Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2013 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

6-18-2013

Building a Taxonomy for Cybercrimes

Lesley Land
The University of New South Wales, l.land@unsw.edu.au

Stephen Smith
Macquarie University, stephen.smith@mq.edu.au

Vincent Pang
The University of New South Wales, Vincent.Pang@unsw.edu.au

BUILDING A TAXONOMY FOR CYBERCRIMES

Lesley Land, Security eCommerce Assurance Research Group, School of Information Systems, Technology and Management, Australian School of Business, The University of New South Wales, L.Land@unsw.edu.au

Stephen Smith, Department of Computing, Macquarie University, Stephen.Smith@mq.edu.au

Vincent Pang, Security eCommerce Assurance Research Group, Australian School of Business, The University of New South Wales, Vincent.Pang@unsw.edu.au

Abstract

Cybercrime incurs an estimate of $110 billion per annum globally (Norton Cybercrime Report 2012). This excludes the non-financial impact. The combined impact presents an enormous problem worldwide, from the point of view of overall management (detection, monitoring and prevention). While there are lists/categories of cybercrimes published in books, government websites, security and crime-related websites, these categories were constructed for different purposes. Moreover, they are not comprehensive, nor are they rigorously developed using empirical data. Their similarities and differences have not been elucidated, accounted for, and reconciled, and we are not confident that all cybercrimes can be classified using existing taxonomies. Creating a single comprehensive taxonomy on cybercrimes has a number of benefits. This paper first summarises the background on "taxonomies", existing taxonomies that have been constructed in Information Systems, and potential benefits of such a taxonomy. It then proposes a methodology for developing and validating a cybercrime taxonomy, and discusses the next steps for this project.

Keywords: Cybercrimes, Taxonomy, Classification, Methodology, Fraud

1 INTRODUCTION

In the film *Dirty Harry*, police inspector Harry Callahan (played by Clint Eastwood) uses "the most powerful handgun in the world" to catch and stop criminals. The arrival of modern information and communication technologies (ICTs), particularly the Internet and mobile technologies, has shifted how crimes are committed. In recent times, there is an increasing amount of technology-enabled related crimes and cybercrimes, which are crimes committed on the Internet and cyberspace. There is also a shift and an increase in the number of white-collar criminals, such as cybercrimes and identity crimes, as these criminals are more educated, IT savvy, and have the know how to use technologies and the Internet to commit crimes. Callahan's "most powerful handgun in the world" is ineffective when dealing with crimes committed in the virtual world.

Cybercrime is a worldwide phenomenon, escalating globally (Kshetri 2009). Law enforcement authorities recognise it as a serious and escalating problem both domestically and internationally. Government and organisations in Australia, estimate financial losses in 2012 $2.0 billion in cybercrime (Norton Cybercrime Report 2012) and $1.4 billion in identity crime (Australian Bureau of Statistics 2012). This does not include the non-financial (e.g. psychological, emotional, and reputational) harm and damage these crimes can cause to individuals, families, societies, communities, businesses, government, and countries as a whole. As technologies constantly change, cybercrimes and identity crimes continue to grow. Unfortunately, law enforcement is lacking behind in understanding how some of these technology-enabled crimes are committed; hence finding it difficult to properly address these problems as they continue to escalate.

As a first step to understand and curb these criminal activities occurring in cyberspace, law enforcement and other government agencies have to find new initiatives and strategies (some of these possibly facilitated by powerful technologies) and develop new laws and policies to implement them. For instance, on the 3rd November 2011, NSW (New South Wales) Police Force in Australia launched a new Fraud and Cybercrime Squad, specifically to target technology-enabled and fraud crimes, and cybercrimes, including identity theft, credit card fraud, the Internet and electronic fraud. Countries, such as Singapore (Guo 2011), Netherlands (Netherlands Ministry of Security and Justice 2011), the United States (Gonzale and Majoras 2007), and Australia (Packham 2013) are planning or have already set up National Cyber Security Centre to counter cyber security threats. The European Union (EU) completed its feasibility study in February 2012, to build a European Cybercrime Centre (ECC) for its 27 member states (Robinson et al. 2012).

While there are lists/categories of cybercrimes or technology-enabled crimes published in books (Clough 2010), government websites (e.g. http://www.scamwatch.gov.au, http://www.scamnet.wa.gov.au), and on the security and crime-related websites, these lists classify cybercrimes and technology-enabled crimes to fit their own purposes. These categories are not comprehensive and are not rigorously developed using empirical data. Moreover, the similarities and differences have not been elucidated, accounted for, and reconciled, and we are not confident that all cybercrimes can be classified using existing taxonomies. Creating a single taxonomy on cybercrimes and technology-enabled crimes has a number of benefits. Firstly, it will enhance the information sharing between the IT security centres and law enforcement agencies within and between countries. Multi-level information sharing through sense-making has been hailed to be important for combating frauds (Jamieson et al. 2009). Secondly, utilising a single common taxonomy will further enhance how police forces, government departments and agencies, and organisations develop security and training policies and prevention procedures; implement and administer compliance and regulatory issues in IS security. For example, policies can address how organisations can better structure teams and allocate limited resources to better manage different types of crimes. Initiatives such as those proposed by Rusch (2011) to develop an international legal regime to combat identity related crime, will also benefit from a common taxonomy which will form a common point of reference for all stakeholders across different countries.

This paper presents a major effort to develop a methodology to construct a single common taxonomy of cybercrimes, which has many advantages, such as facilitating information sharing, and improving security policies. We have adapted and improved the approach of Nickerson et al. (2013) to develop a methodology for constructing a cybercrime taxonomy.

To achieve this end, we will in section 2 define and clarify basic terminologies related to the term "taxonomy", followed by a brief summary of the existing taxonomies that have been constructed in IS. In section 3, we first justify the need for building cybercrime taxonomies and then describe the approach for constructing a single comprehensive cybercrime taxonomy. Lastly, we will explain the current status and next steps for this project.

2 TAXONOMY

Taxonomy is commonly used in biological science to describe, identify and classify organisms. In social science, "*taxonomy* can refer to both the *process* and the *end result*" (Bailey 1994, p. 6). In terms of the taxonomy creation *process*, Simpson (1961), Sneath and Sokal (1973), and Bailey (1994) suggest that "taxonomy" is the theoretical study of classification and identification. As for the *end result*, Bailey (1994) suggests that a "typology" (common in the social sciences) is drawn from *conceptual* classification, while a "taxonomy" (widely used in the biological sciences) is drawn from *empirical* classification (Bailey 1994). This distinction between "typology" and "taxonomy" highlights the importance of empirical validation during the taxonomy creation process. However, Nickerson et al. (2013) could not find in the IS literature any correlation between the development method used and the applying of the term taxonomy and typology as suggested. Thus, the terminologies 'taxonomy' and 'typology' are sometimes used interchangeably. To avoid confusion, we will only refer to 'taxonomy' for both process and end result in this paper.

When reviewing the IS literature, we found diverse and substantial publications on different taxonomies. Taxonomies are built for different purposes and across different areas in the IS discipline. A variety of taxonomies have been constructed to describe and classify complex outcomes (see Graham et al. 1996). We reviewed the "basket of eight" journals as these are recognised top journals of the IS discipline (see http://home.aisnet.org/displaycommon.cfm?an=1&subarticlenbr=346). We search these journals using the keywords 'taxonomy' and 'typology'. Examples of these, their representational formats, and their publication sources are summarised in Table 1.

As Table 1 shows, there are a variety of ways to present taxonomies (i.e. the outputs). There is no rule of thumb of how a taxonomy should be constructed and presented in the IS discipline. For example, a taxonomy output can be a two-dimensional table, a conceptual model or a hierarchy diagram. In addition, the literature also presents a variety of justifications for developing taxonomy in IS research; these include:

(a) To advance current knowledge of a particular topic in IS (Larsen 2003; Rivard et al. 2012; Williams et al. 2008; McKinney and Yoos 2010; Nickerson et al. 2013).

(b) To determine related concepts to the current concept under study (Larsen 2003, p.200).

(c) To assist in theory building (Bapna et al. 2004; Nickerson et al. 2013).

(d) To identify concepts in order to help develop a model and address the research problem (Larsen 2003; Williams et al. 2008).

(e) To improve the overall understanding of a particular topic in practice (Larsen 2003; McKelvey 1978; Rivard et al. 2012; Williams et al. 2008; McKinney and Yoos 2010).

(f) To check that authors submitting research papers have been comprehensive in their approach (Larsen 2003, p.201).

Taxonomy Output	Taxonomy	Reference
Two-dimensional table	A taxonomy utilising user type and type of system support provided to the user	Doke et al. 1994
	A taxonomy of multimedia information systems	Dustdar et al. 1997
	A taxonomy of information technology structure and its relationship to organizational structure	Fiedler et al. 1996
	A taxonomy of information	McKinney and Yoos 2010
	A taxonomy of mobile applications	Nickerson et al. 2013
	A taxonomy of digital service design	Williams et al. 2008
Multiple number of two dimensional tables	A taxonomy for evaluating investments in information systems	Irani and Love 2000
	A taxonomy of information technology implementers' responses to user resistance	Rivard et al. 2012
A sequence ladder diagram	A taxonomy of information systems applications	Farbey et al. 1995
An 'ideal' dimensional table	A taxonomy of knowledge management strategies	Earl 2001
A dimensional diagram and a two-dimensional table	A taxonomy of electronic commerce implementations	Graham et al. 1996
A dimensional diagram	A taxonomy of organizational mechanisms	Nambisan et al. 1999
	A taxonomy of perceived information system development (ISD) political processes	Sabherwa and Grover 2010
A conceptual model	A taxonomy of bidder behaviour and their consequences	Bapna et al. 2004
	A taxonomy of trust measures for e-Commerce	McKnight et al. 2002
A hierarchy diagram	A taxonomy of cues to error detection (CERD) in speech recognition output	Lina et al. 2006
	A taxonomy of information privacy-protective responses	Son and Kim 2008

Table 1 Examples of Taxonomies Published in the IS Literature

Therefore, taxonomies, as shown, are important for IS research when we consider their contributions towards conceptualisation, theorising, and improving the overall understanding the domain each represents. However, there are no systematic approaches to these different outputs of taxonomies. A methodology should be able to reconstruct the taxonomy when something has changed, such as introducing a new technology (e.g. iPad). Thus, we need to develop a methodology to address this problem.

Before deliberating the proposed methodology in next section, we first discuss and present the specific benefits of a taxonomy for classifying cybercrimes.

2.1 Cybercrime Taxonomy

Cybercrime is becoming one of the major threats to citizens, commerce and governments globally; this trend will continue as cybercrime becomes a growing industry over the coming decades, as criminals can perpetrate activities globally, yet seek refuge behind international borders. Governments also realise the potential financial, political and ideological gains in the exploitation of cybercrime activities. There is growing concern as cybercriminal activities are reported on a daily basis (Karena 2012).

The Australian Crime Commission (2011) highlighted that an increase in social networking sites pose a significant threat to people as cybercriminals undertake 'grooming' activities to gain personal information from people with weak or careless security practices. The distribution of networks and the proliferation of mobile devices will also accelerate the risk of cyber threats. Although education and awareness campaigns are useful aids in combating cybercrime, it is nonetheless young people that still largely exhibit poor security behaviours (Jamieson 2008).

Over the coming years, cybercrime activities will become an even greater threat to citizens, governments and industry globally. Cybercrime methods are already changing to many different forms (both physical and virtual); from traditional web hacking, malware, defacement and denial of service (DOS), to financial fraud (identity theft), phishing, bullying, botnets, various internet based frauds and scams, criminal profiteering, international money laundering, exploitation of children and a vehicle for international terrorism. The exponential growth of electronic interconnections between people via broadband and wireless networks creates the opportunity for an exponential growth in cyber threats. We cannot predict the change in technology for the next five years, nor can we expect to predict how criminals may use these systems for unlawful gains. A Senate Select Committee in 2009 heard that a network such as the NBN (National Broadband Network) "has the potential to be a force-multiplier for cybercrime attacks directed at Australian networks and information systems because cyber criminals are attracted to attack, compromise and use systems with high speed broadband access. Compromised computer systems with high speed access significantly increase the impact and effectiveness of most internet based attacks."

We identify a number of benefits for constructing a taxonomy specifically for classifying cybercrimes. Primarily, stakeholders such as government agencies (e.g. law enforcement), international crime fighting authorities (e.g. Interpol), organisations with high security concerns (e.g. financial institutions, insurance companies), and researchers will benefit from a taxonomy for classifying cybercrimes in the following ways:

1. For calculating the financial cost of different cybercrimes to be used by law enforcement, insurance companies, government agencies, or other organisations.
2. For employing different data analysis and business intelligent techniques (e.g. cluster and discriminant analysis, predictive modelling, data mining and drilling) to study and understand the existing and emerging trends of cybercrimes.
3. For the allocation of resources to combat cybercrimes at organisational, national and international levels.
4. For developing research agendas in this domain, including the development of theories to explain the complex phenomena surrounding cybercrimes.

To construct a taxonomy for cybercrimes, we first need to clarify the possible complexity of cyber or cyber-related crimes. We illustrate the complexity of a cyber-related crime using the "Nigerian (419) Scam" which has been used as an exemplar (Stabek et al. 2009). The "Nigerian Scam" is described as an unsolicited email (or fax or any other methods of delivery via the internet) detailing an unfortunate story of the sender (i.e. scammer) and (s)he has a fortune, but (s)he needs the victim to supply an overseas bank account to transfer the money or request a small amount of money for a short term. In return for the victim's assistance, the scammer promises to share some of the fortune with the victim, say 10% for the total amount of wealth. There are variations to this scam, and sometimes different terminologies have been used to refer to the same scam. For example, the "Nigerian Scam" is also known as the "Letter Scam" because the scam was originally sent by post instead of an email. Other terms used to describe the same or similar scam include the "West African Fraud", "419 Scam", and "Advance Fee Fraud" (Stabek et al. 2009). The "419 Scam" makes a reference to the article number of the Nigerian Criminal Code for these types of crimes (Stabek et al. 2009). "Advance Fee Fraud" is the general term given to all fraud-related crimes covering scams such as "Nigerian Scam", which requires a fee to be paid in advance by the victim (Stabek et al. 2009).

Varying terminologies (and their associated definitions) which refer to the same or similar crime can lead to ambiguities, confusion and a reduction of effectiveness when addressing the crime from multiple perspectives (e.g. technical and legal). In particular, metric overlaps can cause bias on crime management information systems (Jamieson et al 2012). Moreover, the "Nigerian Scam" and many other cyber and cyber-related crimes can lead to other crimes such as identity theft, credit card fraud, insurance fraud, internet fraud, or other scams (see http://www.spamlaws.com/nigerian-scams.html). A taxonomy will therefore help to address these issues by clarifying the terminologies and their definitions, and organise them according to their similarities (Bailey 1994). Drawing on the existing literature, we propose a methodology to construct a cybercrime taxonomy. We consider it as a first step towards the initiative to combat the problems of cybercrimes experienced worldwide.

3 METHODOLOGY

Apart from the unstandardised ways of representing a taxonomy, the methodologies used to construct and develop a taxonomy are also varied in terms of formality, rigour, and empirical validation. Most of the methodologies used in the IS literature are *ad-hoc* as described by Nickerson et al. (2013). Others have adopted a methodology for the development of their taxonomy. For instance, Larsen (2003) adopted a seven-step process to develop a taxonomy. Bapna et al. (2004) developed their taxonomy using a more conventional research methodology, by first constructing a conceptual model with variables and constructs. As for the data used in the construction of the taxonomy, the most common data collection approach is the use of case studies (e.g. Dustdar et al. 1997; Earl 2001). Others use meta-analysis on published papers to build a taxonomy (e.g. Larsen 2003; McKinney and Yoos 2010; McKnight et al. 2002; Rivard et al. 2012). Others collect data and use cluster analysis to analyse data in order to construct their taxonomies (e.g. Fiedler et al. 1996; Balijepally et al. 2011).

For maintaining a taxonomy, the whole process of taxonomy construction will normally start from the beginning. Technologies have been constantly changing, so we expect the levels of cybercrime will continue to increase, and the methods to commit the crime will continue to vary. Thus, we need to propose a methodology which allows the taxonomy to be modified iteratively beyond the initial stage of construction, in order to reflect the emerging patterns and crime types.

Even though Nickerson et al.'s (2013) methodology is useful as a generic approach, we found there are a number of restrictions and constraints which do not fit our requirements in the long term. Nevertheless it is the closest fit to our objectives. In addition, they also provide guidelines for the process of taxonomy construction. Consequently, our methodology will be adapted from Nickerson et al.'s methodology, using a number of key principles we deem important:

(a) Bailey's (1984) three-level indicator model is used as a foundation of our methodology as "it offers alternative approaches that involve both conceptualization/deduction and empiricism/induction" (Nickerson et al. 2013, p.9).
(b) We will adopt a design science research paradigm which is built on 'how to do' theoretical foundation (March and Smith 1995; Simon 1996). As with software development, applications need to be tested, the 'generate/test cycle' in the paradigm (Hevner et al 2004) ensures that the taxonomy goes through the testing phase. Thus, testing is performed as part of the construction of taxonomy within each iteration cycle.
(c) The involvement of stakeholders is an essential part of the taxonomy development in order to maximise acceptance of the taxonomy outcome.
(d) The taxonomy will be built conceptually (using the existing literature and knowledge, including key definitions of terms), and empirically (using real data drawn from cybercrime cases data).
(e) The taxonomy is revised / refined / maintained through multiple iterations. When a new case arises, the taxonomy manager (who manages taxonomy) review if the new case can be handled by the existing taxonomy. Otherwise, taxonomy is reconstructed or refined to address the new case, and stakeholders will validate the revised taxonomy.

We believe that our proposed methodology will lead to the construction of a practical and useful taxonomy, which is concise, robust, comprehensive, extendable and explanatory. Our proposed methodology is shown in Figure 2:

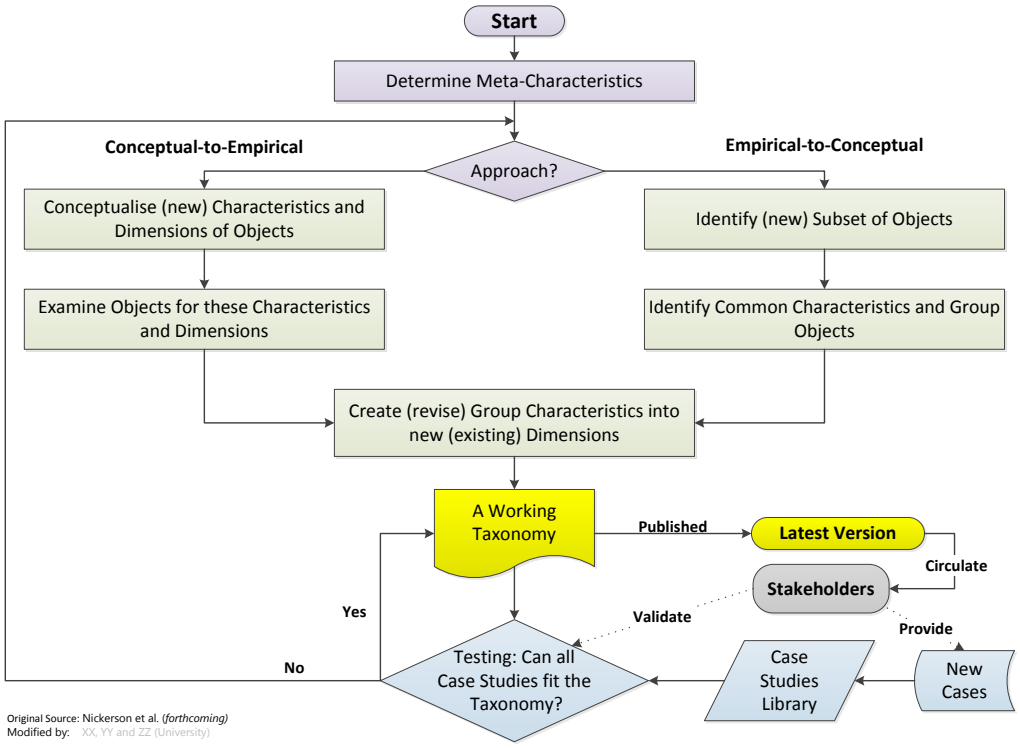

Figure 2. Proposed Methodology for Constructing a Cybercrime Taxonomy

Our arguments for making key changes to that of Nickerson et al.'s (2013) methodology are summarised as follow:

(a) Firstly, we introduce a library of case studies to construct the cybercrime taxonomy. Majority of the taxonomies published in IS discipline are based on either case studies or case studies from secondary sources. The strength of having a library is that we can add new cases to the library as they arise. The cases can either be empirical or conceptual.

(b) The working taxonomy (to be discussed in (c) below) is constructed from case studies recorded in the library. Future changes to the working taxonomy which emerge as a result of new technologies, and/or new crimes resulting from new methods/mechanisms conceived by perpetrators, can be incorporated to the library where a revised working taxonomy can be constructed. We delete the 'ending conditions' from the original Nickerson et al.'s (2013) framework and replace it with the testing phase (to be discussed in (d)) to ensure that the taxonomy can be validated using the case studies from the library. Overall, the iterative and multi-stage approach of our proposed methodology allows the construction of a taxonomy to be prioritised and to be built incrementally, according to the library resources, and the level of stakeholder involvement.

(c) Instead of expecting that a final version of taxonomy be, we suggest that incremental working copies of the taxonomy can be created to reflect changes in the cybercrime environment. The latest version of a working taxonomy can be published at any time. This is like an IT application development where an application is deployed when it is 'ready', and any future enhancements can be released during post implementation. This follows the design science philosophy where building something useful is preferred than looking for a perfect and optimal solution (Hevner et al. 2004; Nickerson et al. 2013).

(d) A testing phase is added specifically to test if all case studies in the library can accommodate the working taxonomy. Any failed case (i.e. the case cannot be classified using the existing working version) will then need to be re-analysed from the top of the loop. That is, it will need to be revised and re-tested again. Testing phase is a key step of the design evaluation method in the design science paradigm (Hevner et al. 2004).

Having discussed the modifications, we now briefly explain each step of Figure 2:

(a) As in the original methodology by Nickerson et al. (2013), our first step is to identify the meta-characteristics, which are the characteristics required for the objective of the taxonomy. The objective is based on the requirements of the users (stakeholders) who will use the taxonomy to perform their job function.

(b) The next step is the selection of an approach: either a conceptual approach or an empirical approach. In our study, we are likely to first adopt a conceptual approach as we, the researchers, have prior knowledge of the research domain, namely cybercrimes. An initial skeletal taxonomy will be constructed from the existing literature prior to the testing phase. It is expected that the taxonomy will be revised using an empirical approach as more cases populate the library, which helps to gain a better understanding of the taxonomy. However, in another instance where the library cases are well populated and the creators have little prior knowledge, the initial taxonomy could be totally (empirically) constructed from the library.

(c) In this step, we conceptualise and identify the characteristics and dimensions of objects (cybercrime types). These help to construct the basic (high level) framework of the taxonomy. Any newly identified characteristics are grouped into dimensions, which in turn, will modify and enhance the taxonomy.

(d) Stakeholder involvement is the stage whereby stakeholders (either individually or collectively) provide feedback about the working version. Occasionally, some negotiation may be necessary at that point to come to a consensus on any proposed changes.

(e) In this stage, a working taxonomy, which can be published as the latest version rather than a final taxonomy is constructed. The control of the taxonomy must be determined by the owner(s) of the taxonomy. The ownership should be determined and agreed upon by all stakeholders.

(f) The initial library will be originally built from cases in the public domain such as newspapers and government papers. These cases will be used to build the initial taxonomy and categorised using the conceptual approach. Real criminal cases will then be used to populate the library and test to ensure a rigorous taxonomy is constructed. In the future, simulation cases can be added to the library to test the taxonomy.

4 CONCLUSION AND NEXT STEP

A taxonomy for cybercrime is a valuable tool for identifying and classifying patterns of cybercrimes. This paper summarised different approaches to creating a taxonomy. Traditionally taxonomies are created from a conceptual model with variables and constructs, whereas we have proposed an approach which adapts from the approach proposed by Nickerson et al. (2013). Our approach adopts a design science research paradigm which is built on 'how to do' theoretical foundation which accommodates changes in technologies and new cybercrimes.

Our investigation has highlighted the need for a cybercrime taxonomy. We have proposed a methodology which supports both its development and maintenance which are crucial for a world of changing technologies and crimes. We believe that the ideas and concepts proposed in this paper will lead to the construction of a practical and useful taxonomy, which is concise, robust, comprehensive, extendable and explanatory. This will lead to the creation a robust cybercrime taxonomy that can be used by academics and practitioners alike.

5 REFERENCES

Australian Bureau of Statistics (2012). ABS Personal Fraud, 2010-2011. Retrieved 3 October, 2012, from http://www.abs.gov.au/ausstats/abs@.nsf/mediareleasesbytitle/B634CE9C7619C801CA25747400263E7E?OpenDocument

Australian Crime Commission, (2011). Cyber Crime. Retrieved 1 April, 2011, from http://www.crimecommission.gov.au/publications/crime-profile-series-fact-sheet/cyber-crime.

Bailey, K.D. (1994). *Typologies and Taxonomies: An Introduction to Classification Techniques (Quantitative Applications in the Social Sciences)* Sage Publications, Thousand Oaks, the United States of America.

Balijepally, V.G., Mangalaraj, G., and Iyengar, K. (2011). Are We Wielding this Hammer Correctly? A Reflective Review of the Application of Cluster Analysis in Information Systems Research. *Journal of the Association for Information Systems*, 12 (5), 375-413.

Bapna, R., Goes, P., Gupta, A., and Jin, Y. (2004). User Heterogeneity and its impact on Electronic Auction Market Design: An Empirical Exploration. *MIS Quarterly*, 28 (1), 21-43.

Clough, J. (2010). *Principles of Cybercrime*, Cambridge University Press.

Dietz, G., and Juhrisch, M. (2012). Negotiating Language Barriers - A Methodology for Cross-Organisational Conceptual Modelling. *European Journal of Information Systems*, 21 (3), 229-254.

Doke, E.R., and Barrier, T. (1994). An Assessment of Information Systems Taxonomies: Time to be Re-Evaluate? *Journal of Information Technology*, 9 (2), p.149.

Doty, H.D., and Glick, W.H. (1994). Typologies as A Unique Form of Theory Building: Toward Improved Understanding and Modeling. *Academy of Management Review*, 19 (2), 230-251.

Dustdar, S., and Angelides, M.C. (1997). Organizational impacts of Multimedia Information Systems. *Journal of Information Technology*, 12 (1), 33-43.

Earl, M. (2001). Knowledge Management Strategies: Toward a Taxonomy. *Journal of Management Information Systems*, 18 (1), 215-233.

Farbey, B., Land, F.F., and Targett, D. (1995). A Taxonomy of Information Systems Applications: The Benefits' Evaluation Ladder. *European Journal of Information Systems*, 4 (1), 41-41.

Fiedler, K.D., Grover, V., and Teng, J.T.C. (1996). An Empirically Derived Taxonomy of Information Technology Structure and Its Relationship to Organizational Structure. *Journal of Management Information Systems*, 13 (1), 9-34.

Gonzales, A.R., and Majoras, D.P. (2007). Combating Identity Theft - A Strategic Plan, A.G.a.F.T. Commission (ed.).

Graham, I., Spinardi, G., and Williams, R. (1996). Diversity in the Emergence of Electronic Commerce. *Journal of Information Technology*, 11 (2), 161-172.

Guo, X. (2011). Singapore to set up National Cyber Security Centre, in: *AsiaOne News*.

Hevner, A.R., March, S.T., Park, J., and Ram, S. (2004). Design Science In Information Systems Research. *MIS Quarterly*, 28 (1), 75-105.

Irani, Z., and Love, P.E.D. (2000). The Propagation of Technology Management Taxonomies for Evaluating Investments in Information Systems. *Journal of Management Information Systems*, 17 (3), 161-177.

Kshetri, N. (2009). Positive Externality, Increasing Returns, and the Rise in Cybercrimes, in: *Commun. ACM*, 52 (12) 141-144.

Larsen, K.R.T. (2003). A Taxonomy of Antecedents of Information Systems Success: Variable Analysis Studies. *Journal of Management Information Systems*, 20 (2), 169-246.

Lina, Z., Yongmei, S., Dongsong, Z., and Sears, A. (2006). Discovering Cues to Error Detection in Speech Recognition Output: A User-Centered Approach. *Journal of Management Information Systems*, 22 (4), 237-270.

March, S.T., and Smith, G.F. (1995). Design and Natural Science Research on Information Technology. *Decision Support Systems*, 15 (4), 251-266.

McKelvey, B. (1978). Organizational Systematics: Taxonomic Lessons from Biology. *Management Science*, 24 (13), 1428-1440.
McKinney Jr, E.H., and Yoos Ii, C.J. (2010). Information about Information: A Taxonomy of Views. *MIS Quarterly*, 34 (2), 329-A325.
McKnight, D.H., Choudhury, V., and Kacmar, C. (2002). Developing and Validating Trust Measures for e-Commerce: An Integrative Typology. *Information Systems Research*, 13 (3), 334-359.
Nambisan, S., Agarwal, R., and Tanniru, M. (1999). Organizational Mechanisms for Enhancing User Innovation in Information Technology. *MIS Quarterly*, 23 (3), 365-395.
Nickerson, R.C., Varshney, U., and Muntermann, J. (2013). A Method for Taxonomy Development and its Application in Information Systems. *European Journal of Information Systems*, 22 (3), 336-359.
Netherlands Ministry of Security and Justice. (2012). National Cyber Security Strategy (Netherlands).
Norton Cybercrime Report. (2012) *Consumer Cybercrime Estimated at $110 Billion Annually*, Retrieved 3 October, 2012, http://www.symantec.com/about/news/release/article.jsp?prid=20120905_02
New South Wales Police, (2012). New Fraud and Cybercrime Squad Launched, Police.
Packham, B. (2013). Julia Gillard announces Cyber Security Centre, Warning a Long Fight Lies Ahead, in: *The Australian*.
Rivard, S., and Lapointe, L. (2012). Information Technology Implementers' Responses to User Resistance: Nature and Effects. *MIS Quarterly*, 36 (3), 897-920 (plus A891-A895).
Robinson, N., Disley, E., Potoglou, D., Reding, A., Culley, D., Penny, M., Botterman, M., Carpenter, G., Blackman, C., and Millard, J. (2012). Feasibility study for a European Cybercrime Centre. Retrieved 1 February 2012, from http://www.rand.org/pubs/technical_reports/TR1218.html.
Sabherwa, R., and Grover, V. (2010). A Taxonomy of Political Processes in Systems Development. *Information Systems Journal*, 20 (5), 419-447.
Simon, H.A. (1996). *The Sciences of the Artificial* (3rd ed.), MIT Press, Cambridge, MA.
Simpson, G.G. (1961). *Principles of Animal Taxonomy*, Columbia University Press, New York.
Sokal, R.R., and Sneath, P.H.A. (1973). *Numerical Taxonomy*, Freeman, San Francisco.
Son, J.-Y., and Kim, S.S. (2008). Internet Users' Information Privacy-Protective Responses: A Taxonomy and A Nomological Model. *MIS Quarterly*, 32 (3), 503-529.
Stabek, A., Brown, S., and Watters, P.A. (2009). The Case for a Consistent Cyberscam Classification Framework (CCCF), in: *IEEE Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing (UIC-ATC)*, Brisbane, Australia
Williams, K., Chatterjee, S., and Rossi, M. (2008). Design of Emerging Digital Services: A Taxonomy. *European Journal of Information Systems*, 17 (5), 505-517.