Assignment D
Tasks 1-4 from Handout

Prepared for
Dr. Steven D. Zink, Ph.D.
2004 Summer Institute
Faculty in Doctoral Program
Nova Southeastern University

Prepared by
Derek J. Sedlack
Doctoral Student, Nova Southeastern University
School of Computer and Information Sciences

November 29, 2004

Task 1

Given the perceived global challenges to network security, most western governments are formulating cooperative strategies to pursue international perpetrators and are planning for contingencies in the case of cyber attacks. Some experts argue that the only way to mitigate the impact of massive cyber attacks is for government to begin mandating security practices and protocols in the private sector. Do you believe such a policy should be pursued? Why/why not?

The implications of global security are daunting with the proliferation and availability of illicit tools and documentation and the possibility to cover a person's tracks over vast distances. Relating the concept of network security could be paralleled with bank security as changes in information availability and timeliness are in a state of constant flux.

The era of horseback posed a number of challenges that had to be overcome during the heist: location of the money, method of extraction, total value, time available, and travel both to and from the deed. Today, the documents that are seemingly the most import, such as nuclear power plants and entire cities' electrical grids, are readily available to any anonymous connection on the Internet with detailed designs including weaknesses. Countermeasures can be estimated, timeframes calculated, and perfect coordination can be planned and practiced with precision before a physical presence is required. Robbers can hack into the central system to determine bank vault amounts, delivery timeframes, and even security mechanisms from the comfort of their hideout thousands of miles away, perhaps from another country on another continent. The Freedom of Information Act and countless cries by the Press on First Amendment rights have created an age of unprecedented unfettered access to previously classified information with naive views such as, "as an access advocate, I believe that information can be used responsibly for socially useful goals" Hammett (1998, p. 4). The issue is whether to take an egalitarian approach, or to assess the worst-case scenario and design a release plan based on that probability – very real in the aftermath of recent terrorist activities.

It is probable that many of the declassified documents should have been made available to the public decades ago, but the unquenchable thirst described by the GOA (2003) has also allowed a myriad of documents to be re-classified because of national security issues. The security risks imposed by making so many documents that were previously believed to be secret are especially notable when coupled with the expansion of government policies to make more information available to the public online. Citizenship is not required to access many of the previously classified documents, a security risk equal to the outsourcing of citizens' health related documents and programming efforts. Understanding the moral issues raised by Ficarrotta (2004) reinforces the global aspect of today's economy and expansion of resources to include either adolescent or illegitimate aspects of outsourcing, including corporate employees residing in different regions.

Wiencek (2004) covered a number of points surrounding outsourcing including employment values and geo-globalized standards. Who controls the ethical decisions made by the employee in a different country, or the social implications of their actions? Who is responsible when a company outsources vital components or entire products that impact the U.S.? Government mandated policies that impact critical decisions made surrounding security in

alien departments may help reduce the potential nightmares created by relying on foreign workers to integrate their culture with American products.

When outsourced workers are not performing at the desired level, or a decision is made to discontinue the relationship, which legal system should be enforced and how are ethical dilemmas handled? Should managers focus on the good of the company, the individual, or the overall economic effect of their decisions? International policies are developing each day with affirmations and dissentions carefully worded to allow either future direction fully available to the winning side. How can American policy be enforced in other countries? Vint Cerf , Internet pioneer, noted that "…if every jurisdiction in the world insisted on some form of filtering for its particular geographic territory, the world wide web would stop functioning" (Ward, 2000, p. 2).

How are cyber attacks to be defined and who should enforce trans-cultural laws or even rule when attackers from another country break local laws? Jennings (2004) found that pioneering Internet executives believed that old business practices did not apply to them, in fact, old corporate governance did not apply, such as the percentage of insider Board members, or the timely delivery of purchased goods. How can American polices relating to these global forces be applied properly to infantile, adolescent, and mature Internet saturated countries with a level of impartiality that neither stifles innovation nor affords rewards for illicit behavior? Virus writers from England to Argentina may have been detected, isolated, and prosecuted locally, but do the countries that sustained billions in damage have any recourse? How can one nation determine appropriate levels of punishment when the ramifications are multi-national, affecting a multitude of nations that employ equally disperse methods of sentencing; probation for first offense DUI in the States compared with amputation for petty theft in the Middle East. Wiencek (2004) raised questions surrounding the definition of legality and morality in connection with global communities and applying the embodiment of these principles from U.S laws to another country would be daunting if not impossible.

Cyber attacks and crimes are a side effect of ubiquitous electronic commerce, which are growing in quantity and ferocity each year. Legislating the private sector may be the most expedient and political answer for a short-term solution, but global governance and enforcement will soon be a vital necessity should the world wish to continue trading goods, services, and funds electronically. Intercepting and modifying information a decade ago not only took a great deal of effort and intelligence, it also took time. Today it is possible to intercept electronic communications and insert forgeries so quickly the lag could simply be attributed to routine Internet congestion. Common off the shelf (COTS) software utilized by curious teenagers is replacing years of highly specialized, high priced skills. The USNRC (2002) determined that large scale network targeted attacks were a definite possibility remotely, anonymously, and on large scale that cause direct, immediate damage, or lay a foundation for future attacks through covert communications or newly acquired launch-points. Surfing anonymizers, switching masks, and IP spoofs are becoming commonplace, making it increasingly impossible for authorities to determine where a crime was initiated, let alone who actually committed the crime. Trojan horse programs coupled with keystroke pirates allow a criminal to virtually commit a crime with another person's hands. Policies may be popular, but a more effective means of tracking, isolation, and prosecution are the only way the Internet will remain a viable means of commerce and banking through the 21st century.

Task 2

Should the U.S. have a stricter policy regarding the international dissemination of its scientific and technical information?

This question is easily answered yes, and no. We will first try and build a case for developing much stricter policies surrounding technical information, how it might apply to scientific data and applications, and historical examples of why the most mundane technical information may now be a matter of national security. It is also possible to explain why information must be shared throughout the international scientific community for the good of mankind.

During the Ronald Regan cold war era, technology experienced explosive growth in the scientific and consumer fields that produced more efficient communications, transportation, and utilities that are now the foundation of our country's infrastructure. The Soviet Union needed that technology in order to remain competitive with the U.S., but lacked the scientific expertise to develop the innovative programs themselves – so they stole it (Hoffman, 2004). The U.S. learned details from the French about the deep-seated Russian spies that had been stealing complicated mechanisms and joint/weld stress information that ran the switching in their pipelines. If the U.S. had not learned about this espionage and sabotaged strategic "bugs" into the software, the U.S.S.R. might have developed enough military-based infrastructure to defeat the United States. The Sept. 11 terrorist attacks on the World Trade Center towers was in part due to the open flight training facilities and scholarly programs to foreign nationals. If the U.S. only allowed few through her borders and even fewer information out, it would be much less likely that terrorist could plan such impacting events.

Berghel (2000) discovered that social security numbers were never designed as identifiers, in fact Social Security numbers were only to be used within the Administration. But the rampant use of SSN through Executive Order 9397 created an information nightmare for the U.S. with every citizen's savings, spending habits, and healthcare requirements now tied to unique numbers that could be easily obtained and utilized for illicit purposes both at home and abroad. A much tighter policy regarding all information dissemination would help ensure that extraordinary efforts would be required to damage the national infrastructure and its inhabitants.

Harris (2004) discussed with Paul Kurtz the level of risk from cyber-security leaks and holes and how NIST and the DoD are working to secure America's electronic commerce as well as developing global agendas that will improve cyber-security, but neglected to mention the effect of outsourcing critical software projects that impact Fortune 500 companies and government projects. Kurtz also failed to mention specific actions surrounding academic research or a plan to safeguard that valuable information. Scalet (2002) found that culpability and inter-corporate volunteerism would go a long way to shore up our programs and Savage (2004) found that some companies are taking matters into their own hands with entities like InfraGuard; dedicated to facilitating the sharing of information between the private sector and the government, but are these programs enough to safeguard our electronic borders? Today's information age is strife with wonton acts of curiosity that formerly would have been a nuisance, are now causing millions or more in damage and crippling the nations commerce. Must all

information now be safeguarded, or is it still beneficial to share important discoveries and developments?

Zink (2004) said that useful information is shared information; information wants to be free. Numerous inventions from one country in recent history have been improved by another culture: Swiss watches have transformed into Japanese digital watches accompanied by calculators and alarms. Global epidemics such as cancer and HIV can only be combated through collaborative efforts on a multinational scale that would be futile without information sharing. Savage and Scalet illustrate that communities require communication for growth and survival, but inter-educational dependencies should not be confined to national interests, for the national interest may be best served internationally.

It is no surprise that the spring of 1969 yielded the first networking communications not between corporate behemoths, but from Stanford to UCLA. The third and forth systems were placed at the University of California and University of Utah respectively, to begin the development of what would become the Internet. Peer review journals and other publications are major contributors to scientific progress, without which it is improbable that modern science, for the better or worse, would not have developed new model theories of black holes, dark matter, or quantum physics, or the famous dispute over who created calculus: Newton from England or Leibniz from Germany. That said, it is also probable that the Internet and information immediacy will reduce the impact of innovation worldwide, as the reduction in timeliness of information will continue to shrink. While Hoffman (2004) stated, “all professionals have the obligation to use their skills and knowledge for the benefit of their clients/patients/users, as well as for the benefit of the general public”, many hackers are sharpening their craft on secure credit card databases, government archives, and secret military stores.

Free information sharing would be a beautiful thing, the second period of enlightenment, but greed and power are warping much of the usefulness intended by the design, but one must remain hopeful. If the government believes that information hording will lead to advantage, the private sector may serve a useful historical perspective. Free information leads to collaboration, like Cummins (2003) note of the detection of the SARS virus in record time due to collaborative efforts. Collaboration, in turn, leads to innovation. Sharing technical and scientific information will ultimately benefit humanity, even though terrorists or combatants of the State may also benefit, the attempt has to be made. Even as courts have found the aggregate dissemination of information constitutionally dangerous (Howard, 1997) and tighter controls are being promoted by a number of governmental organizations under the premise that global warfare has evolved into information war as much as any other (Molandeer, Riddile, & Wilson, 1996). The continuing evolution of science requires sharing and through sharing may come peace and prosperity.

Task 3

This task has several components. (1) Outline critical topics that should appear in any acceptable use policy in a workplace. (2) Choose one of the topics in the outline and write out the policy for that topic in detail as if it were going to be distributed to all staff. (3) Then provide a justification for why you took the stand you did in formulating that particular topic within the policy.

1. Concise business reasons behind the policy
2. Boundaries between corporate and personal resources
3. Scope and limitations covered by the policy
4. Any expectations of privacy in Voice and Data communications
5. Methods of enforcement and disciplinary actions
6. Understanding that acceptance of the policy conveys observance

To all employees:

Citrix values each individual's effort that is required to ensure the survival and competitive advantage of the company. It is prudent for any business to constantly review and revise global policies to ensure that employees at every level of the organization are treated fairly while maintaining a level of compliance that holds the best interest of the company in mind and satisfying legislature imposed upon successful enterprises. Identity theft is a common and costly occurrence in today's society and the fastest growing crime in America. Citrix is dedicated to ensuring that your information and corporate assets remain safeguarded through implemented measures of authentication, verification, and record keeping that allow the detection and prosecution of criminals. The businesses financial losses sustained through espionage could negatively impact the employment of Citrites [what Citrix employs are called] at all levels throughout the organization and aversion requires a consolidated effort. While the law allows the recording of all voice and data communications corporate-wide, Citrix' policy is to use this information only in the event of a crime or to protect against legal action. The corporate officers intend to sustain the profitable, momentous company that all Citrites have created through fair, open policies.

Many scholars (Woodbury, 2004; Huff, Johnson, & Miller, 2004; Hoffman, 2004; Wiencek, 2004) are heralding the need for more ethics in business and a higher level of professionalism as e-commerce disperses corporate locations across nations and continents. Empowerment and enlightenment will serve the purpose of warning that criminal activity will be discovered and prosecuted and that serving the interest of the company is serving the interest of the employee. Enabling moral agents in the workplace provides a better work environment than instilling fear, or encouraging ignorance. When employees feel connected to the establishment it is easier to craft and implement policies that protect the worker from intense scrutiny and the company from liable action. Forcing employees to look at the global impact of their decisions provides strategic thinking that allows personal growth, corporate participation, and visionary innovation that instills competitive advantage and ensures survivability.

Task 4

Is there a legislative solution for spam and other permutation of unsolicited electronic mail? Why/why not?

It is going to be very difficult for legislature to develop a solution that combats spam despite Leonsis' belief that the CAN-SPAM Act was "the right bill at the right time" (Carlson, 2004, p. 1) due to technological mutations that allow the spammers to always remain one step ahead of filtering software through automatic adaptation (Carlson, 2004). Another issue is compliance. While there are conflicting figures, it is clear that companies are not creating advertisement emails according to some rules crafted in the CAN-SPAM Act (FTC, 2003; Gross, 2004; Hicks, 2004) that established fraudulent email as those with: materially falsified headers, falsely identified actual registrant, intent to deceive, and false identification in interest to registrant. The FTC (2003) reported that 66% of all email received during a study had false "from", "subject" lines, or falsity in message text. The study received 86% of addresses posted on web sites and newsgroups received spam and 63% of email list removal requests were not honored. Gross (2004) reported that 99% checked by a California software firm was not CAN-SPAM compliant and some companies have a spam rate of 76% (Hicks, 2004). Is spam management the solution?

The following approaches to spam management are presented by O'Neil and Senf (2003): White / Black Lists, Contextual Analysis, Challenge and Response, Honeypot, Header Analysis, Content Analysis, and Heuristics. Using an inclusion/exclusion list, address verification, or message content validation will all fail from a single fatal flaw: false positive identification. Companies can ill afford to delete real customer email with the fierce competition the information age created, but the costs of fighting spam is equally challenging. AOL simply discards 80% of 2.5 billion daily emails due to spam flags (Hansell, 2003), but how many of those are legitimate, personal or business, that disappear into the abyss – AOL does not bother storing or distributing these messages – requiring 18 full-time employees taking calls from aggravated customers who's email is blocked unfairly. Employing anti-spam software using any of the above methods will still allow on average 10 to 15 percent to get through to the user causing lost productivity (Hansell, 2003). The costs involved are extremely high, and growing.

Spam costs to companies have jumped from ~$800 per employee in 2003 to ~$2,000 in lost productivity (Hicks, 2004), totaling $87 billion for the United States alone and $20.5 billion globally in wasted computing power on email (Hansell, 2004). Companies and educational institutions alike cannot build systems fast enough to handle the sheer volume of spam flooding through their facilities. The costs involved in fighting spam, controlling spam, and recovering time involved will cost the U.S. over $100 billion (including hardware) by the end of the decade with a growth rate of only 5%. The majority, 86%, of spam originates in the United States (Keizer, 2004) and CipherTrust found that a limited number of IPs may be responsible for most spam, so why aren't marketing companies abiding by the law?

The penalties defined by the CAN-SPAM Act, forfeiture of property and fines that cannot exceed 5 years imprisonment, consistent with other fraud-related sentences, but completely inadequate when compared with the potential, or real damage caused. Jeremy Jaynes was sentenced to 9 years in prison for spearheading a huge North Carolina spamming operation – the

first felony prosecution of a spam case in the United States, but only stood to pay a $10,000 fine despite raking in $750,000/month from illegal chargers and stolen credit card numbers (Cox & Saker, 2004). The drug war spent $15 billion in 1997 alone and has managed to incarcerate only 15% marijuana distributors compared to those possessing and attained higher overall numbers than violent offenders compared to 1980 reports (PBS, 1996). While Kenneth Lay faces up to 175 years in prison and over $5 million in fines, the Texas Teachers Union and countless others are left with depleted retirement funds. How many other executives, stock analysts, and accounting partners are being tried for similar fraudulent activities?

Developing a legislative solution for spamming must take place to enable companies and authorities the power to defend the U.S. infrastructure, but harsher penalties and imposed sentences must be mandated to countermand the inundation of spam. Legislation can only go so far since spammers can easily move operations outside of the United States with little or no difference in cost structure. U.S. post requires content, address, and delivery, but electronic mail can be done at a fraction of the cost in even less time. First Amendment rights are going to pose some problems with address blocking denying legitimate business access to email, but better means of identifying spam must be developed. Do not spam lists are being proposed, counterparts to the do not call (telephone) lists already active, but providing criminals means of legitimizing their business with little or no incentive may prove wasteful.

Bibliography

Berghel, H. (2000, February). Identity theft, social security numbers, and the Web. Communications of the ACM, 43(2), 17-21.

Carlson, C. (2004, May). CAN-SPAM leaves lid wide open. Eweek, Messaging & Collaboration. Retrieved on August 21, 2004 from the World Wide Web at http://www.eweek.com/article2/0,1759,1596134,00.asp

Cornell. (2003). OIT procedure and protocols under the USA-Patriot Act. Retrieved on November 12, 2004 from the World Wide Web at http://www.cit.cornell.edu/oit/policy/memos/PatriotAct.html

Cox, J. & Saker, A. (2004). Raleigh spammer faces prison time. NewObserver.com: Local & State. Retrieved on November 24, 2004 from the World Wide Web at http://www.newsobserver.com/news/story/1828341p-8141513c.html

Doyle, C. (2002). The U.S. Patriot Act: A Sketch.(CRS Report for Congress). Washington: Libraryof Congress. Retrieved on July 12, 2004 from the World Wide Web at http://fpc.state.gov/documents/organization/10091.pdf

Ficarrotta, J. C. (2004). Software engineering as a profession: A moral case for licensure. Social, Ethical and Policy Implications of Information Technology. In L. L. Brennan & V. E. Johnson, chapter 12, pp. 204-222. Hershey, PA: Information Science Publishing.

French, M. (2004, April 26). Tech sabotage during the Cold War. Federal Computer Week, 28-30. Retrieved on July 12, 2004 from the World Wide Web at http://www.fcw.com/fcw/articles/2004/0426/feat-strange-04-26-04.asp

FTC. (2003, April). False claims in SPAM: A report by the FTC's division of marketing practices. Retrieved on November 24, 2004 from the World Wide Web at http://www.ftc.gov/reports/spam/030429spamreport.pdf

Gross, G., & IDG News Service. (2004). Small percentage of spam complies with new law. Infoworld: news. Retrieved on July 12, 2004 from the World Wide Web at http://www.infoworld.com/article/04/01/12/HNspamcomply_1.html

Hammitt, H. (1998, June). A constitutional right of informational privacy. *Government Technology,* 22.

Hammitt, H. (2002, June). An end to easy access: Security concerns are superseding agencies' missions to provide useful information to the public. Government Technology, pp. 50+ Retrieved on July 12, 2004 from the World Wide Web at http://www.govtech.net/magazine/story.phtml?id=3030000000010448.0

Hansell, S. (2003). Balancing life and practice: The high, really high or incredibly high cost of spam. LexisOne. Retrieved on November 24, 2004 from the World Wide Web at http://www.lexisone.com/balancing/articles/n080003d.html

Harris, B. (2004, June). Clarity and execution: The next steps in cyber-security. Government Technology, pp. 31-36 Retrieved on July 12, 2004 from the World Wide Web at http://www.govtech.net/magazine/story.php?id=90473

Hicks, M. (2004, June). Spam costs, volumes soar despite new laws. Eweek, Messaging & Collaboration. Retrieved on August 21, 2004 from the World Wide Web at http://www.eweek.com/article2/0,1759,1608661,00.asp

Hoffman, D. E. (2004, February). CIA slipped bugs to Soviets: Memoir recounts cold war technological sabotage. Washington Post. Retrieved on November 21, 2004 from the World Wide Web at http://www.msnbc.msn.com/id/4394002/

Hoffman, G. M. (2004). Ethical challenges for information systems professionals. Social, Ethical and Policy Implications of Information Technology. In L. L. Brennan & V. E. Johnson chapter 7, pp. 118-129. Hershey, PA: Information Science Publishing.

Huff, C., Johnson, D. G., & Miller, K. W. (2004). Virtual harms and real responsibility. Social, Ethical and Policy Implications of Information Technology. In L. L. Brennan & V. E. Johnson, chapter 6, pp. 98-117. Hershey, PA: Information Science Publishing.

Jennings, M. M. (2004). A contrarian's view: New wine in old bottles: New economy and old ethics: Can it work? Social, Ethical and Policy Implications of Information Technology. In L. L. Brennan & V. E. Johnson, chapter 10, pp. 159-182. Hershey, PA: Information Science Publishing.

Keizer, G. (2004). Spam: Made in the U.S.A. TechWeb. Retrieved on July 12, 2004 from the World Wide Web at http://www.techweb.com/wire/story/TWB20040812S0006

Lamont, J. (2002, February). CyberWatch: Protecting critical infrastructures. Retrieved on July 12, 2004 from the World Wide Web at http://www.kmworld.com/publications/magazine/index.cfm?action=readarticle&article_id=1182&publication_id=1

Mitrano, T. (2003, November/December). Civil privacy and national security legislation: A three-dimensional view. EducauseReview, 38(6), 52-62. Retrieved on July 12, 2004 from the World Wide Web at http://www.educause.edu/pub/er/erm03/erm0362.asp

O'Neil, M. & Senf, D. (2003a). Strategies to manage the spam menace: part 1. CIO, Analyst Corner. Retrieved on July 12, 2004 from the World Wide Web at http://www2.cio.com/analyst/report1746.html

O'Neil, M. & Senf, D. (2003b). Strategies to manage the spam menace: part 2. CIO, Analyst Corner. Retrieved on July 12, 2004 from the World Wide Web at http://www2.cio.com/analyst/report1840.html

Patton, S. (2004, June 1). Privacy is your business. CIO, 49-55. Retrieved on July 12, 2004 from the World Wide Web at http://cio.co.nz/news.nsf/UNID/4006968BBAC6CB49CC256EA800690F2E

Rosencrance, L. (2004, May 31). Information highway patrol. Computerworld, pp. 28-29. Retrieved on July 12, 2004 from the World Wide Web at http://www.computerworld.com/securitytopics/security/story/0,10801,93471,00.html?SKC=security-93471

Savage, M. (2004a, June). Californialaw hits firms nationwide. SC Magazine,15.

Savage, M. (2004b, March). Defender of U.S. cyberspace. SC Magazine, 20-23 Retrieved on July 12, 2004 from the World Wide Web at http://www.scmagazine.com/features/index.cfm?fuseaction=FeatureDetails&newsUID=23048cda-cc74-47ec-a13a-335d3a05f629&newsType=Features

Scalet, S. D. (2002a, June 1). Dr. Crime's terminal of doom and other tales of betrayal, sabotage & skullduggery. CIO. Retrieved on July 12, 2004 from the World Wide Web at http://www.cio.com/archive/060102/doom_content.html

Scalet, S. D. (2002b, June 15). They want you for a safer infrastructure. CIO. Retrieved on July 12, 2004 from the World Wide Web at http://www.cio.com/archive/061502/safer_content.html

Spinello, R. A., Gallaugher, J., & Waddock, S. (2004). Managing workplace privacy responsibly. Social, Ethical and Policy Implications of Information Technology. In L. L. Brennan & V. E. Johnson, chapter 5, pp. 74-97. Hershey, PA: Information Science Publishing.

Sprague, R. D. (2004). Liability for system and data quality.Social, Ethical and Policy Implications of Information Technology. In L. L. Brennan & V. E. Johnson, chapter 11, pp. 159-182. Hershey, PA: Information Science Publishing.

Ward, Mark. (2000). Experts question Yahoo auction ruling. BBC News. Retrieved on November 24, 2004 from the World Wide Web at http://news.bbc.co.uk/1/hi/sci/tech/1046548.stm

Wiencek, D. (2004). Ethical challenges of information systems: The carnage of outsourcing and other technology-enabled organizational imperatives. Social, Ethical and Policy Implications of Information Technology. In L. L. Brennan & V. E. Johnson, chapter 9, pp. 141-158. Hershey, PA: Information Science Publishing.

Woodbury, M. C. (2004). What, me, worry?: The empowerment of employees. Social, Ethical and Policy Implications of Information Technology. In L. L. Brennan & V. E. Johnson, chapter 4, pp. 59-73. Hershey, PA: Information Science Publishing.

U.S. General Accounting Office (USGAO). (2003, July). *Management and Preservation Poses Challenges*. (GAO-03-936T). Washington: The Agency. Retrieved on October 12, 2004 from the World Wide Web at http://www.gao.gov/new.items/d03936t.pdf

U.S. National Research Council (USNRC). (2002).Cybersecurity: Today and Tomorrow: Pay Now or Pay Later. Washington: National Academy Press. Retrieved on August 22, 2004 from the World Wide Web at http://www.nap.edu/catalog/10274.html

Zink, S. D. (2004). Information policy, DISS 770. *Graduate School of Computer and Information Sciences Summer 2004 Doctorate Lectures*.