2017

Issues of Implied Trust in Ethical Hacking

Georg Thomas
Charles Sturt University, gethomas@csu.edu.au

Oliver Burmeister
Charles Sturt University, oburmeister@csu.edu.au

Greg Low
Charles Sturt University, greg@sqldownunder.com

Issues of Implied Trust in Ethical Hacking

Georg Thomas
School of Computing and Mathematics
Charles Sturt University
New South Wales, Australia
Email: gethomas@csu.edu.au

Oliver Burmeister
School of Computing and Mathematics
Charles Sturt University
New South Wales, Australia
Email: oburmeister@csu.edu.au

Gregory Low
SQL Down Under
Victoria, Australia
Email: greg@sqldownunder.com

Abstract

This paper discusses the issues of implied trust in ethical hacking. Ethical hackers are considered to be professionals and experts in their field. It is well documented that there is an implied trust toward professionals who are entrusted to undertake a task. Like many similar professions, such as ICT and computer forensics, there is no uniform or mandated code of ethics that an ethical hacker must adhere to. Given the nature of hacking and the potential for misuse and access to sensitive and confidential information, the need to ensure professionalism is maintained through ensuring competence and ethical behaviour is critical.

Keywords Ethical hacking, penetration testing, implied trust, professionalism, code of conduct.

1 Introduction

According to the 2017 Verizon Data Breach Investigations Report (DBIR), 62% of breaches feature hacking (Verizon, 2017). Similarly, the 2017 Telstra Cyber Security report predicts that 59.6% of threats in Asia and 52.6% in Australia will be from external hackers (Telstra, 2017).

Furthermore, the Identify Theft Resource Center identified over 16 million records exposed as a result of over 850 breaches (Identity Theft Resource Center, 2017). Although this sees a drop compared to 2016 where over 36 million records were exposed, it can't be concluded that breaches are on the decline; a single breach can expose millions of records and with the personal information of potentially hundreds of thousands, if not millions of individuals, this is a significant issue.

In addition to data breaches, there has been a series of ransomware attacks. A hacking group called Shadow Brokers is believed to have leaked an NSA exploit named Eternalblue (Goodin, 2017). This exploit, was used as one of the mechanisms to spread two strains of ransomware in 2017; the ransomware known as WannaCry in May, and Petya in June. The effect on victims of the malware was largely devastating, with some organisations forced to shut-down until systems could be restored resulting in significant lost revenue and potential litigation. Some victims have permanently lost data and systems, impacting the business and their clients (Coyne, 2017).

Whether it is a data breach or an attack of some other kind, a vulnerability needs to be exploited in order for it to be successful. These vulnerabilities could be with specific systems and applications or with people and processes. These vulnerabilities are typically discovered by security researchers and hackers. They are then exploited either directly, by the hacker, or using malicious software (malware) that is designed to seek out and exploit the flaws.

In order to defend against these types of attacks, a multilayered approach is generally adopted. Traditionally a defensive approach of implementing technical controls has been used (Thomas, 2017). The implementation of firewalls, anti-virus software, and other access control systems has been the status quo. Over the past few years the focus has shifted from just the technical aspects of information security to include the "human factor" or people based aspects (Eminağaoğlu, Uçar & Eren 2009, p223). With the dramatic increase in phishing; using emails to trick users into divulging secret information, such as usernames and password, the traditional controls are less effective. According to Verizon (2017), phishing attacks were the most prevalent form of social engineering attack to take place.

The contribution of this paper is a better understanding of one of the human factors, namely, that of the ethical hacker.

2 What is Ethical Hacking?

The traditional approach of utilising multilayered technical defences has been augmented over the past decade through the implementation of a security culture within organisations, which included the implementation of security awareness programs. These programs helped users to identify suspicious emails, to use good password practices, and to safeguard their information. These strategies are all known as 'defensive' strategies, because they seek to defend a network or systems from attack by a malicious attacker.

There are, however, also a set of offensive strategies that can be undertaken. Instead of trying to stop an attack, an offensive strategy launches an attack against a network, with the aim of identifying weaknesses that can then be remediated. These offensive engagements are known as penetration tests or red-teaming and are conducted by a specific type of hacker, called an ethical hacker. Ethical hackers use the same tools and techniques as the malicious hackers, however, they do this to test the security of the target network (Graves, 2010, p3). What sets an ethical hacker apart from other types of hackers, is that an ethical hacker is given permission to conduct the hack by the owner of the network.

2.1 Types of hackers

When it comes to classifying hackers, there are generally three types of hacker. These hackers are classified based on their motives and into three categories, which are identified by a 'hat' colour.

2.1.1 Black Hats

Black hat hackers are the malicious hackers, also known as 'crackers' (Graves, 2010, p3). This type of hacker operates illegally and their motives are usually for personal gain or to cause mischief (Thomas, 2017). Often black hat hackers obtain confidential information, such as credit cards, or personal information that can then be sold on channels like the dark web (a set of websites not accessible through

traditional search engines and effectively hidden (Egan, 2017)) and then used to commit fraudulent transactions or steal identities, to name a few uses.

2.1.2 White Hats

A white hat hacker, also known as ethical hackers are hired to hack into systems and networks for the purpose of identifying security weaknesses and vulnerabilities. After identifying these vulnerabilities, a white hat will report their finding back to the owner of the network they assessed, who can then work to remediate the findings.

2.1.3 Grey Hats

In between black and white hats is they grey hat hacker. The motives behind grey hats aren't generally personal, nor are they provided permission by the system owner to hack the target system. Instead, a grey hat hacker may be motivated by a cause, known as hacktivism (Hargrave, 2012), or be sanctioned by a nation state to attack an adversary or gain intelligence.

3 Methodology

An analysis of the current literature on implied trust and professionalism issues on ethical hacking was undertaken. To perform this review, Google Scholar was used to identify the currently available literature. The following search queries were performed:

- "penetration testing" | "ethical hacking" | "red team"
- ("penetration testing" | "ethical hacking" | "red team") & ("implied trust" | professionalism)
- ("penetration testing" | "ethical hacking" | "red team") & ("implied trust")

The first query, which was designed to identify all literature on penetration testing and other related terms (using an "OR" operator) that are indexed returned 17,300 records. To filter this further, the second query required either "implied trust" OR "professionalism" as part of the search. This reduced the search down to 677 records. Finally, a third search was performed to only look at articles that include "implied trust" as a key word. This final search resulted in 18 search results, which represents just 0.1% of the articles written on penetration testing. Papers that did not discuss ethical hacking and either implied trust issues, either directly, or indirectly were not included as part of this paper.

4 Penetration testing and trust

By nature, and to be effective, ethical hacking involves trying to gain access to a system to access confidential and sensitive information. This means, that a certain level of trust needs to be established between the ethical hacker and the party engaging them. Trust is conceptualised as the belief of a person that another party upon whom the individual is dependent will act in his/her interests (Tutzauer, n.d, p5). A professional has superior knowledge, requiring the other party to trust them (Al-Saggaf, Burmeister, and Schwartz, 2017). Li, Rong and Thatcher (2012) explain how one party has a willingness to be vulnerable to the other to carry out the task irrespective of the ability to monitor or control them (Li, Rong, Thatcher, 2012, p20). There are a number of ethical consideration and laws that various countries have regarding the safeguarding of privacy that need to be considered as well (Thomas, Duessel, Meier, 2017, p11), something that could be an issue for an ethical hacker that tests a multi-national organisation.

Penetration testing is a highly technical and complex field. An ethical hacker requires deep knowledge across many areas, including, but not limited to software, hardware, networking, and even human behaviour. The knowledge required by a highly effective ethical hacker includes detail of how these areas work at their most basic level, such as the OSI model (the reference model that show the layers of how communication occurs on a network ("The OSI Model's Seven Layers Defined and Functions Explained", n.d.), software code, and even electronic signals. Because of this, it can be very difficult to evaluate the effectiveness of an ethical hacker, especially if this knowledge isn't possessed by the evaluator. Fabian (2009) highlights that the ability to evaluate a professional's abilities from the outside can be difficult, if not impossible and certain level of belief is required (Fabian, 2009, p54).

To date, there has been little research on ethical issues on ethical hacking. However, there has been some research around ethical issues and issues of professionalism on ICT professionals. Whilst not solely an ICT profession, ethical hacking crosses into the ICT domain as many of the systems involved in the hacking process are either ICT systems, or leverage the use of ICT systems.

As ICT is a relatively new profession (Burmeister 2015), it can also be perceived as immature. There is currently neither a mandatory or unified code of ethics that exists within ICT (Burmeister 2013; Capurro and Britz 2010; Whitehouse et al. 2016). The absence of a code of ethics, which has consequences for violations, increases the risk of a variety of inappropriate behaviours including misrepresentation, taking credit for others' work, privacy and confidentiality issues, and failure to comply with laws. Licensing is also not generally a requirement for ICT professionals (Fabian 2009). All of this is also true for information security professionals and ethical hackers. Although the mainstream certifications such as EC-Council's Certified Ethical Hacker (CEH), ISC2's Certified Information System Security Professional (CISSP), and ISACA's Certified Information Security Manager (CISM) certification all require the acceptance and adherence to each of their respective codes of ethics, they are not uniformed and only required for those that have achieved the certifications.

Although the title "Ethical Hacker" implies ethical behaviour, this may not always be the case. For instance, an ethical hacker needs to keep their knowledge of exploits up to date, and they will likely need to go "underground" to gain this knowledge (Conran 2014). Because ethical hackers may even utilise questionable means to gain intelligence it may result in a question of their professional ethics. Although in this sense it can be argued that ethical hackers are partaking in questionable activities, the rationale for which is likely justified as being for the greater good, it does raise the question: at what point may this justified ethical behaviour become blurred and the practices of the ethical hacker become unethical? Given the already identified need for a specialised skill set and experience to be an effective ethical hacker, it is not out of the question that an 'ethical hacker' may once have been a black hat/malicious hacker. A good example of this is Kevin Mitnick; Mitnick is now a 'white hat hacker' and security consultant, however, in the 1990's he was a notorious hacker who was arrested by the FBI and convicted of seven counts of wire and computer fraud. (Gengler, 1999, p6). Many organisations perform online background checks and review the social networking accounts of applicants as standard practices (Stuart et al. 2015). But this background checking assumes that there's something to find and isn't by any means foolproof.

5 Current Literature Analysis

Of the articles written on ethical hacking, only 0.1% discuss implied trust and 3.9% discuss professionalism. As shown in Figure 1, prior to 2001, there were no records returned for literature that discusses implied trust and ethical hacking. The largest spike was in 2013, where five articles were published. 2013 saw a few significant large breaches, including the Target breach and Adobe breach, and over 822 million records exposed (Hawes, 2014), which could explain the spike during that year.

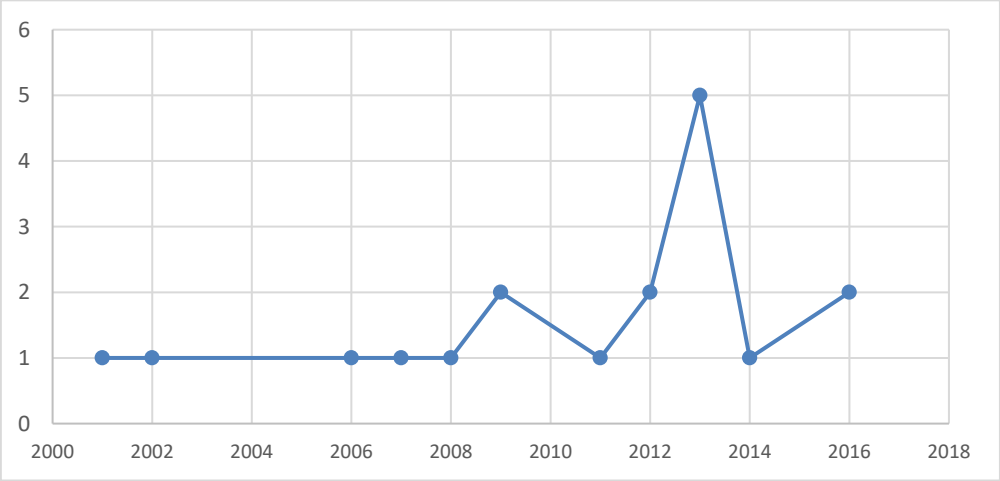

Figure 1 – Articles published year on ethical hacking and implied trust.

As described previously, there is no currently no uniform or mandatory code of conduct for ethical hacking. This same concern has been raised in regard to ICT professionals, where it has been recommended that ACS code of ethics is mandated through National regulations (Bowern, Burmeister, Gotterbarn, Weckert, 2006, p175). More closely, Gay (2012), discusses how implied trust exists between so-called experts and without any standard certification or code of conduct (Gay, 2012, p13). There is also generally no licensing requirement for ICT professionals (Fabian, 2009, p54) and this applies to

ethical hackers too. It was highlighted that there is a level of incompetence in the field of digital forensics, which can lead to issues with investigations and that the lack of a standard code could contribute to the issue. Additionally, a survey of ICT professionals in the UK, found that one third of IT personnel misused their privileges and searched the corporate network for confidential information, including salary information, personal information, board minutes and personal emails (Survey Reveals Scandal of Snooping IT Staff, 2008, p24). Uncovering access to some these items may be part of an ethical hacker's engagement, but ensuring appropriate ethical behaviour through the handling of such confidential information could be a concern.

Ethical hacking, like digital forensics, fall into the "Information Security" field, they are simply different subsets, but still prone to the same issues and vulnerabilities such as misuse of information and the need to ensure competence of the professional. Much of the literature, although discusses ethical hacking and implied trust, does not actually correlate the two. The implied trust discussions in the existing literature are focused on the context of implied trust towards systems and platforms, such as trust toward security platforms (e.g. authentication systems) and well-known websites (e.g. Facebook) or how implied trust is taken advantage of by an attacker, such as spoofing an email as part of a phishing attempt (Cole, 2002, p51).

What is noteworthy, is that the same implied trust manipulation a malicious attacker uses to trick a victim, is how an ethical hacker manipulates a target as part of a test. Other literature simply discusses ethics on teaching ethical hacking to students. Students may use the techniques they have learned irresponsibly, inappropriately or in an illegal manner, which some security educators consider to be unethical and socially irresponsible (Trabelsi, McCoey, 2016, p3-5). Teaching students to hack provides them with knowledge of how to cause damage to computer networks (globally) with the help of university lecturers. This could pose an unimaginable threat (Jamil, Khan, 2011, p 3758). A study undertaken at a Canadian university, noted that there are concerns about the compromise of personal information by the ethical hacker that may result from conducting a penetration test (Abu-Shaqra, Luppicini, 2016, p67).

The focus on education however leaves out one area completely and it might prove fruitful grounds for further research. Namely, "Are these formally trained ethical hackers any match for the 'real' hackers?" This is an area that does not appear to be addressed in any of the literature reviewed, and yet would appear to be a logical extension of the 'educative' focus of several of the article. That is, testing the efficacy of the ethical certifications currently being spruiked.

Jamil et. al (2011) suggest that mandatory security background checks should be undertaken for people who are part-taking in ethical hacking courses. Conducting these checks forms part of good due diligence activities, which many security frameworks such as the International Organization for Standardization (ISO) ISO27001 framework include (International Standards Organization, n.d). The adoption of such a framework by an organisation however, is not mandatory. Whilst some industries have regulatory bodies that mandate that background checks are completed, such as the Securities and Exchange Commission (SEC) and Financial Industry Regulatory Authority (FINRA) in the USA, and the Australian Securities and Investments Commission (ASIC) and the Australian Tax Office (ATO) in Australia, this requirement does not apply uniformly across all industries. Additionally, a background check is not likely to provide complete protection, but rather assist in lowering risk to an acceptable level.

5.1 Current Codes of Conduct

As described, there are currently a number of available codes of conduct that are available from various certification bodies around the world (Burmeister, 2017).

5.1.1 Australian Computer Society (ACS) Code of Ethics

Founded in 1966, the Australian Computer Society is a professional association for the information, communications, and technology (ICT) industry. Although historically focusing on specifically ICT professionals, the ACS launched its cyber security certification for ICT professionals in September 2017 (Pollitt, 2017). All members of the ACS must adhere to the code of ethics.

5.1.2 CREST Code of Conduct

CREST is a not for profit organisation that originated in the United Kingdom, but has since launched chapters across Europe, Middle East, Africa and India (EMEA), The Americas, Asia, and Australia and New Zealand. CREST's purpose is to provide a level of assurance that organisations and their security staff have a level of competence and qualification in conducting security work such as penetration testing, threat intelligence or incident response (CREST®, n.d.). CREST qualified professionals must

abide by the CREST Code of Conduct. The CREST code of conduct is fairly detailed and covers requirements such ensuring regulatory obligations, adequate project management, competency, client interests, confidentiality, and ethics (CREST®, 2016).

5.1.3 EC-Council Code of Ethics

The International Council of E-Commerce Consultants, known as EC-Council was formed after the September 11, 2001 attacks in the United States to address cyber-attack threats (EC-Council, n.d.). EC-Council is best known for its' Certified Ethical Hacker (CEH) certification, which is recognised as a US Department of Defence (DoD) 8570 cyber security certification. The EC-Council Code of Ethics requires confidentiality of discovered information, ensuring that any process or software obtained is legal and ethical, ensuring proper authorisation, adequate project management, continuing professional development, ethical conduct, and not being convicted of any crimes (EC-Council, n.d.).

5.1.4 GIAC Code of Ethics

Global Information Assurance Certification (GIAC) provide some of the most well-known and highly regarded certifications in the security industry. These certifications include penetration testing, security management and digital forensic certifications. Established in 1999, GIAC was established to provide assurance of the skills of information security professionals (GIAC, n.d.). The GIAC Code of Ethics is broken into four sections; respect for the public, respect for the certification, respect for the employer, and respect for oneself. The code mandates that professionals will take responsibility and act in the public's best interests, ensure ethical and lawful conduct, maintaining confidentiality, competency, accurate representation of skills and certifications, and avoiding conflicts of interest (GIAC, n.d.).

5.1.5 ISACA Code of Professional Ethics

ISACA is a professional body established in 1969 with over 140,000 members worldwide that focuses on IT governance (ISACA, n.d.) . Formerly known as the Information Systems Audit and Control Association and focused on IT audit and assurance, ISACA now also includes training and certification for information security and cyber security professionals. The ISACA Code of Professional Ethics mandates that compliance with standards and procedures is maintained, due diligence and professional is taken, legal conduct, confidentiality is maintained, competency, and continuing professional development (ISACA, n.d).

5.1.6 ISC² Code of Ethics

ISC² is an international, non-profit organisation with over 125,000 members in the information security profession (ISC2, n.d.). ISC²'s Code of Ethics consists of four directives; protecting society and public interest, act honourably, honestly, justly, responsibly and legally, be competent, and advanced to protect the profession (ISC2, n.d.).

As previously stated, all current codes of conduct are voluntary and only applicable to individuals who are members or certified individuals of the respective body. There are some certification bodies, however, that do not have a code of conduct requirement. An example is Offensive Security, who provide in-depth training and certification on ethical hacking; their examination is regarded as one of the most difficult and highly regarded certification involving successful passing of a hands-on lab test in order for a candidate to obtain the credential. For those codes that do exist; although they contain similar directives, they are all different and include different levels of detail.

6 Developing a Mandatory, Uniform Code of Conduct

As identified, there are codes of conduct and ethics available from numerous professional and certification bodies. These codes, however, are only mandatory to those who are members or certified by the respective body. There are many similarities between codes, but they are not completely in alignment. There is no identified direct conflict between codes and there are certainly useful attributes from each code that could be used to form a uniform code of conduct for ethical hackers and cyber security professionals alike. In order for the code to be effective, it would need to be mandatory and have adequate oversight. Examples of this include GIAC's Ethics Council and ISACA's Ethics Committee that review ethics matters that don't comply with their code and take action accordingly.

In other professions such as lawyers, doctors, and accountants we see such mandatory codes and the need for those codes to develop and adapt to economic changes, government influence, and changes within the profession (Backof, Martin, 1991). In Australia, legislation such as the Legal Profession Uniform Law is in force and must be adhered to (New South Wales Government, 2015). This legislation

applies to all practicing lawyers and must be complied with. The purpose of the legislation is to ensure all lawyers act ethically and comply with the provisions required and such a requirement of ethical hackers who can potentially access highly confidential and sensitive information and are entrusted to do so should have similar requirements applied.

Unlike most doctors, lawyers and accountants, many cyber security professionals engage with organisations across borders, either locally or internationally. This is especially true when engaged by multi-national companies to review and test their security. This increases the importance of a unified code that is suitable on a global scale and applies to all cyber security professionals engaging in practices such as ethical hacking.

7 Conclusion

The use of ethical hackers as part of a good security strategy is evident and the use of them is likely to increase. There are many ethical implications that need to be considered. Because ethical hackers use the same techniques as malicious attackers, such as the email spoofing example, and often research and gain intelligence through the same questionable challenges, there is a fine line between an ethical white hat hacker, and a malicious black hat hacker; this further highlights the importance of appropriate professionalism and ethical behaviour.

Because of the implied trust relationship between an ethical hacker and the client, the ethical hacker is effectively given permission to access any information they can, much of which could be confidential or sensitive in nature. It has been identified, that ICT professionals have snooped and misused their privileges, and there is no reason why an ethical hacker would not do the same and further research in this area is warranted.

It is clear that implied trust is an issue, and there is merit in further research in this area. This research could include identifying whether there is merit in developing a mandatory, unified code of conduct that applies to ethical hackers and helps ensure appropriate ethical behaviour and levels of competence before an ethical hacker can or should be engaged or some form of licensing requirement.

8 References

Abu-Shaqra, B., & Luppicini, R. (2016). Technoethical Inquiry into Ethical Hacking at a Canadian University. *International Journal of Technoethics* (IJT), 7(1), 62-76.

Al-Saggaf, Y., Burmeister, O.K., and Schwartz, M. (2017) Qualifications and ethics education: the views of ICT professionals, *Australasian Journal of Information Systems*, 20. [LP130100808].

Backof, J. F., & Martin, C. L. (1991). Historical perspectives: development of the codes of ethics in the legal, medical and accounting professions. *Journal of Business Ethics*, 10(2), 99-110.

Bowern, M., Burmeister, O., Gotterbarn, D., & Weckert, J. (2006). ICT Integrity: Bringing the ACS Code of Ethics up to date. *Australasian Journal of Information Systems*, 13(2).

Burmeister, O.K. (2017) Professional Ethics in the Information Age, *Journal of Information, Communication & Ethics in Society*, 15(2).

Burmeister, O.K. 2015. "Improving Professional It Doctorate Completion Rates," *Australasian Journal of Information Systems* (19), 2015-08-18, pp. 55-70.

Burmeister, O.K. (2013) Achieving the goal of a global computing code of ethics through an international-localisation hybrid, *Ethical Space: The International Journal of Communication Ethics*, 10(4), 25-32.

Cohen, F., Lambert, D., Preston, C., Berry, N., Stewart, C., & Thomas, E. (2001). A framework for deception. *National Security Issues in Science, Law, and Technology*.

Cole, E. (2002). *Hackers beware*. Sams Publishing.

Conran, B. 2014. "Why You Shouldn't Hire an Ethical Hacker," *Security* (51:3), Mar 2014

Coyne, A. (2017) “Petya damage to TNT Express systems is likely permanent”. *IT News*. Retrieved from: https://www.itnews.com.au/news/petya-damage-to-tnt-express-systems-is-likely-permanent-468600

CREST®, n.d., “About CREST”. Retrieved from: http://www.crest-approved.org/about-crest/about-crest/index.html

CREST®, 2016, "Code of Conduct for CREST Qualified Individuals". Retrieved from: https://www.crest-approved.org/wp-content/uploads/Code-of-Conduct_Individual.pdf

Dosen, B. (2013). Keamanan sistem informasi materi 2. Retrieved 13 Aug. 17 from http://eprints.binadarma.ac.id/1001/1/KEAMANAN%20SISTEM%20INFORMASI%20MATERI%202.pdf

EC-Council (n.d.). "About EC-Council". Retrieved from: https://www.eccouncil.org/about/

EC-Council (n.d.). "Code of Ethics – EC-Council". Retrieved from https://www.eccouncil.org/code-of-ethics/

Egan, M. (2017). "What is the dark web and the deep web?". *Tech Advisor from IDG*. Retrieved 13 Aug. 17 from http://www.techadvisor.co.uk/how-to/internet/what-is-dark-web-deep-web-3593569/

Eminağaoğlu, M., Uçar, E., & Eren, Ş. (2009). The positive outcomes of information security awareness training in companies–A case study. *Information security technical report*, 14(4), 223-229.

Fabian, R. (2009). Professional Essence. *IT Professional*, 11(3), 54-56.

Gay, J. R. (2012). *A Code of Conduct for Computer Forensic Investigators*(Doctoral dissertation, University of East London).

Gengler, B. (1999). Cyber attacks from outside and inside. *Computer Fraud & Security*, 1999(5), 6-7.

Gersch, J. E. (2013). *ROVER: A DNS-based method to detect and prevent IP hijacks* (Doctoral dissertation, Colorado State University).

GIAC, (n.d.), "About GIAC". Retrieved from: https://www.giac.org/about

GIAC, (n.d.), "GIAC Code of Ethics". Retrieved from: https://www.giac.org/about/ethics

Goodin, D. (2017). NSA-leaking Shadow Brokers just dumped its most damaging release yet. *Ars Technica*. Retrieved 31 July, 2017 from https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet/

Gottenbarn (n.d). An Evolution of Computing's Codes of Ethics and Professional Conduct. Retrieved from http://csciwww.etsu.edu/gotterbarn/artge1.htm

Graves, K. (2010). *Certified Ethical Hacker Study Guide*. Wiley Publishing Inc, Indiana, USA

Grow, B. (2006). Phisher kings court your trust. *BusinessWeek Online*.

Hagan, F. E., & Hagan, F. E. (1997). *Research methods in criminal justice and criminology* (pp. 129-41). Boston: Allyn and Bacon.

Hargrave, V. (2012). "Hacker, Hacktivist, or Cybercriminal?". *Trend Micro*. Retrieved 13 Aug. 17 from http://blog.trendmicro.com/whats-the-difference-between-a-hacker-and-a-cybercriminal/

Hawes, J. (2014). "2013 an epic year for data breaches with over 800 million records lost.", "*naked security by Sophos*". Retrieved from https://nakedsecurity.sophos.com/2014/02/19/2013-an-epic-year-for-data-breaches-with-over-800-million-records-lost/

Identity Theft Resource Center (2017). "2017 – Breach Category Summary". Retrieved Aug 12, 2017 from http://www.idtheftcenter.org/2017-data-breaches.html

International Standards Organization (n.d.), ISO/IEC27000 family – Information Security Management Systems. Retrieved from: https://www.iso.org/isoiec-27001-information-security.html

ISACA, (n.d.). "About ISACA". Retrieved from: http://www.isaca.org/about-isaca/Pages/default.aspx

ISACA, (n.d.). "Code of Professional Ethics.", Retrieved from http://www.isaca.org/certification/code-of-professional-ethics/pages/default.aspx

ISC2, (n.d.), "Cybersecurity and IT Security Professional Organization | (ISC)2. Retrieved from: https://www.isc2.org/About

Jamil, D. A. N. I. S. H., & KHAN, M. N. A. (2011). Is ethical hacking ethical?. *International Journal of Engineering Science and Technology*, 3(5).

Li, X., Rong, G., & Thatcher, J. B. (2012). Does Technology Trust Substitute Interpersonal Trust?: Examining Technology Trust's Influence on Individual Decision-Making. *Journal of Organizational and End User Computing* , *24*(2), 18-38.

Stuart, J.M., Chapple, M., and Gibson, D. 2015. *Certified Information Systems Security Profession Study Guide*, (7th ed.). Indianapolis, IN: John Wiley & Sons.

Mark, W. Principled Assuredly Trustworthy Composable Architectures.

Martin, R. A., Moore, J. W., Seacord, R. C., Sloan, K., Ormerod, M., Mkpong-Ruffin, I., ... & Crocker, M. (2007). Software Security. *Crosstalk*, *801*, 775-5555.

Martin, S., Picard, L., Ayers, M., Hoffman, D. B., & Mock, K. (2008). State of Alaska Election Security Project Phase 2 Report.

McStay, A., Bakir, V. (2015). Assessing interdisciplinary academic and multistakeholder positions on transparency in the post-Snowden leak era. *Ethical Space: The International Journal of Communication Ethics,* 12(3/4), 25-38

Neto, A. (2012). *Security Benchmarking of Transactional Systems*. (Doctoral dissertation, University of Coimbra).

Newton, J. (2013). *Identity theft* (Doctoral dissertation, Cardiff University).

New South Wales Government, (2015). Legal Profession Uniform Law Australian Solicitors' Conduct Rules 2015. Retrieved from: https://legislation.nsw.gov.au/~/view/regulation/2015/244

Pollitt, E. (2017). ACS Launches world-first cyber certification. Retrieved September 30, 2017 from https://ia.acs.org.au/article/2017/acs-launches-world-first-cyber-certification--.html

Rosinger, C., Uslar, M., & Sauer, J. (2013). Threat Scenarios to evaluate Trustworthiness of Multi-agents in the Energy Data Management. In *EnviroInfo* (pp. 258-264).

Survey Reveals Scandal of Snooping IT Staff. (2008). *Software World*, 39(4), 24

Telstra (2017). "Telstra Cyber Security Report 2017"

"The OSI Model's Seven Layers Defined and Functions Explained", n.d., Microsoft. Retrieved from https://support.microsoft.com/en-us/help/103884/the-osi-model-s-seven-layers-defined-and-functions-explained

Thomas, G. A. (2017) "An ethical hacker can help you beat a malicious one", *The Conversation*.

Thomas, G., Duessel, P., & Meier, M. (2017). ETHICAL ISSUES OF USER BEHAVIORAL ANALYSIS THROUGH MACHINE LEARNING. *Journal of Information System Security*, 13(1).

Trabelsi, Z., & McCoey, M. (2016). Ethical Hacking in Information Security Curricula. *International Journal of Information and Communication Technology Education*, 12(1), 1-10.

Tutzauer, C. (n.d.) The Role of Trust in the Successful Implementation of Information Systems. Retrieved from http://www.academia.edu/747081/The_Role_of_Trust_in_the_Successful_Implementation_of_Information_Systems

Verizon (2017). "Verizon Data Breach Investigations Report 2017" http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

Whitehouse, D., Duquenoy, P., Kimppa, K.K., Burmeister, O.K., Gotterbarn, D., Kreps, D., and Patrignani, N. 2016. "Twenty-Five Years of Ict and Society: Codes of Ethics and Cloud Computing," *ACM SIGCAS Computers and Society* (45:3), pp. 18-24.