2007

Cyber Vulnerabilities and the Tourism Industry: Developing a Conceptual Framework

Aaron Olding
University of Tasmania, Aaron.Olding@utas.edu.au

Paul Turner
University of Tasmania, Paul.Turner@utas.edu.au

Cyber Vulnerabilities and the Tourism Industry: Developing a Conceptual Framework

Aaron Olding
School of Information Systems
University of Tasmania
Hobart, Australia
Email: Aaron.Olding@utas.edu.au

Paul Turner
School of Information Systems
University of Tasmania
Hobart, Australia
Email: Paul.Turner@utas.edu.au

Abstract

In the post 9/11 era tourism remains a growing global industry worth an estimated $2bn/day. In response to the physical threat of terrorism, governments and industry have been very active in implementing changes. However, it is noticeable as the industry becomes increasingly reliant on the Internet and other information technologies how little discussion there has been of the potential threats from cyber vulnerabilities. As research in the e-security and e-forensics domains highlights there has been a marked increase in the sophistication and targeting of cyber attacks that has the potential to threaten individual firms, destination brands or the industry as a whole.

In an effort to explore these potential vulnerabilities, examine their impacts and consider meaningful responses, this research-in-progress paper outlines a developing conceptual framework for investigating these issues in a coherent manner. This framework forms the basis for ongoing research into cyber vulnerabilities in the Tasmanian tourist industry

Keywords

Tourism, cyber vulnerabilities, conceptual framework, e-tourism.

Introduction

Responding to potential physical threats faced by tourists, tourism destinations and the tourism industry, security has become a global socio-political and business imperative in the post-September 11, 2001 era (Mansfeld, 2006). A major visible dimension of this new era has been the dramatic increase in security measures aimed at enhancing the safety of travellers. These measures include increased airport baggage screening and associated limits placed on the nature and type of items allowed in hand-luggage, as well as greater scrutiny of travellers entering and exiting countries. Despite these changing circumstances, global tourism continues to grow rapidly with more than 800 million tourist arrivals recorded in 2005 equalling an estimated $2 billion a day (UNWTO, 2006). However, recent research has confirmed that tourists increasingly consider issues of physical safety when making choices between tourist destinations (Pizam and Mansfeld, 2006).

Unsurprisingly, given the business and government focus on physical security, research on tourism and security has itself become a growth industry (Beirman, 2003; Hall & Dallen, 2003; Wilks, 2005; Pizam & Mansfeld, 2006). Noticeably, however there has been very little discussion of the potential threats posed by cyber vulnerabilities. This gap in the research literature is prevalent at the same time as the Internet and other information and communication technologies (ICTs) are becoming increasingly significant in the tourism industry (Buhalis & Deimezi, 2003). The increasing improvement and availability of ICTs has led to their use in many aspects of the tourism cycle from the digitisation of tourism services to the use of the Internet by tourists to investigate potential destinations and travel options. This digitisation means that on-line vulnerabilities that other industries face from the cyber environment are also being faced by those who operate within the tourism industry (including by tourists themselves). There is also the possibility that just as specific tourist destinations (e.g. Bali) have been specifically targeted for attack, that specific tourist industries may find themselves the target for cyber attacks.

In recent years, as research in the e-security and e-forensics domains has highlighted, there has been a marked increase in the sophistication and targeting of cyber vulnerabilities. Cyber attacks are increasingly being

launched by criminals and criminal organisations that have a vested interest in obtaining a financial gain from their on-line activities (Grimes 2005; Deloitte 2006; AusCERT 2006). In Australia according to the AusCERT 2006 Computer Crime and Security Survey, there has been a 10% increase in financially motivated attacks compared to 2005. Added to this is the increasing use of ICT technologies to undertake new types of cyber attacks (such as information level attacks). This highlights the emergence of a 'more malicious cyber environment' that while offering benefits also has inherent and growing risks. Similarly, research work in the cyber warfare domain has highlighted the dangers arising from terrorists utilising new technologies (Janczewski & Colarik, 2007). Combined these issues highlight the potential for cyber vulnerabilities within the tourism industry to be exploited in a manner that may threaten its competitiveness or worse.

In an effort to explore these potential vulnerabilities, examine their impacts and consider meaningful responses, this research-in-progress paper outlines a developing conceptual framework for investigating these issues in a coherent manner and from an industry based perspective that aims overcomes the limitations of the largely 'organisational centric' perspective that much of the current cyber security research takes. This framework forms the basis of ongoing research into cyber vulnerabilities in the Tasmanian tourist industry.

Background on Tourism and New Technology

The United Nations World Tourism Organisation (2007) uses the following definition of Tourism:

> "Tourism comprises the activities of persons travelling to and staying in places outside their usual environment for not more than one consecutive year for leisure, business and other purposes."

The tourism industry is an integral part of the global economy contributing billions of dollars to domestic economies and this holds true for Australia. Tourism in Australia alone made up approximately 8.6% of gross domestic profit in 2004-05 (Tourism Victoria, 2006) equalling an estimated $48.7 billion. With the new development of long-haul jet aircraft, such as Airbus's A380 and Boeing's 787 Dreamliners, the number of international visitors to Australia is expected to grow over the coming years as distance becomes less of an obstacle. Australia's reliance on Tourism however has implications and therefore the industry does need to be protected and continuity assured.

The tourism industry is responsible for attracting and handling domestic and international visitors and can involve a wide range of businesses. Goeldner and Richie (2003) classify the tourism industry in terms of the follow sectors:

Table 1: Tourism Industry Sector Breakdown (Goeldner and Ritchie, 2003: 122)

Travel Trade Sector.	Entertainment Sector
Accommodation Sector	Food Services Sector
Tourism Services	Adventure and Outdoor Recreation
Transportation Sector	Attraction Sector
Events Sector	

It is important to note that businesses and services can have a differing level of involvement in the tourism industry, for example a wilderness tour operator would have a greater dependence on visitors compared to a restaurant that also attracts locals. This level of involvement plays a role in a businesses ability to cope with a downturn in visitor numbers and these downturns can occur for many reasons, from seasonal adjustments to aggressive advertising pushes from competing markets. The tourism industry is one that is continually fighting to maintain and expand visitor numbers and while the strategies can differ, one factor that is having an effect (both positive and negative) is the development of information and communication technologies (ICT).

Just as other industries are embracing the use of ICT, so too is the tourism industry. The use of ICT within tourism, while a growing phenomenon, is one that is having a substantial effect on how tourism operators, visitors and governments are approaching their respective roles. An example of the effect of ICT on tourism can be seen in within the development of the Internet. According to Buhalis (2003:805) "The proliferation of the Internet, as a main stream communication media and as an info-structure for business transactions has generated a wide range of strategic implications for businesses in general". He goes on to say that the Internet (and ICTs in general) offer tourist organisations benefits towards greater "…efficiency, productivity and competitiveness" both between and within organisations. But why is this so? The reason is in the information intensiveness nature of the tourism industry (Buhalis & Deimezi, 2003).

ICTs within the tourism industry are not evenly distributed with some players embracing ICTs rapidly and others continuing to be more cautious. For example, while the airline sector has seen an explosion of on-line

booking services that allow passengers to book their tickets, pick their seats and check-in from home as well as receive SMS or email confirmations, much of the hospitality sector is still evaluating whether ICT will bring in sufficient benefit to justify the required costs in time, money and skills (Chan & Law, 2006).

As in other industry sectors the increasing diffusion of ICTs in tourism has given rise to a new catch-phrase - e-tourism. E-tourism is now used to "…reflect the digitalisation of all processes and value chains in the tourism, travel, hospitality and catering industries." (Buhalis & Deimezi, 2003:103). However, interestingly unlike other uses of the 'e' in other industry sectors, e-tourism does not refer to the use of ICT as the 'tourist destination' or 'experience' but rather as the use of ICT to enhance the effectiveness of tourism operations throughout the whole tourism supply chain (Buhalis & Deimezi, 2003). The major benefits that e-tourism offers is the ability to integrate tourism systems together and offer potential visitors new ways to explore and personalise their travel experiences (Michopoulou & Buhalis, 2006). It also aims to bring the benefits from electronic commerce into the tourism industry by taking e-commerce models and applying them to the tourism business cycle. The use of ICT in tourism has the major benefit of allowing greater interoperability between tourism organisations and thereby opening up the opportunity of meeting the challenge of improving customer value from tourism networks (Hakolahti & Kokkonen, 2006). ICTs are also being used by governments in their support for tourism through the promotion of destinations through information provision. For example, Australia (www.Australia.com) and Tasmania (www.discovertasmana.com) web-sites are being used as a way to present potential visitors with a positive image portal for a range of tourism options and services. The spread and improvement in ICT is also having a major impact in how potential tourists determine their travel locations and activities. According to Vansteenwegen and Oudheusden (2006) electronic guides and online travel planners are starting to play larger roles in travel planning activities as the level of ICT skill among users continues to grow. In fact the Internet is having the greatest effect on how potential visitors undertake tourism related activities particularly prior to travel (Kah & Vogt, 2005).

While the adoption and utilisation of ICTs by these different participants in the tourism industry (tourism providers, governments and visitors) continues to grow and offers real range of benefits, the use may also be opening up a range of new threats and weaknesses that appear little understood by the industry as it rushes into the information age.

Cyber Vulnerabilities and the New Malicious Internet Environment

The increased use and improvement in ICT has had a beneficial effect on many aspects of business and personal life however the reverse is also true. The increased reliance on ICTs means that when systems fail or are temporarily unavailable problems occur. While on one level there is now some general awareness and/or expectation regarding system reliability on the other few are prepared for or aware of how ICTs are increasingly being used to undertake criminal, illegal or inappropriate behaviours (Broucek & Turner, 2005).

ICTs are increasingly an enabler of criminal activity. ICTs can be seen as having the following benefits for the conduct of illicit activity (Savona & Mignone, 2004):

- ICT can overcome the geographic and spatial hurdles that are inherent in traditional crime.
- ICT systems are global and globally available.
- They are generally speedy and allow fast access.
- They can allow a high level of anonymity that can be difficult to break.
- These systems can have a high level of security and encryption.
- ICTs can make use of a range of difference types of information.
- Accessing and purchasing ICT systems can be done at a low cost.
- ICTs are designed to be relatively easy to use.
- ICTs and networks are still highly unregulated and regulation is difficult.
- Investigation of ICT systems is difficult and less well understood than traditional crime.

It is also important to identify that ICT systems allow criminal, illegal or inappropriate behaviours to have different forms (Savona & Mignone, 2004):

1. The subject of a crime in that it may be part of the environment in which the crime takes place. The best example of this is the Internet and the criminal, illegal & inappropriate activities that take place there.

2. The object of a crime in that the activity has an effect on technology. An example would be a denial-of-service attack that makes a web site inaccessible for a period of time.
3. The tools that allow the illicit behaviour to occur. When the ICT is used as an enabler for the behaviour to occur.
4. The symbol of crime in which the incident occurs. Cyber stalking is one such example.

Of course, these ICTs are not restricted to being used in one form and can easily take any number of combinations of the points listed above. They do however illustrate the extent to which ICTs can successful support illicit behaviours.

While the benefits of ICTs can be seen not just in tourism but in many other sectors as well, the use of these technologies has presented some very real threats to those who use and rely on the technology to undertake their business. While the obvious threats that occur due to the use of ICT such as hardware failure, poor security and insufficient training, are to be expected, another type of threat is now emerging. This is the use of ICTs to undertake malicious activities that target these ICT systems and use the reliance on them as a weakness.

A report by the Aladdin Content Security Response Team (2006) has shown that there was a major increase in Spyware and Trojan creation in 2005 compared to 2004 with a 213% and 142% increase respectively. Shimon Gruper, vice president of technologies for the Aladdin eSafe Business Unit attributes this increase due to organised crime identifying and harnessing computer systems. While viruses and worms continue to be the greatest source of cyber attacks for organisations (AusCERT 2006; Gordon et al 2005) the general sophistication of cyber attacks continues to grow

These attacks can be perpetrated in a variety of ways, from exploitation of operating system flaws to phishing (emails that purport to be from an official organisation for the purposes of stealing personal information) attacks via email. In fact according to the Australian Securities and Investments Commission (2006), the number of complaints that have been received in response to phishing scams has increased by 25% over the last 2 financial years. The effect of a cyber security incident on customer confidence can be devastating. The Choicepoint data theft and subsequent identify frauds that resulted caused a U.S. congressional debate on the information collection industry (Gross 2005). In a cyber environment, information is a key commodity for both the cyber attacker and the individuals, businesses and governments that must protect themselves and is the key driving force behind the push to use ICT especially within the tourism industry which has many aspects that are information intensive.

In the context of the issues identified above, this paper argues for the need to develop a conceptual framework within which to be able to explore these potential vulnerabilities, examine their impacts and consider suitable responses. The next section presents this developing conceptual framework.

Developing a Conceptual Framework for Cyber Vulnerabilities in Tourism

Taking into account the importance of the tourism industry to Australia there are aspects of this industry that set it apart from many other industries, especially those industries in which cyber threats have been identified as major issues, for example banking, critical infrastructure & online retailing.

Tourism is a unique business sector in comparison to many others. There is a heavy reliance on moving the customer to the product or service as opposed to getting the product or service to the customer. The tourism sector works by attracting the customer and then moving them from one location to another. The movement of people requires many different systems and service providers, (many of which rely on the flow of information from one provider to another), to work together and be available and online constantly. Therefore it is important that not only physical but cyber vulnerabilities are well understood.

The increasing inter-connectedness of the tourism industry also provides challenges that occur when applying the ‘organisational centric’ approach that much of the current body of cyber security research uses. In an industry where the reliability and information flows of one tourism provider can directly impact another, an organisation can’t ‘lock down’ its systems when they need to be available to others. This of course opens these systems up to higher level vulnerabilities that can’t easily be tackled in the same way.

In order to explore, understand and respond to the cyber vulnerabilities that are faced by the tourism industry in Australia, a framework is required that will form the basis for an investigation. As research into cyber vulnerabilities within tourism has not been undertaken in the past a new framework will need to be created for such an investigation to take place. This framework needs to take an industry wide perspective of the problem and therefore the following framework is being proposed for use in this and any future research. Pizam and Mansfeld (2006) proposed a framework for use in creating a theory of physical vulnerabilities within the tourism industry and it is being proposed that his framework forms the basis for one that will allow an investigation into

the cyber vulnerabilities of the tourism industry. This is a macro-level conceptual framework that at a micro-level could potentially be incorporated into more conventional IT risk management practises.

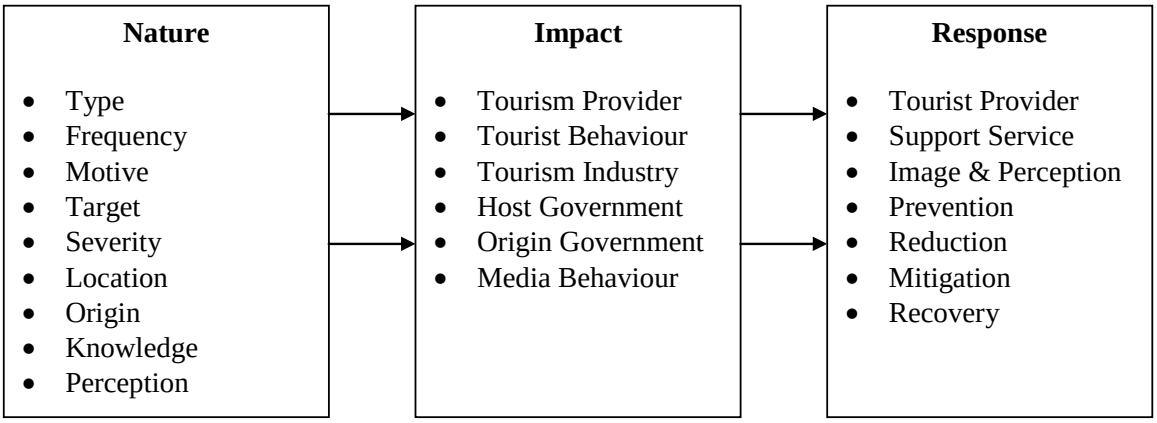

Figure 1: Proposed Conceptual Framework – Based On a framework by Pizam and Mansfeld (2006).

The proposed framework examines cyber vulnerabilities to the tourism industry and examines them from three different aspects:

1. The Nature of the Incident/Threat.
2. The Impact of the Incident/Threat.
3. The Response to the Incident/Threat.

The Nature of the Threat

An examination of the nature of the cyber threats looks at the potential threats and vulnerabilities that exist and attempts to classify them. The nature of a threat is a broad term that identifies the threat and attempts to develop a better understanding of it by breaking it down into its components. For example, depending on the threat this could include examining the motivation behind the attack which will be vary based on whether or not the attack had a specific target (like a denial-of-service attack) or was a general threat (like a mass mailing worm).

In considering the nature of the threat the *intent* is a major component to be considered. The intent is important as it is a driving aspect for the motive behind an attack and could have varying legal implication.

Table 2: Intent behind the Cyber Activity.

	Legal Nature of Cyber Threat			
Intent Behind Incident		**Criminal**	**Illegal**	**Inappropriate**
	Accidental			
	Deliberate			

The above table looks at the nature of the cyber incident and classifies it from a legal perspective as well as the intent behind the cause of the incident. The important objective of this section of the framework is the development of an ***understanding*** of the threats and vulnerabilities that are being faced by tourism organisations.

The Impact of the Threat

The second stage of the proposed framework is the examination of the impact of the threat. The proposed conceptual framework breaks the cyber vulnerabilities into 2 different types based on their impact on either ICT systems and/or the information itself:

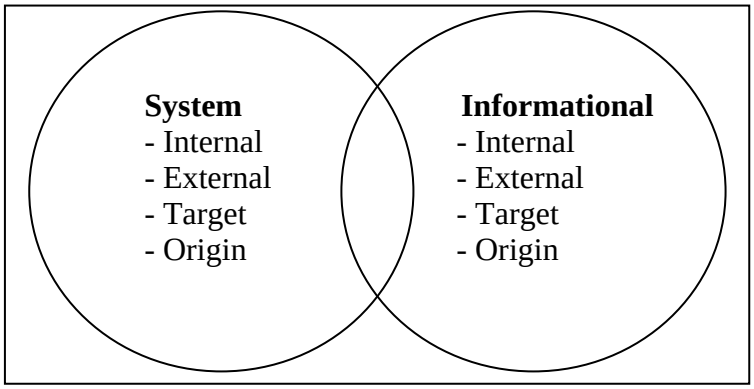

Figure 2: Cyber Vulnerability Threat Model.

System Vulnerabilities

System vulnerabilities are the vulnerabilities that come about from a dependence on ICT systems. When an organisation is dependant on a system in order to undertake business then the effect of not having access or use of that system can be severe. The threat to the system can come from a source internal or external to the organisation. These vulnerabilities may target the organisations' systems or may be the source of the attack.

Information Vulnerabilities

ICT networks (and especially the Internet) are increasingly being used as a means by which individuals and organisations obtain information about a destination. This can cause issues for the subjects of this information in that at present there is not always a way to determine the accuracy of reliability of the information that is being accessed. Information vulnerabilities are compounded by a what is called an 'information level attack' which is the use of information by one party to discredit another, more formally defined as "…attacks that are based on the dissemination of information in such a way that companies, their operations and reputations may be affected." (Lueg, 2001). In the tourism environment where reputation and perception are integral to attracting visitors and information level attack (or even just a bad review) can have a serious effect.

It is essential that an understanding of the location of a threat be understood as the implications for the organisation will differ when an attack originates within the organisations as a majority of cyber security activities are designed to keep cyber threats out of the organisation. Internal threats also have the ability to be much harder to detect and control as internally facing security can have productivity and accessibility issues for organisations.

The important aspect of this part of the framework is to ***assess*** the threat based on its impact on the target while still considering the origin

The Response to the Threat

The third stage of the proposed framework is the examination of the response to cyber incidents be they proactive, reactive or mitigation in nature.

Table 3: Protective Activity based on Incident Type

	Incident Type			
Protective Activity		**Targeted Incident**	**Untargeted Incident**	**Potential Incident**
	Proactive			
	Reactive			
	Mitigation			

The above table uses 3 different incident types and examines them with the protective response undertaken. The protective activity undertaken can be an indicator of how well and how serious a potential threat is taken.

Proactive steps are considered the better approach to protective activity however they tend to only occur when the benefits of such action outweighs the cost as the justification for proactive approaches can be difficult to justify given that the activity should eliminate the threat. Reactive steps are responses to incidents that may become mitigation activities designed to recover from an incident.

The response to a threat/vulnerability is a major indicator of a targets ability to deal with cyber threats as the better the response, the better understanding of the threats that are being faced. For example, the better understanding that an organisation has on the nature of a threat the lesser the impact of an incident and the better their response will be.

This final stage aims to assist in the ***development*** of appropriate responses to the cyber threats that exist.

This model is of course only in the very early stages of development. It is being used as a heuristic device to unpack and deconstruct the conceptual, methodological and substantive problems that arise from cyber vulnerabilities and threats that exist within the tourism industry. What the result of this research will be is still unclear but this model is aiming to be a conceptual starting point.

Conclusion

This research-in-progress paper has investigated cyber vulnerabilities in the tourism industry. This paper commenced by identifying the lack of research into the potential threats posed by cyber vulnerabilities at a time when this growing industry has become increasingly reliant on the Internet and other ICTs. With tourism being such an important aspect of the Australian economy it is clearly important that steps are taken to ensure its protection from a wide range of threats. While the physical threats faced by the tourism industry are well known and well documented the lack of research into cyber threats and vulnerabilities is problematic. This is particularly the case, as the tourism industry has characteristics that set it apart from other industries and as such these cyber vulnerabilities and threats need to be examined from its unique perspective.

In an effort to explore these potential vulnerabilities, examine their impacts and consider meaningful responses, this paper has presented a developing conceptual framework for investigating these issues in a coherent manner. This framework forms the basis for ongoing research into cyber vulnerabilities in the Tasmanian tourist industry

References

Aladdin Content Security Response Team (2006). Study Indicates Attacks Tripled in 2005 – Spyware Sneaks up on Enterprises. Israel, Aladdin Knowledge Systems.

ASIC (2006). Consumer Report 06-192, Australian Securities and Investments Commission.

AusCERT (2006). Computer Crime & Security Survey 2006, Australian Computer Emergency Response Team**:** 43.

AusCERT (2005). Computer Crime & Security Survey 2005, Australian Computer Emergency Response Team: 43.

Beirman, D. (2003) Restoring Tourism Destinations in Crisis, Cabi Publishing

Buhalis, D. (2003). "eAirlines: Strategic and Tactical use of ICTs in the Airline Industry." Information and Management 41: 805-825.

Buhalis, D. and O. Deimezi (2003). "E-Tourism Developments in Greece: Information Communication Technologies Adoption for the Strategic Management of the Greek Tourism Industry." Tourism and Hospitality Research 5(2).

Broucek, V. and P. Turner (2005). 'Riding Furiously in All Directions' - Implications of Uncoordinated Technical, Organisational and Legal Responses to Illegal or Inappropriate On-line Behaviours. EICAR 2005.

Chan, A. and R. Law (2006). Hotel Website Optimization: The Case of Hong Kong. Information and Communication Technologies in Tourism. M. Hitz, M. Sigalam and J. Murphy. Lausanne, Switzerland, Springer, Vienna.

Deloitte (2006). 2006 Global Security Survey. Global Financial Services Industry, Deloitte.

Goeldner, C. R. and J. R. B. Ritchie (2003). Tourism: Principles, Practices & Philosophies, 9th Edition. New Jersey, Wiley & Sons.

Gordon, L., Loeb, M., Lucyshyn, W. and Richardson, R. (2005). 2005 CSI/FBI Computer Crime and Security Survey, Computer Security Institute: 25.

Grimes, R. (2005). Are Attackers Winning The Arms Race? Infoworld. 26th September 2005. www.infoworld.com

Gross, G. (2005). "Lawmakers Call for Choicepoint Investigation." *Computerworld*. Accessed March 3, 2005, <http://www.computerworld.com/governmenttopics/government/policy/story/0,10801,100161,00.htm> .

Hall, M., Dallen, TJ., (eds) (2003) Safety and Security in Tourism: Relationships, Management, and Marketing, Haworth Hospitality Press.

Hakolahti, T. and P. Kokkonen (2006). Business Webs in the Tourism Industry. Information and Communication Technologies in Tourism 2006, Lausanne, Switzerland, Spinger, Vienna.

Janczewski, L. & Colarik, A. (eds)(2007) Cyber Warfare and Cyber Terrorism, Information Science Reference.

Kah, A. and C. Vogt (2005). Understanding Web Travel Search and Purchase Behaviours. 2005 Northeastern Recreation Research Symposium, Newtown Square, PA, USA.

Lueg, C. (2001). "Towards a Framework for Analysing Information-Level Online Activities." 2nd Australian Information Warfare & Security Conference: 7.

Mansfeld, Y. (2006). The Role of Security Information in Tourism Crisis Management: The Missing Link. Tourism, Security & Safety: From Theory to Practise. A. Pizam and Y. Mansfeld. Sydney, Australia, Elsevier / Butterworth-Heinemann.

Michopoulou, E. and D. Buhalis (2006). Developing an eTourism Platform for Accessible Tourism in Europe: Technical Challenges. ENTER 2006, Springer-Verlag,Wien.

Pizam, A. and Y. Mansfeld (2006). Toward a Theory of Tourism Security. Tourism, Security & Safety: From Theory to Practise. A. Pizam and Y. Mansfeld. Sydney, Australia, Elsevier / Butterworth-Heinmann.

Savona, E. and M. Mignone (2004). "The Fox and The Hunters: How ICT Technologies Change the Crime Race." European Journal of Criminal Policy and Research 10(1).

Tourism Victoria (2006), Strategic Plan 2002-2006 - Significance of Tourism, viewed 17th April 2007 <http://www.tourismvictoria.com.au/strategicplan/plan2002_2006/2_significance_tourism/section2_index.htm>.

United Nations World Trade Organisation (2006), *Tourism Highlights 2006 Edition*, viewed 5th May 2007 <http://www.world-tourism.org/facts/metho.html>.

United Nations World Trade Organisation (2007), Facts and Figures: Information Analysis and Know-how, viewed 12th May 2007 < http://www.world-tourism.org/facts/metho.html>

Vansteenwegen, P. and D. V. Oudheusden (2006). Selection of Tourist Attractions and Routing Using Personal Electronic Guides. Information And Communication Technologies in Tourism. M. Hitz, M. Sigalam and J. Murphy. Lausanne, Switzerland, Springer, Vienna.

Wilks, J. (2005) Tourism in Turbulent Times: Towards Safe Experiences for Visitors (Advances in Tourism Research), Elsevier Science.

Copyright