computing@tanet.edu.te.ua
www.tanet.edu.te.ua/computing

ISSN 1727-6209
International Scientific
Journal of Computing

CONSIDERATIONS FOR E-FORENSICS: INSIGHTS INTO IMPLICATIONS OF UNCOORDINATED TECHNICAL, ORGANISATIONAL AND LEGAL RESPONSES TO ILLEGAL OR INAPPROPRIATE ON-LINE BEHAVIOURS

Vlasti Broucek[1)], Paul Turner[2)]

School of Information Systems, University of Tasmania, Private Bag 87, Hobart TAS 7001, Australia
[1)] Vlasti.Broucek@utas.edu.au, http://forensics.utas.edu.au/
[2)] Paul.Turner@utas.edu.au, http://www.utas.edu.au/infosys/

Abstract: *The growing incidence of e-crime and computer misuse has increased demand for effective defensive and offensive solutions. Most responses have tended to focus on discrete sets of technical, organisational or legal challenges, but there is increasing recognition of the need for more integrated solutions that balance security, individual privacy and the generation of legally admissible digital evidence. More importantly, there is also proof to indicate that these fragmented approaches are impairing their own effectiveness due to the inter-relatedness of challenges faced.*

This research paper adopts an e-forensic approach to examine the links between technical, organisational and legal responses to the challenges posed by illegal or inappropriate on-line behaviour. The paper acknowledges some of the numerous challenges that remain unresolved in each approach and argues that future developments must be focused on integrated and balanced solutions that are calibrated to address the dynamic and multi-faceted nature of the forensic computing domain.

Keywords: *Behaviour, Computer Misuse, e-Crime, e-Forensics, e-Security, Law, Privacy*

1. INTRODUCTION*

The evolution of the 'information society' has given rise to numerous opportunities, challenges and risks. In recent years, amongst perhaps the most visible of the risks has been the rapid growth of computer misuse and e-crime that has resulted from the numerous ways that individuals and groups can engage in illegal or inappropriate on-line behaviour [1, 2, 3, 4]. While accurate data on the scale and cost of these activities remains difficult to acquire the most recent survey from the Australian Computer Emergency Response Team [5] estimates that computer attacks on the integrity, availability and confidentiality of networks and systems in Australia have increased to over $15 million in 2004 up 20% on 2003. The 2004 survey also indicated that:

- Malware in the form of viruses, worms or trojans was the most common form of attack and the cause of the greatest financial losses. The majority of attacks were also sourced externally;
- The second most significant cause of financial losses were the theft of laptops and the abuse/misuse of computer network access or resources;
- The two most significant factors contributing to susceptibility to harmful electronic attacks were unpatched or unprotected software vulnerabilities and inadequate staff training and education in security practices.

While the upward trajectory of these figures is alarming in itself, it is likely that the current reality is considerably more serious due to the incidence of non-reporting (AusCERT suggests this may be as high as 75% of incidences) and/or non-detection [6]. Unsurprisingly, the increasing incidence of e-crime and computer misuse has stimulated strong demand from public and private sector organisations for

* Version of this paper has originally been published in P. Turner & V. Broucek (Eds.), *EICAR 2005 Conference Best Paper Proceedings* (pp. 190-203). Saint Julians, Malta: EICAR.

effective ways to respond. This demand has contributed to a diverse range of research and development into technical, organisational and legal aspects of computer misuse and e-crime. At one level, the rapid developments occurring in each of these areas are mostly laudable and exciting, but there is now increasing recognition that the development of truly effective defensive and offensive solutions will require the integration of insights from each. While the complexity of specific issues within each area partly explains the limited collaboration that has occurred to date between researchers, it is also clear that it is inhibiting the development of the integrated solutions and skills that will be required to effectively balance needs for network security, individual privacy and the generation of legally admissible digital evidence. More significantly, there is growing proof to suggest that a consequence of this 'riding furiously in all directions' without an awareness of how developments in one area interact with developments in another is actually impairing the overall effectiveness of the responses developed [7, 8, 9, 10, 11].

In this context, this research paper adopts an e-forensic approach to examine the interrelatedness between technical, organisational and legal responses to the challenges posed by illegal or inappropriate on-line behaviours. The paper acknowledges some of the numerous challenges that remain unresolved in each approach and highlights how responses to these challenges have consequences for developments in other areas, which ultimately limit the effectiveness of current approaches and the more coherent integrated solutions. The paper anticipates that by raising awareness of these issues an important opportunity can be grasped to ensure the future development of integrated solutions that balance the interests for security, legal admissibility and privacy in ways that are calibrated to address the dynamic and multi-faceted nature of the forensic computing domain [9].

2. COMPUTER MISUSE AND E-CRIME

Prior to examining the interrelatedness of technical, organisational and legal responses to computer misuse and e-crime it is useful to briefly classify the types of misuse and the nature and seriousness of associated behaviours.

While existing mechanisms for addressing conventional societal misconduct (including law enforcement, education and security) remain relevant in the digital domain, there are unique challenges for investigation and enforcement of behaviours in cyber-space because of the numerous ways in which individuals and/or groups can use digital technologies to engage in criminal, illegal or inappropriate on-line behaviour. As with conventional investigations when a computer incident occurs there is a need to assess its extent and effect and to rectify any damage caused. However, there may also be the need to gather evidence to identify the perpetrators and their 'intent' as a basis for future responses. From an e-forensic perspective it is these digital evidence acquisition activities, the 'last mile' connection [12] between them and an identifiable perpetrator, questions over the chain of custody, the determination of where the e-crime/misuse has occurred and questions on applicable law and legal admissibility that pose the most challenging technical, organisational and legal questions.

In responding to these questions an important component in ensuring the effective identification of the type of forensic evidence required and the best methods for its collection, analysis and presentation is the ability to classify the type of misconduct as early in the investigation as possible. In this regard, one classification approach has developed based upon the identification of behaviours cross-referenced with types of misuse produced by Broucek and Turner [7, 8] and explored in Hannan, Frings et al [9]. The behaviours are identified as: criminal, illegal or inappropriate. This reflects the varying levels of seriousness of any behaviour committed and the likely penalties that will result from any investigations (i.e. criminal prosecution, civil proceedings or organisational censure or dismissal). The types of computer misuse identified are divided into two categories:

Computer misuse
Computer supported (or aided, assisted) misuse.

The first category involves misuses that "*encompass all offences against the confidentiality, integrity and availability (CIA) of computer data and systems. Examples include illegal access to computer systems or malicious code-writing*" [13]. In this case the evidence collected will need to prove that the activities were intended to result in a specific criminal, illegal or inappropriate result.

The second category is defined as crimes that "*are 'traditional crimes' that can be, or have been, committed utilising other means of perpetration which are now being, or are capable of being, executed via the Internet, computer-related venue (e-mail, newsgroups, internal networks) or other technological computing advancement. For example, intellectual property rights infringement (e.g. digital music and software piracy) and payment system frauds (e.g. credit card fraud via the*

Internet" [13]. In this case the evidence collected will need to prove that the delivery was intentional and the content of the transmission was not altered from the sender to the recipient.

The next three sections of the paper identify key developments and challenges that pertain respectively to technical, organisational and legal responses to computer misuse and e-crime. Each section also highlights the lack of coordination between these responses and considers the implications for the overall effectiveness of responses to criminal, illegal or inappropriate on-line behaviours.

3. TECHNICAL - DEVELOPMENTS, CHALLENGES AND IMPLICATIONS

In terms of broad technical approaches huge advances have been made in the last ten years in the ability of systems to detect intrusions, denial of services attacks and to improve user profiling and network monitoring. However, as AusCERT figures above indicate it would be naïve to suggest that these approaches are wholly effective or even able to keep pace with the growing challenges of computer misuse and e-crime. Indeed, while these approaches may provide tools to address some of the major symptoms of computer misuse, problems remain in detecting, identifying and logging attacks. Additionally, as has been previously demonstrated through cases studies, many of the systems and tools developed within this approach have major limitations in terms of evidence acquisition capabilities [14, 15, 16, 17, 18]. Significantly, it is also important to remain aware of the susceptibility of these systems and tools themselves to attack [19, 20].

As the debates in the e-security and e-forensics literature indicate responding to the challenges of computer misuse and e-crime has produced several streams of research and development including network survivability, self-healing networks, intrusion prevention/protection systems, anti malware systems and e-forensic investigation tools. Whilst various disagreements and debates continue within each of these streams of research there appears to be an increasing awareness of the need to move from reactive to more proactive approaches. These new approaches appear to increasingly acknowledge that the conventional 'fortress model' of perimeter defence is no longer sufficient to address security on networks that have numerous entry points due to the range of devices (wired and wireless) and application service models now commonly deployed. For example, current developments in malware protection (antivirus software) are increasingly displaying a move away from signature-based (reactive) detection of malware exploits towards a more proactive approach of vulnerability protection through the deployment of behavioural-based engines. While this approach clearly offers assistance in protecting systems against new exploits without having to rely on their signature, there has been little consideration of the implications of these systems for user privacy and the collection of digital evidence. Similarly, recent developments by SourceFire (which basically evolved from a Network Intrusion Detection System (NIDS) based on SNORT) have produced a set of tools called the 3D approach of 'discover, determine and defend'.

This approach is represented in the Fig. 1.

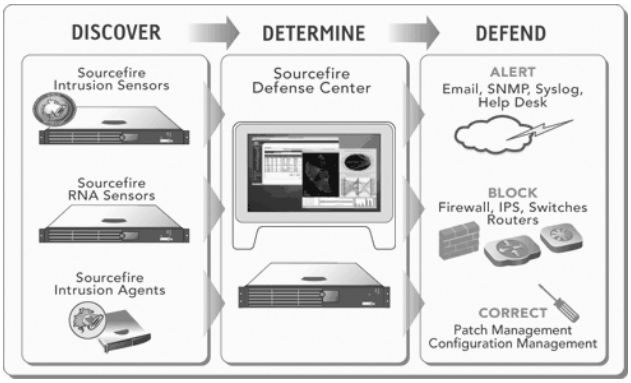

Fig. 1 - SourceFire's 3D approach (from http://www.sourcefire.com/products.html)

SourceFire argue that this approach is the 'only comprehensive intelligent network defense system that unifies intrusion and vulnerability management technologies to provide customers with real-time network security'. At the centre of the system is the SourceFire Defense Centre (SDC) that correlates data from the intrusion sensors and agents with the network intelligence provided by the RNA Sensors to prioritize the most critical security events prior to taking action in real-time. SourceFire claim that as a result of the 'high level of contextual intelligence' organisations can determine why changes occur, whether an attack poses a serious threat and how to best prioritize and shape the response. While the move from intrusion detection systems (IDS) to intrusion protection systems (IPS) offers some significant advantages in terms of security, it also raises numerous questions for the collection of digital evidence as these systems adopt an approach analogous to 'pulling the plug' that inhibits evidence acquisition activities [7, 8]. Given the experience that few if any systems are perfect, it would seem sensible to ensure that more consideration is given to addressing circumstances where systems fail or prove unsuitable for responding to the challenges of illegal or inappropriate on-line behaviours.

An example that illustrates another aspect of the interrelatedness of issues has occurred in the realm of anti-spam software. While many of these systems make valiant attempts to deal with the increasing problem of Spam email, some of the solutions developed may be causing more harm than good. As the direct experience of one of the authors indicates much anti-spam software is language specific and cannot cope with other languages, with the consequence that messages in these languages are frequently marked as SPAM. These types of problems with Spam filtering may lead to the loss of messages (due to them being filtered to the junk mail folder and deleted without being examined). Additionally, given that some anti-spam software tools work on a principle of changing and or adding headers to e-mails to allow users to filter according to these headers, it remains unclear whether such modifications of e-mails might have legal implications, for example:

- If e-mail is used as an official document and a dispute arises, the originating e-mail will be different from e-mail delivered to recipient and thus may become invalid.
- If e-mail is going to be used as an evidence of criminal, illegal or other inappropriate activity, will such a modification render it inadmissible or invalid?

Even where digital data is potentially available there are still numerous technical challenges. For example, EnCase (currently the preferred software e-forensic investigation tool used by Australian law enforcement agencies) has recently been the focus of considerable discussion. While it offers access to file systems other than those used by Microsoft Windows and DOS platforms it is mainly oriented towards the MS Windows environment. Currently it runs only on this platform and it was recently discussed in forensic circles in relation to producing different (potentially incorrect) hash values for disks imaged/investigated on two different platforms (http://groups-beta.google.com/group/infosec-discuss/). This difference appears to be the result of difficulties EnCase has in acquiring access to the HPA (Host Protected Area)[1] part of discs. Given the requirements in many jurisdictions for completeness in the disk image used for evidence, this raises interesting questions on admissibility. While other e-forensic software tools such as Brian Carrier's SleuthKit provide options for both MS Windows and Unix/Linux platforms it too has the limitation, for example not supporting the ReiserFS file system used as a default on the commonly deployed SuSE (now Novell) Linux.

From an e-forensic perspective there is evidence that the various technical responses to the challenges of illegal or inappropriate on-line behaviours are increasingly raising problems for both the collection of data and its admissibility. However, it is clear that given our contemporary experience of computer security that we retain modest expectations of their capabilities. Therefore even whilst arguing for the need for these systems developers to consider issues of evidence acquisition there is a need following Broucek & Turner [15] to acknowledge that:

- These systems may not even be able to collect the data that they are designed to collect;
- Where data is collected it may only be a partial data set
- The data collected may itself be flawed, erroneous or have already been tampered.

More broadly, as technical responses become more 'proactive' they are raising increasing challenges for the conduct of forensic analysis and individual privacy. The nature of many of these new systems is also making the conduct of forensic analysis problematic because the methods that have to be used to access the evidentiary data end-up jeopardizing its legal admissibility. In relation to privacy the need for systems to collect data and also protect privacy is evidenced by work on pseudonymisation techniques for log files and intrusion detection systems [21, 22, 23, 24]. Privacy concerns also emerge not just in relation to those individuals under investigation but also to others whose activities are also part of the data sets being analysed. These knock-on effects involving privacy intrusion raise concerns about breaches of privacy and/or confidentiality without the knowledge or consent of the individual's concerned. With pro-active security measures there are also privacy concerns arising from constant surveillance [21, 22, 23, 24, 25, 26, 27]. The emergence of anomaly based intrusion detection systems that rely on analysis of 'normal' work patterns poses a further threat to privacy as is witnessed by recent efforts to develop privacy protection through pseudonymisation approaches.

[1] HPA is defined as a reserved area for data storage outside the normal operating file system. This area is hidden from the operating system and the file system, and is normally used for specialized applications. Systems may wish to store configuration data or to save memory to the hard disk drive device in a location that the operating systems cannot change.

4. ORGANISATIONAL – DEVELOPMENTS, CHALLENGES AND IMPLICATIONS

With the increasing incidence of computer misuse and e-crime public and private sector organisations have increasingly sought ways to respond. These responses have included increased e-security precautions, computer usage policies, monitoring and education as well as in some instances the establishment and deployment of forensic computing investigation teams. Whilst these responses are sensible and understandable, in some cases their implementation has had unforeseen results that have actually impaired the overall security of the organisations concerned. Partly, this result from draconian measures imposed on users of the systems and partly from a general lack of awareness amongst most users of the implications for e-security of their on-line usage behaviours.

A good example of this relates to how some organisations approach the management of relatively insecure Internet applications such as email and WWW browsers. With email for example, awareness of these security weaknesses has resulted in many organisations restricting access to organisational e-mail systems. From the users perspective this has led to the perception of internal e-mail systems as being 'unfriendly' due to their inaccessibility outside the organisational 'firewall' and/or because organisational policies prohibit their utilisation for private communications. However, as a result of the increasingly important social dimension to e-mail usage most employees solve this 'problem' limited access to email by subscribing to one of the numerous free web-mail services e.g. hotmail.com, yahoo.com, excite.com, etc. This user response in-turn introduces further risks for organisational IS security management particularly as many employees adopt the 'single password for everything' approach. As a consequence the same password may be used on organisational e-mail systems as well as on private web-mail accounts which in-turn dramatically increases the possibility of password sniffing/spoofing type security breaches. This free web-mail services also appear susceptible to a higher incidence of direct or double-click attachment based viruses that can easily migrate to the organisational information systems as a result of employee on-line behaviours. More significantly most of these free web-mail systems also allow the checking of POP3 e-mail accounts. Employees using these services are rarely aware that in doing so they may be allowing unauthorised access to organisational information. Similarly, WWW browsers exhibit many security weaknesses that combine with users online behaviours to compound system security management problems. These include the use of cookies; web browser history and cache files being kept on local drives; active pages - using Java applets, Java scripts ActiveX technologies and executable elements in web pages all of which create potential risks for the spread of malware [28]. Although, of course, it should be noted that it is these very insecurities in email and browsers that are most often exploited to create the invaluable resources for the basis of e-forensic investigations.

Additionally, access to the Internet through web browsers also creates further privacy issues for users and for system management. For example, many organisations use proxy/cache for speeding up, controlling and monitoring access to Internet by using proxy authentication. Proxy authentication and monitoring can create perceptions amongst users of a modern form of 'Panopticon' [29]. In particular, this perception can be created if such monitoring and/or authentication are introduced without proper policies and if the purpose of their introduction is not explained to users. Proxy authentication is generally used only for statistical purposes; however it can create a 'big brother' type of surveillance fear amongst the users that can influence their behaviours in ways that impair overall system security. These examples highlight the need to balance requirements for improved security with those of the right to privacy of employees in a manner that does not compromise the potential for future forensic investigation of illegal or inappropriate on-line behaviours.

Clearly a major element in any organisational IS security management approach must be to provide detailed explanations and demonstrations to users on how their on-line behaviours can potentially harm the security of the organisation. If organisations feel the need to have the option of monitoring on-line behaviours or conducting forensic investigations then staff should be informed of the procedures and the results of any investigations or monitoring. Creating a 'big brother surveillance' perception amongst employees may well be counter-productive in terms of IS security and/or wider organisational goals [29].

From an e-forensic perspective there are also implications of the organisational responses to the incidence of illegal or inappropriate on-line behaviours when they are detected. This is particularly the case in relation to an organisation's ability to accurately handle digital evidence. As a recent Australia case discussed by Ajoy Gosh (University of Technology Sydney) and cited in the AusCERT 2004 computer crime survey [5, p. 9]

illustrates organisations must examine evidence correctly or face the consequences – the case in question concerned 'evidence of transactions made using a junior clerk's userid that were fraudulent'. The clerk was subsequently dismissed and asked to repay the funds or face prosecution. Both the company and clerk (through the Union) organised for the conduct of forensic examinations of the digital evidence by forensic experts. Subsequently it was revealed by the expert engaged by the clerk's solicitor that 'the suspect transactions were in fact made by a company director pretending to be the clerk'. Significantly, it was also revealed that 'the company had requested its forensic consultant to make certain omissions in his report'. The end result was that the clerk received a substantial termination payment and agreed to sign a deed of confidentiality, the dishonest company director resigned and paid back the funds and the alleged fraud was never reported to the Police. This case highlights a number of issues that highlight the interrelatedness of organisational, technical and legal approaches:

- Organisational responses, particularly where they are settled 'out of court' are analogous to the technical response to an incident of 'pulling the plug' in that they inhibit the development of understanding on how best to collect, analyse and present digital evidence. This in-turn is inhibiting the development of case law interpretations on acceptable practices, procedures and approaches to dealing with the admissibility and evidentiary weight of digital evidence;
- The case also reveals the importance of examining links between digital evidence and other types of evidence. This in-turn highlights the problem of 'the last mile' [12] and the significance of conventional investigative techniques and other types of potentially corroborative evidence.

More broadly, as organisations seek to respond to these challenges, they find themselves in a curious position in relation to law enforcement agencies (who under new legislation are increasingly being empowered to respond). The lack of delineation over responsibility for chains of evidence and chains of custody in relation to digital evidence creates uncertainty and further compounds the development of best practices in terms of technical and legal responses to incidents. Finally, there is also the interrelationship between research and development into computer misuse and e-crime and organisational demands for e-security. Anecdotal evidence collected by one of the authors suggests that compliance with e-security requirements placed on staff in law enforcement agencies at State, National and International is inhibiting the ability of these agencies to keep pace with the development of malware and new types of illegal or inappropriate on-line behaviours e.g. some researchers in the field of child pornography have been inhibited from visiting/monitoring certain websites/chat-rooms because of organisational e-security approaches. While clearly safeguards are required, it is important to note that e-criminals do not face any type of restriction on engaging in or developing new on-line behaviours. Indeed, the ingenuity of many types of computer misuse and e-crime display the willingness on the part of perpetrators to use any and all resources at their disposal, to not delineate between domains and to move between digital and physical environments and artefacts on the basis of 'whatever works'.

5. LEGAL – DEVELOPMENTS, CHALLENGES AND IMPLICATIONS

In the post September 11th era the threat of global terrorism has stimulated significant extensions being given to law enforcement agencies. These powers have increasingly been extended into the digital domain through legislative developments at national and international levels e.g. Australian Cyber-Crime Act 2001, 'Patriot Act' in USA, and on-going legislative discussions within the European Union, Council of Europe and the USA. In conjunction with these legislative developments efforts have been made to generate practical tool-kits for investigating computer misuse and e-crime in a manner that will produce legally admissible evidence e.g. CTOSE (Cyber Crime Tools for On-line Search for Evidence) [11, 30]. However, as was discussed above, while these efforts are laudable, numerous questions on the legal admissibility, legal validity/weight, chain of evidence and chain of custody of digital evidence continue to make problematic the development of legal responses to illegal or inappropriate on-line behaviours [15, 31].

More significantly, in the context of the discussions here, even where digital evidence is available and has been accepted as admissible, critical issues have emerged over the understanding of the courts on the nature of this evidence. For example, the MP3 Piracy case involving representatives from the Australian recording industry and three Australian Universities in a dispute over the distribution of MP3s by students and staff at the Universities reveals a 'worrying lack of comprehension of the technical nature of digital logs and data storage' [11, 30, 32]. More specifically, this lack of understanding resulted in the provision of access to data sets that contained information on the on-line activities of thousands of

presumably innocent users and not just data on those alleged to be guilty of computer misuse. This provision of unprecedented access to huge amounts of potentially sensitive data pertaining to the personal, confidential and commercial activities of innocent users is clearly of concern. This is especially the case where access to the data was not handed over to an independent third party but rather to the applicants in the case.

From an e-forensic perspective, not only does the case reveal a lack of forensic readiness on the part of the courts, the applicants and defendants, it also raises questions about the supposed expertise of the forensic experts used in the case. However, quite apart from the consequences of these circumstances in the specific case, other important questions are raised in relation to the potential consequences of these types of approaches being displayed by courts. Indeed as has been argued elsewhere the approach adopted by the Australian Federal Court and the applicants in the case 'is short-sighted and may back-fire on the music industry's desire to crack-down on piracy'. This is because it is probable that many users will now proceed to encrypt all their communications to impede subsequent 'snooping'. The case has also made 'many network administrators in Universities reticent about reporting on suspected computer misuse of their systems'. This is because they are either afraid that they will be held responsible or that they will have to conduct or be involved in e-forensic investigations for which they feel unqualified [11, 30, 32]. The case may also influence the way in which organisations 'back-up' their systems and how long they retain this data. Combined all of these factors are likely to make collection, investigation, generation and presentation of digital evidence of illegal or inappropriate on-line behaviours more difficult.

More broadly, as the law continues to generate responses to the challenges faced it is clear that there are strong interrelationships with public perceptions and changing end-user and organisational behaviours for on-line environments. Critically there is the danger that if legal responses do not show sensitivity towards these interrelationships end-users and organisations seeking to protect themselves will behave in ways that will problematise the acquisition of digital evidence and potentially reduce overall system e-security.

6. CONCLUSIONS

This paper has adopted an e-forensic approach to explore some of the key technical, organisational and legal responses being developed to illegal or inappropriate on-line behaviours and argued that there is a critical need for the development of integrated solutions that acknowledge how in digital environments developments in one area have serious implications for developments in another. This paper has revealed how without a conscious recognition of the interrelatedness of these responses we will continue to create vulnerabilities and/or problems that may actually impair the effectiveness of our overall response to computer misuse and e-crime. In working towards a more integrated solution that balances requirements for network security, individual privacy and the need for legally admissible digital evidence it is useful to extend recommendations previously articulated by Broucek & Turner [30]

- Best practice for digital evidence handling should involve deploying the highest investigative standards at all stages in the identification, analysis and presentation of digital data;
- Targeted training and education of network administrators and end-users in the key principles of digital evidence handling is urgently required. As is education and awareness amongst users of the consequences of their on-line behaviours for system security;
- Opportunities exist for the further refinement of e-forensic methodologies and processes such as those developed by CTOSE and these must include a recognition of the dynamic and multi-faceted nature of the forensic computing domain;
- Enhancing e-forensic professionalism through the rapid development of processes for e-forensic computing competences and certification is an essential element in building and implementing integrated solutions.

While perhaps in the near future at least, we may have to accept continued 'riding furiously in all directions' the need for consideration of how well each approach balances the interests of security, legal admissibility and privacy should be incorporated into our discussions. Ultimately of course we also need to remember that the digital domain itself is also intimately related to the physical world where corroborative evidence and conventional investigative techniques have a role to play.

7. REFERENCES

[1] D. E. Denning, *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, 1999.

[2] B. Etter, *Evaluating the Capacity to Respond to E-Crime*, Australasian Centre For Policing Research, 2000.

[3] B. Etter, *Working in Partnership: The Australasian Response to Electronic Crime*, Australasian Centre For Policing Research, 2000.

[4] B. Etter, *The Challenges of E-Crime for Australasian Law Enforcement*, Australasian Centre For Policing Research, 2000.

[5] Australian Computer Emergency Response Team, *The Australian Computer Crime and Security Survey 2004*, 2004.

[6] B. Etter, *The Forensic Challenges of E-Crime*, Australasian Centre For Policing Research, 2001.

[7] V. Broucek and P. Turner, *Forensic Computing: Developing a Conceptual Approach for an Emerging Academic Discipline*, in H. Armstrong, ed., *5th Australian Security Research Symposium*, School of Computer and Information Sciences, Faculty of Communications, Health and Science, Edith Cowan University, Western Australia, Perth, Australia, 2001, pp. 55-68.

[8] V. Broucek and P. Turner, *Forensic Computing: Developing a Conceptual Approach in the Era of Information Warfare*, Journal of Information Warfare, 1 (2001), pp. 95-108.

[9] M. Hannan, S. Frings, V. Broucek and P. Turner, *Forensic Computing Theory & Practice: Towards developing a methodology for a standardised approach to Computer misuse*, in S.-A. Kinght, ed., *1st Australian Computer, Network & Information Forensics Conference*, Perth, WA, Australia, 2003.

[10] M. Hannan, P. Turner and V. Broucek, *Refining the Taxonomy of Forensic Computing in the Era of E-crime: Insights from a Survey of Australian Forensic Computing Investigation (FCI) Teams.*, *4th Australian Information Warfare and IT Security Conference*, Adelaide, SA, Australia, 2003, pp. 151-158.

[11] V. Broucek, P. Turner and S. Frings, *Music piracy, universities and the Australian Federal Court: Issues for forensic computing specialists*, Computer Law & Security Report, 21 (2005), pp. 30-37.

[12] M. Hannan and P. Turner, *The Last Mile: Applying Traditional Methods for Perpetrator Identification in Forensic Computing Investigations*, *3rd European Conference on Information Warfare and Security*, Royal Holloway, University of London, 2004.

[13] A. Rathmell and L. Valeri, *Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries*, 2003.

[14] V. Broucek and P. Turner, *Intrusion Detection: Issues and Challenges in Evidence Acquisition*, International Review of Law, Computers and Technology, 18 (2004), pp. 149-164.

[15] V. Broucek and P. Turner, *Risks and Solutions to problems arising from illegal or Inappropriate On-line Behaviours: Two Core Debates within Forensic Computing.*, in U. E. Gattiker, ed., *EICAR Conference Best Paper Proceedings*, EICAR, Berlin, Germany, 2002, pp. 206-219.

[16] P. Sommer, *Intrusion Detection Systems as Evidence*, *Recent Advances in Intrusion Detection - RAID'98*, Louvain-la-Neuve, Belgium, 1998.

[17] P. Sommer, *Digital Footprints: Assessing Computer Evidence*, Criminal Law Review Special Edition (1998), pp. 61-78.

[18] P. Sommer, *Intrusion Detection Systems as Evidence*, Computer Networks, 31 (1999), pp. 2477-2487.

[19] A. Arona, D. Bruschi and E. Rosti, *Adding availability to log services of untrusted machines*, *15th Annual Computer Security Applications Conference (ACSAC'99)*, IEEE Comput. Soc, Los Alamitos, CA, USA, Phoenix, AZ, USA, 1999, pp. 199-206.

[20] M. Handley, V. Paxson and C. Kreibich, *Network Intrusion Detection: Evasion, Traffic Normalization, and End-to-End Protocol Semantics*, *10th USENIX Security Symposium*, Washington, DC, USA, 2001.

[21] J. Biskup and U. Flegel, *On Pseudonymization of Audit Data for Intrusion Detection*, *Workshop on Design Issues in Anonymity and Unobservability*, Springer-Verlag, Berlin, Heidelberg, Berkeley, California, 2000, pp. 161-180.

[22] J. Biskup and U. Flegel, *Transaction-Based Pseudonyms in Audit-Data for Privacy Respecting Intrusion Detection*, *Third International Workshop on Recent Advances in Intrusion Detection (RAID 2000)*, Springer-Verlag, Berlin, Heidelberg, Toulouse, France, 2000, pp. 28-48.

[23] J. Biskup and U. Flegel, *Threshold-Based Identity Recovery for Privacy Enhanced Applications*, *7th ACM Conference on Computer and Communications Security (CCS 2000)*, ACM, Athens, Greece, 2000, pp. 71-79.

[24] E. Lundin, *Anomaly-based intrusion detection: privacy concerns and other problems*, Computer Networks, 34 (2000), pp. 623-640.

[25] E. Lundin and E. Jonsson, *Privacy vs Intrusion Detection Analysis*, *The 2nd International Workshop on Recent Advances in Intrusion Detection (RAID'99)*, Lafayette, Indiana, USA, 1999.

[26] H. Kvarnström, E. Lundin and E. Jonsson, *Combining fraud and intrusion detection - meeting new requirements*, *The fifth Nordic Workshop on Secure IT systems (NordSec2000)*, Reykjavik, Iceland, 2000.

[27] M. Sobirey, S. Fischer-Hübner and K. Rannenberg, *Pseudonymous audit for privacy enhanced intrusion detection*, in L. Yngstrom and J. Carlsen, eds., *IFIP TC11 13th International Conference on Information Security (SEC'97)*, Chapman & Hall, London, UK, Copenhagen, Denmark, 1997, pp. 151-163.

[28] V. Broucek and P. Turner, *E-mail and WWW browsers: A Forensic Computing perspective on the need for improved user education for information systems security management.*, in M. Khosrow-Pour, ed., *2002 Information Resources Management Association International Conference*, IDEA Group, Seattle Washington, USA, 2002, pp. 931-932.

[29] M. T. Dishaw, *Monitoring Internet Use In the Workplace: Caution is Advised*, in M. Khosrow-Pour, ed., *2002 Information Resources Management Association International Conference*, Idea Group Publishing, Seattle, WA, USA, 2002, pp. 175-178.

[30] V. Broucek and P. Turner, *Computer Incident Investigations: e-forensic Insights on Evidence Acquisition*, in U. E. Gattiker, ed., *EICAR Conference Best Paper Proceedings*, EICAR, Luxembourg, Grand Duchy of Luxembourg, 2004.

[31] V. Broucek and P. Turner, *Bridging the Divide: Rising Awareness of Forensic Issues amongst Systems Administrators*, *3rd International System Administration and Networking Conference*, Maastricht, The Netherlands, 2002.

[32] V. Broucek, S. Frings and P. Turner, *The Federal Court, the Music Industry and the Universities: Lessons for Forensic Computing Specialists*, in C. Valli and M. Warren, eds., *1st Australian Computer, Network & Information Forensics Conference*, Perth, WA, Australia, 2003.

***Vlasti Broucek**, MSc has been working in the computer industry since 1985, currently, he is a researcher in the School of Information Systems and ICT Manager in the School of Psychology, both at the University of Tasmania, Australia. Vlasti's research focus is on Legal and Technical Issues of forensic computing. Vlasti has an MSc degree from the Czech Technical University in Prague and currently is pursuing a PhD degree at the University of Tasmania under leadership of Dr Paul Turner. Vlasti is publishing extensively in the space of Forensic Computing and received several awards for his work. In May 2004, Vlasti was elected to the post of Scientific Director of European Institute for Computer Anti-virus Research (EICAR).*

***Dr. Paul Turner**, prior to becoming Senior Research Fellow at the School of Information Systems in 2000, was a research fellow at CRID (Computer, Telecommunications and Law Research Institute) in Belgium. Paul has also worked as an independent ICT consultant in Europe and was for 3 years editor of the London-based Telecommunications Regulation Review. Paul's strong research focus has continued at the University of Tasmania, where for 2 years Paul was concurrently Research Manager for the Tasmanian Electronic Commerce Centre (http://www.tecc.com.au). Paul is currently the University's research coordinator for the Smart Internet CRC (http://www.smartinternet.com.au) and also leads a group of five researchers in the e-forensics and computer security domains at the School of Information Systems, University of Tasmania.*