεύονται οι εξαρτώμενες από το πλαίσιο απαιτήσεις ιδιωτικότητας και να επιλέγονται τα κατάλληλα τεχνικά, οργανωσιακά και διαδικαστικά αντίμετρα για την υλοποίηση συστημάτων ηλεκτρονικής διακυβέρνησης που διαφυλάσσουν την ιδιωτικότητα που θα προσφέρουν ηλεκτρονικές υπηρεσίες που εμπιστεύονται οι χρήστες.

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*

Στο χώρο των πληροφοριακών συστημάτων η συμμόρφωση με πρότυπα είναι ιδιαίτερα σημαντική για ποικίλους λόγους, μεταξύ των οποίων είναι η διαλειτουργικότητα, η πιστοποίηση κτλ. Ενώ οι πρόσφατες επισκοπήσεις υποδεικνύουν ότι η αποδοχή διεθνών προτύπων ασφάλειας αυξάνεται και ότι οι οργανισμοί συμμορφώνονται με αυτά διαρκώς αυξάνεται, παρόλα αυτά η πλειοψηφία των οργανισμών εξακολουθεί να μη γνωρίζει τα κυριότερα πρότυπα ασφάλειας ή να μη εφαρμόζει στο σύνολό τους. Η παρούσα εργασία έχει ως σκοπό να διευκολύνει την ενημερότητα των επαγγελματιών ασφάλειας για τα διεθνή πρότυπα ασφάλειας και να συνεισφέρει στην εφαρμογή τους μέσα από ένα πλαίσιο ασφάλειας που προτείνεται. Το προτεινόμενο πλαίσιο ασφάλειας περιλαμβάνει τέσσερα επίπεδα. Για την επεξήγηση των διαφορετικών επιπέδων και την παρουσίαση της εφαρμοσιμότητάς του χρησιμοποιούμε ως μελέτη περίπτωσης ένα πληροφοριακό σύστημα μισθοδοσίας και συντάξεων.

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*

Στην παρούσα εργασία διερευνάται ο τρόπος με τον οποίο η διαδικασία της ενημερότητας ασφάλειας συνδέεται με το ευρύτερο πλαίσιο διοίκησης ασφάλειας πληροφοριακών συστημάτων (ΠΣ) το οποίο εξυπηρετεί. Μέχρι σήμερα, η διαμόρφωση πρωτοβουλιών ενημερότητας ασφάλειας αγνοεί την ιδιαίτερα σημαντική συσχέτιση με το συνολικό πλαίσιο διοίκησης ασφάλειας, και αντίστροφα. Σε αυτή την εργασία τεκμηριώνεται πώς οι δύο διεργασίες μπορούν να ευθυγραμμιστούν, ώστε να διασφαλίζεται ότι οι δραστηριότητες ενημερότητας εξυπηρετούν τη στρατηγική διοίκησης ασφάλειας, αλλά και ότι η διοίκηση

ασφάλειας αξιοποιεί τα οφέλη από τις ενέργειες ενημερότητας. Αυτό πραγματοποιείται μέσα από την ανάλυση των δύο διεργασιών με χρήση ενός πλαισίου ανάλυσης οργανωσιακών διαδικασιών και στη συνέχεια με τη ανάλυση των αναδεικνυόμενων αλληλεπιδράσεων. Η αναγνώριση των αλληλεπιδράσεων αυτών έχει ως αποτέλεσμα να καθίσταται δυνατή η τοποθέτηση της ενημερότητας ασφάλειας στο ευρύτερο πλαίσιο διοίκησης ασφάλειας ΠΣ, σε αντίθεση με την αντιμετώπισή της ως έναν μεμονωμένο μηχανισμό ασφάλειας.

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*

Οι σχεδιαστές πληροφοριακών συστημάτων (ΠΣ) γνωρίζουν την αναγκαιότητα αμοιβαίας κατανόησης και συμφωνίας λειτουργικών και μη λειτουργικών προδιαγραφών ΠΣ. Η αναγκαιότητα αυτή αφορά τόσο το σχεδιασμό «ορθών» συστημάτων όσο και τη διαλειτουργικότητα με άλλα συστήματα. Ενδεικτικό παράδειγμα αυτής της αναγκαιότητας αποτελεί η ασφάλεια πληροφοριών. Στην περίπτωση που οι απαιτήσεις ασφάλειας δε γίνονται αντιληπτές με τον ίδιο τρόπο από όλα τα εμπλεκόμενα μέλη και οι μηχανισμοί ασφάλειας που θα υλοποιηθούν δεν ικανοποιούν διεθνώς αποδεκτούς κανόνες και πρακτικές, τότε το σύστημα που θα σχεδιαστεί είναι πιθανό να μην θα ικανοποιεί το επιθυμητό επίπεδο ασφάλειας και θα είναι δύσκολο να διαλειτουργήσει ασφαλώς με άλλα ΠΣ. Είναι, λοιπόν, σαφής η συνεισφορά των διεθνών προτύπων για το σχεδιασμό και την υλοποίησης μηχανισμών ασφάλειας. Στην παρούσα εργασία παρουσιάζεται μία επισκόπηση των προτύπων διοίκησης ασφάλειας πληροφοριών που έχουν δημοσιευτεί από τον Διεθνή Οργανισμό Προτυποποίησης (International Organization for Standardization) και πραγματοποιείται ταξινόμησή τους σύμφωνα με τις έντεκα ενότητες μέτρων ασφάλειας του ISO/IEC 27001:2005. Η ανάλυση αυτή διευκολύνει τους επαγγελματίες ασφάλειας στην αποτελεσματική διοίκηση ασφάλειας πληροφοριών, καθώς η παρεχόμενη ταξινόμηση των προτύπων μπορεί να συνεισφέρει στην ενημέρωση και κατανόηση της πληθώρας προτύπων ασφάλειας που υπάρχουν.

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

Παρά το γεγονός ότι υπάρχει ανάγκη έρευνας στο χώρο των ψυχικών ασθενειών, η σχετική έρευνα παρεμποδίζεται από τα ζητήματα εμπιστευτικότητας και προστασίας της ιδιωτικότητας που αφορούν τους ιατρικούς φακέλους. Η συγκέντρωση του ιατρικού ιστορικού ασθενών που πάσχουν από την ίδια ασθένεια σε κεντρικές βάσεις δεδομένων όπου μπορούν να εφαρμοστούν προηγμένες τεχνικές εξόρυξης γνώσης θα ήταν ιδιαίτερα πολύτιμες για τους ερευνητές. Η μεγαλύτερη πρόκληση είναι η ανωνυμοποίηση των δεδομένων, ώστε να ικανοποιούνται οι νομικές και ηθικές απαιτήσεις, ενώ παράλληλα να διατηρούνται οι κρίσιμες ιατρικές πληροφορίες. Στην παρούσα εργασία προτείνεται ένα μοντέλο δημιουργία κεντρικού αποθετηρίου ανωνυμοποιημένων δεδομένων ασθενών που πάσχουν από διπολική διαταραχή. Η γνώση αυτή τροφοδοτεί ένα ευφυές σύστημα που διευκολύνει και καθοδηγεί τους κλινικούς γιατρούς στη διαχείριση ασθενών. Οι απαιτήσεις ασφάλειας ικανοποιούνται από την εφαρμογή ελέγχου πρόσβασης με μηχανισμούς ελέγχου πρόσβασης βάσει ρόλων (Role Based Access Control).

C.1 <u>Tsohou A.,</u> *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.*

Η οργανωσιακή κουλτούρα επηρεάζει τον τρόπο με τον οποίο α) γίνεται αντιληπτή η ασφάλεια πληροφοριών, β) εφαρμόζονται τα μέτρα ασφάλειας, και γ) αντιδρούν τα μέλη του οργανισμού στις αλλαγές κουλτούρας που απορρέουν από ένα νέο πρόγραμμα ασφάλειας. Στην περίπτωση εξωτερικής ανάθεσης της διοίκησης ασφάλειας πληροφοριακών συστημάτων είναι πιθανό να προκύψουν ζητήματα εξαιτίας της ανομοιότητας κουλτούρας ανάμεσα στον οργανισμό και τον εξωτερικό πάροχο, όπως για παράδειγμα σύγκρουση μεταξύ των μέτρων ασφάλειας που θέτει σε εφαρμογή ο πάροχος και τις εσωτερικές πολιτικές του οργανισμού. Στην παρούσα εργασία προτείνεται ένα εννοιολογικό πλαίσιο για την αναγνώριση και διαχείριση της ανομοιότητας κουλτούρας από τον οργανισμό στην περίπτωση εξωτερικής ανάθεσης της διοίκησης ασφάλειας πληροφοριακών συστημάτων.