Technoethics and Organizing: Exploring Ethical Hacking within a Canadian University

by

Baha Abu-Shaqra

A thesis submitted to the
Faculty of Graduate and Postdoctoral Studies
in partial fulfillment of the requirements for the
MA degree in Communication

Department of Communication
Faculty of Arts
University of Ottawa

Abstract

Ethical hacking is one important information security risk management strategy business and academic organizations use to protect their information assets from the growing threat of hackers. Most published books on ethical hacking have focused on its technical applications in risk assessment practices. This thesis addressed a gap within the organizational communication literature on ethical hacking. Taking a qualitative exploratory case study approach, the thesis paired technoethical inquiry theory with Karl Weick's sensemaking model to explore ethical hacking in a Canadian university. In-depth interviews with key stakeholder groups and a document review were conducted. Guided by the Technoethical Inquiry Decision-making Grid (TEI-DMG), a qualitative framework for use in technological assessment, findings pointed to the need to expand the communicative and social considerations involved in decision making about ethical hacking practices. Guided by Weick's theory, findings pointed to security awareness training for increasing sensemaking opportunities and reducing equivocality in the information environment.

Table of Contents

Technoethics and Organizing: Exploring Ethical Hacking within a Canadian University

> There is no doubt that the frequency and severity of the cyber threat is accelerating. Protecting Canadians in cyberspace will be a constantly evolving challenge. To effectively address this challenge will require a range of actions and responses. (Public Safety Canada, 2013A)

The threat of cyber-attacks on information assets in the private and public sectors is a growing and evolving threat, warns Public Safety Canada (Public Safety Canada, 2013A, 2013B, 2013C). Individuals, industry, and governments in Canada are embracing the advantages of a digital infrastructure. Canada's governments are increasingly dependent on the Internet. The federal government, for example, offers more than 130 commonly used services online, including tax returns, student loan applications, and employment insurance forms. About 75% of Canadian households paid for Internet service in 2008. A McMaster University study finds 1.7 million Canadians were victims of identity theft in 2008. Identity theft is costing Canadians nearly $1.9 billion each year (Public Safety Canada, 2013A). Over two-thirds of Canadian adults were subject to cyber-crime in 2012 (Public Safety Canada, 2013B). Between 2006 and 2008 about 85% of large Canadian organizations suffered at least one cyber-attack. The loss of intellectual property as a result of these attacks doubled during this period. The increasing reliance on cyber technologies makes Canadians "more vulnerable to those who attack our digital infrastructure to undermine our national security, economic prosperity, and way of life," cautions Minister of Public Safety Vic Toews (Public Safety Canada, 2013A).

> Cyber attacks include the unintentional or unauthorized access, use, manipulation, interruption or destruction (via electronic means) of electronic information and/or the electronic and physical infrastructure used to process, communicate and/or store that information. The severity of the cyber attack determines the appropriate level of response and/or mitigation measures: i.e., cyber security. (Public Safety Canada, 2013A)

Cyber-security is a defensive measure, adopted in response to cyber-attacks. It can be understood as a process of applying information security measures to protect the confidentiality, integrity, and availability (CIA) of information. Hackers pose a security risk in that they can compromise the CIA of information. Information security management is concerned with countermeasures to protect the CIA of information assets from various threats, using principles, best practices, and technologies. Once hackers access a computer system, they can steal or alter the information stored on it, or corrupt its operations and program it to attack other computer systems (Dhillon, 2007; Peltier, 2005; Reynolds, 2012; Stamp, 2011).

Hacking: A Growing and Evolving Problem

Most cyber-attacks share four characteristics that, in part, account for their growing popularity. First, they are often inexpensive. Many hacking tools are cheap to buy or can be downloaded for free from the Internet. Second, they are easy to use. Attackers with only basic skills can cause significant damage. Third, they are effective. Even minor attacks can cause extensive damage. Finally, they are low risk. Attackers can evade detection and

prosecution by hiding their tracks through a complex web of computer networks (Public Safety Canada, 2013A, 2013B).

The evolution of cyber-attack tools and techniques has accelerated dangerously in the recent past (Public Safety Canada, 2013A, The Threat, para. 1). The frequency of hacker attacks increases year after year. And every year "those seeking to infiltrate, exploit or attack our cyber systems are more sophisticated and better resourced than the year before," says Public Safety Canada (2013A, Introduction, para. 5). Governments have responded to the changing technical environment and the new threats it raises with bureaucratic and legal frameworks. Launched on 3 October 2010, Canada's Cyber Security Strategy is the federal plan against cyber-security threats. The main objectives of the strategy are to secure government systems and to work with others to secure systems outside of government. The strategy is built on three pillars: securing government systems, partnering to secure vital cyber systems outside the federal government, and helping Canadians to be secure online. The Canadian Cyber Incident Response Centre operates within Public Safety Canada and is more concerned with cyber-security outside the federal government. The 2010-2015 Action Plan developed by Canada's Cyber Security Strategy outlines several countermeasures and initiatives, including the bureau Shared Services Canada, which aims to streamline and secure the management of federal information technology infrastructure; GetCyberSafe, a national public awareness campaign on cyber-security; $155 million in federal funding to reinforce the security, stability, and resilience of the digital infrastructure; as well as supporting cyber-security research and development. In the US, the Government Information Security Reform Act of 2000 makes it mandatory for federal agencies to develop and

implement risk-based, cost-effective policies and procedures for information security management. One important countermeasure to cyber-security threats used by the public and private sectors is ethical hacking.

Hacking and Ethical Hacking

Ethical hacking can be conceptualized through three disciplinary perspectives: ethical, technical, and management. First, from a broad sociocultural perspective, ethical hacking can be understood on ethical terms, by the intentions of hackers. In a broad brush, ethical hackers espouse benevolent intentions and are considered white hats. Black hats espouse malevolent or unethical intentions. Hackers may be motivated by a multitude of reasons, including profit, protest, challenge, or publicity (Sterling, 1993). Engebretson (2011) argues if hackers have the intent to provide the organization "a realistic attack simulation so that the company can improve its security through early discovery and mitigation of vulnerabilities, the attacker should be considered a white hat" (Setting the Stage, para. 10). In contrast, if the intent is to "leverage information for personal profit or gain, the attacker should be considered a black hat" (Setting the Stage, para. 10). Second, from an organizational perspective, ethical hacking can be defined in technical terms as security testing or risk assessment. Third, from a management perspective, ethical hacking can be defined as a risk management strategy. In the computer security context, a hacker is someone who seeks and exploits weaknesses in a computer system or computer network (Sterling, 1993). Cyber-terrorism is,

> the intentional use of threatening and disruptive actions, or attacks waged through

> computers, the Internet, and technology-based networks or systems against information and data, infrastructures supported by computer systems, programs, and networks in order to cause harm or to further ideological, political, or similar objectives, influence an audience, or cause a government to change its policies. (Corzine & Cañas, 2008; Denning, 2000; Matusitz, 2005, 2008, 2009, as cited in Eid, 2010, p.2)

For organizations, hacking is a risk to be managed. Organizations take a pragmatic risk based approach to managing information security risks, using ethical hacking as one method. Risk assessment outlines what threats exist to specific assets and the associated risk levels. Risk mangers use risk levels to select appropriate security defenses and countermeasures to lower the risk to an acceptable level (Engebretson, 2011; Landoll & Landoll, 2005; Peltier, 2005). Ethical hackers must differentiate themselves from malicious hackers by always acting in a professional manner, argues Graves (2010).

Thesis Rationale, Research Question, and Theoretical Framework

Ethical hacking is a relatively new term in information security literature. It can be defined from several perspectives. A review of literature finds the majority of published books on ethical hacking either application or certification oriented, emphasizing the use of ethical hacking as a risk assessment process. The books largely serve as a manual or a how-to guide (Engebretson, 2011; Graves, 2010; Harper et al., 2011; Harris, Harper, Eagle, & Ness, 2007; Landoll & Landoll, 2005; Simpson, Backman, & Corley, 2010). The texts typically outline the relevant laws and regulations. However, little attention is given to non-

technical and non-legal aspects. The important contribution to knowledge of this thesis lies in filling in a gap in the literature that results from the scarcity of research on the communicative and socio-cultural considerations involved in the implementation of ethical hacking, while the dominant scholarship is application and certification oriented (technical and legal aspects).

The thesis explores the question, "What are the meanings, ethics, uses and practices, and value of ethical hacking in a Canadian university?" by applying technoethical inquiry theory (Luppicini, 2008A, 2008B, 2010) and Karl Weick's (1969, 1979, 1995, 2001, 2009) theory of organizing to a case study. Technoethical inquiry theory (TEI) is a systems theory that highlights knowledge gathering from multiple perspectives, including ethical, technical, political, legal, historical, communicative, and sociocultural (Luppicini, 2010). The thesis applies TEI to frame a multi-stakeholder understanding about ethical hacking use in an organization by exploring stakeholder perspectives about communicative, ethical, management, technical, and sociocultural aspects. TEI explores these perspectives against empirical pragmatic ethical principles. These perspectives are then weaved together to frame a holistic and grounded understanding about the uses and value of ethical hacking in an organization. (The term stakeholder is used in the thesis to denote that the interview participants hold differing priorities and interests regarding ethical hacking organizational implementation by virtue of being in different organizational positions or departments--they have different stakes in the effective implementation of ethical hacking being part of different user communities or beneficiaries of the technology.) The goal of TEI is to uncover relevant information related to the perceived effectiveness and ethical dimensions of ethical

hacking use in an organization for key stakeholder groups. TEI assesses technology—its value and use for the organization—by weighing the benefits against the costs with emphasis on efficiency and fairness. First, the goals or ends are gauged against the side effects. Second, the means are gauged against the ends. Third, actions where the output fails to balance the input are eschewed because they are either inefficient or unfair. As such, TEI provides an ethical basis for a decision-making model. The term fairness is used in the thesis in two ways. First, fairness refers to stakeholder perceptions about fairness in implementing ethical hacking practices in the organization. Second, in applying TEI-DMG (technoethical inquiry theory decision-making grid) to assess the findings, fairness refers to a broader inclusion of perspectives and stakeholder priorities in the decision-making process about ethical hacking organizational practices.

To provide further depth of analysis, the thesis applies Weick's (1969, 1979) sensemaking model to examine the communicative aspects of ethical hacking. The thesis explores organizational perceptions among stakeholder groups about the meanings and ethics of ethical hacking, equivocality in the information environment resulting from variances in perceptions about the explored aspects, and how the organization communicates about these aspects (underlying communicative routines). The thesis applies Weick's theory to study the process of organizing. The major goal of organizing is to reduce the equivocality in the information environment. Equivocality refers to the existence of multiple interpretations of the same event. It is an equivocal environment if individuals can put forth many viable explanations for the event. This can create or exacerbate unpredictability in the information environment. So the emphasis of praxis is on reducing potential sources of unpredictability,

and on reaching common understandings among various stakeholders. Unpredictability potentially arising from variances in perceptions can be reduced through the use (selection) of assembly rules (e.g., standard operating procedures) and communication cycles (ongoing interpersonal and cross-functional communication). Examining the organizing processes of enactment, selection, and retention of ethical hacking can shed light on how perceptions are constructed. First, the thesis looks for indicators of equivocality in perceptions among stakeholders about the meaning, ethics, uses and practices, and value of ethical hacking. Second, it examines potential causes or sources of equivocality in organizational communication practices and in the language and symbols used in the organization to refer to ethical hacking practices. Weick's model advised on how to reduce unpredictability in the information environment, that is, on how to improve the efficiency of the communication process among stakeholders.

TEI is well suited for examining applications of technology in their organizational context for three main reasons. First, the meaning of a technology, as well as its perceived organizational value (and how to assess it), emerge from within the information environment of the organization through interaction. Second, TEI aligns with the pragmatic philosophical orientation of ethical hacking as an information security risk assessment strategy with its emphasis on improving efficiency in information security performance. Third, the pragmatic philosophical orientation of TEI aligns with the risk-based management approach to hacking whereby decisions on investments in countermeasures are based on a cost-benefit analysis – do the benefits of investments in a countermeasure outweigh the potential costs and side effects? TEI aligns with the qualitative case study methodology, including triangulation via

data derived from multiple stakeholder groups. A qualitative case study methodology is suited for capturing the unique complexities of a single case (Stake, 1995). It is especially appropriate when there is a scarcity of literature on the subject (Stebbins, 2011). In the present study, it is used to explore how the university understands and implements ethical hacking within its unique organizational context. Data collection consists of semi-structured in-depth interviews with various stakeholder groups, as well as organizational documentation. The interview participants, university professors and industry professionals, were sought out for their expert knowledge about scholarly research in ethical hacking, industry best practices in information security management, and ethical hacking practices at the research site. The thesis pairs TEI with Weick's model (TEI-KW) to frame a systemic and grounded understanding about ethical hacking—its meanings, ethics, uses and practices, and value for the organization—and places these understandings within the broader literature and industry-wide best practices in information security management. Finally, the thesis applies the TEI Decision-making Grid (TEI-DMG) to investigate the use and value of ethical hacking in the organization and to make recommendations for supporting efficient and fair ethical hacking practices.

Thesis Organization

This thesis is divided into six chapters. The introduction chapter first furnishes the organizational and the academic justification for the thesis. It then discusses how researches have conceptualized ethical hacking, mainly as a risk assessment process used in information security risk management. Finally, it elaborates the research rationale and the research

purpose. Chapter 2 is the literature review. First, it situates ethical hacking within information security management literature and within industry-wide practices. Then, it discusses the theoretical framework, its epistemological roots, and how it is applied to the case study. Chapter 3, the methodology, covers the strategy of inquiry, the data collection and sampling strategies, researcher access to organizational data, and the data validation protocols. Chapter 4 is the Findings. Interview and documentation data are sorted into themes which address the research question. First, the interview data is coded into the ethical hacking elements. Under each inquiry element, themes which address the research question are identified and elaborated. Topic themes which emerged from the document review process can help the researcher incorporate the documentation data into the interview themes to frame organizational understandings about each element. Chapter 5 covers advanced data analysis and discussion. The organizational understandings are contextualized within ethical hacking literature and broader industry practices. The research question is split into two sub-questions. TEI is applied to sub-question a, and Weick's model is applied to sub-question b. The thesis applies Weick's model to explore the communicative aspects and to suggest recommendations for performance improvement. Further, the researcher explains the theoretical basis for using TEI-DMG in technological assessment and decision making, and then proceeds to apply the grid to the case study, making a set of recommendations towards ethical and efficient technology use. The thesis closes with the conclusion chapter which discusses the summary and significance of the findings, study limitations, contribution to theory and communication research, and future research opportunities.

Literature Review

This chapter had two goals. The first goal was to situate the study within ethical hacking research. The second goal was to explain the theoretical framework (TEI-KW) and its philosophical underpinnings. The thesis first situated ethical hacking within information security management literature. The concepts of risk management and risk assessment in information security were explained because they represent the broader literature and organizational context of ethical hacking practices. Then, ethical hacking theory and research were discussed. The organizational information security concerns were discussed. Then, ethical hacking as a risk management strategy, that is, as a risk assessment process, was discussed. Finally, the role of policy in information security management was discussed. A discussion of ethical hacking theory and research began with a brief account of the historical image of hackers in the 1980s and early 1990s among computer security professionals. Two main differences between ethical hacking and hacking were explained, namely, differences in strategic goal (prevention versus exploitation), and in the realism of ethical hacking (the nature of hacking simulation). Attention then turned to how ethical hacking was studied, and then how the thesis studied it. After situating ethical hacking within information security risk management literature, the second area of focus for the chapter was discussed. The thesis explained the theoretical framework, its epistemological roots, and how it was applied to the case study. The epistemological roots of empirical pragmatism were explained to demonstrate their correspondence to the philosophical underpinnings of TEI. TEI and Weick's sensemaking model were then explained, their theoretical applications in literature, and how the thesis applied them to the case study.

Risk Management and Risk Assessment

An organization's information security concerns can be understood through the consideration of three information security risk management considerations, namely, information assets, threats, and vulnerabilities. Threats that can exploit system vulnerabilities represent risks to organizations. Organizations take a risk based approach to information security management. One important information security risk management strategy is ethical hacking. An organization's risk management goals, guidelines, procedures, and employee responsibilities are typically detailed in an information security policy (Engebretson, 2011; Graves, 2010; Harper et al., 2011; Harris, Harper, Eagle, & Ness, 2007; Landoll & Landoll, 2005; Reynolds, 2012).

An asset is any hardware, software, information system, network, or database which an organization uses to achieve its business goals. A basic organizational information security goal would be safeguarding the information assets against hacker threats. Important information assets for educational organizations may include student data, employee data, or research data. Perpetrators of computer crime may be hackers aiming to test the limits of a system or to gain publicity, or they may be cybercriminals, cyberterrorists, or spies. Computer attacks can come from viruses, worms, Trojan horses, rootkit, spam, phishing, and distributed denial-of-service (DoS). In a DoS attack, a hacker attacks the availability elements of systems and networks. Identity theft through social engineering and phishing schemes are important security concerns for many businesses. Information theft, such as stealing passwords, is a confidentiality attack because it allows someone other than the

intended recipient to access the data (Graves, 2010; Reynolds, 2012; Stamp, 2001).

Computer security incidents are a growing concern for at least three reasons. First, the computing environment is increasing in complexity. The number of entry points into a network is increasing and with it the possibility of security breaches. Expanding and changing systems introduce new risks. Second, there is a growing reliance on software, sometimes with known vulnerabilities. (Reynolds, 2012). Third, many hacking tools are easy to obtain from the Internet and to use (Public Safety Canada, 2013A, 2013B). But while some information security incidents or vulnerabilities can be linked to broad industry trends or technological developments, other sources of vulnerabilities are more internal in nature. Organizational sources of vulnerabilities can be related to poor system design or implementation. Examples include not updating the application software and not reconfiguring default passwords. Weak passwords represent a security vulnerability for most systems (Harper et al., 2011; Landoll & Landoll, 2005; Reynolds, 2012).

Organizations typically take a risk based approach to information security management, whereby the probability of an attack and the potential damage are considered against investment costs. Risk is "a threat that exploits some vulnerability that could cause harm to an asset." It is "a function of the probability that an identified threat will occur, and then the impact that the threat will have on the business process" (Peltier, 2005, p.16). "One instance of risk within a system is represented by the formula (asset*threat*vulnerability)" (p. 8). The Risk Management Guide of the National Institute of Standards and Technology defines risk assessment as "the process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards

that would mitigate this impact" (Landoll & Landoll, 2005, p. 10). According to the General Security Risk Assessment Guidelines, ASIS International (2003), the basic components of a risk assessment plan include, identifying assets, specifying loss events (threats), assessing the frequency and impact of events, recommending mitigation options, conducting a cost/benefit analysis, and making decisions. The goal of risk assessment is "to identify which investments of time and resources will best protect the organization from its most likely and serious threats" (Reynolds, 2012, p. 103).

Risk assessment results outline what threats exist to a specific asset and the associated risk level for each threat. Risk levels help risk managers select appropriate control measures, safeguards, or countermeasures to lower the risk to an acceptable level (Landoll & Landoll, 2005; Peltier, 2005). The concept of reasonable assurance guides the decision making process: managers must use their judgement to ensure that the cost of control does not exceed the system's benefits or the risks involved. The risk management process "supports executive decision-making, allowing managers and owners to perform their fiduciary responsibility of protecting the assets of their enterprises" (Peltier, 2005, p. 10). Risk assessment is a reliable method for measuring the effectiveness of an organization's information security system (Landoll & Landoll, 2005). For risk management to be successful, it must be supported by senior management and concerned employees and groups, and the concept of ownership of assets established through an asset or information classification policy that spells out the roles and responsibilities of company employees in protecting company information (Peltier, 2004A, 2004B, 2005). Periodic security audits are an important prevention tool used to evaluate whether an organization has a well-developed

security policy and whether it is being followed (Peltier, 2005; Reynolds, 2012).

Organizations typically have an information security policy for managing hacking threats which stipulates risk assessment and management goals, guidelines, procedures, and employee responsibilities. A security policy can refer to several documents or policies governing the use of hardware and software within an organization, the use of mobile devices, issues of physical security, or ongoing education of users and staff. A security policy should detail prevention, detection, and response measures. The security of any system or network is "a combination of technology, policy, and people and requires a wide range of activities to be effective" (Reynolds, 2012, p. 102). People are the weakest link. Users are a key part of the security system and they have certain responsibilities. For example, users must help protect an organization's information systems and data by guarding their passwords and prohibiting others from using them, and by following organizational guidelines with respect to downloading from the Internet (Dhillon, 2007; Peltier, 2005; Reynolds, 2012).

Ethical Hacking Theory and Research

The terms hacking and ethical hacking share a complex, intertwined history. A historically grounded understanding of ethical hacking can begin with an account of the historical image of hackers in the 1980s and early 1990s among computer security professionals as ethical, knowledgeable IT professionals, and how the mass media reversed this image in popular culture. Originally, hacker meant,

> 1. A person who enjoys learning the details of computer systems and how to stretch their capabilities—as opposed to most users of computers, who prefer to learn only the minimum amount necessary. 2. One who programs enthusiastically or who enjoys programming rather than just theorizing about programming. (E. S. Raymond, The New Hacker's Dictionary, MIT Press, Cambridge, MA (1991)

The view of ethical hackers as ethical and technologically knowledgeable IT professionals seems rooted in a historical professional perception about hackers. The term hacker had a positive connotation in the 1980s and early 1990s among computer security professionals. A hacker was someone with computer skills, and with technical and educational penchant for computer systems and software. Hackers typically had strong programming and computer network skills. Some of their job duties were similar to those of today's ethical hackers (Harper et al., 2011; Harris, Harper, Eagle, & Ness, 2007; Palmer, 2001; Sterling, 1993). "As malware and attacks emerged, the press and the industry equated the term 'hacker' with someone who carries out malicious technical attacks" (Harris, 2007, Ethics of Ethical Hacking, para. 27). Palmer (2001) writes that since calling someone a hacker was originally meant as a compliment, "computer security professionals prefer to use the term 'cracker' or 'intruder' for those hackers who turn to the dark side of hacking" (p. 770).

According to the International Council of Electronic Commerce Consultants (EC-Council), a professional certification body best-known for its Certified Ethical Hacker certification, certified ethical hackers acquire the same knowledge, follow the same steps (scan, test, hack, and secure), and use the same tools as black hats. Although ethical hackers and hackers use the same knowledge base, follow the same steps, and use the same software,

they differ on the strategic goal of hacking, and the extent of hacking (realism level). First, while ethical hackers aim to prevent unauthorized access, hackers aim to break in or to penetrate a computer system for some personal gain or cause. Second, in practice, organizational security testing related to ethical hacking does not necessarily include penetration (exploitation of identified vulnerabilities).

A countermeasure is,

> An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken. (IETF RFC 2828)

For Harris (2007), responsible hacking books should give information about how to break into systems as well as about defence and prevention measures. If hacking books and hacking classes are responsible they should address both how to discover vulnerabilities as well as "how to implement preventive measures to help ensure that these vulnerabilities are not exploited" (The Controversy of Hacking Books, para. 3). Farmer and Venema (1993) provided several specific examples of how hackers can gather information about their targets, how the information can be exploited to gain control of the target, and how such attacks can be prevented (Palmer, 2001). They gathered up "all the tools that they had used during their work, packaged them in a single, easy-to-use application, and gave it away to anyone who chose to download it" (Palmer, 2001, p. 770). They called their program Security Analysis Tool for Auditing Networks, or SATAN.

Ethical hackers "go through the same processes and procedures as unethical hackers, so it only makes sense that they use the same basic toolset" (Harris, 2007, Chapter 3, The

Dual Nature of Tools, Para. 2). Palmer (2001) calls such simulation a realist approach. Ethical hacking as a realist technique of simulation emerged for the first time in the open-source community of Usenet in December of 1993. With the goal of raising the overall level of security on the Internet and intranets, two computer security professionals, Farmer and Venema (1993), "discussed publicly, perhaps for the first time, this idea of using the techniques of the hacker to assess the security of a system" (Palmer, 2001, p. 770). The realism of ethical hacking as a strategy is in duplicating the real conditions as closely as possible so as to test the readiness of the system for actual attempts of security breach. There are real-life organizational constraints to conducting a free-hand security assessment by ethical hackers. An ethical hacker has to provide the client with knowledge about ongoing hacking activities. This creates a paradox since no simulation can truly duplicate the real conditions.

The literature review on ethical hacking demonstrated that the predominant scholarly attention has been given to technical aspects of ethical hacking. In the professional and technical contexts, it has been mostly equated with risk assessment and penetration testing. The majority of published books on ethical hacking were either application or certification oriented. Application oriented texts largely served as a manual or a how-to guide for performing penetration testing (Engebretson, 2011; Graves, 2010; Harper et al., 2011; Harris, Harper, Eagle, & Ness, 2007; Landoll & Landoll, 2005; Simpson, Backman, & Corley, 2010). Certification oriented texts prepare IT security professionals for several information security related certifications set at various levels of competencies and skills. The texts typically outline the relevant laws and regulations. However, little attention is given to non-

technical and non-legal aspects. The thesis addressed the scarcity of research on communicative, ethical, management, technical, and sociocultural considerations involved in the implementation of ethical hacking in an organizational context. The thesis explored the question, "What are the meanings, ethics, uses and practices, and value of ethical hacking in a Canadian university?" by applying TEI (Luppicini, 2010) and Weick's (1969, 1979) theory of organizing to the case study.

The Epistemological Roots of Empirical Pragmatism

Scholars interested in business ethics typically discuss two kinds of business ethics: normative and empirical. Normative theories deal with questions of what should happen while empirical theories deal with questions of why and what is. Normative business ethics is rooted in philosophy and the liberal arts and generally considered the domain of philosophers and theologians. Normative ethical theories develop standards against which the propriety of business practices can be evaluated. By contrast, argue Rosenthal and Buchholz (2000A), the empirical approach "focuses on identifying definable and measurable factors within the individual psyches and social contexts that influence individual and organizational ethical behavior" (p. 36). Empirical business ethics is rooted in management and the social sciences and commonly employed by management consultants and business school professors. It is explanatory, descriptive, or predictive in approach and assumes that an organization is objective and amenable to impartial exploration and discovery (Rosenthal & Buchholz, 2000A). Empiricism can be understood as the view that all knowledge has its source in experience (Talisse & Aikin, 2008).

Normative approaches to ethical decision making include virtue ethics and deontology. Virtue ethics focuses on the character of a person rather than on specific actions. Deontology argues that decisions should be made considering one's duties and other's rights. By contrast, teleology (consequentialism) is an empirical approach which argues that the morality of an action is contingent on the action's outcome or result. Broadly, moral behaviours are social and collective while ethical behaviours are individual. Teleological theories hold that the end consists in an experience or feeling produced by the action. For hedonism, this feeling is pleasure—one's own (egoism), or everyone's (utilitarianism), broadly expressed as the "greatest happiness of the greatest number." Teleological-type theories differ on what they consider valuable (axiology), that is, on the nature of the end that actions ought to promote. They include utilitarianism and pragmatism which share the philosophical orientation of judging the morality of actions by their consequences. Actions that are wrong are wrong simply in virtue of their effects, thus, instrumentally wrong. For pragmatism, the end of action is satisfaction and adjustment. Utilitarianism and pragmatism were closely linked in that they both judge the morality of actions based on their consequences. Utilitarianism was a doctrine that proposed to appraise moral rules and codes by the standard of effectiveness in furthering "the greatest good of the greatest number." Pragmatists are generally concerned with how to make actions more successful (Talisse & Aikin, 2008). When "pragmatism's standard of 'what works out for the best' is construed as being collectively optimific at the communal level, then 'the best' simply and directly comes to 'the greatest good of the greatest number'" (Rescher, 2012, p. 181).

Rosenthal and Buchholz (2000A, 2000B, 2001) argued for a pragmatic approach to

business ethics. Grounding their analysis in the classical American pragmatism of John Dewey and William James, they argued that the pragmatic understanding of science and the scientific method and of the fact-value split offered a new way to understand the normative-empirical business ethics dichotomy. They argued that the traditional and pervasive understanding of the scientific method as the method of attaining knowledge is reductionist. In the traditional method, riding a wave of logical positivism, scientific knowledge provided a literal description of objective fact and excluded lived qualitative experience as providing access to the natural world. "Nature as objectified justified nature as an object of value-free human manipulation" (Rosenthal & Buchholz, 2000A, p.38). The mind-matter split implicit in the traditional understanding of scientific study is illusory. For the pragmatist, humans are within nature not outside of it and causally linked to it. Humans are active, creative agents who through meanings help structure the objects of knowledge and who thus cannot be separated from the world known (Rosenthal & Buchholz, 2000A). John Dewey used Heisenberg's principle of intermediacy to argue, "what is known is seen to be a product in which the act of observation plays a necessary role. Knowing is seen to be a participant in what is finally known" (Dewey, 1984, p. 163). Human activity partially constitutes the nature people experience. For pragmatism,

> with its emphasis on broad empiricism and ontological emergence, both facts and values emerge as wedded dimensions of complex contexts which cannot be dissected into atomic bits. The entire fact-value problem as it has emerged from the past tradition of moral philosophy is misguided from the start. (Rosenthal & Buchholz, 2000A, p.46)

Moral behaviours cannot be adequately evaluated apart from the contextual situations in

which they arise. These contextual situations involve causal relations in two senses. First, certain historical and cultural conditions are the cause of the value experiences and the moral beliefs of participants. Second, "these beliefs lead to particular types of consequences because of causal relations between our belief guided actions and the consequences they bring about" (p. 47).

Bunge's Pragmatic Value Theory

Rosenthal and Buchholz (2000A, 2000B) argued that the pragmatic understanding of science and the scientific method saw no split between fact and value in seeking the truth (gaining knowledge). It was a line of reasoning which Mario Bunge (1967, 1976, 1977, 1979) largely adopted in his conception of technoethical inquiry theory. The fact-value distinction posed a special problem for moral philosophers who wanted to make normative statements about what businesses ought to do. Rosenthal and Buchholz (2000A) asked: How can the validity of statements be established? How can they be seen as anything other than mere opinion which can be easily dismissed in a scientific culture? Bunge (1977) had an answer. For him, ethics can be conceived as a branch of technology; ethical inquiries can be treated as technological inquiries are treated. Researchers can evaluate moral rules or statements as they would technological rules: moral rules ought to be fashioned as rules of conduct deriving from scientific statements and value judgements.

In his seminal essay, *Towards a Technoethics*, Bunge (1977) offered three lessons moral philosophy can learn from contemporary technology. First, the classical distinction between what is and what ought to be can no longer be maintained. Second, facts and values

become blended in action. In decision theory, for example, values and facts (statistical data) together guide decision making. Third, moral norms can no longer be considered immutable or infallible and separate from facts or knowledge; knowledge and practical experience or experimentation guide and advise values, and vice versa. Researchers' final recommendations or norms are thoughtful outcomes of their research and work.

Bunge (1977) presented a value theory that can serve as a basis for weighing means, goals, and side effects, and thus offer help in making or adopting rules of conduct that are technically feasible and morally right. He suggested three technoethical rules for the researcher: 1) Evaluate goals jointly with side effects; 2) match the means and the goal technically and morally, and employ only worthy practical means and optimal knowledge; and 3) eschew any action where the output fails to balance the input because it is either inefficient or unfair. Bunge's (1977) formula, which was further developed and framed by Rocci Luppicini (2010) as the five steps of TEI, argued for the use of factual knowledge and objective valuation to evaluate ethical rules. TEI applied the scientific method—knowledge gathering, setting standards, and following procedures—to evaluate normative principles and practices.

Technoethical Scholarship

The emergence of technoethics as a formal field can be connected to a "marriage of scholarship on technology and ethics that spread from specialty areas within Philosophy to other disciplines concerned with social and ethical issues regarding technology" (Luppicini, 2010, pp. 30-31). A number of scholarly works in the philosophy of technology focused on

technology as it bears on human work and life (Luppicini, 2009). Heidegger (1977) argued that modern technology allowed new relationships to the world not previously possible. The work of Jonas (1979, 1985) and Mitcham (1997, 2005) provided grounding for technoethics by bridging the philosophy of technology with interdisciplinary scholarship in science, technology, and society (STS) studies. Technology was also the locus of scholarly work within the humanities and social sciences through technocritical scholarship by Ellul (1964), Franklin (1990), and Kuhn (1962). Research from the philosophy of technology and technocritical writings was primarily concerned with how technology influenced social order. But the ethical considerations raised in this body of work—as well as the development of several theories of technology, including technological determinism, cultural theory, and actor-network theory—helped set the stage for the advent of technoethics (Luppicini, 2010). Importantly, such work "bridged philosophical inquiry into technology with related work within the applied sciences and Social Sciences" (p. 38). Applied ethics research "further grounded technoethics by bringing philosophical inquiry into the context of real world human problems and bringing real events, practices, and research activity into focus" (Luppicini, 2009, p. 7). This in turn set the stage for a number of areas in applied ethics to evolve (Luppicini, 2009).

Based on a conception of technology as a relational concept between humans on the one hand, and the design, development, and application of technology, on the other, technoethics can be defined as an "interdisciplinary field based on a relational orientation to technology and human activity which creates new knowledge and builds on technology focused areas of ethical inquiry" (Luppicini, 2009, p. 3). One way to describe technoethics is

by identifying “its key areas of academic research and study derived from various branches of applied ethics and other areas of academic scholarship with a technology focus” (p. 7). The attention technoethics gives to the ethics of the relationship surrounding humans and technology can serve as a throughline which connects historically disparate disciplinary areas of scholarship on ethics and technology. By focusing on the relational aspects between humans and technology—in that, areas of applied ethics can be seen as utility areas and sites of interaction—technoethics offers a unique framework which transcends traditional silos within academia in support of interdisciplinary scholarship on ethical aspects of various types of technologies. The holistic and systemic theoretical orientation of technoethics allows for the mixing of research approaches, including postpositivist, interpretive, constructivist, and critical. Technoethics can organize scholarship on ethical aspects of technological innovations around themes (areas) of applied ethics, such as computer ethics, engineering ethics, biotech ethics, nanoethics, artificial morality, and neuroethics (Luppicini, 2009, 2010). The thesis elaborated scholarship in technoethics according to how research corresponded to the speciality areas of applied ethics rather than according to the philosophical or epistemological orientation of the research design. The thesis focused on areas which bear on the analysis of information security management, namely, computer ethics (including information ethics), and Internet ethics and cyberethics. An outline of the theoretical and historical foundations of these areas was followed by a review of technoethical scholarship in each area. (See Luppicini, 2009, for an exhaustive review of technoethical scholarship in areas of applied ethics.)

Applied Ethics in Technoethical Scholarship

Computer ethics is a key area of technoethics which focuses on the human use of computer and computing technology in a number of sub-areas, including graphic interfaces, visual technology, artificial intelligence, and robotics (Luppicini, 2009). In *The Human Use of Human Beings*, Wiener (1954) was the first scholar to explore basic questions of computer ethics. Work in this area continued in the 1970s and 1980s with Weizenbaum's (1976) critical research on the human aspects of computer use, and Moor's (1985), and Johnson's (1985) scholarship on ethical guidelines for computer use. Since the late 1980s and early 1990s, ethical issues arising from the development and application of information technologies extended the boundaries of computer ethics to theoretical work in information ethics (see Floridi & Sanders, 2003). The technoethical area of applied ethics in Internet ethics and cyberethics addressed computing technologies for the Internet (e.g., spyware, antivirus software, and web browser cookies) emerging in the late 1980s and early 1990s and which raised social, regulatory, and ethical challenges (Luppicini, 2009). In 1989, the Internet Architecture Board (IAB) created the first comprehensive set of guidelines to guard against unethical Internet activity, such as compromising the privacy of users, gaining unauthorized access to Internet resources, and compromising the integrity of computer-based information (Internet Architecture Board, 1989).

Branches of applied ethics within technoethical scholarship have overlapping philosophical orientations and research interests. However, research may focus on a certain technology or area of technological application and the related historical, theoretical, methodological, or ethical dimensions. Alternatively, research may focus on a specific

technoethical concern or concept. Finally, research may have a general philosophical emphasis on the ontology or epistemology of technology.

Follows are examples of studies emphasizing the area of computer ethics (including information ethics). Wareham (2013) developed a respect-based account of the ethical criteria for the moral status of persons to examine whether artificial agents could have the high degree of moral status attributed to human persons (computer ethics). Sullins (2009) argued that recent artificial agents having artificial intelligence such as robots may be considered artificial moral agents (computer ethics). Kennedy (2013) investigated the perceived virtue in virtuality within technoethics through a survey of ten IT master students (computer ethics). Stahl et al. (2012) developed a methodology for an ethical analysis using the description of emerging ICTs (information ethics). Charlesworth and Sewry (2009) articulated information ethics as a conceptual model for studying computer ethics (information ethics). Follows are examples of studies emphasizing the area of Internet ethics and cyberethics. Cerqui and Warwick (2009) argued for an anthropological approach to demystifying the underlying cultural values in technologies using the notion of privacy (Internet ethics). Lin and Luppicini (2013) applied actor-network theory to study communicative and technical organizational influences related to the use of the cyber surveillance hacker technology GhostNet in cyber espionage (cyberethics). Eid (2010) discussed four severe cyber-terrorism cases which occurred within the last decade, and presented a theoretical model for effective media decision-making during terrorism attacks (cyberethics). Roberts (2009) explored methods used to combat cyber identity fraud in light of their relation to privacy and civil liberties (cyberethics). Jenkins (2001) investigated

Internet pornography and child exploitation (cyberethics). Finally, Adam (2002) examined the problem of cyberstalking (cyberethics). Technoethical analysis in applied ethics may emphasize broad philosophical aspects of technology. Vries (2009) explained the complex, multidimensional nature of technology, and presented a multi-disciplinary approach to understanding technoethics. Agazzi (2012) examined the two opposing arguments regarding the ethical evaluation of science and technology in order to determine to what extent both might be right. Crabb and Stern (2012) examined the share of ethical responsibility for five technology phenomena (traps) among end-users, businesses, and government.

Applying Technoethical Inquiry Theory

Technological advances have a transforming revolutionary effect on society, argued Moor (2005). According to Moor's law (2005), as the social impact of technological revolutions grows, ethical problems increase. Technoethics is broadly concerned with the responsible use of technology for advancing human interests in society. The broad technoethical question is, how can technoethics guide technology development and application to leverage society? Technoethics has been defined in a variety of ways (e.g., Bao & Xiang, 2006; Galvan, 2001; Jonas, 1985). Technoethics as understood in this thesis rests on a pragmatic worldview concerning the relation between technology and human welfare. Technoethics,

> attempts to provide conceptual grounding to clarify the role of technology in relation to those affected by it and to help guide ethical problem-solving and decision making in areas of activity that rely on technology. (Luppicini, 2009, p. 4)

TEI can be used to examine whether a practice is effective (efficient and ethical)—whether the end justifies the means, and whether the benefits outweigh the costs and side effects. TEI is a scientific method in that it stipulates specific rules and steps for conducting an ethical inquiry into the value and utility of technological practices using a pragmatic decision-making framework, weighing ends (output) of actions against the means (input) in terms of efficiency (perceived output benefits exceed perceived input costs) and fairness (including considerations of side effects). TEI is a value theory that provides the conceptual grounding for this assessment. The guiding principles of TEI are as follows: 1) Technoethical inquiry treats technology as a self-producing social system on the basis of knowledge creation (facts and values); 2) The derivation of meaning about system operations involves multi-perspective and multi-aspect inquiry; and 3) The third principle places communication (achieving mutual understanding) as a core goal. A successful TEI identifies "all relevant knowledge (facts and values) and priorities (value ranking) applicable to the technological relations to which a technoethical inquiry is applied" (Luppicini, 2010, p. 70). Value ranking was made using TEI-DMG as a qualitative assessment of stakeholder priorities. It referred to participant ethical hacking value assessments in step 3. For example, if a participant deemed a certain technical practice (e.g., software use) as efficient and fair, the participant got 1 point for technical aspects. If a participant chooses two technical solutions and one communicative solution, the participant is assigned two points for technical and one point for communicative priorities.

TEI is a social systems theory and methodology for guiding technological systems research in technology assessment and design. It is well suited for examining ethical hacking

because, first, it places ethical and technical elements at the core of organizational studies. Second, it can be used to frame a multi-perspective, multi-stakeholder view of how ethical hacking practices are meeting the needs of the organization and at what potential cost through the consideration of technical knowledge (facts and values) relevant to the design context. Third, its pragmatic philosophical orientation aligns with organizational management practices and their emphasis on efficiency and improvement. Drawing on entrenched scholarship in technoethics from Bunge (1977), TEI assumed a pragmatic orientation to moral norms grounded in human activity and existing knowledge. The five steps of TEI (Luppicini, 2010) can help frame an understanding about perceived ethical dimensions (whether actions are ethical or unethical) as well as efficiency considerations involved in ethical hacking implementation. The five TEI steps (Luppicini, 2010, p. 73) can be listed as follows:

Step 1: Evaluate the intended ends and possible side effects to discern overall value;

Step 2: Compare the means and intended ends in terms of technical and nontechnical aspects (moral, social);

Step 3: Reject any action where the output (overall value) does not balance the input in terms of efficiency and fairness;

Step 4: Explore relevant information connected to the perceived effectiveness and ethical dimensions of ethical hacking in a Canadian university for key stakeholder groups; and

Step 5: Consider technological relations at a variety of levels.

Weick's Theory of Organizing

Weick's basic sensemaking model (1969, 1979), which the thesis adopted, emphasizes key processes that link interaction and organizing. It emphasizes communication processes for resolving equivocality in the information environment. In later scholarship, Weick elaborated his theoretical framework to account for other aspects of sensemaking opportunities and processes; for example, sensemaking in crisis situations (Weick 1988, 1990), and sensemaking when it fails (Weick, 1993). Weick, Sutcliffe, and Obstfeld (2005) argue for a reconceptualization of organizing to frame a more future oriented, more action oriented, and more macro oriented understanding, as well as to incorporate identity considerations.

Weick's sensemaking perspective has influenced many communication researchers, some of whom have been more true to the basic sensemaking model, and others who built on or paired his thesis with other theoretical prisms in search of a more holistic or a more interdisciplinary perspective (see Miller, 2002). Some researchers explored Weick's model more explicitly. Kreps (1980) explored the role of equivocality in the sensemaking process and found that the equivocality of an enacted environment drives communication cycles for sensemaking. Bantz explored the ways in which the environment is enacted within a newsroom (1980), and the ways in which the media industry is enacted through relationships among news organizations (1989). Louis (1980), and V. D. Miller and Jablin (1991) adopted Weick's model to explore how employees can make sense of equivocal as well as non-equivocal information environments. Miller, Joseph, and Apker (2000) examined how employees make sense of ambiguously defined organizational roles. Weber and Ann Glynn (2006) elaborated the larger social and historical contexts in sensemaking by incorporating

institutional theory.

Weick theorizes how organizations organize and make sense of organizing through interaction (Weick, 1969; 1979; 1995; 2001; 2009). Organizing is "the resolving of equivocality in an enacted environment by means of interlocked behaviors embedded in conditionally related process" (Weick, 1969, p. 11). Drawing on a variety of theories, Weick's complex model seeks to illuminate the process of organizing. The major goal of organizing is to reduce the equivocality (or to make sense) in the information environment. Equivocality is the unpredictability inherent in the information environment. It can be reduced through the use (selection) of assembly rules (e.g., standard operating procedures) and communication cycles (ongoing interpersonal and cross-functional communication).

Weick's definition of the organizing process can be unpacked by considering the interrelated processes of enactment, selection, and retention (Miller, 2002). Enactment processes are organizational environments in which activities or experiences are imbued with meaning by organizational participants. Participants bracket (notice) events in such a way that the environment becomes constituted. How employees behave in the stream of experience will affect the organizational environment they encounter. Only "through interlocked behaviours can the meaning of particular environmental events and displays be negotiated" (Miller, 2002, p. 200). Selection processes involve the "placement of items into frameworks, comprehending, redressing surprise, constructing meaning, interacting in pursuit of mutual understanding, and patterning" (Weick, 1995, p. 6).

For Weick, equivocality refers to the existence of multiple interpretations of the same event, not ambiguity about the meaning of an event. It is an equivocal environment if

individuals can put forth many viable explanations for the event. The problem of equivocality is one of confusion not ignorance (Miller, 2002). The level of equivocality influences the way in which sense can be made. Equivocality is likely to be high in organizations in a highly competitive or quickly changing business environment or during a time of crisis (Miller, 2009). When equivocality is low employees can rely on established ways of doing things (rules). But when equivocality is high, and the complexity of the environment allows for multiple explanations of the same event, the use of communication cycles is suggested, where employees introduce and react to ideas that help make sense of their equivocal environment (Miller, 2009). Employees interact with each other and with others to craft and make sense of their new or changing organizational roles. Interpersonal communication among employees can reduce confusion around organizational meanings and uses of ethical hacking. Equivocality can be reduced by providing communication opportunities for people to interact and create the relevant knowledge.

Weick's theory emphasized the notions of environment (physical and cultural context), interdependence, permeability, and requisite variety (highly uncertain information environments require complex communication cycles) (Miller, 2009). It helped in explaining how understandings about ethical hacking were communicated at the organizational level. Environmental organizing procedures can suggest whether the organizational communication strategy is effective—does it identify and resolve equivocality in the information environment—and suggest ways to reduce equivocality.

Cyber-security actors eliminate the risk of hacking by reducing unpredictability in the information environment about ethical hacking organizational aspects. The defining

characteristics of risk are mainly exposure and uncertainty (for the case to be considered risk). By reducing unpredictability, cyber-security actors are eliminating the risk because the existence of risk requires uncertainty (which can be understood equally to unpredictability). Cyber-security actors eliminate the risk of hacking by reducing unpredictability in the information environment about ethical hacking organizational aspects. The defining characteristics of risk are mainly exposure and uncertainty (for the case to be considered risk). By reducing unpredictability, cyber-security actors are eliminating the risk because the existence of risk requires uncertainty (which can be understood equally to unpredictability).

Applying Weick's Theory of Organizing

Active agents "structure the unknown" (Waterman, as cited in Weick, 1995, p. 41); they construct "sensible, sensable events" (Weick, 1995, p. 4). For Weick (1995), sensemaking involves "the placement of items into frameworks, comprehending, redressing surprise, constructing meaning, interacting in pursuit of mutual understanding, and patterning" (p. 6). The central questions for a sensemaking inquiry typically revolve around how active agents construct, why, and with what effects (Weick, 1995). Investigators into sensemaking practices and processes have conceptualized it in different ways. For Louis (1980), the activity of placing stimuli into frameworks is most visible when predictions break down, suggesting sensemaking is influenced by expectations. When an expectation is disconfirmed, an ongoing activity is interrupted. Hence a relevant question would be, how do people cope with interruption? The joint influence of expectations and interruption suggests that sensemaking "will be more or less of an issue in organizations, depending on

the adequacy of scripts, routines, and recipes already in place" (p. 5). Other researchers who have looked at sensemaking with an emphasis on the placement of stimuli into frameworks include Dunbar (1981), Goleman (1985), Starbuck and Milliken (1988), and Westley (1990). For Starbuck and Milliken (1988), sensemaking "involves placing stimuli into some kind of framework" which enables people to "comprehend, understand, attribute, extrapolate, and predict" (p. 51). In a close reading, Ring and Rands (1989) defined sensemaking as "a process in which individuals develop cognitive maps of their environment" (p. 342). They used the term "understanding" to refer to a mutual activity. Other researchers used the seven properties of sensemaking to frame an inquiry into sensemaking activities since these properties suggest what is sensemaking, how it works, and where it can fail (Weick, 1995). Weick (1969, 1979, 1995) had conceptualized sensemaking as a process that is grounded in identity construction, retrospective, enactive of sensible environments, social, ongoing, focused on and by extracted cues, and driven by plausibility rather than accuracy. For example, Dutton and Dukerich (1991) focused their analysis of sensemaking on issues of identity: using the image of the mirror metaphor to articulate an interconnected and intersubjective creation of identity in relation to the organizational image. Meryl Louis (1980) saw sensemaking as a thinking process that uses retrospective accounts (rather than strategies) to explain surprises. People use assumptions as predictions about future events. Discrepant events trigger a need for explanation; for a process that can explain discrepancies. The sensemaking debate also includes discussions about whether sensemaking results in action (Sackman, 1991; Thomas, Clark, & Gioia, 1993), whether it is more likely to inform action (Feldman, 1989), and whether sensemaking is a private or a singular activity (Gioia &

Chittipeddi, 1991; Ring & Rands, 1989).

To make sense of ethical hacking use in the organization, the thesis examined existing equivocality regarding ethical hacking aspects among key stakeholder groups, as well as potential sources of equivocality--organizational communication practices, employees' perceptions about the technology and its implementation, and the language and symbols used to refer to ethical hacking organizational practices.

Chapter Conclusion

This chapter achieved two goals. First, it situated the present study within ethical hacking research. Second, it explained the theoretical framework (TEI-KW) and its philosophical underpinnings. The chapter first situated ethical hacking within information security management literature. The concepts of risk management and risk assessment in information security were explained to present the broader literature and organizational context of ethical hacking practices. Then, ethical hacking theory and research were discussed. The organizational information security concerns were discussed. Then, ethical hacking as a risk management strategy of risk assessment was discussed. Finally, the role of policy in information security management was discussed. A discussion of ethical hacking theory began with a brief account of the historical image of hackers in the 1980s and early 1990s among computer security professionals. Two main differences between ethical hacking and hacking were explained: differences in strategic goals, and in the realism of ethical hacking. Attention then turned to how ethical hacking was studied, and then how the thesis studied it. After situating ethical hacking within information security risk management

literature, the second area of focus for the chapter was discussed. The thesis explained the theoretical framework, its epistemological roots, and how it was applied to the case study. The epistemological roots of empirical pragmatism were explained to demonstrate their correspondence to the philosophical underpinnings of TEI. TEI and Weick's sensemaking model were then explained, their theoretical applications in literature, and how the thesis applied them to the case study.

Methodology

The thesis explores the question "What are the meanings, ethics, uses and practices, and value of ethical hacking in a Canadian university?" by applying technoethical inquiry theory (Luppicini, 2010) and Weick's (1969, 1979, 1995) theory of organizing to a case study. This chapter first addresses the methodological justification for the thesis. It then discusses the suitability of the qualitative exploratory case study methodology for addressing the thesis question. An explanation of the research design is followed by the rationale for the selection of the research site and sampling strategy. Data collection and analysis procedures are then discussed. A discussion of the applied reliability and validity protocols follows. Finally, some ethical considerations are noted.

Methodological Justification

TEI is a specialized theory of socio-technical systems that highlights knowledge gathering from multiple perspectives and it aligns with the qualitative case study methodology. TEI adheres to core pragmatist assumptions. It defers to the primacy of practice. It does not treat ethical theories independent of their experience. Instead, "it views theory and practice as emerging from experience (and existing knowledge) within the environment" (Luppicini, 2010, p. 66). Pragmatist tools such as case-based reasoning and casuistry are used to study technological systems. Case analysis is a particularly appropriate method for the investigation of systems explanations of organizational functioning, and particularly useful in conjunction with Weick's theory of organizing, argues Miller (2009).

This is because the case study methodology supports the systemic exploration and conceptualization of organizational phenomena and practices. As a systemic approach, TEI understands the use of a technology (and the meanings created about the technology) as a process of interaction among the various system components (active agents). So to understand how a technology is used and perceived, researchers must examine the dynamics of interaction from the various stakeholder perspectives involved.

The Case Study Methodology

For Creswell (2003, 2007), research design must address three concerns: knowledge claims or theoretical perspectives, strategies of inquiry, and methods of data collection and analysis. The research approach must meet the research requirement for attention to the organizational context. The strategy, the case study methodology, must allow for contextual, in-depth exploration of the study topic. Building on Rossman and Rallis (1998), Creswell argues that qualitative research takes place in a natural setting which enables the researcher to develop a level of detail about the place or individual and to be involved in the experiences of the participants. Largely inductive in nature, qualitative research is fundamentally interpretive in developing a description of a setting or individual, analyzing data for themes or categories, and drawing conclusions about their meanings.

The qualitative researcher uses reasoning that is multifaceted and iterative "with a cycling back and forth from data collection and analysis to problem reformulation and back" (Creswell, 2003, p. 183). Qualitative research emphasizes context because the meaning of a social act or statement greatly depends on its context (Neuman, 2010). A pragmatist

knowledge claim to qualitative research is pluralistic and problem-centred, and is concerned with consequences of actions and real-world practice (Creswell, 2003). Two approaches are suitable for pragmatic research: experimental and case study (Yin, 2003). Case studies allow researchers to explore a program, event, activity, process, or individuals in depth (Creswell, 2003). Case study methodology is suitable for addressing the complexity of a single case (Stake, 1995). It deals with contextual variables and relies on multiple sources of evidence. It can be thought of as a comprehensive method, covering the logic of design, and data collection and analysis techniques. A case study,

> is an empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident. (Yin, 2003, p. 13)

Social scientists employ various strategies of inquiry—case study, experiments, surveys, histories, and archival research—to give meaning to real-life events (Yin, 1994). Three considerations guide the choice of research strategy: the type of research questions, the desired amount of control over the research events, and whether the focus of the investigation is on a contemporary phenomenon within a real-life context. The case study methodology is well suited for exploring "how" and "why" questions–when the study focus in on operational links rather than on frequencies or incidences.

The thesis research design was chosen for two main reasons. First, exploratory research is wholly justified when the literature review indicates a scarcity of studies in the area or phenomenon of interest (Stebbins, 2001). Second, the epistemological underpinnings of exploratory research presume facts are best reached through a holistic, multi-perspective

investigation; facts are created through social interaction rather than being "out there" waiting to be found or measured. It is thus suited for an in-depth understanding of ethical hacking practices as they exist and develop within an organization. The qualitative case study methodology,

• Supports the systemic exploration of organizational practices (Miller, 2009);

• Aligns with TEI in its systemic and theoretical orientation regarding data collection and analysis—including triangulation via data derived from multiple perspectives and stakeholder groups;

• Is well suited for capturing the unique complexities of a single case (Stake, 1995);

• Is suitable when the study focus is on operational links rather than on frequencies (Yin, 1994);

• Is suitable when little control over events is expected (Yin, 1994);

• Is suitable when the focus of the study is on contemporary phenomena within a real-life context (Yin, 1994).

Data Collection and Analysis

Interviews are useful when participants cannot be observed directly. Advantages of interviews include more researcher control over the line of questioning, and the ability to obtain historical and primary information (Creswell, 2003). In-depth interviews allow researchers to collect the respondents' perceptions of their world. Researchers use interview quotations to illustrate key analytical points. In-depth interviews are typically done "to

solicit people's descriptions and explanations of events taking place in their own environment" (Eid, 2011, p.10).

For data collection, the researcher relies on in-depth interviews with five IT and information security experts with first-hand knowledge about ethical hacking practices at the participating research site. Further, the researcher conducts a comprehensive document review. Finally, the researcher uses a research journal where he keeps a record of important milestones in the thesis development as well as of developments related to the thesis research design. The interview participants, university professors and industry professionals, are sought out for their expert knowledge about scholarly research in ethical hacking, about industry best practices in information security management, and about ethical hacking practices at the research site. A purposeful data sampling strategy, and sampling of insiders' expert resources provided by the thesis supervisor's professional contacts, is used in pursuit of an ethical and comprehensive analysis. Interview experts have a minimum of one year experience in IT and information security management.

In-depth, focused (Yin, 1994), and semi-structured interviews are conducted within a set time (1 hour) at various university locations. The face-to-face interview sessions are audio recorded and the relevant parts are transcribed for accuracy and attentive analysis. Further, interview notes are taken. The data is coded against the theoretical propositions (Yin, 1994) of TEI. The thesis uses the illustrative pattern matching method (Neuman, 2010) as the analytic strategy to frame an organizational understanding about each ethical hacking element. The interviews are first transcribed in five separate documents. In each, a table is created to sort expert responses into categories, as they address the thesis elements of inquiry

—the meanings, ethics, uses and practices, and value of ethical hacking. The findings are then merged into one table. The juxtaposition of the findings helps the researcher identify common understandings as well as variations in perceptions about the meanings, ethics, uses and practices, and value of ethical hacking in an organization.

The scientific and theoretical justifications for the case study can be stated as follows. Scientific justification: Cyber-security actors can eliminate the risk of hacking by reducing unpredictability in the information environment about ethical hacking organizational aspects. The defining characteristics of risk are mainly exposure and uncertainty (for the case to be considered risk). By reducing unpredictability, cyber-security actors are eliminating the risk because the existence of risk requires uncertainty (which can be understood equally to unpredictability). Theoretical justification: First, the theory (TEI-KW) as applied is suitable for the research site because the level of complexity of the theory corresponds to a level of complexity within the organization (requisite variety rule). Second, there is complete alignment between the theory and its object of research, ethical hacking, as both are oriented toward pragmatic ethics (which allows the researcher to use TEI-KW for the study of ethical hacking and the qualitative assessment of the effectiveness of its use).

The university is chosen as the research site because i) the needed expert knowledge in internal and external (industry-wide and academic) ethical hacking aspects is found there, ii) there is important cooperation from the IT department in conducting the interviews, iii) the research site implements state-of-the-art IT and information security technologies and practices, and iv) the research site has a complex IT and information security organizational

structure to match the complexity of the used theoretical framework (the law of requisite variety).

Access to Organizational Data

The nature of the organizational data about ethical hacking meanings, the uses and practices which the researcher had access to, and the difficulties in obtaining access to organizational data, can be understood within the context of concern from the IT department about divulging information which malicious hackers can use to compromise the integrity of the organizational information security system. Information which can give malicious hackers an understanding about the organizational information security architecture or practices can be seen as potentially creating a vulnerability. Expert C noted about publishing organizational information security policies online, "if you have something posted online and the bad guys look at it, they know what they have to do to break into somebody's system" (personal communication, April 24, 2014). Interview participants at the research site had concerns about exposing information which malicious hackers can exploit.

To acquire permission to conduct in-depth interviews about ethical hacking practices with IT staff at the participating organization, the principal researcher first had to address two main concerns raised by the IT executive office: 1) Concerns about creating a security vulnerability at the organization by divulging sensitive information about technical or management ethical hacking practices, or by disclosing the identity of the research site or an interview participant; 2) Concerns about safeguarding employee (participant) confidentiality and about job security. At least two participants requested that their job titles not be

disclosed. The IT department would kindly cooperate with the researcher after the two main mechanisms which the thesis will adopt to manage these two concerns were explained. First, the thesis will employ the validation protocol triangulation of observers (Neuman, 2010) or member checking (Stake, 1995) which will give the interview participants the opportunity to review their contributions and quotes, and to correct them if necessary before they are included in the final thesis copy. Second, the organization's name will be dropped from the thesis. The site will be identified as a Canadian university.

Reliability and Validity

The concepts of reliability and validity in qualitative research are first explained. A discussion of the adopted validation protocols follows. Reliability and validity are concepts that address the truthfulness, credibility, or believability of findings (Neuman, 2010). Reliability refers to the replicability of a researcher's results–the extent to which another researcher can make similar observations under identical or very similar conditions (Creswell, 2003; Neuman, 2010; Stake, 1995; Stebbins, 2002; Yin, 1994). Reliability means dependability or consistency (Neuman, 2010). Researchers must be consistent in how they make observations; for example, through the use of explicit interview questions and research procedures (Neuman, 2010; Yin, 1994). Validity in exploratory research (credibility or trustworthiness) refers to whether a researcher can gain an accurate impression of a group, a process, or an activity, and how so (Stebbins, 2002). Validity suggests truthfulness. It refers to "how well an idea 'fits' with actual reality"; or "how well we measure social reality using our constructs about it" (Neuman, 2011, p. 175). Qualitative researchers are more interested

in achieving authenticity than in realizing a single version of Truth (Neuman, 2010). Authenticity means, “offering a fair, honest, and balanced account of social life from the viewpoint of the people who live it every day” (Neuman, 2011, p. 181).

Reliability requires clarity about the followed procedures of data collection, analysis, and interpretation to ensure consistency. Hence researchers are encouraged to develop a case study protocol, keep an organized case study database, and maintain a chain of evidence (Yin, 1994). Reliability also requires clarity on the logic linking the data to the research propositions or questions, the operational measures used for the concepts or theories, and the criteria used to interpret the data (Yin, 1994). The thesis enhanced the reliability of the research methodology by providing details about the participant recruitment process, the data collection methods (the interviewing process and interview questions, as well as documentation gathering), and data analysis (relying on theoretical propositions from the 5 steps of TEI). Beside reliability, qualitative researchers try to enhance the credibility of their research in various ways.

Data Validation Protocols

Neuman (2010) presents four types of triangulation used in social research: triangulation of measure, triangulation of observers, triangulation of theory, and triangulation of method. Stake (1995) suggests investigator triangulation. Creswell (2003) recommends researchers expressly clarify the biases they bring to the study. Building primarily on Neuman (2010), Stake (1995), and Yin (1994) the thesis employs four triangulation protocols to ensure the accuracy of the findings. First, in triangulation of measure (Neuman,

2010) or triangulation of data (Yin, 1994), the researcher uses different sources of data (five information security management experts who represent key stakeholder groups, beside organizational documentation), and different measures of ethical hacking (including technical, legal, ethical, communicative, and management perspectives) in order to increase the validity of the study. Second, in triangulation of method (Stake, 1995), the researcher conducts in-depth interviews with key stakeholder groups within the organization, as well as a document/website review. Third, in triangulation of observers (Neuman, 2010) or member checking (Stake, 1995), the researcher consults the participants on the findings (the interview transcripts) so as to counter possible selective perception and interpretation by the researcher. Fourth, in triangulation of theory, the researcher uses two complementary theoretical lenses, TEI and Weick's theory of organizing. Rigor in the thesis research design and analysis comes from having clear research procedures, and from implementing four data validation protocols.

Ethical Considerations

Interview participants are asked to sign a consent form stipulating voluntary participation and their right to withdraw, and demonstrating the purpose of the study, procedures of the study, and benefits of the study. The researcher takes steps to protect the confidentiality of the interview data by safeguarding all the working manuscripts in a secure office with limited access. Finally, the researcher applies for ethical clearance in his institution given the fact that the empirical research involves human subjects.

Chapter Conclusion

This chapter first addresses the methodological justification for the thesis. It then explains the research design. This is followed by a statement about the rationale for the selection of the research site and sampling strategy. Data collection and analysis procedures are then discussed. An explanation of the implemented data validation protocols follows. Finally, some ethical considerations are noted.

Findings

The thesis adopted two complimentary research methods, in-depth interviews and a document review, to explore ethical hacking use in a Canadian university. The researcher conducted in-depth semi-structured interviews with five IT and information security experts who represent key stakeholder groups within the organization. Interview and document data were used to answer the thesis question, "What are the meanings, ethics, uses and practices, and value of ethical hacking in a Canadian university?" In terms of data analysis, data addressing the thesis question (the inquiry elements) were coded against the theoretical propositions (Yin, 1994) of TEI (the 5 steps) during open coding. First, the transcribed interviews were coded. Eight main topic themes emerged. The organization had a dedicated computer services website accessible from its main webpage. The researcher examined the website and identified and analyzed eighteen documents containing data addressing the inquiry elements (the meanings, ethics, uses and practices, and value of ethical hacking). The documents were categorized into four types (informational, policy, reports, and news) and topic themes under each document type were identified. Themes which addressed the four inquiry elements were merged with the eight interview themes to frame organizational understandings about each ethical hacking element. The following two sections (Document Review, and Semi-structured Interviews) described the process of data collection and organization, that is, the data sources, and how the data were identified, selected, and sorted into themes which addressed the thesis question. This was followed by an elaboration of the eight themes. The chapter ended with a recapitulation of the key points.

Document Review

The organization under study had a dedicated computer services website accessible from its main webpage. The researcher studied this website and identified documents and data which addressed the inquiry elements. Eighteen documents were identified and used in the thesis. Four general document types were identified: informational, policy, reports, and news (the latter, news briefs, had no value for this study). For each of the first three document types, topic themes were identified. Data addressing the inquiry elements from these themes were coded in alignment with the theoretical framework, supplementing the eight interview themes.

Semi-structured Interviews

The researcher conducted in-depth face-to-face semi-structured interviews with five IT and information security experts who represented key stakeholder groups within the organization. Interviews were conducted within a set timeframe of one hour and followed a set of predetermined questions. The interview participants, university professors and information security industry professionals, were sought out for their expert knowledge about 1) scholarly research in ethical hacking; 2) broad industry trends and best practices in information security management, including information security compliance management, risk assessment and compliance software, and typical information security policy objectives; 3) organizational practices in ethical hacking, especially in information security management and risk assessment practices; and 4) organizational communication routines that may underlie various perceptions about ethical hacking aspects. Interview experts had a minimum

of one year experience in IT and information security management. A purposeful data sampling strategy, and sampling of insiders' expert resources provided by the thesis supervisor's professional contacts, were used in pursuit of an ethical and comprehensive study.

Based on the analysis, the following eight themes, representing organizational understandings, were identified and articulated. The first theme captured participant views about the intended ends and possible side effects of ethical hacking practices within the organization. The second theme summarized the perceived means of ethical hacking. The third theme summarized the perceived value of ethical hacking. The fourth theme addressed participant views about the management uses and practices of ethical hacking within the organization, while the fifth theme addressed their views about the technical uses and practices of ethical hacking within the organization. Theme 6 presented key stakeholder perceptions about the organizational communicative uses and practices of ethical hacking—communicative routines and technological relations. Theme 7 presented organizational perceptions about the meanings of ethical hacking. The final theme presented organizational perceptions about the ethics of ethical hacking.

Theme 1: Intended ends and possible side effects of ethical hacking. Perceptions about the intended ends of ethical hacking use in the organization included a perception of ethical hacking as a management tool used in pursuing organizational management goals (Expert A, Expert D, Expert C, and organizational documentation P2), and a perception of ethical hacking as a technical tool used in vulnerability assessment (Expert B and Expert E).

For Expert A, ethical hacking was used to achieve "continuous improvement of information security, in partnership with the greater community." For Expert D, Expert C, and according to documentation P2, ethical hacking was used to protect the information assets. The end goal of ethical hacking use was "to make sure that the application that you are trying to protect is protected," said Expert C. According to organizational documentation P2, information assets, including software, software applications, and data, should be protected from unauthorized alteration or damage--from potential threats to confidentiality, integrity or availability of information. For Expert B, a main goal of ethical hacking was to discover systemic vulnerability sources. Ethical hacking was used to "run in-house vulnerability testing on servers, assess the vulnerabilities in the used software, and explore new sources of vulnerability" (Expert B). For Expert E, in general, the goal of ethical hacking was to identify vulnerabilities and fix them before a hacker exploits them (Expert E had limited knowledge about organizational ethical hacking practices).

Perceptions about possible side effects or drawbacks of ethical hacking use in the organization entailed social/PR, technical, and financial perspectives. The primary concern for Expert B and Expert A was social/PR, namely, that ethical hacking had a PR stigma. Ethical hacking "has a PR stigma. People may fear their information will be compromised during ethical hacking," said Expert A. The primary concern for Expert E and Expert C was technical, namely, that ethical hacking can damage the information system or destroy data if not performed properly. Secondly for Expert C, the system may remain exploited after ethical hacking was performed. A second concern for Expert A was technical, namely accidental damage to the system during ethical hacking procedures. The main concern for

Expert D was financial, namely, that documents related to ethical hacking (reports and strategy) can get stolen. A second concern for Expert D was financial, namely, that investments were needed to upgrade the system. A second concern for Expert E was financial, namely, that ethical hacking may be costly.

Theme 2: Perceived means of ethical hacking. Organizational perceptions about ethical hacking means included perceptions that the organization used both commercial and open source technologies in information security risk assessment practices (Expert B, Expert D, Expert E, Expert A, and Expert C). Expert B, Expert D, Expert E, and Expert A emphasized the use of open source technologies, while Expert C emphasized the use of commercial software.

Primarily for Expert A, the organization can use open source technologies for threat risk assessment. Secondly, the organization can use well established standardized threat risk assessment methodologies. For Expert B, the university would typically use some commercial ethical hacking software, but "when it comes down to the difficult stuff, I think it is mostly open source." For Expert D, primarily, the "IT professional staff can use open source as long as they consult with their superiors." Secondly, the organization can use hacking open source software such as "script kiddy and download" for free, or it can buy commercial software costing up to $5,000. Primarily for Expert C, commercial software may be more suitable than open source because some application programs that are more suitable for the organization are commercial rather than open source, and commercial software vendors are more likely to have more readily available updated security patches than are

open source. Secondly, “budgetary constraints may drive an organization to the open source route.” For Expert E, in general, the information security testing methodology as well as the used software tools were open source based, though commercial tools were also available.

Theme 3: Perceived value of ethical hacking. The perceived value of ethical hacking for the organization can be located in its utility in risk assessment procedures, and can be understood from management, technical, and communicative perspectives. Different stakeholders emphasized different perspectives.

Expert B and Expert C emphasized the use of ethical hacking as a pragmatic value system to help make decisions about suitable countermeasures by weighing the risks of being attacked and associated damage costs against the cost and effectiveness of countermeasures, that is, by weighing the costs against benefits. Said Expert B,

> To determine value, estimate how likely is an attack to happen, what are the consequences of that happening, and what would be the cost of preventing this from happening. Consider the costs against the benefits.

Second for Expert B and Expert C, ethical hacking was a process or a methodology to help decision makers understand and prioritize risks. The organization cannot perform ethical hacking against all the applications in the environment, they said. “You have to prioritize,” argued Expert C. “The Internet layer should be protected first, and then you can work on other things.”

Similarly, Expert E and organizational documentation P2 emphasized the use of ethical hacking as a process to help decision makers understand and prioritize risks. Expert E

argued the professional hacker “asks the client about the value of the assets, assesses the threats and the potential attacks on the assets, and examines the security mechanisms.” The organizational documentation P2 indicated its emphasis on ethical hacking as a process by defining risk assessment as a process of determining the different threats to the information assets, estimating the probability of their occurrence and potential consequences, and determining the costs of increased protection. Second for Expert E and organizational documentation P2, the value of ethical hacking can be found in its utility as a pragmatic, risk based value system for decision making.

Expert D argued that the use of ethical hacking technologies was subject to organizational goals and constraints including, the technology’s CPU power consumption, its price, its ease of use and implementation, its features, the reporting method, and the after sales support. Finally, for Expert A the value of ethical hacking for the organization was in the fact that ethical hacking procedures and technologies are well established, especially in open source.

Theme 4: Management uses and practices of ethical hacking. The organization used ethical hacking in information security management in five ways: compliance management (Expert A, Expert D, and Expert C), threat risk assessment (Expert A, Expert E, and Expert B), network assessment (Expert D), design implementation (Expert C), and vulnerability testing (Expert B).

Primarily for Expert A, ethical hacking was used to test whether the system was compliant with information security standards (Expert A). “Most of the industry focuses on

security compliance, or security testing, or security validation, or security certification," said Expert A. Second for Expert A, threat risk assessment was used as an information security risk management tool. For Expert C, first, ethical hacking as pen testing was used to verify the implementation of the recommended security design; second, it was used in compliance verification. Expert C and Expert D explained that the university must comply with Canadian privacy laws, including the federal privacy act, access to information act, and Personal Information Protection and Electronic Documents Act, as well as be PCI compliant. One compliance requirement under PCI DSS is to regularly monitor and test the computer network.

For Expert D, ethical hacking was used "in network and applications assessment—which includes testing for systemic vulnerabilities—to lower the risk of illegal access of computing resources." Second for Expert D, ethical hacking was used "to verify that policies are being observed and standards are being met." Expert B said ethical hacking was used in vulnerability testing and in information security threat risk assessment. Expert E argued that, in general, ethical hacking as threat risk assessment was a systematic approach to understanding a) what are the threats, b) what are the assets, c) what is the value of the assets, and d) what is the possibility people will attack these assets.

Theme 5: Technical uses and practices of ethical hacking. Expert E, Expert A, Expert D, and Expert C agreed that the two main organizational uses of ethical hacking as a technical tool related to its use in risk assessment and vulnerability assessment practices. Expert B emphasized its application in social engineering.

For Expert A, threat risk assessment is a well-established methodology, part of which is a procedure, and another part involves making value decisions about the damage that can occur from an attack, monetary or public relations. Said Expert A, "for each vulnerability you have to assess what is the value of the damage that can occur, and that can be monetary or public image." For Expert D, ethical password hacking, as part of risk assessment, tests the ability to hack a password by using the default factory password search, the dictionary search, social engineering, man-in-the-middle attack, and the brute force search methods. Expert E said that, in general, uses of ethical hacking as a technical tool included its use in vulnerability testing, and its use in threat risk assessment. For Expert B, organizational uses of ethical hacking as a technical tool or strategy included its use in social engineering. For example, Expert B said, an ethical hacker can "gather secure information from users and report on the results, for example, how many users gave their passwords." Expert C outlined three types of information security testing (simulation scenarios of ethical hacking), subject to the organizational constraints and needs. First, doing pen testing on a QA server or on a production sever. Second, conducting two security levels of pen testing—the organization may give the professional hacker some details about the information system, specifically, the IP, the URL, and the password test user name. Third, the ethical hacker can choose between performing vulnerability assessment and penetration testing.

Theme 6: Communicative uses and practices of ethical hacking.

Communicative routines. Organizational understandings about ethical hacking communication routines can be stated as five organizing/administrative concerns. First, there

were no standard methods to communicate about ethical hacking (Expert E, Expert B, and Expert D). As Expert B put it, "There is no standard method of communicating about ethical hacking issues. The IT staff can communicate through email, telephone, memos, or at meetings." Second, there was no standard language used for ethical hacking (Expert E, Expert B, and Expert D). In the words of Expert D, "the use of language about ethical hacking is not standardized." Third, the IT department was decentralized, and decision-making was decentralized (Expert D, Expert B, and Expert C). Fourth, communication among the various IT staff about ethical hacking practices was on a need to know basis (Expert C, Expert D, Expert A, and organizational documentation). "You only notify those people who are supposed to know about this. You do not notify the entire organization or the entire IT that you are going to do pen testing" (Expert C). Fifth, communication among the various IT staff about ethical hacking practices usually took place through email (Expert D and Expert C), telephone, memos, or at meetings (Expert D).

Technological relations. Technological relations explored participant perceptions about how the organization communicated with its users about their roles and responsibilities regarding information security practices, including what information the organization makes available to users. The emphasis of the organizational documentation pertaining to information security management was on password security management, social engineering schemes aimed at stealing personal data (spam, phishing, and Trojans), and viruses. The university's website posted several documents—policies and informational reports—specifying user responsibilities in protecting their accounts as well as in protecting the

organization's information assets against damage or misuse. Expert B, Expert A, and Expert E focused on efficient and autonomous technology use, while Expert D and Expert C focused on security awareness training.

Expert B argued that, typically, "the information system handles most of the concerns regarding password selection and password properties." For Expert A and Expert E too, it was important to focus on making the technology easy to understand, use, and implement. "If the technology is hard to use, it can be easy to misuse," said Expert A. Expert D argued that security awareness training can help organizations improve organizational communication about ethical hacking, password security, and user roles and responsibilities. "Awareness training can help the organization establish a baseline about the meanings, ethics, and value of ethical hacking" (Expert D). For Expert C, security awareness training can help users learn about social engineering and phishing schemes and how to prevent them, and about good password management practices. "You tell the audience in the awareness training … do not click on any links unless you are sure about it," said Expert C.

Theme 7: Ethical hacking meanings. Organizational understandings about ethical hacking meanings leaned toward a technical perspective, seeing it as hacking (Expert A, Expert E, Expert B, and Expert C), and as vulnerability assessment (secondly for Expert A, Expert E, and Expert B). Secondly for Expert C, ethical hacking was pen testing. Expert D saw ethical hacking primarily as network assessment.

Expert A said ethical hacking was "a hacking process performed to discover vulnerabilities and to test the effectiveness of the information security safeguards in place."

Expert B argued, “the term ethical hacking is used in opposition to hacking, to distance yourself from malicious hackers,” adding, “ethical hacking is just hacking.” Expert D said ethical hacking was “network assessment, which includes assessing the vulnerability of the network, systems, applications, and how users sign in.”

Theme 8: Ethical hacking ethics. Organizational understandings about the ethics of professional ethical hackers fell under two themes. It was ethical in that it followed a technical process; and it was ethical in that it followed a legal process. In other words, ethical hacking was seen as a technical process of risk assessment (Expert E, Expert B, and Expert A), and as a legal process of risk assessment (Expert D, Expert E, and Expert C).

Expert B put it bluntly, “there is nothing ethical about ethical hacking. It is a technical process.” Expert A argued that ethical hacking “refers to how you do the hacking, not why you do the hacking; the ethics is about the process of hacking, not the reason the hacking is being done.” Expert D said ethical hackers have legal authorization from top level management to perform hacking, they “hack the system officially, in the legal sense.” Expert C remarked that ethical hacking was “money making in the ethical way, in the legal way. Ethical is legal.”

Chapter Conclusion

Interview and document data addressing the inquiry elements were identified, sorted, and coded in alignment with the theoretical framework during open coding. Eight topic themes which represent organizational understandings about each ethical hacking element

were identified and elaborated. First, the interviews were transcribed. Eight themes emerged during the open coding of the interviews. The organization had a dedicated computer services website. The researcher examined the website, and identified and analyzed eighteen documents containing data addressing the inquiry elements. The documents were categorized into four document types (informational, policy, report, and news) and topic themes under each document type were identified. Themes which addressed the elements of inquiry were merged with the eight interview themes to frame organizational understandings about each ethical hacking element. Finally the eight themes were elaborated.

Advanced Analysis and Discussion

This chapter connected the research question, the theoretical framework, and the findings. The chapter began with a review of the coding and the analytic strategy. Data coding was performed against the theoretical propositions (Yin, 1994) of TEI. The thesis used the illustrative pattern matching method (Neuman, 2010) as the analytic strategy for interpreting the data. In chapter 4, themes were identified under each inquiry element. These themes represented organizational understandings. The organizational understandings were now contextualized within ethical hacking literature and broader industry practices. Discussion then turned to how TEI-KW was applied to the thesis question. The thesis question was split into two sub-questions. Each sub-question was expressed in three specific questions. TEI was applied to sub-question *a*, and Weick's model was applied to sub-question *b*. Further insights were presented from technological assessment of ethical hacking organizational use by applying TEI-DMG, and from analysis of communicative ethical hacking organizational practices by applying Weick's model. The insights comprise recommendations to the executive office of the IT department in support of a more ethical and efficient implementation of ethical hacking practices. Specifically, guided by TEI-DMG, findings pointed to the need to expand the communicative and social considerations involved in decision making about ethical hacking organizational use. Further, in line with Weick's theory, findings pointed to security awareness training for increasing sensemaking opportunities among stakeholders and reducing equivocality in the information environment. The assessment and recommendations section was followed by the conclusion section.

Coding and the Analytic Strategy

Data analysis involves preparing the data for analysis, representing the data, mapping and coding connections and themes, and interpreting them. The "recursive process of analysis begins immediately with the first data-collection episode and continues throughout the study" (Jackson, Gillies, & Verberg, 2001, p. 242). Analysis of qualitative data typically involves coding or organizing the data into conceptual categories, and using an analytic strategy to interpret the findings (Neuman, 2010). Data coding was performed against the theoretical propositions (Yin, 1994) of TEI. The thesis used the illustrative pattern matching method (Neuman, 2010) as the analytic strategy to interpret the data. The illustrative method anchors or illustrates theoretical concepts with empirical evidence. It applies theory to a concrete social setting and organizes data based on theory. "Preexisting theory can provide conceptual empty boxes that you fill with the empirical evidence" (Neuman, 2011, p. 353). In the pattern matching variation of this analytic strategy, concepts or patterns identified in the findings are matched to those derived from theory. The process of coding can have three phases at three abstraction levels (Strauss, 1987). In open coding, or the first pass, the researcher tags the text with broad concepts. In a second review, or axial coding, the researcher focuses on the connections among open codes to define the themes. Finally, in selective coding, the researcher chooses themes that are likely to guide the research process (Neuman, 2010). To code the interviews and organizational documentation, the thesis used the same elements of inquiry developed early in the study—the meanings, ethics, uses and practices, and value of ethical hacking. The inquiry elements were articulated into themes.

The researcher then contextualized the themes (the organizational understandings about the ethical hacking elements) within ethical hacking literature and broad industry practices.

RQ. What are the Meanings, Ethics, Uses and Practices, and Value of Ethical Hacking in a Canadian University?

The discussion now turns to how TEI-KW was applied to the thesis question, "What are the meanings, ethics, uses and practices, and value of ethical hacking in a Canadian university?" The thesis question was split into two sub-questions. Each sub-question was expressed in three specific questions. TEI was applied to examine sub-question *a*. Weick's model was applied to examine sub-question *b*. Sub-question a) What is the value, and what are the management and technical uses and practices of ethical hacking in a Canadian university? The first question was, 1) What is the value of ethical hacking? (It covered the three themes: Theme 1: Intended ends and possible side effects of ethical hacking, Theme 2: Perceived means of ethical hacking, and Theme 3: Perceived value of ethical hacking). The second question was, 2) What are the management uses and practices of ethical hacking? (It covered Theme 4: Management uses and practices of ethical hacking). The third question was, 3) What are the technical uses and practices of ethical hacking? (It covered Theme 5: Technical uses and practices of ethical hacking). Sub-question b) What are the meanings, ethics, and communicative uses and practices of ethical hacking in a Canadian university? The first question was, 1) What are the meanings of ethical hacking? (It covered Theme 6: Ethical hacking meanings). The second question was, 2) What are the ethics of ethical hacking? (It covered Theme 7: Ethical hacking ethics). The third question was, 3) What are

the communicative uses and practices of ethical hacking? (It covered Theme 8: Communicative uses and practices of ethical hacking).

Sub-question a) What is the value, and what are the management and technical uses and practices of ethical hacking in a Canadian university?

1) What is the value of ethical hacking?

Intended ends and possible side effects of ethical hacking. Participant perceptions about ethical hacking ends/goals fell under two broad themes, namely, management aspects and technical aspects. Expert A, Expert D, Expert C, and organizational documentation P2 saw ethical hacking mainly as a tool used to pursue organizational management goals, that is, they emphasized its management utility for the organization. Expert B and Expert E saw it mainly as a technical tool used in vulnerability assessment.

Ongoing improvement in information security performance is a strategic information security management goal. A second management goal is safeguarding the information assets (Dhillon, 2007; Engebretson, 2011; Graves, 2010; Landoll & Landoll, 2005; Peltier, 2004A, 2004B, 2005; Reynolds, 2012). For Expert A, ethical hacking can be used as a management tool to pursue "continuous improvement of information security, in partnership with the greater community." For Expert D, Expert C, and organizational documentation P2 ethical hacking was used to pursue the information security management goal of safeguarding information assets—more specifically for Expert C, to "make sure that the application that you are trying to protect is protected." For the organization (organizational documentation P2), information assets included software, software applications, and data, which are to be

protected from unauthorized alteration or damage--from potential threats to confidentiality, integrity or availability.

The definition of ethical hacking as risk assessment was the predominant view in ethical hacking books (e.g., Engebretson, 2011; Graves, 2010; Harper et al., 2011; Harris, Harper, Eagle, & Ness, 2007; Landoll & Landoll, 2005; Simpson, Backman, & Corley, 2010). Vulnerability assessment (identifying weaknesses or security holes) is part of a broader risk assessment process. If an exploit penetrates or breaks in an identified vulnerability, hacking is said to take place (ibid). For Expert B, ethical hacking was used to a) run in-house vulnerability testing on servers, b) assess the vulnerabilities in the used software, and c) explore new sources of vulnerabilities. For Expert E, in general, the goal of ethical hacking was to identify vulnerabilities and fix them before a hacker exploits them.

Organizational understandings about side effects or drawbacks resulting from implementing ethical hacking in the organization entailed social/PR, technical, and financial perspectives. For Expert B and Expert A, ethical hacking had a PR stigma. The main side effect for an organization using ethical hacking is harm resulting from a public/PR stigma about ethical hacking. Ethical hacking "carries a stigma because it may be perceived to pose a threat to their private or confidential information" (Expert A). Ethical hacking "is sometimes misunderstood by some people, especially regarding the aim of hackers, who fear it would compromise their information" (Expert B). Some people may fear that their information will be compromised during ethical hacking (Expert B and Expert A). This is a social aspect since the aim of ethical hackers may not be clear to some people (Expert B). Palmer, 2001, Sterling, 1993, and online sources made the point that a hacked business can

suffer from a negative public image. Expert A and Expert B proposed that public knowledge about in-house ethical hacking practices may stigmatize the organization or tarnish its public image.

The technical aspects focused on the risk of damage or harm to the information system or data. For Expert E and Expert C, a main concern was that if ethical hacking was not performed properly, it can break the system or destroy data. “In a lot of cases you try to do penetration test or pen test on business critical systems and you end up breaking it” (Expert C). A second concern for Expert C was that the system may remain exploited after ethical hacking was performed: “How do you ensure that you have reversed the effect of the damage you have done to the system?” A second concern for Expert A was accidental damage to the system during ethical hacking procedures. “By the very nature of hacking you may accidentally do harm. There is a vulnerability to damage” (Expert A). A primary concern for Expert D was that documents related to ethical hacking (reports and strategy) can get stolen. Two experts expressed financial concerns as secondary considerations. Expert D said the organization may have to make new investments in information security measures, including a system upgrade, following an ethical hacking assessment. Expert E expressed concern that ethical hacking practices may be costly for the organization.

Perceived means of ethical hacking. Organizational understandings about ethical hacking means (technologies or practices) used in the university focused on the technical application of ethical hacking, as a risk assessment methodology using software programs. Expert B, Expert D, Expert E, Expert A, and Expert C agreed both commercial and open

source resources were used in information security risk assessment practices. But while Expert B, Expert D, Expert E, and Expert A emphasized the use of open source technologies, Expert C emphasized the use of commercial software.

Expert A argued that the organization can use open source technologies for threat risk assessment. It can use well established standardized methodologies from government resources such as the harmonized standards from the RCMP and others, or from the open source community. Expert B said organizational ethical hacking means included the use of commercial and open source software. The university would typically use some commercial ethical hacking software "but when it comes down to the difficult stuff, I think it is mostly open source." Expert D said the IT professional staff can use open source as long as they consult with their superiors. "Script kiddy and download" hacking software, free (open source) or commercial (costing up to $5,000) can be used. Expert E argued that, in general, the information security testing methodology as well as the used software tools were open source based, though commercial tools were also available. Expert C, however, argued that commercial software may be more suitable than open source because, first, some application programs that are more suitable for the organization are commercial rather than open source. Second, commercial software vendors are more likely to have more readily available updated security patches than are open source. Third, "budgetary constraints may drive an organization to the open source route."

Perceived value of ethical hacking. The value of ethical hacking for the organization can be located in its utility in risk assessment procedures, and can be understood from a

management, technical, and communicative perspectives. From a management perspective, the organizational value of ethical hacking can be located in its utility as a value system (a risk based approach) for decision making about suitable countermeasures. From a technical perspective, the organizational value of ethical hacking can be located in its utility as a process to understand and prioritize security risks. From a communicative perspective, the organizational value of ethical hacking can be located in its utility as risk assessment procedures. Different stakeholders emphasized (prioritized) different perspectives.

The reference to risk assessment procedures in literature tended to overlook what can be considered as two distinct uses of risk assessment technologies—namely, risk assessment as a process or methodology, and as a pragmatic value system. Reynolds (2012), for example, made reference to the pragmatic value system of risk assessment, arguing that the goal of risk assessment was "to identify which investments of time and resources will best protect the organization from its most likely and serious threats" (p. 103). A more direct reference to the pragmatic value system of risk assessment (weighing the perceived benefits against the perceived costs and side effects) was seen in the description of the risk assessment steps by the General Security Risk Assessment Guidelines, ASIS International (2003). According to the guidelines, the basic components or steps in a security risk assessment protocol include: identifying assets; specifying loss events (threats); frequency of events; impact of events; options to mitigate; feasibility of options; cost/benefit analysis; and decision.

Expert B and Expert C emphasized the use of ethical hacking as a pragmatic value system to help decide (judge) about suitable countermeasures by weighing the risks of being

attacked and associated damage costs against the cost and effectiveness of countermeasures, that is, by weighing the costs against benefits. For Expert B, to determine value, "consider the costs against the benefits," that is, estimate how likely is an attack to happen, what are the consequences of that happening, and what would be the cost of preventing this from happening. Expert C said, "I prefer the risk based approach in dealing with threats because the amount of effort you want to put in from a security standpoint depends on the level of risk." Expert C added, the "first question I ask when I go to … project meetings or meet the sponsors is, if you lose this data, what will be the impact on you, what will be the impact on the organization? That makes them think about the costs, monetary or otherwise."

Second for Expert B and Expert C, ethical hacking was a process or a methodology to help decision makers understand and prioritize risks. The organization cannot perform ethical hacking against all the applications in the environment, they said. "You have to prioritize," argued Expert C. "The Internet layer should be protected first, and then you can work on other things." Expert E emphasized the use of ethical hacking as a process or methodology to help decision makers understand and prioritize risks. Expert E argued, the professional hacker 1) asks the client about the value of the assets, 2) assesses the threats and the potential attacks on the assets, and 3) examines the security mechanisms. Organizational documentation P2 also emphasized ethical hacking as a process for decision making, defining risk assessment as the process of determining the different threats to the information assets, estimating the likelihood of their occurrence, evaluating their consequences, and determining the costs of increased protection.

Second for Expert E and organizational documentation P2, the value of ethical hacking can be found in its utility as a risk based value system for decision making. For Expert D, the value of ethical hacking for the organization can be located in the technical criteria used in decision making about ethical hacking countermeasures. Expert D argued that the use of ethical hacking technologies is subject to organizational goals and constraints including, the technology's CPU power consumption, its price, its ease of use and implementation, its features, the reporting method, and the after sales support. For Expert A, the value of ethical hacking for the organization can be understood from a communicative perspective, namely, in the fact that ethical hacking procedures and technologies are well established, especially in open source.

2) What are the management uses and practices of ethical hacking?

Organizational information security concerns. The organization's information security concerns or strategic goals can be understood through the consideration of three risk management considerations: information assets, threat sources, and vulnerability sources.

The broad organizational concern would be safeguarding the information assets (Expert E, Expert D, Expert B, Expert C, and organizational documentation P1 and P2. For Expert E, information assets are typically research data and employee data. For Expert C, research data are the most important information assets to any university. Other important information assets include student information, employee information, and alumni information (Expert C). For Expert D and Expert B, the information assets would be student grades. Expert D argued that in an academic environment, safeguarding student grades is the

main information security concern. Expert B said, “there is fear of students hacking into the system and giving themselves A plus.” Organizational documentation P2 defined information assets as computer systems, application software, programs, and associated data whether electronic or in print. The policy identified student marks and other student data as important assets, classifying such data, which is maintained by professors and teaching assistants, are administrative data. A business report posted on the university’s website identified the student information system as an important information asset.

Data theft or identity theft through social engineering and phishing schemes are major security concerns (Expert D, Expert B, and Expert C). Threat sources to information security can be internal or external (Expert A). Internal threats may come from a university student who may want to steal the identity of an employee or a classmate to change academic grades (Expert D and Expert B). Or a student may steal another student’s password and impersonate the user and send out emails to malign the reputation of the student (Expert C). External threats would include competitors or resellers of information after the university’s research data (Expert C and Expert E).

Vulnerability sources are either known or unknown (Expert A). They include online databases about users in the black market, online techniques to compromise websites, viruses, and vulnerabilities in software (Expert A). For Expert B, the university is faced with three main kinds of vulnerabilities: not updating the software, not reconfiguring default passwords, and from social engineering and phishing schemes. Expert C argued that academic openness and social engineering schemes represent the two important sources of organizational vulnerabilities. “The biggest concern for me is allowing everybody to have

access to everything on the Internet." Even a simple Google search can represent a security threat. "If you click on a link, there is a chance your system will get compromised without you even knowing about it. The bad guys will install links that will steal your personal information. The bad guys have figured out how to make google index or give their links higher rating" (Expert C). Secondly, said Expert C, "the weakest link in security is the human link." A target for social engineering would be "a researcher who could have a competitive advantage." Someone may try to steal the research data through a phishing scheme.

The specific information security topics which the organization chose to address on its website indicate what it considered important security vulnerabilities. The university's website posted educational or informational reports, variously called pamphlets, flyers, guidelines, and so on, comprised of short paragraphs and often point-form statements, prescriptive in tone, and usually making direct reference to its intended audience as users. Password protection in particular was addressed the most, in at least three informational reports discussing password standards and password management best practices, beside at least two security policies which included provisions on the protection of data against threats and unauthorized access. The documents made the point that weak passwords were an important organizational vulnerability. Further, organizational documentation also included at least one informational report about each of spam, phishing, Trojans, identity theft, and viruses.

Management uses and practices of ethical hacking. The organization used ethical hacking in information security management in at least five ways: compliance management (Expert A, Expert D, and Expert C), threat risk assessment (Expert A, Expert E, and Expert B), network assessment (Expert D), design implementation (Expert C), and vulnerability testing (Expert B).

Primarily for Expert A, ethical hacking is commonly used in compliance management. "Most of the industry focuses on security compliance, or security testing, or security validation, or security certification." Ethical hacking "is used to validate and test whether the system is compliant." Ethical hacking was used in the organization to test whether the system was compliant with information security standards (Expert A). Second, for Expert A, threat risk assessment was used as an information security risk management tool. For Expert C, first, ethical hacking as pen testing was used to verify the implementation of the recommended security design; second, it was used in compliance verification, as part of a security audit which aims to verify procedural as well as technical controls. For Expert D, ethical hacking was used in network and applications assessment to lower the risk of illegal access to computing resources. Second for Expert D, it was used to verify that policies were being observed and standards were being met. Expert B said ethical hacking was used in vulnerability testing and in information security threat risk assessment. Expert E argued that, in general, ethical hacking as threat risk assessment is a systematic approach to understanding a) what are the threats, b) what are the assets, c) what is the value of the assets, and d) what is the possibility people will attack these assets.

Typical policy objectives or concerns regarding ethical hacking. Three main organizational policy objectives or concerns were expressed. First, the need to balance between academic openness and information security (Expert C). Second, the need to align policy development and goals with the need to support password safety practices (Expert A). Third, security policies regarding the use of software and hardware resources have to be communicated clearly to everybody (Expert E).

Expert C argued that from the university's perspective, "it is challenge to write a security policy." The policy must aim to strike a balance between academic openness and information security. Expert C argued, "When you have an open environment where you are not supposed to block anything, when you have researchers who may need access to anything, it is hard to write a very strict policy." Expert C added, the policy should not divulge too much information about the organization's security standards lest malicious hackers use this information to their advantage. Expert A argued that organizational policies and system design should support password safety practices among users. "We have a problem at this university. When you have to have three different passwords for three different services, it causes people to write them down and create vulnerability." Expert E emphasized the need to clearly communicate organizational security policies regarding the use of software and hardware resources to users and employees.

3) What are the technical uses and practices of ethical hacking?

Technical uses and practices of ethical hacking. Expert E, Expert A, Expert D, and Expert C agreed that the two main organizational uses of ethical hacking as a technical tool

related to its use in risk assessment and vulnerability assessment practices. Expert B emphasized its application in social engineering.

For Expert A, threat risk assessment is a well-established methodology. The steps include 1) “The first thing is to catalogue what you have”; 2) “Then you have to identify what vulnerabilities you have, and for each vulnerability you have to assess what is the value of the damage that can occur, and that can be monetary or public image”; 3) Next is to assess the likelihood of an attack. For Expert D, ethical password hacking, as part of risk assessment, tests the ability to hack a password by using the default factory password search, the dictionary search, social engineering, man-in-the-middle attack, and the brute force search methods. Expert E said that, in general, uses of ethical hacking as a technical tool included its use in vulnerability testing, and its use in threat risk assessment. For Expert B, organizational uses of ethical hacking as a technical tool or strategy included its use in social engineering. For example, Expert B said, an ethical hacker can gather confidential information from users and report on the results, such as how many users gave their passwords.

Expert C offered a nuanced view about the application of ethical hacking in risk assessment practices, by outlining three types of information security testing (simulation scenarios of ethical hacking), subject to the organizational constraints and needs. First, doing pen testing on a QA server or on a production sever. “The best practices in the bigger organizations you do pen test against a QA system,” which “should be a replica of the production system although it may have less data but the pen tester can still reveal all the vulnerabilities of the system.” Second, the organization can conduct two security levels of

pen testing. “The organization tells ethical hackers … we treat you like the bad guys, you have no information about us. So you do the network scanning, you find the IPs, you create a user ID, you hack into the system and tell us how bad we are. If you say you cannot find anything and you are secure from that perspective, then we will give you the design, we will tell you the exact IPs, we will create a test user ID and password for you and now you do the actual pen test, and now see if our application is vulnerable or not.” Expert C said most organizations provide the IP, the URL, and the password test user name. Third, choosing between vulnerability assessment and penetration testing.

> Vulnerability is a hole that you are trying to find in a system … Once you find the vulnerabilities you get to know how to break into the system. Hence you identify the tools you need to break into the system. Penetration testing is when you actually exploit—use the code or the tool to exploit those vulnerabilities. (Expert C)

Ethical hacking value, and management and technical practices: Key findings. This section summarized the key findings pertaining to the value, and the management and technical uses and practices of ethical hacking in a Canadian university. First, the intended ends and possible side effects, the perceived means, and the perceived value of ethical hacking use were reviewed. Second, the management uses and practices of ethical hacking, including the information security and the policy concerns were presented. Finally, the technical uses and practices of ethical hacking were presented.

There were two main perspectives (understandings) about the intended ends of ethical hacking use in the organization. First, ethical hacking was used to pursue the

information security management goal of safeguarding information assets (Expert D, Expert C, and organizational documentation P2). Second, ethical hacking was used in pursuit of continuous improvement in information security performance (Expert A). The main side effect for an organization using ethical hacking is harm resulting from a public/PR stigma about ethical hacking practices. Ethical hacking carries a stigma because it may be perceived to pose a threat to the privacy or confidentiality of information (Expert A and Expert B). Expert D and Expert E said that ethical hacking practices may be costly for the organization. For example, the organization may have to make new investments in information security measures following an ethical hacking assessment (Expert D). Organizational understandings about ethical hacking means (technologies and practices) used in the university focused on the technical application of ethical hacking as a risk assessment methodology using software programs, commercial and open source (Expert B, Expert D, Expert E, Expert A, and Expert C).

The value of ethical hacking for the organization can be located in its utility in risk assessment practices—namely, in its utility as a pragmatic value system, and as a risk assessment methodology. Ethical hacking as a pragmatic value system can guide decision making about suitable information security countermeasures by weighing the risks of being attacked and associated damage costs against the cost and effectiveness of countermeasures (Expert B and Expert C). Ethical hacking as a process or methodology can help decision makers understand and prioritize information security risks (Expert B, Expert C, Expert E, and organizational documentation P2).

In an academic environment, important information assets would include the student information system and student grades (Expert B, Expert D, and Organizational documentation P2), research data (Expert C), and employee data (Expert E). Data theft or identity theft through social engineering and phishing schemes were major organizational information security concerns (Expert D, Expert B, Expert C, and organizational documentation P2 and informational type documents). Internal threats may come from a university student who may want to steal the identity of an employee or a classmate to change academic grades (Expert D and Expert B). External threats would include competitors or resellers of information after the university's research data (Expert C and Expert E). One important source of vulnerability to hacker attacks was academic openness (Expert C). Another source was software or software applications, which included not updating the software and not reconfiguring default passwords (Expert B). Other important vulnerability sources included social engineering and phishing schemes, and virus threats (Expert D, Expert B, Expert C, and organizational documentation P2 and informational type documents). The organization used ethical hacking in information security management in at least five ways: compliance management (Expert A, Expert D, and Expert C), threat risk assessment (Expert A, Expert E, and Expert B), network assessment (Expert D), design implementation (Expert C), and vulnerability testing (Expert B). Two expressed important organizational policy objectives or concerns were the need to balance between academic openness and information security (Expert C), and the need to align policy development and goals with the need to support password safety practices (Expert A, Expert B, and Expert C).

The two main organizational uses of ethical hacking as a technical tool related to its use in risk assessment and vulnerability assessment practices (Expert E, Expert A, Expert D, and Expert C). There are three types of ethical hacking or information security testing (simulation) scenarios, subject to the organizational constraints and needs. First, performing penetration testing on a QA server or on a production server. Second, the organization can conduct two security levels of penetration testing, depending on the information the organization gives to ethical hackers about the specifics of the information system. Third, choosing between vulnerability assessment and penetration testing (Expert C).

Sub-question b) What are the meanings, ethics, and communicative uses and practices of ethical hacking in a Canadian university?

1) What are the meanings of ethical hacking?

Ethical hacking meanings. Organizational understandings about ethical hacking meanings leaned toward a technical perspective, seeing it as hacking (Expert A, Expert E, Expert B, and Expert C), and as vulnerability assessment (secondly for Expert A, Expert E, and Expert B). Secondly for Expert C, ethical hacking was pen testing. Expert D saw ethical hacking primarily as network assessment.

Expert B said ethical hacking was "just hacking." The use of the term "ethical" is meant to dispel the bad image of hackers. The term ethical hacking is used in opposition to hacking, "to distance yourself from malicious hackers." Secondly for Expert B, ethical hacking referred to a technical process of "trying to find vulnerabilities in the system before the bad guys do, using the same means." For Expert E, ethical hacking was a practice in the

IT industry which involved using hacking technologies to identify vulnerabilities in a network infrastructure. Ethical hacking was also called vulnerability assessment, pen testing, and hacking (Expert E). Expert C said ethical hacking was hacking or pen testing "in the ethical way, in the legal way." Expert A argued that ethical hacking was a hacking process performed to discover vulnerabilities and to test the effectiveness of the information security safeguards in place. For Expert D, ethical hacking was primarily network assessment, which includes assessing the vulnerability of the network, systems, applications, and how users sign in.

There were four different meanings for ethical hacking among the five stakeholder groups: hacking, vulnerability assessment, pen testing, and network assessment. Literature review sharply contrasted with these findings. Published ethical hacking books mostly equated ethical hacking with risk assessment and penetration testing (e.g., Engebretson, 2011; Graves, 2010; Harper et al., 2011; Harris, Harper, Eagle, & Ness, 2007; Landoll & Landoll, 2005; Simpson, Backman, & Corley, 2010). Only one participant, Expert C, and as a secondary view, defined ethical hacking as "pen testing."

According to the International Council of Electronic Commerce Consultants (EC-Council), a professional certification body best-known for its Certified Ethical Hacker certification, the definition of an "Ethical Hacker" is "very similar to a Penetration Tester. The Ethical Hacker is an individual who is usually employed with the organization and who can be trusted to undertake an attempt to penetrate networks and/or computer systems using the same methods and techniques as a Hacker." The definition of ethical hacking as hacking among IT professionals within an organizational setting (the case study site) was consistent

with the view that the term hacking still carried a positive connotation among IT and computer professionals (Palmer, 2001; Sterling, 1993).

2) What are the ethics of ethical hacking?

Ethical hacking ethics. Organizational understandings about the ethics of professional ethical hackers fell under two themes. It is ethical in that it follows a technical process, and it is ethical in that it follows a legal process. In other words, ethical hacking as a technical process of risk assessment (Expert E, Expert B, and Expert A), and ethical hacking as a legal process of risk assessment (Expert D, Expert E, and Expert C).

Expert E recognized ethical hacking as a technical process of threat risk assessment, arguing it was "a systematic approach to understanding a) what are the threats, b) what are the assets, c) what is the value of the assets, and d) what is the possibility people will attack these assets." Expert B argued there was nothing ethical about ethical hacking, "it is a technical process" of risk assessment. Expert A argued "the ethics is about the process of hacking, not the reason the hacking is being done." The ethical hacking process for Expert A, a) does not harm and there is no intent to do harm; b) stipulates an ethical responsibility to avoid harm; c) reports on the findings; d) "recognizes that there are guidelines about what you can do"; e) "recognizes that there is a moral imperative toward the public good"; and f) "recognizes that it is done at a professional capacity."

Expert D and Expert C emphasized the legal aspects of ethical hacking. For Expert D, ethical hackers a) have legal authorization from top level management to perform hacking. They can "hack the system officially; in the legal sense"; b) follow best practices;

c) follow organizational policies; and d) recommend to mitigate information security holes. For Expert C, ethical means following a policy or a legally binding agreement. “Ethical is legal.” Ethical hackers follow a legal process. They must have permission to hack. “They must have a contract signed with an organization giving them permission to expose company data before starting to hack” (Expert C). Secondly for Expert E, ethical hackers are usually invited by the asset owner to perform hacking to find vulnerabilities and fix them. They get access legally to the resource, and communicate the results to the owner of the assets.

A meta-ethical analysis can further help clarify the nature of ethical hacking ethics. Garner and Rosen (1967) outline three key meta-ethical questions that can be used to conduct a meta-ethical analysis: 1) What is the meaning of moral terms or judgments? 2) What is the nature of moral judgments? And 3) How may moral judgments be defended? These meta-ethical questions are elaborated in a table (The Meta-ethics of Ethical Hacking Table) from several perspectives, including theoretical, empirical, scholarly, and commercial. Follows are outlines of the descriptive meta-ethics of ethical hacking considered from two other perspectives (other than the participants).

For EC-Council (the International Council of Electronic Commerce Consultants), the certification institution for the Certified Ethical Hacker designation (www.eccouncil.org), A Certified Ethical Hacker is

> a skilled professional who understands and knows how to look for weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of the target system(s).

An “Ethical Hacker” is

> an individual who is usually employed with the organization and who can be trusted to undertake an attempt to penetrate networks and/or computer systems using the same methods and techniques as a Hacker.

Descriptive ethics of ethical hacking found in several well-cited ethical hacking texts include: 1) Ethical hackers should address both systemic vulnerabilities as well as preventive measures (Harris, 2007; Palmer, 2001); 2) The practices of professional ethical hackers are governed by a legal framework. Ethical hackers should always obtain permission from the data owner before attempting to access the computer system or network (Graves, 2010; Palmer, 2001); and 3) Ethical hackers should gain the trust of clients (Ibid); they should take “all precautions to do no harm to their systems during a pen test” (Graves, 2010, para. 1).

Therefore a descriptive account of ethical hacker ethics can be stated as follows: Ethical hackers are skilled and knowledgeable IT and information security professionals usually employed with an organization and who look for vulnerabilities in target systems and can be trusted to “undertake an attempt to penetrate networks and/or computer systems using the same methods and techniques as a Hacker”; and who use the same knowledge and tools as malicious hackers but in a lawful and legitimate manner to assess the security posture of target systems. Ethical hackers should address both systemic vulnerabilities as well as preventive measures.

3) What are the communicative uses and practices of ethical hacking?

Ethical hacking communicative practices: Communicative routines. Participant views were used to frame an understanding about how the IT staff routinely communicated about ethical hacking issues in the organization, among itself and with other users. Organizational understandings about ethical hacking communication routines can be stated as four organizing/administrative concerns. First, there were no standard methods to communicate about ethical hacking (Expert E, Expert B, and Expert D). Second, there was no standard language used for ethical hacking (Expert E, Expert B, and Expert D). Third, the IT department was decentralized, and decision-making was decentralized (Expert D, Expert B, and Expert C). Fourth, communication among the various IT staff about ethical hacking practices was on a need to know basis (Expert C, Expert D, Expert A, and organizational documentation).

Generally speaking, said Expert E, there was no standard way to communicate about ethical hacking within organizations, and there was no standardized language for ethical hacking. The findings can be communicated in a Vulnerability Assessment Report which can advise risk management decisions. Such a report usually includes sections of introduction, planning and schedule, procedures, findings and analysis, and (optional) recommendations (Expert E). The IT department was decentralized, and decision-making was decentralized (Expert D, Expert B, and Expert C). Expert D said that the IT staff worked as independent units: a) they did not necessarily tell each other about ongoing activities, for example, during information security testing; and b) the use of language about ethical hacking was not standardized. Expert D elaborated that there was no standard method of communicating about ethical hacking issues. The IT staff did not necessarily use the term to mean the same

thing or to refer to the same concept or process. IT professionals in various units would have different perceptions about ethical hacking. “They would not have common knowledge” (Expert D). Expert B agreed, there was no standard method of communicating about ethical hacking issues whether within the various IT units or across the university, and there was no standardized language or terminology for ethical hacking.

Expert C said communication among the various IT staff about ethical hacking practices was usually on a need to know basis, and only to those involved in a project. When a security architect performs pen testing “to verify if the security recommendations were implemented,” usually only those directly involved in the testing process are notified. “You do not notify the entire organization or the entire IT that you are going to do pen testing. You do notify, for example, the network monitoring team or the server team” (Expert C). Expert A made a similar point, saying the organizational communicative practices regarding ethical hacking can be understood in relation to compliance with information security standards. Organizational documentation P2 assigned managers of administrative units, among other managerial and executive staff, responsibility for restricting information to those who really need it to perform their assigned functions for all sensitive information assets. Communication among the IT staff about ethical hacking practices usually took place through email (Expert D and Expert C), telephone, memos, or at meetings (Expert D).

Ethical hacking communicative practices: Technological relations. Technological relations explored participant perceptions about how the organization communicated with its users (university students and employees) about their roles and responsibilities regarding

information security and ethical hacking practices. Expert B, Expert A, and Expert E focused on efficient and autonomous technology use, while Expert D and Expert C focused on security awareness training. The university's website posted several documents—policies and informational reports—addressing user responsibilities in protecting their accounts as well as the organization's computer resources against damage or misuse.

Expert B argued that typically the information system handles most of the concerns regarding password selection and password properties. Second, the university's website had information about identity theft and about password security best practices. Third, sometimes the university sends out emails to students to warn them about phishing schemes. For Expert A and Expert E, it was important to focus on making the technology easy to understand, use, and implement. Expert A argued that if the technology is hard to use, "it can be easy to misuse; if the system is not usable and the system is not understandable, you are going to have more flaws and it will be hard to understand what is going on." For Expert E, in general, users do not need to have a lot of knowledge about information security to be able to protect themselves or to be protected. The organization's IT system should be able to enforce security policies such as a strong password policy.

Expert D and Expert C argued that security awareness training can help organizations raise the awareness of their employees and students about ethical hacking uses and value, best practices in password security management, and user roles and responsibilities. Awareness training can help the organization establish a baseline about the meanings, ethics, and value of ethical hacking, added Expert D. For Expert C, security awareness training can help users learn about social engineering and phishing schemes and how to prevent them,

and about good password management practices. “You tell the audience in the awareness training do not open something suspicious, and if you open do not click on any links unless you are sure about it,” said Expert C. Awareness training can be about how users should change their passwords on a regular basis, and about how to use a strong password (Expert C).

The emphasis of the online organizational documentation pertaining to information security management (as suggested by its focus on the specific topics covered) was on password security management, social engineering schemes (spam and phishing) aimed at stealing data or identity, Trojans used in identity theft, and viruses. User responsibly regarding the protection of information assets was stated in at least two organizational documents, beside a dedicated document detailing user-client code of conduct. Documentation about user code of conduct for computing resources began with reminding users that they are responsible for all use of their account and computing resources. One policy statement (P1) outlined user responsibility to promote responsible, ethical, and secure use of the facilities and services, including the security of their own access codes, programs, and data files. The policy added that users were not allowed to access, change or destroy another’s data, files, or programs. Another informational report told users it is their responsibility to make sure that all their account passwords are as difficult to guess as possible, and that they could be held “legally responsible” for any damage caused by someone using their accounts.

Ethical hacking meanings, ethics, and communicative practices: Key findings.

This section summarized the key findings pertaining to the meanings, ethics, and communicative uses and practices of ethical hacking in a Canadian university. First, perceptions about the meanings of ethical hacking were reviewed. Second, perceptions about the ethics of ethical hacking were reviewed. Finally, perceptions about the communicative uses and practices of ethical hacking, including communicative routines and technological relations, were presented.

Organizational understandings about ethical hacking meanings leaned toward a technical perspective, seeing it primarily as hacking (Expert A, Expert E, Expert B, and Expert C), and secondly as vulnerability assessment (Expert A, Expert E, and Expert B). Ethical hacking was also seen as pen testing (Expert C), and as network assessment (Expert D). Published ethical hacking books mostly equated ethical hacking with risk assessment and penetration testing (e.g., Engebretson, 2011; Graves, 2010; Harper et al., 2011; Harris, Harper, Eagle, & Ness, 2007; Landoll & Landoll, 2005; Simpson, Backman, & Corley, 2010).

Expert B and Expert A saw that the ethics of ethical hacking resided in its nature as a technical process of risk assessment. The ethics "is about the process of hacking, not the reason the hacking is being done" (Expert A). The ethical hacking process "is done at a professional capacity" while recognizing that "there is a moral imperative toward the public good," said Expert A. Expert D and Expert C emphasized the legal dimension of ethical hacking. Expert C said "Ethical is legal." Ethical hackers have legal authorization from top level management to perform hacking (Expert C and Expert D) through a legally binding

agreement (Expert C). Literature review reflected an emphasis on the professionalism of ethical hacking (e.g., Graves, 2010; Palmer, 2001) and on its legal imperative (Engebretson, 2011; Graves, 2010; Harper et al., 2011; Harris, Harper, Eagle, & Ness, 2007; Landoll & Landoll, 2005; Palmer, 2001).

Organizational understandings about ethical hacking communicative routines can be stated as four organizing/administrative considerations. First, there were no standard methods to communicate about ethical hacking (Expert E, Expert B, and Expert D). Second, there was no standard language used for ethical hacking (Expert E, Expert B, and Expert D). Third, the IT department was decentralized, and decision-making was decentralized (Expert D, Expert B, and Expert C). Fourth, communication among the various IT staff about ethical hacking practices was on a need to know basis (Expert C, Expert D, Expert A, and organizational documentation).

Communicative technological relations explored participant perceptions about how the organization communicated with its users (students and employees) about their roles and responsibilities regarding information security and ethical hacking practices. Users learned about their roles and responsibilities regarding information security best practices from online documents (the university's website). Sometimes the university sent out emails to students to warn them about phishing schemes (Expert B). Other sources of information for users included strategically placed information placards (Expert C), and posts on the users' virtual accounts (Expert D). The emphasis of the informational type documents pertaining to information security management aspects was on password management best practices, social engineering schemes (spam and phishing) aimed at stealing data or identity, Trojans

used in identity theft, and viruses, while the emphasis of the policy type documents was on setting user and staff responsibility regarding information security and ethical hacking practices.

To improve the organizational performance in information security communicative practices, Expert B, Expert A, and Expert E favoured the adoption of efficient and autonomous software programs. For example, Expert B said that typically the information system ought to handle most of the concerns regarding password selection and password properties. On the other hand, Expert D and Expert C argued that security awareness training can help organizations raise the awareness of their employees and students about ethical hacking uses and value, best practices in password security management, and user roles and responsibilities. For example, Expert C said security awareness training can help users learn about social engineering and phishing schemes and how to prevent them, as well as about good password management practices.

Assessment and Recommendations

TEI was used to gather, sort, and analyze the interview and documentation data pertaining to ethical hacking use in a Canadian university. The attention now turns to the assessment and recommendations about the organizational use of ethical hacking to explore efficiency and fairness considerations. The researcher applied TEI and Weick's organizing theory to assess the communicative and technological performance of ethical hacking use in the organization, and then to recommend actions for performance improvement using the empirical pragmatic lens of TEI. A technological empirical pragmatic analysis or assessment

using TEI-DMG was performed. An analysis of communicative aspects using Weick's model followed. Each analysis was followed by a set of recommendations.

Technological assessment

TEI assesses technology—its use and value for the organization—by weighing the perceived benefits against the perceived costs and side effects (Bunge's, 1977, pragmatic value theory). The researcher examined the two most prevalent perceptions about ethical hacking value in the organization. First, from a management perspective, the value of ethical hacking was found in its utility as a value system. This emphasis was seen from Expert B and Expert C. This was the secondary view for Expert E and in the organizational documentation P2. Second, from a technical perspective, the value of ethical hacking was found in its utility as a risk assessment process. This emphasis was seen from Expert E and in the organizational documentation P2. This was the secondary view for Expert B and Expert C.

From a management perspective, the perceived organizational benefits were found in the use of ethical hacking as a pragmatic value system which can help decision makers decide about suitable security measures by weighing the risks of being attacked and the associated damage costs against the cost and effectiveness of countermeasures, that is, by weighing the costs against benefits. As a value system, this application of ethical hacking had no monetary costs or side effects. But its efficiency and fairness were limited by its personal application, that is, in personal decision making, regardless how decisions may affect other stakeholders.

From a technical perspective, the perceived benefits were found in the use of ethical hacking as a process or a methodology of risk assessment performed using either open source or commercial software to help decision makers understand and prioritize security risks. As a risk assessment process, ethical hacking had significant potential costs and side effects, including a PR stigma for the organization (Expert A and Expert B), the necessary software can be costly (Expert E and Expert D), and security testing can damage the information system or destroy valuable data if not performed properly (Expert C, Expert E, and Expert A). In a decentralized organization, and where communication about information security testing processes was on a need to know basis (Expert C, Expert D, and Expert A), it may be difficult to ensure efficient and fair application of risk assessment processes. The decision about how to apply risk assessment processes will depend on those making the decision and their specific priorities.

Recommendations: Technological assessment

Technoethics "attempts to provide conceptual grounding to clarify the role of technology in relation to those affected by it and to help guide ethical problem-solving and decision making in areas of activity that rely on technology" (Luppicini, 2010, p. 5). The following outlined the suitability of the TEI decision making grid (TEI-DMG) for technology assessment and for efficient and ethical decision making within organizations. The researcher then applied the grid (TEI steps 1 to 3) to the case study for an assessment of ethical hacking value within the organization (see TEI Decision-making Grid). Finally, the

researcher presented a more comprehensive assessment of the organizational priorities about ethical hacking use, and a set of recommendations derived from the insights of the analyses.

Software and computer engineers need to weigh technical, management, legal, ethical, communicative, as well as social considerations in organizational decision-making about controversial technologies which have broad social and political implications. Hence a qualitative decision making approach is needed which can integrate the diverging and the intersecting interests and values of stakeholders. TEI-DMG can be thought of as a priority list of interests and values for supporting ethical and efficient decision-making. The priority levels for disciplinary perspectives for each stakeholder were weighed and mapped on the decision making grid. Each incidence of emphasis on a certain disciplinary perspective was given one plus point.

On considering TEI-DMG, assessment from TEI steps 1 to 3 showed that the predominant organizational concern was about technical aspects of ethical hacking, at about 44%, followed by management aspects at about 26%, financial aspects at about 14.5%, and communicative aspects at about 6%. The findings suggest that a more expansive consideration of communicative, social, legal, and policy perspectives in decision making about ethical hacking organizational practices would be needed for efficient and fair implementation of the technology. The Stakeholder Priorities grid showed a similar picture, overall—an organizational emphasis on technical aspects at about 46%, and on management aspects at about 21%. However, an interesting picture emerged—the recession of the financial consideration to about 4%, and the rise of the communicative interest to about 12%. The explanation for this difference in emphasis on the financial aspects may be

because steps 1 to 3 specifically inquires about ethical hacking means, which is related to a discussion about the cost of ethical hacking software. The rise in relative importance in the communicative aspects may be explained by the fact that communicative aspects were a focus of step 4. Guided by TEI-DMG, findings pointed to the need for a more inclusive or expansive disciplinary decision-making purview about ethical hacking organizational use. Specifically, findings pointed to the need to expand the communicative and social considerations involved in decision making about ethical hacking organizational practices.

Analysis of communicative aspects

The assessment of communicative aspects explored perceptions among stakeholders about the meanings and ethics of ethical hacking, equivocality in the information environment about explored ethical hacking aspects, and how the organization communicated about these aspects (the underlying communicative routines). Four out of five participants (Expert A, Expert E, Expert B, and Expert C) saw that ethical hacking primarily meant hacking, a technical process. Second (secondly for Expert A, Expert E, and Expert B), it meant vulnerability assessment. Third (secondly for Expert C), it meant penetration testing. Fourth, it meant network assessment (Expert D). Organizational understandings about the ethics of professional ethical hackers fell under two themes. It is ethical in that it followed a technical process, or it is ethical in that it followed a legal process. In other words, ethical hacking was seen as a technical process of risk assessment (Expert E, Expert B, and Expert A), and as a legal process of risk assessment (Expert D, Expert E, and Expert C).

Variances in perceptions among key stakeholder groups about the various ethical hacking inquiry elements were commonplace. Interview data shows that there was no uniformity in perceptions among the key stakeholder groups about the meanings and ethics of ethical hacking. On the meanings of ethical hacking, there were four meanings for ethical hacking among the five stakeholder groups. Hacking was the predominant view, followed by vulnerability assessment. On the ethics of ethical hacking, stakeholder groups were split almost in half, one side seeing it as ethical by virtue of it being a technical process (Expert E, Expert B, and Expert A), and the other view deemed it ethical in that it followed a legal process (Expert D, Expert E, and Expert C).

Communication routines potentially underlying organizational perceptions about ethical hacking elements can be stated as five organizing/administrative considerations. First, there were no standard methods to communicate about ethical hacking (Expert E, Expert B, and Expert D). Second, there was no standard language used for ethical hacking (Expert E, Expert B, and Expert D). Third, the IT department was decentralized, and decision-making was decentralized (Expert D, Expert B, and Expert C). Fourth, communication among the various IT staff about ethical hacking practices was on a need to know basis (Expert C, Expert D, Expert A, and organizational documentation). Finally, communication among the various IT staff about ethical hacking practices usually takes place through email (Expert D and Expert C), telephone, memos, or at meetings (Expert D).

Recommendations: Communicative aspects

The following focused on how to reduce equivocality about ethical hacking in the information environment so as to improve the efficiency of the communicative practices. Weick's organizing theory was used to study the process of organizing, with an emphasis on the organizing processes of enactment and selection of ethical hacking practices. During enactment, the participant brackets an event or an act such that the environment becomes constituted in a particular way. "Selection involves the imposition of various structures on enacted equivocal displays in an attempt to reduce their equivocality" (Weick, 1979, p. 131). The primary function of organizing is to make sense of the information environment. Much of the sensemaking takes place during the selection phase. Hence selection processes are an opportunity for sensemaking. The major goal of organizing is to reduce the equivocality (to make sense) in the information environment. For Weick, equivocality refers to the existence of multiple interpretations of the same event. The problem of equivocality is one of confusion not ignorance (Miller, 2002). It is an equivocal environment if individuals can put forth many viable explanations of an event. This can create or increase unpredictability in the information environment. So the emphasis of praxis is on reducing potential sources of unpredictability, and on reaching common understandings among various stakeholders.

Weick's model advised on how to reduce unpredictability in the ethical hacking information environment, and in doing so improve the efficiency of the communication process among stakeholders. The use (selection) of assembly rules (e.g., standard operating procedures) and communication cycles (ongoing interpersonal and cross-functional communication) can help reduce the variance in perceptions among stakeholders. Interpersonal communication among employees can reduce confusion around organizational

meanings and uses of ethical hacking. Equivocality can be reduced by providing communication opportunities for participants to interact and create the relevant knowledge.

Equivocality is likely to be high in organizations in a highly competitive or quickly changing business environment or during a time of crisis (Miller, 2009). When equivocality is low employees can rely on established ways of doing things (rules). But when equivocality is high, and the complexity of the environment allows for multiple explanations of the same event, communication cycles are suggested, where employees introduce and react to ideas that help make sense of their equivocal environment (Miller, 2009). Equivocality about ethical hacking meanings and uses in the university can be expected to be high, not least because the university's IT department has to weather the storm of a quickly changing technological environment. The IT department at the university was comprised of several semi-autonomous units and decision-making was decentralized (Expert D, Expert B, and Expert C). Second, there was no standard language used for ethical hacking (Expert E, Expert B, and Expert D). Third, communication among the various IT staff about ethical hacking practices was on a need to know basis (Expert C, Expert D, Expert A, and organizational documentation P1 and P2). IT professionals in various units would have different perceptions about ethical hacking. "They would not have common knowledge," as Expert D noted. As such, the IT department can consider adopting communication cycles, in the form of scheduled and ongoing interpersonal meetings. This would give stakeholders the opportunity to reduce the confusion around ethical hacking meanings and uses and create common understandings as they interact.

The interview participants offered two main ways which can help reduce the equivocality in the ethical hacking information environment. Expert B, Expert A, and Expert E focused on efficient and autonomous technology use, while Expert D and Expert C focused on security awareness training. The latter would be a communication opportunity for stakeholders to interact and create common understandings about ethical hacking meanings, uses, and value. Expert D argued that security awareness training can help organizations improve organizational communication about ethical hacking, password security, and user roles and responsibilities. Awareness training can help the organization establish a baseline about the meanings, ethics, and value of ethical hacking, added Expert D. Expert C argued that security awareness training can help users learn about social engineering schemes and how to prevent them, and about best practices in password management. In line with Weick's theory, findings pointed to information security awareness training for increasing sensemaking opportunities among stakeholders and reducing equivocality in the information environment about both user roles and responsibilities regarding information security aspects and about the meanings, ethics, uses and practices, and value of ethical hacking.

Chapter Conclusion

This chapter connected the research question, theoretical framework, and the findings. The coding method and analytic strategy were explained. The organizational understandings were contextualized within ethical hacking literature and broader industry practices. Next, discussion turned to how TEI-KW was applied to the thesis question. The thesis question was split into two sub-questions. Each sub-question was expressed in three

specific questions. TEI was applied to sub-question *a*. Weick's model was applied to sub-question *b*. Technological assessment and communicative analysis were followed by a set of recommendations to the executive office of the IT department in support of effective (efficient and ethical) ethical hacking organizational practices—specifically, recommending broader inclusion of communicative and social perspectives in decision-making, and more IT stakeholder interaction towards reducing unpredictability in the information environment and increasing common understandings.

Conclusion

This chapter discussed four topics. First, a summary of the findings reviewed how TEI-KW was applied to answer the thesis question, and the major findings and recommendations. Second, it reviewed the notable findings about organizational ethical hacking and information security practices and contextualized them within ethical hacking literature. Third, the thesis contributions to communication research, communication theory, and applied technoethics were explained. A discussion about the limitations of the study was followed by recommendations for future research.

Summary of the Findings

The thesis applied TEI-DMG to explore the uses and value of ethical hacking in an organization and to derive recommendations in support of efficient and fair ethical hacking practices. The thesis found disproportionate emphasis on the technical perspective, followed by the legal perspective. The findings suggest to the IT executive office at the participating organization the need for a more expansive or inclusive process to ethical hacking decision making. This can be achieved by expanding stakeholder perspectives, especially communicative and social perspectives, in the decision-making process. Communicative analysis was performed using Weick's model. Variances in perceptions among stakeholders about ethical hacking meanings, ethics, uses and practices, and value were commonplace. The communicative routines potentially underlying these variances included, first, the IT department was comprised of semi-autonomous decentralized units. Secondly, communication among the IT staff about ethical hacking aspects was on a need to know

basis. Third, there was no standard language within the organization to refer to ethical hacking practices. Finally, there was no standard method to communicate about ethical hacking aspects within the organization. In light of Weick's model, the thesis recommended using security awareness training to help reduce equivocality in the information environment and increase sensemaking opportunities towards reaching common understandings.

Findings pointed to users as central actors in upholding information security at the research site. This came as no surprise, since humans represent the weakest link in the information security chain. The study found users were vulnerable to social engineering schemes, unwittingly unleashing a malicious code, and to facilitating unethical hacking (security breaches) due to setting weak passwords. Findings suggested the IT department put much stock in efficient and autonomous technology for information security. But the university can augment information security defences by reaching out and educating its broad community of users, specifically, by implementing a security awareness training program. The goal of security awareness training is to promote good security practices and behaviours among users through mechanisms centred on communicative interaction. For example, creating a virtual portal to coordinate awareness training activities, such as a newsletter, brown bag lunches, and annual information security examination; and providing information which users may need, such as relevant polices, learning resources, and resources for recognizing and reporting security incidences (Palmer, 2001; Wright & Kakalik, 2007).

Importance of the Findings

This section reviewed notable findings about ethical hacking use and information security practices within the organization and contextualized them within ethical hacking literature. There were two main perspectives about the intended ends of ethical hacking use in the organization. First, ethical hacking was used to pursue the information security management goal of safeguarding information assets (Expert E, Expert D, Expert B, Expert C, and organizational documentations P1 and P2). Second, ethical hacking was used to pursue continuous improvement in information security performance (Expert A). Safeguarding the information assets and demanding ongoing improvement in information security performance represented two basic strategic information security management goals for organizations (Engebretson, 2011; Graves, 2010; Harris, 2007; Landoll & Landoll, 2005; Peltier, 2004A, 2004B, 2005; Reynolds, 2012). The main side effect for an organization using ethical hacking was a scarring on its reputation or public image, argued Expert A and Expert B. Palmer (2001), Sterling (1993), and online sources made the point that a hacked business can suffer from a negative public image. But the argument made by Expert A and Expert B, that public knowledge about in-house ethical hacking practices may shake the organization's public image, could not be validated by peer-reviewed literature.

Interview data pointed to the value of ethical hacking in risk assessment as a method to understand, prioritize, and make decisions about suitable security countermeasures. Expert B and Expert C emphasized the use of ethical hacking as a pragmatic value system to guide decision making about suitable countermeasures. Expert E and organizational documentation P2 emphasized the use of ethical hacking as a process to help decision makers understand and prioritize information security risks. References to risk assessment procedures in

literature tended to overlook the distinction. Reynolds (2012), for example, made reference to the pragmatic value system of risk assessment, arguing that the goal of risk assessment was "to identify which investments of time and resources will best protect the organization from its most likely and serious threats" (p. 103). A more direct reference to the pragmatic value system of risk assessment (weighing the perceived benefits against the perceived costs and side effects) was seen in the description of the risk assessment steps by the General Security Risk Assessment Guidelines, ASIS International (2003). According to the guidelines, the basic components or steps in a security risk assessment protocol include: identifying assets; specifying loss events (threats); frequency of events; impact of events; options to mitigate; feasibility of options; cost/benefit analysis; and decision.

Typical information assets for a university would be student grades (Expert D and Expert B) and research data (Expert C). Users were central actors in upholding information security at the university. Users were vulnerable to social engineering schemes, unwittingly unleashing a malicious code, and to having their accounts hacked due to setting weak passwords. The organization used ethical hacking in information security management in a primary way—in compliance management (Expert A, Expert D, and Expert C). Expert C and Expert D explained that the university must comply with Canadian privacy laws, including the federal privacy act, access to information act, and Personal Information Protection and Electronic Documents Act, as well as be PCI compliant. One compliance requirement under PCI DSS was to regularly monitor and test the computer network.

Findings suggested that the term ethical hacking was polysemic. Within the participating organization, it was used to refer to distinctly different information security

concepts or practices. There were four different meanings for the term ethical hacking among the five stakeholder groups: hacking, vulnerability assessment, penetration testing, and network assessment, beside risk assessment (Expert B and Expert D) and threat risk assessment (Expert A and Expert E). Published books on ethical hacking made distinctions among the processes of vulnerability assessment, penetration testing, and network assessment (Graves, 2010; Harper et al., 2011; Harris, Harper, Eagle, & Ness, 2007; Landoll & Landoll, 2005).

Organizational understandings about the ethics of ethical hackers fell under two broad themes, namely, ethical hacking as a technical process of risk assessment (Expert E, Expert B, and Expert A), and ethical hacking as a legal process of risk assessment (Expert D, Expert E, and Expert C). This thesis suggested that part of what made the technical hacking process ethical was its insistence on addressing preventive measures (Harris, 2007; Palmer, 2001). Harris (2007) argued that ethical hacking books should address both how to discover vulnerabilities as well as "how to implement preventive measures to help ensure that these vulnerabilities are not exploited" (The Controversy of Hacking Books, para. 3). The legal imperative of ethical hacking organizational practices was clear—ethical hackers conducted their security testing under the terms of a legally binding contract between them and the data owner. Reviewed ethical hacking books reflected an emphasis on the professionalism of ethical hacking—though the specifics which can be used to frame or define risk assessment processes as ethical were not entirely unclear, though one clear aspect of such professionalism was the legal imperative.

Building on Graves (2010), Harris (2007), and Palmer (2001) this thesis presented the following understanding of professional ethical hacking. First, ethical hackers should address both systemic vulnerabilities as well as preventive measures (Harris, 2007; Palmer, 2001). Second, they should always obtain permission from the data owner before attempting to access the computer system or network (Graves, 2010; Palmer, 2001). Third, they should gain the trust of clients (Graves, 2010; Palmer, 2001). Fourth, they should take "all precautions to do no harm to their systems during a pen test" (Graves, 2010, para. 1).

Contributions to Communication Research, Communication Theory, and Technoethics

An argument was made that pairing Weick's sensemaking model with TEI made it possible to address the paucity of organizational communication research on ethical hacking. The expanded disciplinary context afforded by TEI helped the researcher capture the complexity surrounding ethical hacking meanings and communicative practices (contribution to communication theory). Second, pairing the two models facilitated the conceptualization of a theoretically grounded model for conducting analysis of communicative aspects within organizations to guide effective decision making (contribution to communication theory). Furthermore, an argument was made that organizations can use TEI-DMG in the area of technology assessment and management in support of efficient and fair technological applications. Second, the thesis presented a specialized, theory-based model which information security risk managers can use to guide effective decision making about ethical hacking organizational practices (contribution to technoethics).

Contribution to communication research. The important contribution to knowledge of this thesis lies in filling in a gap in the literature that results from the scarcity of research on the communicative and socio-cultural considerations involved in the implementation of ethical hacking, while the dominant scholarship is application and certification oriented (technical and legal aspects). The thesis addressed the paucity of organizational communication research on non-technical and non-legal aspects of ethical hacking. The thesis applied Weick's theory of organizing to study the communicative aspects of ethical hacking use in the organization. Weick's model rests on a postpositivist systemic epistemology congruent with data collection through observing and measuring aggregate behaviours. But the model can incorporate interpretive perspectives. The thesis explored key stakeholder perceptions about the meanings and ethics, and the communicative practices of ethical hacking within an organization. Pairing Weick's sensemaking model with TEI allowed for a holistic and systemic examination of ethical hacking communicative aspects. The expanded disciplinary context afforded by TEI helped the researcher capture the complexity surrounding ethical hacking meanings and communicative practices. To illustrate this point, consider the broad thesis question, "what is ethical hacking in the organization?" Ethical hacking can be understood by considering ("measuring") ethical hacking from various perspectives (e.g., management and technical, beside communicative). Ethical hacking meanings for key stakeholders were "hacking" and "vulnerability assessment." Ethical hacking was "ethical" because it followed an ethical process (professional risk assessment requires the inclusion of preventive measures). Further, it was ethical because it was legal. The management perspective suggested ethical hacking was a management tool

for protecting the information assets and for achieving ongoing improvement in information security. The technical perspective affirmed the prime understanding about the utility of ethical hacking as a risk assessment process. Thus the thesis could draft a grounded description or definition of ethical hacking, as a technical and legal hacking process conducted professionally as a risk assessment process for protecting the information assets and achieving ongoing improvement in information security.

Contribution to communication theory. To explain the thesis contribution to communication theory, the present application of Weick's model is situated within Weick's organizational communication research. Investigators into sensemaking processes have conceptualized organizing activities in different ways. Some researchers studied sensemaking practices with an emphasis on the placement of environmental stimuli into conceptual frameworks (e.g., Dunbar, 1981; Goleman, 1985; Starbuck & Milliken, 1988; Westley, 1990). Others used the seven properties of sensemaking as a basis to frame an inquiry into organizing activities (e.g., Dutton & Dukerich, 1991; Louis, 1980). Others used the concept of equivocality as a central analytical probe. Louis (1980), and V. D. Miller and Jablin (1991) adopted Weick's model to explore how employees can make sense of equivocal as well as non-equivocal information environments. Miller, Joseph, and Apker (2000) examined how employees make sense of ambiguously defined organizational roles. Kreps (1980) explored the role of equivocality in organizational sensemaking process. Taking a pragmatic philosophical orientation, the thesis presented a distinct application of Weick's model for use by organizations as a basis for a theoretically grounded model for

conducting an in-house analysis of communicative aspects to guide effective (efficient and ethical) decision making. The thesis built on Weick's analytical thrust—that the major goal of organizing was to reduce the equivocality in the information environment. Equivocality referred to the existence of multiple interpretations of the same event, which is a source of unpredictability in the information environment. The thesis exploited a theoretical-philosophical alignment between the goal of organizing and TEI's pragmatic goal of performance improvement.

Contribution to technoethics: Applied technoethics. First, TEI-DMG can be used by organizations in the area of technology assessment and management. This thesis has shown that information security managers can use the grid as a decision making tool to help guide effective decision making about ethical hacking and information security risk management practices. The process of risk assessment encompasses two distinguishable components: a procedure for gathering and organizing information about the perceived threats and vulnerabilities, and a risk based, pragmatic value system supporting cost-effective decision making about suitable countermeasures. TEI-DMG can be appended to the value based decision making component of the risk assessment procedure to help identify and involve perspectives and stakeholders for effective decision making.

Second, the thesis applied TEI-KW with TEI-DMG to investigate the use of ethical hacking in an organization by conducting a qualitative assessment of stakeholder priorities across three disciplinary perspectives (communicative, management, and technical). It presented a specialized, theory-based model which organizations (information security risk

managers) can employ to guide effective decision making about ethical hacking practices. To clarify the thesis contribution to the field of technoethics, the thesis research is situated within the applied research areas of technoethics. Within technoethical scholarship, the two closely related and intersecting applied research areas of computer ethics, and Internet ethics and cyberethics bear on the study of information security management, especially when information assets are connected to the Internet grid (hacking is most likely to happen via the Internet). The technoethical area of applied ethics in Internet ethics and cyberethics addressed computing technologies for the Internet, including various software applications used in unethical activities, as well as guidelines to guard against unethical Internet activity, such as compromising user privacy and gaining unauthorized access to resources (Luppicini, 2009).

Depending on what aspect of information security management practices was under scrutiny, an applied technoethical research area can be determined. For example, if the emphasis of analysis was on the use of information management programs (e.g., a student information system) the area of research more closely aligned with the research emphasis would be computer (and information) ethics. If the analytical concern was primarily with the legal terms of reference for information protection, the relevant realm would be Internet ethics and cyberethics (especially Internet ethics). If the analytical concern was with the use of computing Internet technologies to gain unauthorized access using hacking/ethical hacking technologies, the relevant realm would be Internet ethics and cyberethics (especially cyberethics). The analytical focus of the thesis was on ethical hacking organizational uses and practices, including its use as a risk assessment technology. Internet ethics and

cyberethics would be the appropriate applied ethics research area. Follows are examples of studies in this area covering various aspects of computing Internet technologies to help situate the thesis. Lin and Luppicini (2013) employed actor-network theory to examine communicative and technical organizational influences related to the use of the cyber surveillance hacking technology GhostNet in cyber espionage. Eid (2010) discussed four severe cyber-terrorism cases which occurred within the last decade, and presented a theoretical model for effective media decision-making during terrorism attacks. Roberts (2009) explored methods used to combat cyber identity fraud in light of their relation to privacy and civil liberties. Jenkins (2001) investigated Internet pornography and child exploitation. Finally, Adam (2002) examined the problem of cyberstalking. In comparison, this thesis constituted an organizational case study which applied a pragmatic analytical model to guide effective decision making. As such, it derived specific, environmentally grounded (structurally and culturally) recommendations in support of improved ethical hacking organizational practices. As a contribution in applied technoethics, the thesis presented a specialized, theoretically grounded model for conducting in-house analysis (assessment) of ethical hacking organizational use to guide effective decision making aimed at improvement.

Limitations of the Study

The study had two main sources of limitations, namely, theory based limitations and method based limitations. The first limitation was in the application of TEI. Disciplinary perspectives on ethical hacking studied were limited to four, namely, communicative,

management, technical, and sociocultural. A second theoretical limitation was the absence of a specialized theoretical model for exploring the management aspects. A limitation in method was the number of data sources (only five interviews were conducted). Another limitation in method was in the number of data collection methods used, that is, only in-depth interviews and a document/website review were used.

Recommendations for Future Research

The following research recommendations built on the present thesis and retained its emphasis on the study of technology communication, management, and ethical pragmatic qualitative assessment within organizations. Recommendations were made for interdisciplinary sociotechnical research grounded in organizational information theory (e.g., Weick, 1969, 1979), technoethics (Bunge, 1977; Luppicini, 2010), and information systems management frameworks. Two research directions were suggested.

Future research within the same organization can build on the present thesis to examine aspects of the design and implementation of an information security awareness training program (including structural, cultural, and technical aspects) by incorporating management information systems and knowledge management frameworks with TEI-KW. The security awareness training program can be framed as an optimization effort and a multi-aspect change management and performance management challenge for the organization in the use of information technology and information security technologies.

Another research direction would be to augment TEI with specialized organizational communication theoretical lenses (in addition to Weick's model) to help achieve a broader

understanding about ethical hacking communicative and cultural practices to guide performance improvement through effective decision making. Anthony Giddens's structuration theory can be used to examine how organizational structures can shape the outcome, and how the outcome in turn can reconstitute the structures. Edgar Schein's model of professional culture can be used to examine culture as a group phenomenon, as a pattern of basic assumptions, and as an emergent process to help understand the alignment of the organizational culture (artifacts, values, assumptions) with the technical goals and practices. The proposed model can be further augmented with a strategic communication theoretical model in risk and crisis management—an adaptation of Eid's (2008) crisis decision making model—to guide effective decision making within organizations during information security breaches or data loss (hacking) incidents. Finally, research ideas based on methodology included increasing the sample size of participants, conducting the survey on more than one organization (three to five organizations, to investigate industry trends and best practices), and using additional data collection methods, such as direct observation and questionnaires.

References

Adam, A. (2002) Cyberstalking and Internet pornography: Gender and the gaze. *Ethics and Information Technology, 4*, 133-142.

Agazzi, E. (2012). How Can the Problems of An Ethical Judgment on Science and Technology Be Correctly Approached?. In R. Luppicini (Ed.), *Ethical Impact of Technological Advancements and Applications in Society* (pp. 30-38). Hershey, PA: . doi:10.4018/978-1-4666-1773-5.ch003

Bantz, C. R. (1980). Organizing the news: Extending newswork theorizing through Weick's organizing formulation. Paper presented at the annual meeting of the Speech Communication Association, New York.

Bantz, C. R. (1989). Organizing and the social psychology of organizing. *Communication studies*, *40*(4), 231-240.

Bao, Z. & Xiang, K. (2006). Digitalization and Global Ethics, *Ethics and Information Technology*, 8: 41-47.

Buchholz, R. A., & Rosenthal, S. B. (2001). A philosophical framework for case studies. *Journal of Business Ethics*, *29*(1-2), 25-31.

Bunge, M. (1967). *Scientific Research II: The Search for Truth*. New York: Springer.

Bunge, M. (1976). The philosophical richness of technology. Proceedings of the Biennial Meeting of the Philosophy of Science Association. Volume 2: Symposia and Invited Papers (pp. 153–172).

Bunge, M. (1977). Towards a technoethics, *Monist*, *60*(1). 96-107.

Bunge, M. (1979). A systems concept of society: Beyond individualism and holism, *Theory and Decision*, *10*(1), 13-30.

Cerqui, D., & Warwick, K. (2009). Technoethics: An Anthropological Approach. In R. Luppicini, & R. Adell (Eds.) *Handbook of Research on Technoethics* (pp. 32-43). Hershey, PA: . doi:10.4018/978-1-60566-022-6.ch003

Charlesworth, M., & Sewry, D. (2009). Ethical Theories and Computer Ethics. In R. Luppicini, & R. Adell (Eds.) *Handbook of Research on Technoethics* (pp. 186-204). Hershey, PA: . doi:10.4018/978-1-60566-022-6.ch013

Crabb, P. B., & Stern, S. E. (2012). Technology Traps: Who Is Responsible?. In R. Luppicini (Ed.), *Ethical Impact of Technological Advancements and Applications in Society* (pp. 39-46). Hershey, PA: . doi:10.4018/978-1-4666-1773-5.ch004

Creswell, J. W., (2003), Research design: Qualitative, Quantitative, and Mixed Methods Approaches. Thousand Oaks: Sage Publications.

Creswell, J.W., (2007). *Qualitative inquiry and research design: Choosing among five approaches*. Thousand Oaks: Sage Publications.

Dewey, J. (1984). The Quest for Certainty. In Jo Ann Boydston (Ed.), *The Later Works (1981-1989)* (pp. 144-152). Carbondale and Edwardsville: Southern Illinois University press.

Dhillon, G. (2007). *Principles of information systems security: Text and cases*. NY: John Wiley & Sons.

Dunbar, R. L. (1981). Designs for organizational control. *Handbook of organizational design*, *2*, 85-115.

Dutton, J. E., & Dukerich, J. M. (1991). Keeping an eye on the mirror: Image and identity in organizational adaptation. *Academy of management journal*, *34*(3), 517-554.

Eid, M. (2008). *Interweavement: International media ethics and rational decision-making*. Boston, MA: Pearson.

Eid, M. (2010). Cyber-Terrorism and Ethical Journalism: A Need for Rationalism. *International Journal of Technoethics (IJT), 1(4)*, 1-19.

Eid, M. (Ed.). (2011). *Research methods in communication*. Boston, MA: Pearson.

Ellul, J. (1964). *The technological society*. NY: Vintage Books.

Franklin, U. (1990). *The real world of technology*. Concord: House of Anansi Press Limited.

Galván, J. (2001). Technoethics: acceptability and social integration of artificial creatures. Retrieved June 30, 2007 from http://www.eticaepolitica.net/tecnoetica/jmg_acceptability%5Bit%5D.htm

Engebretson, P. (2011). *The basics of hacking and penetration testing: Ethical hacking and penetration testing made easy*. [Books24x7 version] Retrieved March 26, 2013, from http://common.books24x7.com.proxy.bib.uottawa.ca/toc.aspx?bookid=44730

Farmer, D., & Venema, W. (1993). Improving the security of your site by breaking into it. (Unpublished technical report).

Feldman, M. S. (1989). *Order without design: Information production and policy making*. Stanford University Press.

Floridi, L. & Sanders, J. (2003). Computer ethics: Mapping the foundationalist debate. *Ethics and Information Technology, 4(1)*, 1-24.

Garner, R. T., & Rosen, B. (1967). *Moral philosophy: A systematic introduction to normative ethics and meta-ethics*. New York: Macmillan.

Gioia, D. A., & Chittipeddi, K. (1991). Sensemaking and sensegiving in strategic change initiation. *Strategic management journal*, *12*(6), 433-448.

Goleman, D. (1985). *Vital lies, simple truths: The psychology of self-deception*. New York: Simon & Schuster.

Graves, K. (2010). *CEH certified ethical hacker study guide*. John Wiley & Sons.

Harper, A., Harris, S., Ness, J., Eagle, C., Lenkey, G., & Williams, T. (2011). *Gray hat hacking: The ethical hacker's handbook*, third edition. McGraw-Hill/Osborne.

Retrieved June 7, 2013, from http://common.books24x7.com.proxy.bib.uottawa.ca/toc.aspx?bookid=40079

Harris, S., Harper, A., Eagle, C., & Ness, J. (2007). *Gray hat hacking*. McGraw-Hill, Inc.

Heidegger, M. (1977). The question concerning technology. In Lovitt, W. (Ed.), *The question concerning technology and other essays* (pp.13-39). New York: Harper and Row.

Internet Architecture Board. (1989). Retrieved August 24, 2014, from http://tools.ietf.org/html/ rfc1087

Jackson, W. (1999). *Methods: Doing social research*. Prentice Hall Allyn and Bacon Canada.

Jenkins, P. (2001) *Beyond tolerance: Child pornography on the internet*. New York University Press.

Johnson, D. (1985) *Computer ethics*. NJ: Prentice-Hall

Jonas, H. (1979). *The imperative of responsibility: In search of ethics for the technological age*. Chicago: Chicago University Press.

Jonas, H. (1985). *On technology, medicine and ethics*. Chicago: Chicago University Press.

Kennedy, M. (2013). Virtue and Virtuality: Technoethics, IT and the Masters of the Future. In R. Luppicini (Ed.), *Moral, Ethical, and Social Dilemmas in the Age of Technology: Theories and Practice* (pp. 1-18). Hershey, PA: . doi:10.4018/978-1-4666-2931-8.ch001

Kreps, G. (1980). A field experimental test and reevaluation of Weick's model of organizing. In D. Nimmo (Ed.), *Communication Yearbook 4* (pp. 389-398). New Brunswick, NJ: Transaction Books.

Kuhn, T. (1962). *The structure of scientific revolutions*. Chicago: University of Chicago Press.

Landoll, D. J., & Landoll, D. (2005). *The security risk assessment handbook: A complete guide for performing security risk assessments*. CRC Press.

Lin, X., & Luppicini, R. (2013). Socio-Technical Influences of Cyber Espionage: A Case Study of the GhostNet System. In R. Luppicini (Ed.), *Moral, Ethical, and Social Dilemmas in the Age of Technology: Theories and Practice* (pp. 112-124). Hershey, PA: . doi:10.4018/978-1-4666-2931-8.ch009

Louis, M. R. (1980). Surprise and sense making: What newcomers experience in entering unfamiliar organizational settings. *Administrative Science Quarterly*, 226-251.

Mitcham , C. (1997). *Thinking ethics in technology: Hennebach lectures and papers*, 1995-1996. Golden, CO: Colorado School of Mines Press.

Mitcham, C. (2005). *Encyclopedia of science, technology, and ethics*. Detroit: Macmillan Reference USA.

Luppicini, R. (2008A). Introducing technoethics. In R. Luppicini & R. Adell (eds.), *Handbook of research on technoethics* (pp. 1-18). Hershey: Idea Group Publishing.

Luppicini, R. (2008B). The emerging field of technoethics. In R. Luppicini & R. Adell (Eds.), *Handbook of research on technoethics* (pp. 1-19). Hershey, PA: Information Science Reference.

Luppicini, R. (2010). *Technoethics and the evolving knowledge society: ethical issues in technological design, research, development, and innovation*. Information Science Reference-Imprint of: IGI Publishing.

Luppicini, R. (2013). *Moral, Ethical, and Social Dilemmas in the Age of Technology: Theories and Practice* (pp. 1-379). Hershey, PA: IGI Global. doi:10.4018/978-1-4666-2931-8

Miller, K. (2002). *Communication theories*. McGraw-Hill.

Miller, K. (2009). *Organizational communication: Approaches and processes*. Wadsworth Publishing Company.

Miller, K., Joseph, L., & Apker, J. (2000). Strategic ambiguity in the role development process. *Journal of Applied Communication Research*, 28, 193-214.

Miller, V. D., & Jablin, F. M. (1991). Information seeking during organizational entry: Influences, tactics, and a model of the process. *Academy of Management Review*, 92-120.

Moor, J. H. (1985). What is computer ethics. In T. W. Bynum (Ed.), *Computers and ethics*. Basil Blackwell, pp. 266-275.

Neuman, W. L. (2010). *Social research methods: Qualitative and quantitative approaches*. Pearson.

Neuman, W. L. (2011). Social research methods: Qualitative and quantitative approaches. In M. Eid (Ed.), *Research methods in communication* (341-377). Boston, MA: Pearson.

Palmer, C. C. (2001). *Ethical hacking*. *IBM Systems Journal*, *40*(3), 769-780.

Peltier, T. R. (2004A). *Information Security Policies, Procedures, and Standards: Guidelines for effective information security management*. Boca Raton, FL: Auerbach publications.

Peltier, T. R. (2004B). Risk analysis and risk management. *Information Systems Security*, *13*(4), 44-56.

Peltier, T. R. (2005). *Information security risk analysis*. Auerbach Publications.

Public Safety Canada. (2013A). Canada's Cyber Security Strategy. Retrieved from http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-eng.aspx

Public Safety Canada. (2013B). An Open Letter to Canadians on Cyber Security Awareness. Retrieved from http://www.publicsafety.gc.ca/cnt/nws/nws-rlss/2013/20131003-eng.aspx

Public Safety Canada. (2013C). Harper Government announces action plan for cyber security. Retrieved from http://www.publicsafety.gc.ca/cnt/nws/nws-rlss/2013/20130418-eng.aspx

Rallis, S., & Rossman, G. (1998). Learning in the field: An introduction to qualitative research. *Learning in the field: an introduction to qualitative research*.

Rescher, N. (2012). *Pragmatism: The restoration of its scientific roots*. Transaction Publishers.

Ring, P. S., & Rands, G. P. (1989). Sensemaking, understanding, and committing: Emergent interpersonal transaction processes in the evolution of 3M's microgravity research program. *Research on the management of innovation: The Minnesota studies*, 337-366.

Roberts, L. D. (2009). Cyber Identity Theft. In R. Luppicini, & R. Adell (Eds.) *Handbook of Research on Technoethics* (pp. 542-557). Hershey, PA: . doi:10.4018/978-1-60566-022-6.ch035

Rosenthal, S. B., & Buchholz, R. A. (2000A). *Rethinking business ethics: A pragmatic approach*. New York: Oxford University Press.

Rosenthal, S. B., & Buchholz, R. A. (2000B). The empirical-normative split in business ethics: A pragmatic alternative. *Business Ethics Quarterly*, 399-408.

Reynolds, G. W. (2012). *Ethics in information technology*. Boston, MA: Cengage Learning.

Sackmann, S. (1991). *Cultural knowledge in organizations: Exploring the collective mind*. Sage Publications, Inc.

Simpson, M., Backman, K., & Corley, J. (2010). *Hands-on ethical hacking and network defense*. Cengage Learning.

Stahl, B. C., Heersmink, R., Goujon, P., Flick, C., van den Hoven, J., Wakunuma, K., Ikonen, V., & Rader, M. (2012). Identifying the Ethics of Emerging Information and Communication Technologies: An Essay on Issues, Concepts and Method. In R. Luppicini (Ed.), *Ethical Impact of Technological Advancements and Applications in Society* (pp. 61-79). Hershey, PA: . doi:10.4018/978-1-4666-1773-5.ch006

Stake, R. E. (1995). *The art of case study design*. Sage Publications.

Stamp, M. (2011). *Introduction in information security: Principles and practice*, Second Edition, John Wiley & Sons, Inc., Hoboken, NJ, USA.

Starbuck, W. H., & Milliken, F. J. (1988). Executives' perceptual filters: What they notice and how they make sense. *The executive effect: Concepts and methods for studying top managers*, *35*, 65.

Stebbins, R. A. (Ed.). (2001). *Exploratory research in the social sciences* (Vol. 48). Sage Publications.

Sterling, B. (1993). *"Part 2(d)". The hacker crackdown*. McLean, Virginia: IndyPublish.com

Strauss, A. L. (1987). *Qualitative analysis for social scientists*. Cambridge University Press.

Sullins, J. (2008). Artificial moral agency in technoethics. In R. Luppicini & R. Adell (eds), *Handbook of research on technoethics* (pp. 205-221). Hershey: Idea Group.

Talisse, R. B., & Scott, F. A. (2008). *Pragmatism: a guide for the perplexed*. London.

Thomas, J. B., Clark, S. M., & Gioia, D. A. (1993). Strategic sensemaking and organizational performance: Linkages among scanning, interpretation, action, and outcomes. *Academy of management Journal*, *36*(2), 239-270.

Vries, M. J. (2009). A Multi-Disciplinary Approach to Technoethics. In R. Luppicini, & R. Adell (Eds.) *Handbook of Research on Technoethics* (pp. 20-31). Hershey, PA: . doi:10.4018/978-1-60566-022-6.ch002

Wareham, C. (2013). On the Moral Equality of Artificial Agents. In R. Luppicini (Ed.), *Moral, Ethical, and Social Dilemmas in the Age of Technology: Theories and Practice* (pp. 70-78). Hershey, PA: . doi:10.4018/978-1-4666-2931-8.ch005

Weber, K., & Glynn, M. A. (2006). Making sense with institutions: Context, thought and action in Karl Weick's theory. *Organization Studies*, *27*(11), 1639-1660.

Weick, K. (1969). *The Social Psychology of Organizing*. Reading, Massachusetts: Addison-Wesley.

Weick, K. (1979). *The social psychology of organizing*. Reading, Massachusetts: Addison-Wesley.

Weick, K. E. (1988). Enacted sensemaking in crisis situations [1]. *Journal of management studies*, *25*(4), 305-317.

Weick, K. E. (1990). The vulnerable system: An analysis of the Tenerife air disaster. *Journal of management*, *16*(3), 571-593.

Weick, K. E. (1993). The collapse of sensemaking in organizations: The Mann Gulch disaster. *Administrative science quarterly*, 628-652.

Weick, K. E. (1995). *Sensemaking in organizations*. SAGE Publications, Inc.

Weick, K. E. (2001). *Making Sense of the Organization*. Malden, MA: Blackwell.

Weick, K. E. (2009). *Making Sense of the Organization: Volume 2: The Impermanent Organization* (Vol. 2). Wiley.

Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (2005). Organizing and the process of sensemaking. *Organization Science*, *16*(4), 409-421. Retrieved from http://search.proquest.com/docview/213832611?accountid=14701

Weizenbaum, J. (1976). *Computer power and human reason: From judgment to calculation*. New York: Freeman.

Weber, K., & Glynn, M. A. (2006). Making sense with institutions: Context, thought and action in Karl Weick's theory. *Organization Studies*, *27*(11), 1639-1660.

Westley, F. R. (1990). Middle managers and strategy: Microdynamics of inclusion. *Strategic Management Journal*, *11*(5), 337-351.

Wiener, N. (1954). *Human use of human beings*. Houghton Mifflin, 2nd ed, Doubleday Anchor.

Wright, M. A., & Kakalik, J. S. (2007). *Information security: Contemporary cases*. Sudbury, Mass: Jones and Bartlett Publishers.

Yin, R. K.(1994). *Case study research: Design and methods*. Thousand Oaks: SAGE Publications.

Yin, R. K., (2003). *Case study research: Design and methods*. Third Edition. Thousand Oaks: Sage Publications.

Appendices

Appendix: Invitation Letter to Participants

Recruitment Invitation for an MA Thesis Study

Date:

Hello,

Thesis Title: Technoethics and Organizing: Communicative, Ethical, Management, Technical, and Sociocultural Aspects of Ethical Hacking in a Canadian University

You are cordially invited to participate in an MA thesis about ethical hacking in a Canadian university. The thesis explores ethical hacking understandings, uses and practices, and value within an organization, with a focus on communicative, ethical, management, and technical aspects.

The perceived benefits for the participants are self-reward for their contributions to academic research. The main benefit to society will be a contribution toward a scholarly understanding of ethical hacking and its role in information security management in an organizational context.

Participants will be invited to respond to interview questions for a session of about 30 minutes in duration. Interviews will take place in person or over the phone during normal working hours or at times more suitable for the participants. The interview period is proposed for March 24 to April 21, 2014. Please feel free to indicate an interview time and place suitable for you in the relevant fields in the appended consent form.

Before interviews are conducted, participants are invited to sign a consent form highlighting their rights—such as the right to withdraw from the study at any time without suffering any negative consequences—and other pertinent information related to the nature of the study and the ethical conduct of the study, including information about participant identification and research site identification in the thesis, potential study risks, and information confidentiality.

Thank you for your time and consideration.

I look forward to hearing from you.

Sincerely,

(Researcher)

Appendix: The Meta-ethics of Ethical Hacking Table

Perspective	**Ethics Type** (What is the nature of moral judgments?)	**Ethical is...**	**Meta-ethics** (What is the meaning of moral terms or judgments?)	**Philosophy/ Epistemology/Axiology** (How may moral judgments be defended?)
TEI-KW (Technoethical Inquiry Theory paired with Weick's Sensemaking model)	Normative (prescriptive)	Ethical is effective. Effective: Efficient and fair.	Efficient and fair according to TEI steps 1-3: Efficient: On weighing goals against side effects, and means against ends, the output (overall value) balances the input. Fair: refers to stakeholder perceptions about fairness in implementing ethical hacking practices in the organization.	Teleological-Pragmatic-Instrumental
TEI-DMG (TEI Decision-making Grid)	Normative (prescriptive)	Ethical decision-making is effective decision-making. Effective: Holistic/efficient and fair.	Holistic means multi-disciplinary and inter-disciplinary (systemic). A holistic approach supports efficient decision-making by virtue of being more informed decision making. Fairness refers to a broader inclusion of perspectives and stakeholder priorities in the decision-making process about ethical hacking organizational practices.	Teleological-Pragmatic
Ethical Hacking as Information Security Risk Assessment	Normative (prescriptive)	From a technical perspective, ethical hacking is a process to understand and prioritize security risks. The goal of risk assessment is "to identify which	Ethical action is action effective in achieving a reasonable risk level. Risk levels help risk managers select appropriate security controls and countermeasures to lower	Teleological-Pragmatic-Risk-based; Instrumental-Rational

		investments of time and resources will best protect the organization from its most likely and serious threats" (Reynolds, 2012, p. 103). From a management perspective, ethical hacking is a pragmatic value framework for ethical hacking decision-making. According to the General Security Risk Assessment Guidelines (ASIS International, 2003) the basic components or steps in a security risk assessment protocol include: identifying assets; specifying loss events (threats); frequency of events; impact of events; options to mitigate; feasibility of options; cost/benefit analysis; and decision.	the risk to an acceptable level (Landoll & Landoll, 2005; Peltier, 2005).	
Certification /Commercial According to the International Council of Electronic Commerce Consultants (EC-Council) (www.eccouncil.org)	Descriptive Ethics	A Certified Ethical Hacker is "a skilled professional who understands and knows how to look for weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of the target system(s)." An "Ethical Hacker" is "an individual who	Ethical hackers are skilled and knowledgeable (IT and information security) professionals usually employed with an organization and who look for vulnerabilities in target systems and can be trusted to "undertake an attempt to penetrate networks and/or computer systems using the same methods and techniques as a Hacker"; and who use the same knowledge and tools as malicious hackers but in a lawful and legitimate manner to assess the security posture	Teleological-Pragmatic; Virtue Ethics

		is usually employed with the organization and who can be trusted to undertake an attempt to penetrate networks and/or computer systems using the same methods and techniques as a Hacker."	of target systems.	
Literature Review Graves (2010), Harris (2007), and Palmer (2001).	Descriptive Ethics	Ethical hackers should address both systemic vulnerabilities as well as preventive measures (Harris, 2007; Palmer, 2001). The practices of professional ethical hackers are governed by a legal framework. Ethical hackers should always obtain permission from the data owner before attempting to access the computer system or network (Graves, 2010; Palmer, 2001). Ethical hackers should gain the trust of clients (Graves, 2010; Palmer, 2001). And they should take "all precautions to do no harm to their systems during a pen test" (Graves, 2010, para. 1).	Ethical hacking is holistic and strategic. Ethical hacking is legal. Ethical hacking is virtuous action.	Teleological-Pragmatic-Systemic; Rational/Legal; Virtue Ethics.
Interview Participants	Descriptive Ethics	For key stakeholder groups: 1) Ethical hacking was ethical in that it followed a technical-pragmatic process of risk assessment (Expert E, Expert B, and Expert A). Expert B	Ethical hacking constitutes economical and legal organizational choices in information security risk management.	Rational-Instrumental

		argued that there was nothing ethical about ethical hacking, “it is a technical process.” Expert A argued “the ethics is about the process of hacking, not the reason the hacking is being done.” 2) Ethical hacking was ethical for being a legal process (Expert D, Expert E, and Expert C). For Expert C, “ethical is legal.” Ethical hackers “must have a contract signed with an organization giving them permission to expose company data before starting to hack.” For Expert E, ethical hackers are usually invited by the asset owner to perform hacking to find vulnerabilities and fix them.		

Appendix: Ethics Approval Certificate

File Number: **Date (mm/dd/yyyy):** 03/28/2014

Université d'Ottawa University of Ottawa

Bureau d'éthique et d'intégrité de la recherche Office of Research Ethics and Integrity

Ethics Approval Notice

Social Science and Humanities REB

Principal Investigator / Supervisor / Co-investigator(s) / Student(s)

First Name	Last Name	Affiliation	Role
		Arts / Communication	Supervisor
		Arts / Communication	Student Researcher

File Number:

Type of Project: Master's Thesis

Title: Technoethics and Organizing: Communicative, Technical, Ethical, and Sociocultural Aspects of Ethical Hacking in a Canadian University

Approval Date (mm/dd/yyyy)	Expiry Date (mm/dd/yyyy)	Approval Type
03/28/2014	03/27/2015	Ia

(Ia: Approval, Ib: Approval for initial stage only)

Special Conditions / Comments:

N/A

File Number: **Date (mm/dd/yyyy):** 03/28/2014

Université d'Ottawa University of Ottawa

Bureau d'éthique et d'intégrité de la recherche Office of Research Ethics and Integrity

This is to confirm that the University of Ottawa Research Ethics Board identified above, which operates in accordance with the Tri-Council Policy Statement and other applicable laws and regulations in Ontario, has examined and approved the application for ethical approval for the above named research project as of the Ethics Approval Date indicated for the period above and subject to the conditions listed the section above entitled "Special Conditions / Comments".

During the course of the study the protocol may not be modified without prior written approval from the REB except when necessary to remove participants from immediate endangerment or when the modification(s) pertain to only administrative or logistical components of the study (e.g. change of telephone number). Investigators must also promptly alert the REB of any changes which increase the risk to participant(s), any changes which considerably affect the conduct of the project, all unanticipated and harmful events that occur, and new information that may negatively affect the conduct of the project and safety of the participant(s). Modifications to the project, information/consent documentation, and/or recruitment documentation, should be submitted to this office for approval using the "Modification to research project" form available at: http://www.research.uottawa.ca/ethics/forms.html.

Please submit an annual status report to the Protocol Officer four weeks before the above -referenced expiry date to either close the file or request a renewal of ethics approval. This document can be found at: http://www.research.uottawa.ca/ethics/forms.html.

If you have any questions, please do not hesitate to contact the Ethics Office at extension 5387 or by e-mail at: ethics@uOttawa.ca.

Signature:

Protocol Officer for Ethics in Research
For Chair of the Social Sciences and Humanities REB

(613) 562-5387 • Téléc./Fax (613) 562-5338
www.recherche.uottawa.ca/deontologie/
www.research.uottawa.ca/ethics/