Ethics in Security Testing

Prepared by: Nick Dunn, Managing Security Consultant

Table of contents

Executive summary

This paper discusses the similarities and differences between professional ethics in the information security industry and ethics in the hacker community. Sources of conflict between the two and shared values of the two are discussed in order to find some reconciliation and come to an understanding of how a shared set of ethics is possible. A reconciled set of ethics allows hackers to function within the corporate world without compromising their principles and allows the commercial world to benefit from some of the more progressive ideas within the hacker community.

A reconciled set of ethics allows hackers to function within the corporate world without compromising their principles and allows the commercial world to benefit from progressive ideas within the hacker community.

Introduction

In this paper we will take a look at the similarities and differences between conventional notions of professional ethics and hacker ethics. This is being done primarily to attempt to reconcile the two in a professional setting where 'ethical hacking', or offensive security, is used as a technique for locating security vulnerabilities and assessing the security posture of systems. The aim is to reconcile the two stances and provide a model that allows ethical hackers, their employers and their clients to perform their work without compromising their principles.

In some professional settings, the word 'hacker' is frequently used in a dismissive or insulting sense, to describe a skilled programmer or IT expert who fails to document their work, writes unreadable or unmaintainable code, accesses systems without authorisation or behaves in some other way that is regarded as unprofessional or unethical (at least by those applying the label in this way). The aim here is to take a more balanced view than this and to examine both the ways in which hacker ethics can contribute to the information security profession and whether or not a hacker who holds these ethics can contribute to the information security industry without a betrayal of their beliefs or integrity.

Before starting, it is important to provide some definitions to ensure that the discussion has some clarity and consistency:

Hacker

The word 'hacker' will be used throughout the paper in its broader, generally-accepted, and least-rigorous sense. That is, to describe an intellectually-curious technology enthusiast with an interest in puzzle solving, programming, creative use of technology, information security and finding novel, usually faster routes to achieving objectives. The word will be used in both of its popular senses to mean someone who uses innovative routes to both achieving objectives and breaking computer security.

There is an opinion amongst the group of expert programmers who describe themselves as hackers, that the word 'cracker' should be used for anyone who attempts to break security, while the word 'hacker' should be reserved for someone who creates innovative technology solutions or applies clever programming tricks [1]. As these two categories are not mutually exclusive and the 'cracker' definition has failed to enter popular culture or common usage, the paper will not make this distinction.

Professional Ethics

The phrase 'professional ethics' will be used to describe the generally recognised standards that a professional adheres to in order to carry out their duties, in what is accepted as a correct and responsible manner. This will be explained and elaborated further in the 'Professional ethics' section below.

The distinction between morality and ethics is an important point to consider as part of this definition. Ethics is the correct way to behave in terms of professionalism and in doing a good job in terms of the defined criteria for that job. Morality can be subjective, and it is possible to do a job that some may consider immoral, such as designing weapons systems, while still adhering to professional ethics, such as documenting the system correctly, ensuring it is maintainable, training others to ensure succession planning, etc.

Offensive Security

Although much of this paper has wider applications, with regards to information security in a wider context and IT in general, the paper will concentrate on 'offensive security'. In this context, offensive security refers what is also known as ethical hacking or penetration testing. This is taken in its broadest sense, to include network and web application security testing, along with adjacent activities that are distinct from traditional penetration testing, but fall within the same area, such as source code security review, threat modelling, mobile application security testing and other related areas. The primary aim of this type of testing is to discover security vulnerabilities in systems prior to release so that the systems can be hardened to improve the security and safety of assets.

This expression is not being used in the paper to refer to the security consultancy company, Offensive Security, unless otherwise stated.

Ethical Hacking

This is a term synonymous with offensive security and describes the security testing of an organisation’s systems (generally known as penetration testing) by those with sufficient skills.

Professional ethics

Wikipedia defines professional ethics as "the personal, and corporate standards of behaviour expected by professionals." [2]

In this context, a profession is distinguished by certain characteristics, including:

- mastery of a particular intellectual skill, acquired by training, education and experience;
- adherence by its members to a common set of values and code of conduct; and
- acceptance of a duty to society as a whole.

Although the Wikipedia definition of professional ethics can seem somewhat broad and lacking in specifics, it goes on to detail these standards in the following list and to further discuss the presence of professional bodies which set and enforce professional standards:

- Honesty
- Integrity
- Transparency
- Accountability
- Confidentiality
- Objectivity
- Respect
- Obedience to the law
- Loyalty

When considering professional ethics in IT, and more specifically, in the information security profession, there are several codes of conduct and codes of ethics that are published by professional organisations and certification providers. We will consider these below in order to give more context to the discussion.

The main professional body for IT in the UK is the BCS [3], although, as will be discussed later, IT professionals and employers do not view membership of a professional body as having the same weight or authority that other professions do.

The BCS Code of Conduct [4] is a general charter for IT professionals and describes the standards expected of a BCS member, grouping them under four broad categories:

- The Public Interest
- Professional Competence and Integrity
- Duty to Relevant Authority
- Duty to the Profession

This code provides detail on a BCS member's obligation to be competent and knowledgeable, to be honest, to perform the work to the best of their ability and to fulfil obligations to fellow professionals. Fulfilling obligations to fellow professionals can include things such as providing a correct scope before work starts, documenting work correctly to assist future maintenance and succession planning in order to ensure that suitably trained staff are in place to administer and maintain any systems that are deployed.

There are professional organisations for information security professionals but, again, employers and professionals both place greater weight on practical experience than membership of a professional organisation.

The Institute of Information Security Practitioners (IISP) [5] has a code of ethics for security professionals [6] which very much reflects the spirit and intentions of BCS Code of Conduct, but is tailored to fit information security professionals. An extract from the IISP's code of conduct is shown below:

> **Code of Conduct**
>
> This code of conduct is intended to guide members in their professional and personal conduct. Members of the Institute of Information Security Professionals shall:
>
> - Act at all times in accordance with the institute's values;
> - Maintain competency and currency in their respective fields;
> - Promote best practice in information security;
> - Act only within their level of competence;
> - Promote and carry out professional services in accordance with the relevant technical and professional standards;
> - Act within the law;
> - Act in a manner consistent with the good reputation of the institute and the profession;
> - Respect the confidentiality of information acquired during the course of their duties and should not use or disclose any such information without proper and specific authority or unless there is a legal or professional requirement to do so;
> - Recognise the potential for any conflict of interests and, where appropriate, take steps to resolve or avoid any such conflict;
> - Support the professional education and development of other members of the profession and other individuals involved in information security.

The Association of Information Security Professionals (AISP) [7] is a body which is responsible a group of professional certifications known as CREST. This certification is respected throughout the United Kingdom, Australia, Europe, and Asia, and there are plans to raise its profile in the USA. It is respected throughout the industry and frequently listed as a requirement by employers, which is unusual in an industry which does not generally hold professional bodies or certifications in high regard.

It maintains a CREST Individual Code of Conduct [8] which reflects many of the values for professional behaviour found in both the BCS and IISP codes of conduct and ethics. The most interesting differences are the requirement to not carry out work if the practitioner does not have the necessary security knowledge and the requirement for ongoing learning to take place throughout the holder's career. Note that the requirement is for sufficient 'information security and associated specialist knowledge', not for sufficient 'technical knowledge' and encourages learning, rather than forbidding the practitioner to carry out any work:

> Understand their limitations of information security and associated specialist knowledge. They must seek advice from appropriately qualified colleagues who have the necessary expertise for any areas that the Member is not qualified for. The Member must not make misleading claims about their expertise.

> [...]
>
> 2.5 Competencies
>
> 2.5.1 All CREST Qualified Individuals must maintain their technical competencies. They must:
>
> i. Keep up to date with technological advances through training, technical publications and specialist groups within professional bodies and recognise that information gained solely from the internet may not be validated.

In terms of other non-profit professional organisations for information security, the Information Systems Security Organisation (ISSA) [9] and International Information System Security Certification Consortium ISC(2) [10] also have ethics codes. These are very similar to the BCS and IISP codes and cover the same areas of being honest, acting for the good of the public and acting for the good of the profession.

The hacker ethic

It is a little flawed to view hackers as a single uniform group since the group is very large and connected by a shared interest and/or profession. Contrary to some of the myths perpetuated by popular culture, hackers are a diverse group who fail to fit the stereotype of teenage, male loner. In addition to the variations in age, culture and beliefs, the group is made up of both professional hackers, working as security consultants and penetration testers, and hobbyist hackers who may work outside the industry but who carry out security research and experiment with technology in their spare time.

Hacker culture has no central authority, hierarchy, formal organisation or codes of conduct. It is, however, generally accepted that the group has a number of shared ideals and heroes, or at least individuals held in high esteem. In the absence of any written codes or single statement, one approach is to use some of the most frequently cited texts describing hacker culture, particularly those which are viewed as having the same weight of authority both inside and outside the hacker community.

The book, Hackers, by Steven Levy [11], has been regarded as a one of the best descriptions of hacker culture and beliefs, since it first appeared in 1984. As it is so highly regarded by both historians of technology and hackers, it will be used as one of the documents to describe the community and its beliefs. Levy's book tells the story behind the first group to identify themselves as hackers, during the 1950s at Massachusetts Institute of Technology (MIT) and those who subsequently came after them, laying the groundwork for the hacker attitude and ethic. It moves on to the 1970s and the birth of Apple under Steve Wozniak and Steve Jobs, before finishing with the birth of the Open Source Movement under Richard Stallman in the 1980s.

The general principles of the hacker ethic are summarised in the preface, where Levy describes four core beliefs:

- Sharing
- Openness
- Decentralization
- Free access to computers

These principles were very much a product of their times, having evolved from a time when access to computers was restricted in many senses. The machines of the time were expensive and available only to companies and universities with the resources to purchase and maintain one. Even if a computer was present at an organisation, access was restricted both physically and by the availability of time slots. The thirst for knowledge and for opportunities to use these fascinating machines laid the foundations for the hacker fascination with circumventing security measures and playing with the latest technology.

Chapter 2 of the book is titled 'The Hacker Ethic' and describes a set of values and beliefs held by the hackers at MIT that Levy encountered. Levy makes it clear that this ethic was not a formal or written code of conduct and describes the ethic as being "silently agreed upon". The description, beginning on page 39, gives the following list:

- Access to computers - and anything which allows thinking and learning - should be unlimited and total
- All information should be free
- Mistrust authority - promote decentralisation

- Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race or position
- You can create art and beauty on a computer
- Computers can change your life for the better

Although there is a slight contradiction in Levy's claim that these principles are silently agreed upon but at the same time accepted by the entire community, much of the chapter is clearly recognisable as today's concept of a hacker and in the underpinning ideas of the open source software that allows the internet and Web to function.

The epilogue of Levy's book is titled, jumping the gun somewhat, 'Last of the True Hackers'. It discusses Richard Stallman's ideas of free and open source software and the origins of the 'copyleft' licence. At the time this was both a new, and old, ethical concept that arose from a desire to return to the freely distributed communal software of earlier times during the first decades of licenced proprietary software. This has, of course, become one of the more recognisable features of the hacker community and the modern hacker is known for a preference for open source software and a willingness to contribute to open source projects.

In The Hacker Ethic and the Spirit of the Information Age [13], Pekka Himanen discusses the work ethic of hackers and, like Levy, recognises the hacker ideal of attempting to improve the world. Himanen views the hacker ethic from a cultural point of view, discussing the work ethic of hackers and their willingness to contribute to projects in their free time, along with their views on privacy and freedom of information. Himanen's starting point is very much takes up where Levy's book ended, as it begins with a discussion of the open source software which both supports the internet and also allows more productive use of it. Himanen discusses Max Weber's The Protestant Work Ethic and the Spirit of Capitalism in which work is viewed as 'a calling', where an individual works because it is the right thing to do, performing this work in the best way possible for the good of society. Himanen argues that the work of hackers such as Linus Torvalds, who have transformed the world by voluntarily contributing to open source software projects is similar to Weber's Protestant Work Ethic, with contributors doing their best to improve technology and improve the world for themselves and others.

Himanen also discusses hacker ethics (as opposed to the hacker work ethic), and discusses a few central themes that are very similar to the principles described by Levy:

- De-centralisation
- Free speech and opposition to censorship
- Personal privacy and freedom from surveillance

The two defining descriptions of hacker ethics put forward by Levy and Himanen are recognised as being accurate and authoritative by those both inside and outside the hacker community. Additionaly they have a number of points in common, with both models concentrating on the improvement of the world, with a belief that the best way to achieve this is through decentralised, uncensored free access to information.

The Hacker Manifesto by The Mentor [Loyd Blankenship] [14] appeared in Phrack magazine in 1986 and is a statement of both ethics and morals. It differs from the works of Levy and Himanen, in that it is the work of a hacker documenting their own beliefs, not an outsider documenting the beliefs of others.

It is focused on the idea of hacking as exploring new systems and circumventing unjust boundaries. Although more than 30 years old and quite short, it is mentioned online on a large number of websites and social media platforms, as encapsulating the beliefs and attitudes of hobbyist hackers, especially during their formative years. Many of the online comments describe it as an extremely accurate representation of their own thoughts and opinions.

Unlike the sets of ethics described above, it takes the form of a fictional conversation between a persecuted young hacker and an authoritarian enemy. It does not give a list of beliefs in the same way that Levy and Himanen do, but describes the hacker sense of curiosity, thirst for knowledge and love of exploration. The main themes are, again, the need for free access to information and to technology and the belief that a person's mind is important, while skin colour, religion, gender and sexuality are not reasons to cast judgement against anyone.

Reconciling the ethical stances

Although the descriptions of professional ethics and hacker ethics that have been discussed so far may seem quite different, a closer examination shows the differences to be largely superficial in many areas. In addition a gradual convergence of the two has taken place in some areas such as the increasing prevalence of open source software which has seen the hacker concept of free information and freedom to modify software evolve into a new business model and new source of software for businesses. In another area the growing use of bug bounty programs by commercial organisations has seen hacker frustrations about the futility, or sometimes dire consequences, of reporting bugs to commercial organisations turned on their head with hackers being actively encouraged to find bugs in a company's software.

Decentralisation

Decentralisation is a key concept in both Levy and Himanen's descriptions of hacker ethics. While this might seem to conflict with traditional, top-down management concepts found in many companies, a narrow view such as this does little justice to the hacker concept of decentralisation or to the modern world of business.

For hackers, decentralisation is a general concept that can improve a system's robustness and prevent its misuse. The classic example of this concept is the Internet, with its lack of central control and consequent ability to self-organise and to recover from errors or damage. Another decentralised solution that is currently transforming the business world is the Blockchain concept, which underlies cryptocurrencies and the general concept of a distributed ledger.

The more democratic styles of management which have arisen in the latter half of the twentieth century and early part of the twenty-first century have as much in common with the hacker concept of open exchange of information in order to reach the best solution as they do with traditional management ideas.

Professional Competence

The subject of professional competence plays a significant role in professional ethics. The general definition of professional ethics and the codes of conduct of professional organisations such as the BCS and IISP all state that a professional should not undertake work unless they have sufficient technical competence. The words "only undertake to do work or provide a service that is within your professional competence" in the BCS professional charter might seem to be in a paradoxical conflict with the hacking community, which views 'learning by doing' as one of the best models and encourages research into new technologies. It's important to take the view here that security levels need a certain minimum level of technical knowledge, their knowledge should not necessarily be the same type of knowledge that a system administrator or programmer would need. The CREST Code of Conduct shows a suitable middle path, stating clearly that both security knowledge and technical knowledge of the system are needed and that it is acceptable to learn on the job if suitable help and advice is available:

Understand their limitations of information security and associated specialist knowledge. They must seek advice from appropriately qualified colleagues who have the necessary expertise for any areas that the Member is not qualified for. The Member must not make misleading claims about their expertise.

Diversity

The ideal discussed by Levy and others of hackers' respect for ideas, intelligence, programming skills or work ethic, regardless of ethnicity, gender, sexuality or beliefs is something that many professions aspire to but very few seem to have achieved. In information security, the professional and commercial world falls short of its own aims, as well as the aims and the generally perceived reality of the hacker world.

In light of reported sexual harassment at IT security events [15], the hacker community cannot view itself as completely guilt-free in regard to sexism, misogyny or other harassment [16]. As the reports often arise at 'professional' events, rather than the more purist, hobbyist events, it can still be argued that the professional community has more catching up to do than the hacker community. Recent progress in this area includes The Event Code of Conduct [17], which has been adopted by a number of hacker events and information security events in order to better protect attendees from harassment. Further details can be found in the book ‘IN Security’ by Jane Frankland [18].

Freedom of Information

The 'all information should be free' point from Levy's description of the 'silent, unspoken' hacker manifesto and Himanen's description of hackers' love of freedom of information can appear to be a potential cause of a great degree of friction between information security professionals and those siding with either of these models of the hacker ethic. The presence of NDAs in projects, contractual obligations applied to security researchers or the enforcement of indictments against security researchers represent an artificial restriction on the flow of information.

There is a need for a sense of pragmatism and compromise, similar to that discussed below in relation to the NDA for OSCP and OSCE. In a business context, freedom of information is helpful in many contexts but not others and compromise is necessary on both sides. The use of open source software and availability of open source intelligence are two contributions from the hacker community that have greatly benefitted the commercial world. Equally, NDAs are required in order to protect confidential information and to protect the viability of the business.

Professional Bodies and Certifications

The information security profession differs from a number of other professions in two aspects of conventional professional ethics:

- Membership of a professional body
- Certifications and/or qualifications

Although membership of a professional body is described by Wikipedia as one of the characteristics of professional ethics, it is not widely adopted in any information security profession or in the IT industry as a whole and not viewed as a necessity by employers. It would seem that, in this respect, information security professionals have a great deal in common with other IT professionals. The BCS has 75,000 members [2]. Although this is a numerically large group, it is less than 10 percent of the UK's total of 931,000 IT professionals [19]. This is in sharp contrast to professions such as law or medicine where membership of a professional body is a requirement, rather than optional.

A review of penetration tester jobs on employment websites, carried out while writing this whitepaper, found no openings which required membership of a professional body. Professional experience was the principal requirement in the job openings, with no stated minimum education requirement, although CREST certification was a common requirement in the UK and OSCP certification was a common requirement elsewhere.

Interestingly, the hacker community holds some certifications in much higher regard than others and several exams which have only a multiple choice aspect and a candidate can prepare for by 'cramming' are viewed as somewhat worthless by many in the hacker community. The key feature of the respected certifications is not just their difficulty, but the fact that they test skills rather than memory. The CREST penetration testing exams, OSCP and OSCE all require a candidate to prove their skills by hacking a number of systems in a limited time frame in order to prove competence (or more correctly, something above the level of regular competence).

These certifications also stand as an example of a situation where hackers are prepared to accept non-disclosure agreements, rather than allowing information to be free to all. The content of the exam is not disclosed and the overwhelming majority of hackers are happy for this to happen in return for the exams remaining a genuine measure of skill rather than an ability to memorise answers. The NDA is seen as a valid cost of the certification remaining a genuine measure of skill.

Vulnerability Disclosure

In the past, the disclosure of vulnerabilities in commercial products has been a source of controversy, particularly when the vulnerabilities were found and disclosed by researchers who were working in their spare time. The three categories used to classify types of vulnerability disclosure were:

Full Disclosure: A researcher publicly discloses all known details of the vulnerability to a public forum without giving prior notification to the product vendor

Coordinated Disclosure: A researcher discloses details of the vulnerability to the vendor first and does not publicly reveal details until the vendor has patched the product (this definition is a recent addition, as the Responsible Disclosure model, below, was felt to be flawed by some researchers)

Responsible Disclosure: A researcher discloses details of the vulnerability to the vendor first and does not publicly reveal details until the vendor has had time to patch the product (this disclosure sometimes takes place if the vendor has had time but has been unresponsive or taken to long in the opinion of the researcher)

Non-Disclosure: A researcher discloses details of the vulnerability to the vendor only and does not publicly reveal any details

Full Disclosure falls into a conflicting position in regard to hacker ethics, satisfying the 'all information must be free' condition, but not necessarily satisfying the 'do no harm' condition. In the past, this type of public disclosure of vulnerabilities resulted in a number of cases of exploits being available before systems could be patched.

The Responsible Disclosure model indicated an evolution of software vendor attitudes and an increasing readiness to acknowledge flaws found by independent researchers, eventually giving birth to vendors paying bug bounties to researchers. The recent addition of the Coordinated Disclosure, which puts forward the idea that Responsible Disclosure is not sufficiently ‘responsible’, began because some vendors and other groups felt that timeframes that were being imposed did not give sufficient time to implement a fix and were placing companies and users at risk [18].

More recently, the increasing number of bug bounty programmes has greatly reduced the number of vulnerabilities being reported to open forums and an increasing number vulnerabilities being disclosed directly to vendors something closer to the Coordinated Disclosure or Non-Disclosure models.

This very much echoes the traditional hacker view that the finder of such flaws should be rewarded rather than being ignored or, in extreme cases, prosecuted. It stands as another example where the hacker community has led the way for the business community, and in this case helped to create a new business model.

Conclusion

Reconciling the hacker ethic with conventional professional ethics for IT and information security is possible and there is no requirement for dilution or abandonment of hacker beliefs in order for an individual holding these beliefs to function correctly in a work environment without compromising their values.

Both parties can benefit from a reconciliation and merging of the two ethical positions and it can be argued that in some areas, hacker ethics have paved the way for the professional ethics of the information security industry and for innovation within the information security profession and the IT industry as a whole.

A stance which satisfies the conditions of professional ethics and hacker ethics is possible, as discussed earlier and can be summarised as follows:

Decentralisation – This is something to aspire to but not rigidly adhere to. It should be an aim for management in general and for professionals to act co-operatively and democratically, reaching decisions through discussion and gathering of correct and relevant information. Systems, both technical and managerial, should avoid single points of failure and should have some element of self-correction where feasible.

Benefit to Society and the Wider World – The professional commitment to the public interest, honesty and integrity are reflected in the hacker ethic of wanting to make the world a better place through technology. Professional ethics and hacker ethics are very similar in this regard, with both communities having similar aims and intentions.

Competency and Currency – A hacker or information security professional should have a minimum level of technical knowledge which allows them to understand software, networks and web applications, along with what can be considered an expert level of knowledge in the field of information security which allows them to assess systems to an appropriate level. In addition, they should keep abreast of current trends in technology and information security, ensuring that, in particular, their knowledge of testing/hacking tools and techniques stays up to date.

Respect for Diversity – It is important that others are not judged according to their race, religion, gender or sexuality. In the workplace, professional community and hacker community, someone should only be judged by their attitude and ability. Nobody should feel harassed, persecuted or intimidated in the workplace, the community or at any event.

Freedom of Information – A hacker or information security professional should distribute research findings to the wider community, where such an action is legal, feasible and does not violate NDAs. Where new code and tools have been developed that may help others, these should be released to the community, preferably under an open source licence.

Respect for Privacy – An individual's personal privacy should not be violated and their personal data should be protected. NDAs should not be violated and findings that would endanger the community or the public should not be disclosed.

Certification – Information security professionals should undertake a certification that demonstrates their professional competence through practical demonstration of their skills. Certifications that demonstrate practical skills should be accorded a higher status than those that test a candidate's ability to memorise a set of answers that are available in the public domain.

Research and Responsible Disclosure – Research into products and vulnerabilities should be carried out without breaking the law and without causing undue harm to the wider community and public. Vulnerabilities should be disclosed in a manner that allows the vendor to fix them promptly and minimises any risk of attackers from abusing the vulnerability before it is fixed.

References

[1] **How to Become a Hacker by Eric S. Raymond**

http://www.catb.org/esr/faqs/hacker-howto.html

[2] **Wikipedia - Professional Ethics**

https://en.wikipedia.org/wiki/Professional_ethics

[3] **BCS**

https://www.bcs.org

https://en.wikipedia.org/wiki/British_Computer_Society

[4] **The BCS Code of Conduct**

https://www.bcs.org/category/6030

[5] **Institute of Information Security Professionals (IISP)**

https://www.iisp.org

[6] **IISP Code of Ethics**

https://www.iisp.org/imis15/iisp/Membership/How_to_Apply/IISP_Code_of_Ethics/iisp/Member/IISP_Code_of_Ethics.aspx

[7] **Association of Information Security Professionals (AISP)**

http://www.aisp.sg/

[8] **CREST Code of Conduct**

https://www.crest-approved.org/wp-content/uploads/2016/05/Code-of-Conduct_Individual.pdf

[9] **ISSA Code of Ethics**

https://www.issa.org/page/codeofethics

[10] **International Information System Security Certification Consortium**

https://www.isc2.org/

[11] **ISC2 Code of Ethics**

https://www.isc2.org/Ethics

[12] **Hackers by Steven Levy**

https://www.amazon.co.uk/Hackers-Heroes-Computer-Revolution-Anniversary/dp/1449388396/

[13] **The Hacker Ethic and the Spirit of the Information Age by Pekka Himanen**

https://www.amazon.co.uk/Hacker-Ethic-Spirit-Information-Age/dp/B00284XZ7Q/

[14] **The Hacker Manifesto by The Mentor [Loyd Blankenship]**

http://phrack.org/issues/7/3.html#article

[15] **Sexual Harassment at Cyber Security Conferences**

https://theintercept.com/2018/06/19/metoo-cybersecurity-infosec-sexual-harassment/

https://www.forbes.com/sites/kateoflahertyuk/2018/08/15/sexual-harassment-in-the-cyber-security-industry-how-one-woman-is-fighting-back/#56f6e4ee576e

[16] **John Draper Allegations**

https://arstechnica.com/tech-policy/2017/11/iconic-hacker-booted-from-conferences-after-sexual-misconduct-claims-surface/

[17] **Code of Conduct for Events**

http://cybersecuritycapital.com/event-code-of-conduct/

[18] **IN Security by Jane Frankland**

http://cybersecuritycapital.com/community/in-security-the-book/

[19] **Total number of IT professionals in the UK**

https://www.statista.com/topics/4218/tech-companies-in-the-united-kingdom-uk/

[20] **Coordinated Vulnerability Disclosure**

https://www.ecfr.eu/article/commentary_time_to_talk_europe_and_the_vulnerability_equities_process

https://www.ncsc.gov.uk/blog-post/vulnerability-co-ordination-pilot

> “Reconciling the hacker ethic with conventional professional ethics for IT and information security is possible and there is no requirement for dilution or abandonment of hacker beliefs in order for an individual holding these beliefs to function correctly in a work environment without compromising their values.”

About NCC Group

NCC Group is a global expert in cyber security and risk mitigation, working with businesses to protect their brand, value and reputation against the ever-evolving threat landscape.

With our knowledge, experience and global footprint, we are best placed to help businesses identify, assess, mitigate & respond to the risks they face.

We are passionate about making the Internet safer and revolutionising the way in which organisations think about cyber security.

Headquartered in Manchester, UK, with over 35 offices across the world, NCC Group employs more than 2,000 people and is a trusted advisor to 15,000 clients worldwide.