The Importance of Ethical Conduct by Penetration Testers in the Age of Breach Disclosure Laws.

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

Oliver Burmeister
Charles Sturt University

Gregory Low
SQL Down Under

Abstract

Across the globe, there has been a noticeable increase in the adoption of breach disclosure laws that are designed to protect the privacy of individuals. To validate the security controls implemented by an organisation to protect sensitive data, penetration testers are often engaged to test the security of information systems and to report any vulnerabilities. Using an interpretivist, constructivist approach, this article reports on a pilot study that compares USA and Australian approaches to ethical hacking. The need for regulation of ethical hacking to help protect organisations from unethical conduct was a recurring theme. With the changes in privacy regulations across the world, unauthorised disclosure of personal and privileged information could result in significant consequences. This paper explores the importance of ethical conduct by penetration testers based on empirical research and the potential for misuse of information.

Keywords: Penetration Testing, Ethics, Privacy legislation, Data Misuse, Privacy.

1 The Rise of the Breach Disclosure Law

Although privacy laws can be dated back to the 15th century and the breach of confidentiality tort to the early twentieth century (Solove, 2006, p17), the last decade has seen an emphasis on privacy relating information systems in security and other areas, as it relates to electronic data (Solomon, 2014; Weidenmier and Ramamoorti, 2006; Thomas, Duessel and Meier, 2017; Thomas, Burmeister and Low, 2017; Bowern, Burmeister, Gotterbarn and Weckert, 2006; Burmeister, Islam, Dayhew and Crichton, 2015; Livari and Livari, 2011). Privacy is difficult to define as what one person considers privacy, may not be reflected by another. At a high-level privacy could be defined as the right for an individual to keep their information private. Li et al. (2013) saw privacy as a social concept and privacy breaches in terms of societal perceptions. Personal information is defined as "Information or an opinion about an identified individual, or an individual who is reasonably identifiable" (Office of the Australian Information Commissioner, 2018). This includes information such as credit information, health information, tax information, and other sensitive information.

Closely associated with the concept of privacy is that of confidentiality, and thus with breaches of confidentiality (Bernoth, Dietsch, Burmeister and Schwartz, 2014). Bernoth et al. (2014, p 454) claimed that "In discussing breaches of confidentiality it is important to remember that there are justifiably instances when breaches ought to occur and, therefore, not all breaches

are unethical." Similarly, as seen in the discussion section of this article, there are legitimate times when an ethical hacker breaches privately held, confidential information.

The latest iterations of privacy laws across the globe generally impose specific notification requirements and often significant financial penalties for non-compliance in relation to the unauthorised disclosure of personal information. Commonly referred to as breach notification, in the event that an organisation believes that personal information they hold is disclosed to an authorised party, there may be notifications requirements depending on the laws of the jurisdiction (Muntermann & Roßnagel, 2009).

In 2017, Verizon (2018) confirmed over 2,216 data breaches, and the Identity Theft Resource Center (2017) reported that over 174,402,528 records were exposed. The number of breaches reported by Verizon is up 14.5% from 2016 and 2,462.2% from 2008 and these are only those that were reported or discovered. While it is likely that the sophistication of cyber incident detection systems and a general increase in awareness may account for much of the increase compared to 10 years ago, the disclosure of over 174 million records in 2017 itself is alarming and it is unsurprising that governments across the world have started to address the issue of data security through legislation.

2 Ethical Hacking

Penetration testing, also known as ethical hacking, is an offensive manoeuvre carried out by a security professional with the aim of gaining access to an organisations' systems or data to validate the effectiveness of the security controls that have been implemented. Traditionally, a defensive approach through the use of multilayered technical controls such as firewalls, network segmentation, and antivirus software was used to protect organisations (Thomas, Burmeister, Low, 2017). This purely technical approach then evolved to address people-based aspects otherwise known as the "human factor", largely driven by a significant increase in email-based attacks or 'phishing attacks' (Eminağaoğlu, Uçar & Eren 2009, p223).

The term 'hacker' originated at MIT in the 1960's to describe someone who had the ability to understand and manipulate technology. Although this is still true of hackers, their skills have evolved outside of just technical capabilities to include the ability to manipulate people. Additionally, hackers are now categorised into three distinct categories that identify their motives.

2.1 Black Hat Hackers

A black hat hacker also known as a 'cracker' (Graves, 2010, p3) is a hacker with malicious intent. The intent of a black hat hacker is usually financially motivated, however, there are other motives also, such as causing disruption to systems or committing espionage. Black hat hackers operate illegally and can be individuals, teams, part of an organised crime syndicate, or even terrorist groups. According to Verizon (2018), in 2017, 50% of breaches were attributed to organised crime and 76% of breaches were financially motivated.

2.2 White Hat Hackers

A white hat hacker also known as an ethical hacker is a hacker who uses their skills for the purpose of protecting organisations against malicious hackers by identifying vulnerabilities in an organisation's security controls. Through a formal engagement, a white hat hacker uses the same tools and techniques as a black hat hacker to test the security of the target organisation (Graves, 2010, p3). White hat hackers are generally bound by contractual obligations such as

non-disclosure agreements and specific rules of engagement that provide authorisation, which allows them to conduct tests that would otherwise be illegal (Thomas, Low and Burmeister, 2018).

2.3 Grey Hat Hackers

Between the black and white hat hackers is the grey hat hacker. Grey hat hackers are still considered to operate illegally, but their motives aren't generally considered malicious. Unlike a black hat, a grey hat may provide more 'white hat' services, such as identifying weaknesses in systems that they then highlight to the organisation with the weakness. This is conducted without authorisation, however. Nation state hackers are also considered grey hats as what they do can also be considered questionable. On the one hand, nation state hackers act in the best interests of the country they are representing as part of cyber warfare and helping to keep the nation they represent safe through intelligence gathering. On the other hand, the targeted nation would consider the hack to be unauthorised and illegal (Burmeister, Phahlamohlaka and Al-Saggaf, 2015).

An interesting additional grey hat category is the hacktivist. Where a hacker is motivated by the promotion or defence of a cause, rather than for personal or financial gain, this is known as hacktivism (Hargrave, 2012). The term hacktivism is a portmanteau of hack and activism. Mikhaylova (2014) describes hacktivism as an emerging form of political and social participation. Common examples of hacktivism include the defacement of websites or the leaking of confidential (and often classified) information to the public or media. Two well-known hacktivist groups are Anonymous (Carter, 2012) and WikiLeaks (Thomas, Low, Burmeister, 2018; Beyer, 2014; Ludlow, 2010).

3 The Breach Disclosure Law Landscape Today

Although laws around privacy and the security of personal information have existed for some time, there has been a noticeable increase in laws and regulations that specifically require the disclosure of a data breach. Previously, it was largely up to the discretion of an organisation whether they disclosed a breach and often times, unless a breach made headlines, it would likely go unreported. In many cases, breaches were not even identified by the organisations who were the victims of the breach. In 2016 the average time it took for a breach to be detected was 99 days, down from 146 days in 2015 (Mandiant, 2017). This alarming data means that on average, an attacker has almost four months to exfiltrate data from an organisation before they are detected. Although it varies from organisation to organisation, current internet speeds would allow very substantial volumes of data to be leaked. Such data, if personally identifiable and depending on the type, could be sold on the dark web. The dark web is part of the deep web (not searchable by stand search engines such as Google) that has been hidden and requires special browsers to access. It is commonly used to sell illegal items and personal information that is sold could be used to enable identify theft, and from that, credit card fraud (Chertoff, Simon, 2015).

It is of no surprise that governments and lawmakers have now started to address the issue to ensure that those who are affected by a breach are notified in a timely manner. Although it can be argued that once your personal information is disclosed it can be difficult, if not impossible, to contain it, having the awareness that one's personal information was disclosed would allow individuals to take steps to help to protect themselves from fraudulent activities. Many countries including Australia, Canada, and the Philippines have already, or are in the process

of, implementing data breach disclosure laws. Not all countries and jurisdictions have implemented such laws, but the number is increasing.

3.1 Australia

The Notifiable Data Breaches scheme came into effect on February 22, 2018. This amendment to the Privacy Act 1988 requires that eligible organisations are required to notify affected individuals who may suffer serious harm and the Australian Privacy Commissioner in the event of a breach of personal information (Office of the Australian Information Commissioner, 2018). The Office of the Australian Information Commissioner (OAIC) provides some guidance on securing personal information which includes recommending testing of the security controls in place.

Since the scheme came into effect, there has been a steady increase in reported breaches each quarter, with a total of 812 breaches reported as at 31 December, 2018. Most of the reported incidents were due to malicious or criminal attack (Office of the Australian Information Commission, 2018).

3.2 Canada

Canada's data breach disclosure requirement came into effect on November 1, 2018 (Ling, 2018). These requirements are an amendment to the Digital Privacy Act (2015) and require that affected individuals and the Canadian Office of the Privacy Commissioner (OPC) are notified in the event of breaches of personal information that may result in a "real risk of significant harm" (Government of Canada, 2018).

3.3 Europe

Possibly the most stringent regulations to date are those of the European Union (EU). The EU General Data Protection Regulation (GDPR) came into effect on May 25, 2018 and superseded the existing Directive 95/46/EC that has been in place since 1995 (Thomas, 2018). GDPR has a number of noteworthy requirements that include investigation and reporting of a suspected breach within 72 hours, the right to be forgotten, the right to access data held by an entity, the right to data portability, and the right to have errors in the data rectified (European Commission, n.d.).

3.4 Philippines

The Data Privacy Act of 2012 in the Philippines requires that the National Privacy Commission and affected data subjects be notified in the event that personal sensitive information or other information that may be used to commit identify fraud or real risk of serious harm is acquired by an unauthorised person (Wall, 2017).

3.5 The United States

At the time of writing the United States does not have a uniformed data breach disclosure law, however most states have now enacted data breach disclosure laws (Romanosky, Telang, Acquisiti, 2011). States such as New York have even gone as far as making specific security requirements law, however these requirements, such as those in the NYDFS Cybersecurity Regulation (23 NYCRR 500) only apply to financial services and insurance (New York State Department of Financial Services, 2017).

3.6 Specific Regulations

In addition to country or state specific legislation there are a number of other specific regulations that must be considered. These regulations, although not as broad, generally apply to industries that are more susceptible to breaches of privacy. The Health Insurance Portability and Accountability Act of 1996 or HIPAA in the United States has a specific Breach Notification Rule, which requires covered entities to notify affected individuals and the US Department of Health and Human Services in the event of a breach of personal information (U.S. Department of Health & Human Services, 2013). In Australia, the Australian Prudential Regulation Authority (APRA) has proposed a new standard that requires entities which they regulate to notify APRA of material information security incidents (Australian Prudential Regulation Authority, 2018).

3.7 Other Laws

In addition to specific breach disclosure laws, there are relevant laws that should be considered, such as those that relate to computer crimes. Section 10.7 of the Australian Criminal Code Act of 1995 (Cth) for example, covers computer offences. The offences include the unauthorised access, modification, or impairment of data. Likewise, the European Union has a Directive for attacks against information systems. The Directive 2013/40/EU requires measures to help prevent attacks and identity theft as well as sufficient penalties for those that carry out attacks against information systems.

4 Ethical Hacking and Breach Disclosure Laws

Many of these new laws and regulations either recommend or require that appropriate compliance and assurance is considered. Ethical hacking is seen as one method for the prevention of unauthorised disclosure of electronic records by identifying vulnerabilities within systems (Myers, Frieden, Bherwani, Henning, 2008). This is highlighted in a few examples such as the Office of the Australian Information Commissioner that provides guidance on securing personal information. This guidance includes regular testing of systems including considering what type of information is used for testing and, if it is personal information, managing the associated risks (Office of the Australian Information Commissioner, 2015). APRA's proposed standard includes the requirement for systematic testing and assurance to test the effectiveness of security controls (Australian Prudential Regulation Authority, 2018) as does the NYDFS Cybersecurity regulation (New York State Department of Financial Services, 2017). Although not specifically required by HIPAA, the National Institute of Standards and Technology in the United States recommend penetration testing (ethical hacking) be conducted as part of their guidance for implementing the HIPAA Security Rule (Scholl et al., 2008).

5 Method

An interpretivist, constructivist research approach was undertaken. The use of qualitative research is aimed at exploring and understanding the human problem (Creswell, 2009, p4). Due to the nature of the research, this approach was the most suitable as the research aims to first identify and confirm the issue and then gain insight into it.

Through an interview process, the research aimed to gain an understanding of the ethical issues that surround ethical hacking. Purposive sampling involving 28 participants from law firms in Australia and the United States of America, and ethical hackers from consulting firms.

After an informed consent process, each participant was asked a series of interview questions. The questions chosen were targeted and based on the type of participant. All participants were asked whether they could identify any ethical issues and concerns with penetration testing in general and in the context of their roles. Law firm participants were asked whether they were aware if their respective firms had undertaken penetration testing previously and if so, had there had been a due diligence process associated with those engagements. Ethical hacker participants were asked whether they had gained access to confidential information and what was the course of action by which they had obtained such data. Interview audio was recorded and transcribed for analysis and a process of thematic coding the data was then undertaken. This process of coding involved naming and labelling segments of data to categorize, summarize and account for them (Charmaz, 2006). The resultant data was analysed for common themes and interpreted along with the triangulation between identified themes and categories, and the literature. The focus of this article is data obtained which relates to data breach legislation.

6 Discussion of results

Current literature is largely focused on academic research. Jamil and Khan (2011) discuss issues of teaching students to hack without knowing their true intentions. The article further discusses how the outcome of these teachings could result in both bad and good behaviours of students (Jamil, Khan, 2011). This literature also focuses on those that are being taught to hack through academic institutions and doesn't consider existing professionals who have changed into the ethical hacking field. Radziwill, Romano, Shorter, and Benton (2015) discuss how teaching students to hack in school, although it may start out innocently, could result in students stumbling into black hat hacking and facing legal consequences. There is also the possibility that such unethical behaviour by students is encouraged, but this hasn't been explored and could be examined in further research. The legal implications of ethical hacking need to be considered. Because ethical hackers are studying criminal activity, some of the activities the ethical hacker undertakes cannot be distinguished from the crimes themselves (Brodkin, 2009).

6.1 Confidentiality

The thematic analysis revealed confidentiality of information as a major theme related to data breaches. 67% of the research participants and 90% of legal professionals highlighted the importance of confidentiality. This concern is supported by the requirement for legal privilege by legal professionals.

> *"[Law firms have a] duty of confidentiality to our clients. This is managed in some ways through reciprocal confidentiality agreements that are imposed upon pen-testers, but I think there is always an inherent uneasiness about the potential that a pen-tester may access some client's information." – Partner, Australia*

> *"Clients need to have absolute faith when they engage a lawyer that the flow of their information remains private and is protected." – Lawyer, Australia*

> *"We need to ensure that client confidences are maintained because that's one of the real primary reasons why clients come to a law firm. They have an expectation of absolute confidence in relation to their confidential information" – Lawyer, Australia*

> *"In the US, each state has their own ethics rules but as far as I am aware all states have rules regarding confidentiality of information to preserve the attorney client privilege and that's fiercely guarded. The idea is it's a very protected privilege because the idea is that you want your clients to be forthcoming with you; and we want to instil trust and confidence in our clients and our relationships so it's an ethical obligation to protect that attorney client privilege." Lawyer, United States*

This requirement for legal privilege is the same in Australia and the United States, with the same requirements from the Australian Solicitors Conduct Rules and the American Bar Association.

Taking evidence is something that was also a common occurrence by penetration testers. This practice is to provide proof that a vulnerability exists and highlight the type of information or system that was accessed. It is not uncommon for such evidence to be included in the final report. The question of how this information, especially if sensitive, was protected by the testing firm was raised. One respondent stated:

> *"If access is gained, how is that information protected and what sort of systems do they [ethical hackers] have in place to make sure that information doesn't go any further?" – Law Firm Security, Australia*

> *"if there was to be some sort of compromise [of the ethical hacking provider], potentially sensitive information could be exposed or at worst case modified which in terms of wills and stuff like that could be very disastrous for the parties involved" – Lawyer, Australia*

> *"The last thing you want is just to have a rogue cowboy pen-testing from home, and they lose their laptop on the bus on the way to work and all of your data is sitting on their laptop and it gets lost." Law Firm Security, Australia*

When considering what the data breach disclosure laws are designed to do; help reduce the unauthorised disclosure of personal information; it is important to consider not only what personal information an organisation holds but who has access to it.

Data breach disclosure laws largely rely on organisations performing some level of duty of care. The consequences of a breach, in jurisdictions that have breach disclosure laws would likely result in public disclosure, and could result in significant impact to the breached organisation. Law firms for example, have a duty to ensure the confidentiality of their clients' data and unauthorised access of that information could result in serious reputational and financial harm.

> *"Rules around privilege or loss of privilege if disclosed would be disastrous" (Lawyer, Australia)*

> *"with the new laws around disclosing [a breach], everyone is most concerned not necessarily in the actual loss of the data or the breach itself, but in having to come out and admit that that breach has then happened." – Lawyer, Australia*

> *"from a legal point of view, one thing that always comes up is the data that lawyers manage and control, depending on the law firm, and who your customers are, but [the data] could be subject to privacy legislation such as the GDPR" Security Consultant, United States.*

There may also be additional implications, such as compliance with 'the right to be forgotten' requirement of GDPR for information that may have been taken as evidence or inadvertent

disclosure into the public domain. It is important to consider these regulatory issues and laws that various countries have regarding the safeguarding of privacy (Thomas, Duessel, Meier, 2017).

6.2 Regulation

Another theme to emerge from the data was that of regulation. Ethical hackers should be regulated or licensed, as a form of professionalism and this too relates to the issue of data breaches.

> *"By chartering and coming together as a regulated professional organisation, you can explore whether things like insurance, standards, and discipline are mandatory. Effectively like doctors and lawyers, which is to say that you are not entitled to practice without this certification." (Partner, Australia)*

> *"I think the credentialization of the profession if you want to call it that is, is a good and worthy objective. But I think there's a differentiation between the professions that you mentioned as examples [lawyers, doctors, and accountants] and that specific advances that are made in technology absolutely outstrip any of the other areas." – Lawyer, United States.*

> *"Like any sort of profession, I think it's important to have some sort of regulation, it gives outsiders the view that it's more credible pursuit and also some comfort. We talk about background checks or whatever it might be, [regulation ensures this] is being done and to make sure it's competent testing and there's no risks brought by the testers themselves." Lawyer, Australia*

Not only is ICT a relatively new profession, but within ICT, ethical hacking is rarely identified as one of the job classifications for an ICT professional (Weidenmeir and Ramamoorti, 2006; Burmeister, 2015; 2017). There is currently neither a mandatory or unified code of ethics that exists within ICT (Capurro and Britz, 2010; Burmeister, 2013; Whitehouse et al., 2016) or that applies to ethical hackers. While there are codes of conduct or ethics available, these are considered voluntary and only mandatory for those who are members or certified by various certification bodies such as ISC2, ISACA, or EC-Council to name a few (Thomas, Burmeister, Low, 2018). Many of the interview participants raised the issue of regulation or licensing, but also questioned the effectiveness of such regulation and licensing citing the rate that technology advances, compliance issues, and costs as key issues.

Risk management is at the core of a successful security program (Stoneburner, Goguen, & Feringa, 2002) and the engagement of an ethical hacker assists in identifying risk areas that need to be addressed.

> *"It was important from our point of view that the individuals we engaged to do the testing don't add to that risk." – Law firm CISO, Australia*

> *"When we engage in work there are a lot of requirements such as background checks, financial checks, reputation checks, etc."- Partner, Australia*

> *"They're [the ethical hacking provider] a recognised and trusted body that you're working with and that there is a set standard contractual agreement put down in terms of non-disclosure. You always look for those kinds of points when you're actually dealing with the providers that you're seeking to do the testing with." - Lawyer, United States*

It is clear that there are several regulations and laws that are aimed at preventing or at the very least requiring disclosure of a breach. It is key that any ethical hacker is aware of the regulations and laws that apply to them when conducting an engagement. The United States provides a good example of how requirements can vary. Each state can potentially have their own laws and requirements, and from a lawyer's perspective, they would expect an ethical hacker who could be conducting an engagement across different jurisdictions to be compliant.

> *"An ethical hacking company would want to be certain that they are in compliance with those ethics rules and conducting the hacking in the way that would be in compliance with every State's ethical rules." – Lawyer, United States*

In the event that an ethical hacker acts unethically, the increase in risk to an organisation could be significant depending on the realised consequences. While it is fairly clear that criminal and malicious attacks would be subject to the computer offences section of the Australian Criminal Code Act, the applicability of criminal consequences should also be considered when the act of an ethical hacker meets the criteria of a serious offence, regardless of whether they were provided authorisation to conduct a test or if they contravene a law from another jurisdiction even unknowingly.

The unprofessionalism of inadequate testing could result in a threat exploiting a vulnerability, which may result in unauthorised disclosure of information or disruption. Inappropriate information handling or access by the ethical hacker themselves, could also result in unauthorised disclosure and even the misuse of information.

> *"You're giving access to a person who is an outside third party, so do you have an obligation to notify clients? (as part of legal professional ethics requirements)"- Partner, United States*

> *"if there was to be some sort of compromise, potentially sensitive information could be exposed or at worst case modified which in terms of wills and stuff like that could be very disastrous for the parties involved"- Lawyer, Australia*

Because in many instances an ethical hacker is provided with instructions to gain access to any data they can, or they may inadvertently come across it in the course of performing their engagement, it is possible that information that may have contractual obligations protecting it may be accessed. In these instances, there is a requirement to notify the client and possible litigation against the firm may result.

7 Conclusion

The increase in breach disclosure laws around the world has heightened the need for organisations to further protect their sensitive information. This need, and the increased hostility on the Internet in general, is leading to a large demand for cyber security professionals. In the USA alone, NIST (2018) suggest an increase of over 300,000 new professionals, above an existing base of over 700,000 professionals. The relative inexperience of the cyber security professional population is itself a cause for concern, both in terms of maintaining professional and ethical standards, and in terms of achieving effective outcomes, and being able to monitor the quality of those outcomes. A significant percentage of this large group of cyber security professionals will at some point be involved in ethical hacking activities, yet to date there has been little research on the importance of ethical conduct by these ethical hackers.

Organisations need to consider the risks and how they might address those risks. If an ethical hacker gains access to personal information at an organisation they are testing, controls to secure and handle such information appropriately must be considered, to avoid inadvertent disclosure that could affect not only the target firm, but the privacy of the individuals that the data relates to.

This paper identified the need to consider a regulatory approach to ethical hacking that includes requirements such as a uniformed code of ethics and licensing requirements. There may be some difficulties with this approach however, especially when it comes to cross jurisdiction testing. Like in law, accounting, or medical licensing, it may be necessary to look at bridging or multi-jurisdiction licensing options to ensure compliance with laws of specific countries.

As most organisations that employ ethical hackers are not able to assess their effectiveness, there is also a need to be able to assess and monitor the performance of ethical hackers. It is likely that there is a need for organisations to perform higher-level forms of phishing attacks against the ethical hackers, to see if they are finding what they should, and to ensure they are responding appropriately to the knowledge they appear to have gained during the attack.

With the demand for cyber security professionals who conduct ethical hacking services and the importance and sensitivity of such a role, more research and a more formal approaches to ensure appropriate ethical and professional conduct, and compliance is required.

References

Australian Prudential Regulation Authority (2018). APRA to introduce first prudential standard aimed at tackling growing threat of cyber attacks. Retrieved from: http://www.apra.gov.au/MediaReleases/Pages/18_10.aspx

Bernoth, M., Dietsch, E., Burmeister, O. K., & Schwartz, M. (2014). Information Management in Aged Care: Cases of Confidentiality and Elder Abuse. *Journal of Business Ethics*, 122. doi:10.1007/s10551-013-1770-7

Beyer, J. L. (2014). The emergence of a freedom of information movement: Anonymous, WikiLeaks, the Pirate Party, and Iceland. *Journal of Computer-Mediated Communication*, 19(2), 141-154.

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). http://dx.doi.org/10.3127/ajis.v13i2.50

Brodkin, J. (2009). The legal risks of ethical hacking. Network World (Online). Retrieved December 17, 2015 from http://www.networkworld.com/news/2009/042409-usenix-hacking.html

Burmeister, O. K. (2017). Professional Ethics in the Information Age. *Journal of Information, Communication & Ethics in Society*, 15(4), 348-356.

Burmeister, O. K., Islam, M. Z., Dayhew, M., & Crichton, M. (2015). Enhancing client welfare through better communication of private mental health data between rural service providers. *Australasian Journal of Information Systems*, 19, doi:10.3127/ajis.v19i0.1206.

Burmeister, O. K., Phahlamohlaka, J., & Al-Saggaf, Y. (2015). Good Governance and Virtue in South Africa's Cyber Security Policy Implementation. *International Journal of Cyber Warfare and Terrorism*, 5(1).

Burmeister, O.K. (2015). "Improving Professional IT Doctorate Completion Rates," *Australasian Journal of Information Systems* (19). http://dx.doi.org/10.3127/ajis.v19i0.1073

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).

Carter, A. (2012). "From Anonymous to shuttered websites, the evolution of online protest", CBC. Retrieved from: https://www.cbc.ca/news/canada/from-anonymous-to-shuttered-websites-the-evolution-of-online-protest-1.1134948

Charmaz, Kathy (2006). *Constructing grounded theory: A practical guide through qualitative analysis.* Sage Publications Inc., Thousand Oaks, California. P43.

Chertoff, M., & Simon, T. (2015). The impact of the dark web on internet governance and cyber security. https://www.cigionline.org/publications/impact-dark-web-internet-governance-and-cyber-security

Creswell, J. (2009). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches, Third Edition*. Sage Publications Inc. Thousand Oaks, California

Criminal Code Act of 1995 (Cth). Retrieved from: http://www5.austlii.edu.au/au/legis/cth/consol_act/cca1995115/sch1.html

Capurro, R., & Britz, J. B. (2010). In search of a code of global information ethics: The road travelled and new horizons. *Ethical Space: The International Journal of Communication Ethics*, 7(2/3), 28-36.

Davis Wright Tremaine LLP (2016) Summary of U.S. State Data Breach Notification Statuses. Retrieved from: https://www.dwt.com/statedatabreachstatutes/

Directive 2013/40/EU (2013). Retrieved from: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF

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.

European Commission (n.d.) Protection of personal data. Retrieved from: https://ec.europa.eu/info/law/law-topic/data-protection_en

Government of Canada (2018). Digital Privacy Act. Retrieved from http://laws-lois.justice.gc.ca/eng/AnnualStatutes/2015_32/FullText.html

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

Identity Theft Resource Center (2017). *Data Breach Reports*. Retrieved from: http://www.idtheftcenter.org/images/breach/2017Breaches/DataBreachReport_2017.pdf

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, N., Qardaji, W., Su, D., Wu, Y., & Yang, W. (2013). Membership privacy: a unifying framework for privacy definitions. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security* (pp. 889-900). ACM.

Ling, T. (2018). *Canada: Security Breach Notification Requirements Commence on November 1, 2018*. Retrieved from: http://www.bakerinform.com/home/2018/4/6/canada-security-breach-notification-requirements-commence-on-november-1-2018

Livari, J., & Livari, N. (2011). Varieties of user-centredness: an analysis of four systems development methods. *Information Systems Journal*, 21(2), 125-153. doi:10.1111/j.1365-2575.2010.00351.x

Ludlow, P. (2010). Wikileaks and hacktivist culture. The Nation, 4, (25-26).

Mandiant (2017). *M-Trends 2017: A View from the Front Lines*. Retrieved from: https://www.fireeye.com/blog/threat-research/2017/03/m-trends-2017.html

Mikhaylova, G (2014), *The "anonymous" movement: Hacktivism as an emerging form of political participation*. Retrieved from: https://digital.library.txstate.edu/bitstream/handle/10877/5378/MIKHAYLOVA-THESIS-2014.pdf?sequence=1

Moher D, Liberati A, Tetzlaff J, Altman DG, The PRISMA Group (2009). *Preferred Reporting Items for Systematic Reviews and MetaAnalyses: The PRISMA Statement*. PLoS Med 6(7): e1000097. doi:10.1371/journal.pmed1000097

Muntermann, J., & Roßnagel, H. (2009). On the effectiveness of privacy breach disclosure legislation in Europe: Empirical evidence from the US stock market. In Nordic *Conference on Secure IT Systems* (pp. 1-14). Springer, Berlin, Heidelberg.

Myers, J., Frieden, T. R., Bherwani, K. M., & Henning, K. J. (2008). Ethics in public health research: privacy and public health at risk: public health confidentiality in the digital age. *American Journal of Public Health*, 98(5), 793-801.

National Privacy Commission (n.d.) Republic Act 10173 – Data Privacy Act of 2012. Retrieved from https://privacy.gov.ph/data-privacy-act/

New York State Department of Financial Services (2017). Cybersecurity Requirements for Financial Services Companies. Retrieved from: https://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf

National Institute of Standards and Technology (NIST) (2018). *New Data Show Demand for Cybersecurity Professionals Accelerating*. Retrieved from: https://www.nist.gov/news-events/news/2018/11/new-data-show-demand-cybersecurity-professionals-accelerating

Office of the Australian Information Commissioner (n.d.). *Notifiable Data Breaches scheme*. Retrieved from: https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme

Office of the Australian Information Commissioner (2017). *Guide to securing personal information*. Retrieved from: https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information

Office of the Australian Information Commissioner (2017). *What is personal information?* Retrieved from: https://www.oaic.gov.au/agencies-and-organisations/guides/what-is-personal-information#how-does-the-privacy-act-define-personal-information

Radziwill, N., Romano, J., Shorter, D., & Benton, M. (2015). *The ethics of hacking: Should it be taught?* Software Quality Professional, 18(1), 11-15. Retrieved from http://search.proquest.com.ezproxy.csu.edu.au/docview/1764191740?accountid=10344

Romanosky, S., Telang, R., & Acquisti, A. (2011). Do data breach disclosure laws reduce identity theft?. *Journal of Policy Analysis and Management*, 30(2), 256-286.

Scholl, M, Stine, K., Hash, J., Bowen, P., Johnson, L., Smith, C., Steinberg, D. (2008). SP 800-66 Rev. 1 – An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. *National Institute of Standards & Technology*. p31

Solomon, D. B. (2014). Employee and Organization Security Value Alignment Through Value Sensitive Security Policy Design. (PhD Dissertation), Nova Southeastern University, Retrieved from http://nsuworks.nova.edu/gscis_etd/4

Solove, D. (2006). A brief history of information privacy law. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=914271

Stoneburner, G., Goguen, A. Y., & Feringa, A. (2002). *Sp 800-30. Risk Management Guide For Information Technology Systems*. http://www.icsdefender.ir/files/scadadefender-ir/paygahdanesh/standards/NIST%20-%20800-30R0%20-%20Risk%20Management%20Guide%20for%20IT%20Systems.pdf

Thomas, G. (2018). *Should my Australian Business be Concerned about GDPR*? Retrieved from: https://www.praesecure.com/2018/02/28/should-my-australian-business-be-concerned-about-gdpr/

Thomas G., Burmeister, O. K., Low, G. (2017). Issues of Implied Trust in Ethical Hacking: *Proceedings for the Australasian Conference on Information Systems 2017 conference*. Hobart.

Thomas, G., Duessel, P., & Meier, M. (2017). Ethical Issues Of User Behavioral Analysis Through Machine Learning. *Journal of Information System Security*, 13(1).

Thomas G., Low G., Burmeister O. (2018) "Who Was That Masked Man?": System Penetrations—Friend or Foe?. In: Prunckun H. (Eds) *Cyber Weaponry. Advanced Sciences and Technologies for Security Applications*. Springer, Cham

U.S. Department of Health & Human Services (2013). *Breach Notification Rule*. Retrieved from: https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

Wall, A. (2017). *Summary: Philippines Data Privacy Act and implementing regulations. International Association of Privacy Professionals*. Retrieved from: https://iapp.org/news/a/summary-philippines-data-protection-act-and-implementing-regulations/

Weidenmier, M. L., & Ramamoorti, S. (2006). Research opportunities in information technology and internal auditing. *Journal of Information Systems*, 20(1), 205-219.

Whitehouse, D., Duquenoy, P., Kimppa, K. K., Burmeister, O. K., Gotterbarn, D., Kreps, D., & Patrignani, N. (2016). Twenty-five years of ICT and society: codes of ethics and cloud computing. *ACM SIGCAS Computers and Society*, 45(3). doi:10.1145/2874239.2874242

Verizon (2018). *2018 Data Breach Investigations Report*, 11th Edition. Retrieved from: https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf