AC 2007-2158: THE ROLE OF INFORMATION WARFARE IN INFORMATION ASSURANCE EDUCATION: A LEGAL AND ETHICAL PERSPECTIVE

Andrew Hoernecke, Iowa State University

Thad Gillispie, Iowa State University

Benjamin Anderson, Iowa State University

Thomas Daniels, Iowa State University

The Role of Information Warfare in Information Assurance Education: A Legal and Ethical Perspective

Abstract

Typically, information assurance (IA) professionals utilize information warfare (IW) techniques learned in professional development courses when performing vulnerability and security assessments. With cyber crime on the rise, both government and industry have come to rely on academia to properly train future IA professionals, reducing the need for professional developmental courses. This presents a topic for debate since there is some disagreement if it is legally or ethically appropriate to teach IW techniques in an academic setting due to the many risks involved.

In order to address the questions raised by teaching these skills, we examine the legal and ethical responsibilities of IA professionals and how this affects educational programs. We identify several key knowledge areas and skill sets that IA professionals require and examine the benefits and risks that are associated with teaching these skills. The legal aspects of the issue are addressed by examining important computer security laws, such as the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley (SOX) Act and the Federal Criminal Code, and how they affect education at the institution, instructor and student level. Evaluation of the ethical issues is done by using the ACM Code of Ethics as well as two ethical theories: utilitarianism, based on maximizing the good consequences for society; and deontology, where ethical actions are based on an individual's duties and the rights of others.

We conclude by offering our recommendations for creating an IA program by addressing the need for cyber defense exercises and test-bed environments. In addition, we provide some topics for consideration on how to safely teach these skills and reduce the possibility of an incident.

Introduction

Computer engineering programs aim to provide students with the skills they need to design, build, and deploy computer systems. With our increasing reliance on computers and networks for personal and business applications comes the need to protect such systems from malicious attacks. For this reason, many universities have added courses, degrees, and certifications focusing on computer and network security. These programs, often referred to as information assurance (IA) programs, teach the skills required to secure software, systems, and networks. Unfortunately, in the wrong hands the tools and information presented could be used for malicious purposes.

Some experts argue that students should not be taught the specifics on how computer systems are attacked and compromised; however, these information warfare (IW) techniques are easily found on the Internet through a simple search. Since a strong understanding of attack principles is necessary to successfully protect systems and networks, this knowledge proves to be a necessary tool for IA professionals. Still, the decision to include IW skills in a computer engineering or IA program can be a difficult one, especially determining at what skill and maturity level students can fully appreciate the ramifications of their actions outside the learning environment.

In this paper, we will first carefully define the terms information assurance and information warfare. Once complete, we move on to discuss the risks and benefits of teaching IW skills. This assessment will consider the potential for damage and disruption of computer systems, from either deliberate misuse of these skills by an attacker or the accidental misuse by a student or professional. We then examine the possible implications to the students, instructors and universities involved in this education.

Next we address the legal aspects by examining important computer security laws, such as the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley (SOX) Act and the Federal Criminal Code, and how they affect education at the institution, instructor and student level. This is followed by an evaluation of the ethical issues using two different ethical theories: utilitarianism, based on maximizing the good consequences for society; and deontology, where ethical actions are based on an individual's duties and the rights of others.

After identifying and examining the legal and ethical issues, we present a means to mitigate the risks associated with teaching IW techniques in order to more fully incorporate such training at the university level. We conclude by offering our recommendations for creating an IA program that includes IW training in a safe, legal and ethical manner.

Background

To understand the educational environment being discussing, it is first important to define what is meant by an IA program. For the purpose of this paper, IA is defined as “measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.”[1] Accordingly, IA programs must provide students with the skills and knowledge required to create, deploy and maintain systems that allow these criteria to be met. A clear relation to computer engineering can be established since a system created without allowing for these attributes would in many cases be useless.

It is also important to have a clear definition of IW since different definitions exist depending on the context. Here IW will be defined as “the offensive and defensive use of information and information systems to deny, exploit, corrupt, or destroy an adversary’s information, information-based processes, information systems, and computer-based networks while protecting one’s own.”[2] Examples of specific actions that can be performed using IW skills include the following.

- Gathering information on the target including email addresses, available services, usernames, and passwords
- Watching network traffic to view and analyze packet contents
- Scanning systems to determine types of hardware, operating systems, and services being used to identify vulnerable systems and software

- Exploiting vulnerabilities to disable or gain control of a system

While skills can be used by an attacker to damage, disable or take control of computer systems, they can also be used by an IA professional. The difference between the two can be in the skill set, intention, or methodology of the individual who is utilizing this knowledge.[3] It is important to consider these differences in order to understand the goal of teaching IW techniques in an IA program.

For example, the skill set of an attacker may range from a very novice individual using tools found on the Internet with little or no working knowledge of what they are actually doing, to a professional hacker who writes his own tools and may have more knowledge than most IA professionals. Additionally, an attacker may be able to spend days or even weeks concentrating his efforts to exploit a single vulnerability. On the other hand, an IA professional cannot focus on a single vulnerability, but instead must spread out their time ensuring none of the vulnerabilities can be exploited in order to protect the systems' security.

Further, once an IA professional has identified vulnerabilities that exist, the severity and potential risk of the each vulnerability must be determined. Since potential vulnerabilities do not necessarily imply a risk as other protective measures may make it impossible for an attacker to exploit them, the knowledge, skills and perspective of an attacker are crucial in order to properly assessed the actual risk and correctly allocate security resources.

While these skills are beneficial to the IA professional, we must also ask if they are appropriate for students. Although there are legal reasons that require the use of these skills by IA professionals, these tasks must still be carefully monitored to prevent abuse. The use of IW skills and techniques can often result in access to passwords and other personal data that could be maliciously used or sold by the IA professional. This kind of access to information is why ACM's Code of Ethics addresses respecting the privacy of others and honoring confidentiality. However, while a professional may have sufficient motivation for using knowledge responsibly, the same is not necessarily true of a student.

However, we must address IW training for students as the increasing need for these professionals has caused industry and government to rely on academia to create these professionals. In particular, the U.S. Government, through the National Security Agency created an outreach program for Centers of Academic Excellence in IA in order to "reduce vulnerability in our national information infrastructure by promoting higher education in information assurance (IA), and producing a growing number of professionals with IA expertise in various disciplines."[4]

The need for increased education in IA is further compounded due to the recent passing of The Sarbanes-Oxley Act (SOX) and the Health Insurance Portability and Accountability Act (HIPAA). SOX requires an assessment of internal controls and procedures regarding the processing of financial data, including information technology (IT) systems, and may involve penetration testing.[5, 16] HIPAA requires a risk analysis of any system that maintains or transmits "electronic protected health information" which includes identifying and documenting potential threats and vulnerabilities and assessing current security measures.[6] Combined, these have increased the need for individuals properly trained in IW. This can also be seen in the increase of "Ethical Hacking" programs such as the Cutting-Edge Hacking Techniques course offered by the SANS Institute.[7]

If the growing demand means academia is required to create IA professionals, then the issue is whether the legal and ethical concerns associated with teaching IW skills outweighs the need for IW skills. In order to answer this question, we must examine some of the actual risks with teaching these skills before we can analyze the legal and ethical concerns.

Risks Associated With Information Warfare

Risks exist in many areas of research and education. As we push back the bounds on what is possible, we deal with many dangerous situations in education. In chemistry, students often use chemicals that are flammable, toxic or explosive; in biology or agriculture, students may work with pathogens that may be harmful to inhale, or could cause damage if released into the environment. Computer engineering is no different as poorly written software can bring down systems and networks.

A notable difference arises in that most computer engineering students do not regularly compromise computer systems during their class work, and when problems do occur they are generally confined to the machines they are directly working with. However, teaching IW skills often requires students to target systems across the network or the Internet. Since the network will blindly route the traffic to the given destination, this creates the opportunity of someone "missing" their intended target.

For example, if the student is targeting an IP address of 10.5.131.204, (an IP address that is not normally routable), and incorrectly types the IP address as 1**0**0.5.131.204 or 1**1**0.5.131.204, the attack will be sent to an actual destination, regardless of where in the world it is. Even if no damage is done by this attack, the accidental target may detect it and be forced to take action, costing them time and money. The section of the U.S. Code that deals with computer law does make the distinction that the access must be intentional, so there is some protection against accidents.[8] However, the question would be if the attack was intentional, but the target was unintentional if the law would apply in these cases.

Another potential risk of teaching these skills is the possibility of students applying them outside of a class environment in a malicious manner. If a student intentionally gains access to a system without authorization, they could be held accountable under U.S. Law. This means pranks against a business or the university could result in federal charges against the student carrying up to 5 years in prison for the smallest infraction and up to 20 years for a more egregious violation.

Perhaps the greatest potential risk of teaching IW would be of training professional cybercriminals. The use of computers for identity theft, phishing and spam has resulted in a strong criminal economy. According to an FBI projection cybercrime robs U.S. businesses of $67.2 billion a year, and over the past two years U.S. consumers lost more than $8 billion to viruses, spyware and online fraud schemes.[9]

Teaching IW would provide the students with the knowledge and skills needed to compromise systems and/or steal personal data. These compromised systems often contain a hidden malicious software package that allows unauthorized remote control of the machine. Collections of these controlled systems, known as botnets, have become a commodity item, with established rates for the "sale" of these systems. An unscrupulous individual looking to make money on this activity could enroll in an IW program to gain the skills required to engage in this new activity. Although this threat is potentially very real, the actually risk is likely small due to the amount of work and money required to complete an IA program.

These risks must be taken into account when determining the legal and ethical issues that surround the teaching of IW in an IA program.

Legal Analysis

While the authors have addressed the legal issues to the best of their ability, this paper should not be used as a substitute for professional legal advice. In addition, the authors take no responsibility for any actions taken based on the interpretation of this paper.

The first important legal point to make is that the law does not make it criminal to perform any kind of attack or analysis on a computer system that the user owns or has received permission to operate on or against. In practice, it is common to create a written document with the specific IP addresses of the systems to be tested to avoid any legal issues down the road. For an academic program, as long as the systems used in teaching and lab work are properly identified and permission is given to use those systems there are no legal issues regarding these techniques.

As mentioned in the section on risks associated with teaching IW, it is possible for accidents to occur, with something as simple as mistyping an IP address redirecting the attack to another system. If damage or access to a system is unintentional, it is not covered under the U.S. Criminal Code.[8] While it is unlikely that a single incident would be prosecuted, care must be taken to avoid claims of negligence in these activities. As with other types of accidents, such as car accidents, unless there was some sort of negligence occurring, criminal charges are rarely filed. Since the law is concerned with the intentional damage or access to a system, accidents that do occur should carry little or no legal penalty.

It is also important to consider that cybercriminals may utilize IW classes as a way to learn or hone their skills. The law is very clear that damage or access to a computer system without authorization is a criminal offense. As such, any students that would use IW skills in such a manner would have to face the consequences of their actions. However, this would be no different than a chemistry student being charged with using their knowledge to manufacture drugs or explosives. The relevant question for this discussion is whether this activity would have any legal repercussions to the university or the instructor.

In order to be an accessory to a crime, the individual must "be aware that the crime is gong to be committed or has been committed."[10] If the program were restricted to those who could have a legitimate use for learning IW, then there would not seem to be a reason to know that a crime would be committed using those skills. It is possible that an instructor could learn of such intent from one of their students, and it would then be up to the instructor to contact the appropriate authorities.

While it would seem there are no legal reasons that would prevent teaching IW, these skills do carry some risk to the student as well. For this reason, the authors would encourage any IA program that includes teaching IW to include some education on the legal use of the skills being taught.

There are more than legal issues to be considered when teaching IW as the ethical aspects are also considerable. As mentioned previously, there might not be any legal responsibility in the event of a mis-targeted attack, but that does not mean that such an accident does not violate the ethical rules surrounding the field.

Ethical Analysis

Although the legal argument mandates the need for well trained security professionals, the issue of teaching IW techniques must also be analyzed from an ethical perspective. This section will evaluate the ethicality of teaching these techniques by applying the theories of utilitarianism and deontology. These issues will also be related back to the ACM Code of Ethics, one of the most definitive ethical standards used for professionals in computer industries.

Before proceeding, it should be noted that there do exist arguments claiming unauthorized hacking to be ethically acceptable, although generally these arguments apply only if no harm is done in the process. It is important to note that this is not the argument being made in this paper. The authors see unauthorized hacking to be in conflict with the ethical duties of a student or security professional. Nevertheless, the arguments presented in this section can stand independent of the ethicality of unauthorized hacking.

From a utilitarian perspective, an act or social policy is ethically acceptable if the consequences of that result produce the greatest amount of good for the greatest number of people affected. In this instance, one must measure the good produced by teaching IW techniques to potential IA professionals in the classroom as opposed to teaching only the fundamentals and theory of IT. [11]

Of course, the fundamentals and theory are important for every IT professional; however, for many, such as those responsible for designing or securing systems, this may not be enough. These individuals need to know how an IT system can be exploited in order to properly protect it. As an analogy, imagine the person responsible for designing the lock on your house has no knowledge of how a burglar might go about trying to pick that lock. The person certainly will be able to design a functioning lock using only the fundamental knowledge of how a lock works, but what would happen when a malicious person decides to try to break such a lock? Is there any chance that the lock maker could have anticipated the vulnerabilities that a malicious person could exploit without having any knowledge of how a lock could be picked in the first place? Most people probably would not feel comfortable entrusting their lives, belongings, and families to this type of lock maker, so they should also not feel comfortable trusting their sensitive data to this type of IA professional.

Having extensive knowledge of how IT systems could be exploited provides an advantage in designing a system to prevent this from happening. To ensure that peoples' systems and data are properly safeguarded as previously discussed, aspiring IA professionals need proper training. Having IA professionals well versed on fundamentals, theory, and IW methods gives these individuals the knowledge they need in order to design, setup, and use IT systems in a safe and secure fashion. For these reasons, training IA professionals extensively on IW techniques is the most ethically acceptable option from a utilitarian perspective.

The ethical basis of teaching IW techniques can also be discussed from the perspective of deontology. Deontology is an ethical theory which is founded on the principles of duty and obligation. Here we will focus on Kantian rule deontology which attempts to use objective and impartial rules to determine moral obligations. Specifically, this ethical theory focuses on the categorical imperative, which urges all rules, duties and principles to be universally binding without exception for all people.[11]

Several duties can be imagined that apply to this situation. First, does not a university have the duty to give students the most useful information available in their chosen field of study? This is a duty that most would agree can be applied universally and impartially. Students pay a university to become experts in their chosen fields, and while a university education cannot take the place of years of experience, it seems to be an intrinsic responsibility for a university to impart the most useful knowledge available. By now it should be clear that IW skills are not only useful but necessary to many IA professionals, and therefore this duty would mandate that these skills be taught to individuals in this field.

From a different perspective, do students have a duty to attempt to learn whatever skills and knowledge they can in order to best perform their future jobs to the best of their ability? This duty also seems to be universally applicable. First, by fulfilling this duty the student will be able to later perform a job to the best of his or her ability. In addition, it should be considered that most universities are quite selective and many reject more applicants than they accept. If the student does not want to fulfill this duty, it seems they should not attend the university and instead allow a student who is willing to fulfill this duty to receive the education. It then follows that students seeking to fulfill this duty should, whenever possible, seek out an education that will be most beneficial to them in the future. In the field of IA, this education would include instruction on IW techniques.

Some may argue that IW should not be taught because a university has a duty to ensure material being taught can not be used in a malicious way. However, those detractors would not actually be willing to apply this duty universally to all subject areas, and thus this argument does not hold up as being valid under rule deontology. It is certainly well known that information taught in fields such as biology, physics, chemistry, and agriculture could be used with malicious intent with devastating effects, however, society has determined that the benefits of teaching these disciplines outweighs the potential threat of misuse. Without applying the duty universally, it cannot be used as an argument against the ethical basis of teaching IW techniques under rule deontology. In this case a more realistic duty would be that students have the duty to use their knowledge in a responsible manner. This could be applied universally and impartially.

Now, consider a rule stating that IW knowledge should be available universally. At first this prospect many seem to be an unethical proposition, however, imagine a situation where IW warfare knowledge truly was disseminated universally, in other words all people would be taught this information. Certainly this would increase the number of people who had malicious intent that would know this knowledge; however, if every computer programmer, every network administrator, and even every computer user had this knowledge, those with malicious intent would have a much more difficult time doing any damage since everyone would know how these attacks work, and how to protect themselves from them. In the event the rule is applied universally and impartially, not only would the rule stand up to rule deontology, but it would likely result in safer computer use for everyone.

Further, the ACM Code of Ethics supports this type of comprehensive education.[12] Examples of this include Specific Professional Imperatives 2.2, 2.6, and 2.7 which require "acquiring and maintaining professional competence," "giving comprehensive evaluation of computer systems including possible risks," and "improving public understanding of computing and its consequences." Only by having a full-spectrum education could an IA professional possibly hold up these responsibilities. The Code of Ethics also has limitations on the use of this knowledge. One is required to obey the law, honor the rights of other users such as privacy and confidentiality, and prevent harm to others. Clearly, IA is a balancing act; however, adequately protecting an IT system without the necessary knowledge is a virtually impossible task to complete successfully.

Under all three ethical frameworks, students and professionals have the responsibility of acting in a careful and responsible manner. Negligence could clearly result in unnecessary harm with no added benefit, and thus would violate the basic principle of utilitarianism. It would also violate the duties to not cause unnecessary harm to satisfy deontology and the ACM Code of Ethics. Although accidents will likely still occur, by practicing carefully and responsibly in a controlled environment, potential harm can be minimized or even eliminated.

Of course, even in a structured environment it is possible to have a small number of students who may have malicious intent. However, it is most likely that the vast majority of malicious individuals would not attend a university to learn these skills. In these cases it would be evident that the benefit from having well trained professionals will outweigh the danger posed by the malicious few. Also, it would be these students, not the university, who are acting unethically.

Considerations and Recommendations

This section will give some recommendations on what actions can be taken in order to provide or receive an appropriate IA education in light of the ethical analysis presented in this paper. First, two specific goals for IA education will be presented, after which specific recommendations and guidance will be given on how these goals could best be accomplished. Emphasis will be given on maximizing the effectiveness of the education while minimizing the potential risks.

As a first goal we recommend is that the IA community should strive to provide and seek out comprehensive education that includes in-depth training on IW techniques along with the related fundamentals, theories, and critical thinking skills. An emphasis should be placed on practical experience in a safe environment in order to ensure the tools can be used effectively and safely. Utilizing this type of education will give IA professionals the broad knowledge base that is needed to create and defend secure IT systems. This method is supported not only by the legal and ethical analysis presented earlier in this paper but also by experts in the field. John Davey, from the Department of Defense, and Helen Armstrong, from Edith Cowan University, expressed these sentiments in a 2001 conference paper for the 5th National Colloquium for Information Systems Security Education:

> "Cyberwarfare is an area of education where practical application of the theory is essential. Within business and defense environments the aim is to, at best win the game, or at worst, not lose the game. Experience solidifies learning and the only way to master the skills involved in cyberwarfare is to have hands-on experience. If an organization wishes to stay equal to, or one step ahead of an adversary, proficiency in the art of defensive and offensive cyberwarfare is required."[13]

Davey and Armstrong go on to compare computer security to any other disaster prevention or recovery field. They claim that IW attacks should be treated as emergency situation. Because of this, they stress that the defense team must be well trained in scenarios involving both attack and defense tactics.

Another institution that teaches both sides of the IA war is the United States Military Academy at West Point. There, two separate course paths are offered—one for computer science majors, and another for international relations majors. Both paths not only study the methods of attack on IT resources, but also include hands-on exercises that address the subject.[14]

As a second goal for IA education is to ensure students and professionals have an understanding of how vulnerabilities are formed in software or hardware, how they can be prevented in the design and development phases, and how to correct or secure already existing vulnerabilities. This can be done by teaching students and professionals how to correctly and safely use penetration testing and vulnerability assessment tools in all phases of a product's lifecycle, from design to implementation and maintenance. This will help to keep pace with current and emerging threats and allow better risk management, preparation, and mitigation. Also, these types of assessments are commonly mandated through laws or corporate policies, as previously discussed, and thus provide a way for IA professionals to get a thorough evaluation of the risks to the systems they maintain. This practice is often essential for finding ways to avoid or mitigate these threats. Now, not all vulnerabilities can be completely eliminated, and for this reason it is important that IA professionals be able to find ways to minimize these remaining risks.

One way we feel these goals can be accomplished is through cyber defense exercises. Generally these exercises work by having one or more teams of students responsible for setting up and protecting a network. Services such as DNS, mail, and web must be setup just as in a real network. Students are generally given wide latitude to choose their own operating systems, server applications, and network configuration, as this also helps them learn what works well and what does not. The setup phase can last 1-2 weeks, depending on the situation, during which time the students' network(s) are isolated from any attacks.

The exercise itself can last any amount of time, but often occurs over 12-24 hours. In this phase two additional teams participate, referred to here as the red and green teams. The red team is made up of educators, industry professionals, or sometimes students who play the role of attackers that attempt to find and exploit vulnerabilities in the systems on the students' network(s). The green team fills the role of the common user and must utilize and evaluate the services setup on the students' networks. For example, they may send emails, surf the Internet, transfer files, or perform other functions common on a computer network. The green team aspect adds a realistic dimension to the exercise by requiring the students to have to balance usability with security. For example, although setting up a system to require passwords that contain random characters with a minimum length of 30, may be quite secure, it would never meet the usability requirements of a real computer network.

These exercises teach students the importance of preparation and planning as well as allow the defending team to respond to attacks from the red team by closing security holes and changing defenses. At the conclusion of the exercise the students are given a debriefing by the red team in which the methods used to find security holes, which vulnerabilities were most useful for the attacks, and how to best prevent similar problems in the future are discussed. This allows the students to learn which of their security measures were effective and which were not, and also which of the measures made it difficult for the users of the green team to perform their tasks since that would have a real impact on the setup's feasibility in the real world.

Another recommendation for accomplishing the aforementioned goals is the development of new test-bed and virtualization environments that better simulate real-world environments. Being able to experiment in a simulated real-world setting will make it easier to educate new IA students without endangering real networks. This will help control and reduce the risk of accidental damage to equipment or information during the training of students, or during the testing and development of new security products and devices. These test-beds could also aid industry in the development of new security products by enabling them to be more thoroughly tested to ensure that they operate effectively before introducing them into a real environment.

According to the recently published report by the President's IT Advisory Committee, one of the top 10 areas needing increased research and development is "modeling and test beds for new technologies".[15] The committee feels that:

> "One of the barriers to the rapid development of new cyber security products is the paucity of realistic models and test-beds available for exercising the latest technologies in a real-world environment."

Such test beds would provide a host of opportunities for furthering security product development as well as education. Without the creation of versatile test bed environments that allow modeling large or complex networks, it will become more difficult to develop and effectively test new security technologies. We believe that many of the concerns stated earlier in this paper could be allayed through the use of these types of environments.

Conclusions

Based on the legal and ethical analysis of this issue, we do not believe that the teaching of IW techniques should be blocked by these issues any longer. It is clear that professionals in this field need this knowledge in order to create and adequately protect information systems. In a position relating to any type of security there is a high degree of trust that must be given to this person; without it, he or she would never be able to do his or her job properly. The fact that a small number of these trained individuals may end up using their knowledge for the wrong purposes does not justify the damage that would be done by not training anyone.

Certainly, the invention and use of dangerous technologies is inevitable. Automobiles, for example, can be very lethal in the wrong hands, but society has decided that the benefits outweigh the risks. Control measures have been put in place such as traffic signals and signs, and every driver is required to take a driver's education course and pass a test before getting behind the wheel. Although people are injured every day for the misuse of automobiles, we still do not deny their use to all of society. With new technology comes new risks; and education, not prohibition, is the key to the safe advancement of technology.

In IA, just as in driving, education is the key. IA students need a broadly based, comprehensive education to be best prepared to handle future challenges in this field. It is more advantageous for these students to get this type of education in a safe and controlled environment instead of on the job in an emergency situation or by seeking out this potentially dangerous information alone. Institutions that offer classes that cover topics such as IW methodologies and hold cyber defense exercises are helping to prepare today's students to be at the forefront of the IA field. These methods help teach students guidelines for proper use and safe implementation.

We feel that it would be imprudent to ban or disallow the teaching of information based on a fear of misuse when this practice would prevent so many positive advances. By encouraging proper education and use of emerging technologies hopefully we can foster an environment where these technologies can positively contribute to our society.

Bibliography

1. The Committee on National Security Systems, "National Information Assurance (IA) Glossary*", CNSS Instruction No. 4009*, June 2006.

2. Ivan Goldberg, Institute for the Advanced Study of Information Warfare, "Information Warfare, I-War, IW, C4I, Cyberwar", December 2006, http://www.psycom.net/iwar.1.html.

3. Information Systems Audit and Control Association, "IS Auditing Procedure: Security Assessment—Penetration Testing and Vulnerability Analysis", July 2004, www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=18750.

4. National Security Agency, "Centers of Academic Excellence", http://www.nsa.gov/ia/academia/caeiae.cfm.

5. Gregg Stults, "An Overview of Sarbanes-Oxley for the Information Security Professional", Sans Institute, May 2004, http://www.sans.org/reading_room/whitepapers/legal/1426.php.

6. Department of Health & Human Services, "Basics of Risk Analysis and Risk Management", *HIPAA Security Series*, Vol. 2, Paper 6. June 2005.

7. SANS Institute, "Course: Security 517 – Cutting-Edge Hacking Techniques – Hands On", January 2007,

http://www.sans.org/training/description.php?tid=392.

8. 18 U.S.C. § 1030.

9. Byron Acohido and Jon Swartz, USA Today, “Cybercrime flourishes in online hacker forums”, October 2006, http://www.usatoday.com/money/industries/technology/2006-10-11-cybercrime-hacker-forums_x.htm.

10. Law.com, ALM Properties, Inc, “Legal Dictionary”, February 2007, http://dictionary.law.com/default2.asp?typed=accessory&type=1&submit1.x=0&submit1.y=0&submit1=Look+up.

11. Herman Tavani, *Ethics and Technology: Ethical Issues in an Age of Information and Communication Technology 1st edition,* Hoboken, NJ: John Wiley and Sons, Inc., 2004.

12. ACM Council, Association for Computing Machinery, “ACM Code of Ethics and Professional Conduct”, October 1992, http://acm.org/constitution/code.html.

13. H. Armstrong and J. Davey, “Educational Exercises in Information Warfare—Information Plunder and Pillage”. *5th National Colloquium for Information Systems Security Education*, 2001

14. J. Schumacher and D. Welch, “Preparing to Defend Against Cyberattack”, *1st Annual IEEE Information Assurance Workshop*, 2000

15. President’s Information Technology Advisory Committee, “Cyber Security: A Crisis of Prioritization”, February 2005, http://www.nitrd.govpitac/reports/20050301_cybersecurity/cybersecurity.pdf.

16. 15 U.S.C. § 7262.