Global Information Assurance Certification Paper

Pornography on the Workplace Network

GIAC Security Essentials
Certification (GSEC)
Practical Assignment
Version 1.4c

Option 1 - Research on Topics
in Information Security

Submitted by: Michael J. Hanson
16 March 2005

SANS Course Location: Washington, DC

Table of Contents

List of Tables and Figures

Abstract/Summary

Primarily the computer security professional's job involves mapping architecture, building machines, and preventing attacks. But what happens when an incident happens that is non-technical in nature uses a technical device? The world of pornography is creeping into the workplace, inviting with it vulnerabilities to users and systems. While the technical aspect of the incident response may be familiar, the personnel aspect often is not. This document shows the vulnerabilities of pornography in the workplace, incident handling steps, and a survey of commercial applications for aiding in investigations.

Introduction

Norman Cousins once said, “The trouble with this wide open pornography…is not that it corrupts, but that it desensitizes; not that it unleashes the passions, but that it cripples the emotions; not that it encourages a mature attitude, but that it is a reversion to infantile obsessions; not that it removes blinders, but that it distorts the view” (Sumerlin).

Pornography has become the leading industry on the Internet and otherwise, grossing $12 billion dollars per year in the United States. According to the University of Nebraska at Omaha, that figure is more than the National Football League, National Basketball League, and Major League Baseball combined. Along with that amount of income, the pornography industry is responsible for costing American business vast amounts of dollars in wasted productivity and disciplinary action. This is evidenced by the statistic that more than 60% of Fortune 500 companies surveyed have disciplined or fired employees based on an Internet access issue.

As the computer security professional, from time to time, one will likely be called away from the task of monitoring the networks for intrusions from the outside world and be forced to assist the Human Resources office or Personnel Security office to deal with a trusted insider. This paper will explore some of the occasions where trusted insiders have violated the personal and technological trusts that their organization has given, the vulnerabilities of this activity, the role of the security professional in protecting one’s organization, and the technical tools available to thoroughly investigate incidents.

Violated Trust

Though, it was not the first case to go to trial, one such disciplinary action accorded within the walls of the Central Intelligence Agency (CIA). The case, United States v. Simons, has now become the legal focal point regarding pornography in the workplace.

On July 17, 1998, Clifford Mauck came to work at Science Applications International Corporation (SAIC) expecting the day to be like any other day. Little did he know that his efforts to become more familiar with a customer’s firewall would launch one of the most cited technology and privacy legal cases in the past decade. Now that the seven year anniversary of the initial action on this case is approaching, it is appropriate to brief this case and its applicability to the information technology and security conscious society our sector finds its paradigm.

Mark L. Simons was employed as an electronic engineer at the Foreign Bureau of Information Services (FBIS), a division of the CIA. With this employment, FBIS provided Simons with a computer with Internet access and an un-shared office. This access was supposed to be used solely for official government business and specifically prohibited accessing unlawful material. FBIS instituted their policy[1] regarding employees' Internet usage in June 1998, which included the provision that electronic audits would be employed to ensure compliance.

In an effort to better understand capabilities of the FBIS firewall and to monitor for inappropriate use of computer resources, FBIS contractor Mauck began exploring the firewall by entering certain search keywords. On two days in July 1998, Mauck entered the keyword "sex" into the firewall database and found a large number of Internet "hits" originating from Simons' computer. By a simple review of the website names, Mauck determined that there was no official FBIS purpose for visiting those websites.

Mauck reported the discovery to FBIS, who managed the initial investigation. The initial investigation consisted of viewing the websites in question (determined to contain pictures of nude women), remotely examining Simons's computer to determine whether Simons had downloaded any picture files from the Internet (over one thousand such images were found), remotely printing the file names, and copying all of the files on the hard dive of Simons's computer (again, remotely).

After coordination with the responsible Federal Bureau of Investigation (FBI) Special Agent (SA), the FBI executed a warrant to locally copy the hard drive on August 6, 1998. The warrant was based several images of child pornography that the FBI viewed on the remotely copied hard drive. On September 23, 1998, the FBI physically seized and removed the computer and diskettes. The evidence revealed over fifty pornographic images of minors.

Simons was denied early retirement, fired by FBIS, and indicted on one count of knowingly receiving child pornography[2] and one count of knowingly possessing material containing images of child pornography.[3] After a non-jury trial, Simons was found guilty on both counts, sentenced to eighteen months imprisonment

[1] The policy read as follows: Audits. Electronic auditing shall be implemented within all FBIS unclassified networks that connect to the Internet or other publicly accessible networks to support identification, termination, and prosecution of unauthorized activity. These electronic audit mechanisms shall…be capable of recording:

- Access to the system, including successful and failed login attempts, and logouts;
- Inbound and outbound file transfers;
- Terminal connections (telnet) to and from external systems;
- Sent and received e-mail messages;
- Websites visited, including uniform resource locator (URL) of pages retrieved; and
- Date, time, and user associated with each event.

[2] 18 U.S.C. 2252A(a)(2)(A)

[3] 18 U.S.C. 2252A(a)(5)(B)

and three years supervised probation, and required to register as a State Sex Offender. Simons's appeal of the verdict was essentially denied. [4]

Samples of Other Cases in Recent Times

CIA has not been the only entity to be affected by pornography in the workplace.

In June 2002, the Massachusetts Attorney General reported indicting Robert Whitty of Barnstable, Massachusetts's town government for possession and dissemination of child pornography. The investigation began when a co-worker came across pornographic files on the computer assigned to Whitty while performing routine upgrades to all computers within the department.

During June 2003, investigators found that there continues to be "significant misuse" of the Internet at the IRS. *USA Today* reported that investigators from the Treasury Department found that IRS employees accessed banned websites for personal e-mail, games, and sexually explicit material. "Nobody should collect a government salary to sit on their behinds and play around in chat rooms," said Senator Charles Grassley of Iowa, who oversees the Senate committee that covers the Treasury Department and IRS.

An employee, who downloaded pornographic images while at work, was fired on January 22, 2004 from the McCombs School of Business at the University of Texas, according to the *Daily Texan*. He was the fifth UT employee fired for looking at pornography at work in an eight month span. A task force was considering, at that time, installing filters or other monitoring software to prevent additional abuse of UT computers.

The *Las Vegas Sun* reported that Carl Lobsien, a twenty-six year employee of the Clark County, Nevada government, was arrested in January 2004 on charges of downloading more than 400 image files of child pornography onto his computer at the Public Works Department. Lobsein's activities led to at least one attack (denial of service) on the county's computer system due to a virus brought in through one of the downloads.

Vulnerabilities to the Organization

[4] Simons appeal to the 4th Circuit Court of Appeals was affirmed in part and denied in part. In short, the FBI failed to leave a copy of the warrant and inventory of evidence seized (copies of the hard drive and diskettes), but that error was deemed to not be prejudicial to Simons' guilt or innocence. However, because of this error, Simons could seek financial compensation upon lower court approval. Simons' argument that his expectation of privacy was violated was denied due to FBIS' interest in "the efficient and proper operation of the workplace" was outweighing Simons' privacy in his assigned office and computer.

There are multiple vulnerabilities that exist within the cyber-world due to insiders accessing pornography. The first, most notably, is financial. Cyberslacking, as the BBC calls the wasting of time on the Internet, cost British small businesses almost £1.5 billion in 2002 ($2.85 billion US). Scholars believe that any company that comprehensively tackled time wasting could see profits jump by 15%. However, these individuals caution that stopping cyberslacking does not solely involve pornography, but includes monitoring of individuals for sending information to job agencies or competitors, shopping, and other personal activities.

Secondly, according to Colin Barrow of the Cranfield School of Management in England, few other forms of employee time-wasting, such as consistent lateness, had the potential to do real harm like abusing e-mail and net access did. "A lot of people are not only wasting their time, but are potentially creating legal liability for the company while wasting their time." The inappropriate activity sought out, if seen by others in the workplace, could also be construed by employees as cause to bring legal action. The courts now grant judgments for sexual harassment far more often than they did initially. Today, courts will be more likely find an illegal hostile environment present when the workplace includes sexual propositions, pornography, extremely vulgar language, sexual touching, degrading comments, or embarrassing questions or jokes (Mann and Roberts). Internet pornography makes these activities easier to perpetuate and disseminate around the workforce. The UK Department of Trade and Industry placed the average cost of clearing up such an incident at £33,000 ($50,000 US) (BBC). Besides the legal costs and consequences, this activity in the public eye could seriously damage a firm's image and brand before its customer base.

Pornography, though, does not only come on static webpages. Research from Palisade Systems (Greenspan) indicates that 42% of all file searches are for pornographic movies or images. Peer to peer (P2P) network analysis comes with a more shocking statistic. Based on a review of 22 million searches, Palisade showed that 73% of all movie searches were for pornography and 24% of image searches were for child pornography. Only 3% of searches were for non-porn or non-copyrighted materials.

Table 1: P2P Searches by File Type

Movies	47%
Music	37%
Images	7%
Software	5%
Documents	3%

Source: Pallisade Systems (Greenspan)

A separate study conducted by Central Command (Greenspan) revealed that

61% of their respondents were unaware of the risks associated with the downloading of files. Besides making networks vulnerable to the sharing of classified or trade secret information, users could very easily release or spread viruses, install spyware or malware, and clog bandwith. Though not as substantial as e-mail attachments, ICSA labs (Greenspan) put Internet downloads as accounting for 11% of 2002's virus infections. Through these infections, attackers now have additional doors to enter into one's network and cause extreme damage to not only an organization's computer system, but their corporate strategy and documentation, as well.

Role of the Security Professional

Though it may not be the information security officer's forte, like with most things, protecting your organization starts with policy. Without a basis to conduct user training from and without rules and regulations to identify and correct bad behavior, an organization attempting to address this problem may only be spinning its wheels. While most corporations and government agencies have become adept at adopting policies to cover insubordination, violence in the workplace, sexual harassment, and safety violations, often the charge to adopt information technology policy is years behind. To compensate, organizations temporarily adapt old policy language to cases like shopping over the Internet, viewing pornography, writing personal e-mail, day trading, and forwarding chain mail to name a few. The older policies of misuse of company resources for non-business use and theft (of pay for misappropriated time) are most frequently cited (Johnson).

However, the amount of time needed to reach a substantive burden of proof with regard to these adaptations can be variable from firm to firm and also lead to a potential risk of inequitable application. While the medium may be the only differing component in weighing the significance of employee Doe bringing in a pornographic magazine and having it in his desk versus employee Jones downloading an image from playboy.com, the potential vulnerabilities and resources involved can make the difference in the outcome of a case.

Within the aspect of policy there are several things to consider. First, does the organization already have a written policy with regard to Internet and computer use? If so, be sure that all the language is up to date and provides for appropriate application and enforcement. If not, when drafting this document, be sure that there is buy-in from all areas and decision makers (i.e. focus on the bureaucratic divisions, management/non-management, racial/ethic diversity). Policies that are inclusive in their construction are likely to receive a higher rate of acceptance across the user population.

Second, one must then determine what this document should state. Raymond Hogge, of a Virginia-based law firm, listed several lessons learned after US v.

Simons went to appeal. These comments, modified from writings in 2001, continue to hold sage advice today. The policy should:

1. … be written and communicated to all employees. The employer should be prepared to prove that it was received [perhaps with a "click-through" banner]. It should be consistently enforced – every time.
2. … inform employees that the computing system, and all communications (sent and received) are property of the employer. Users have no reasonable expectation of privacy in the employer's equipment.
3. … inform employees that Internet access and the computer system itself is to be used for business purposes only. Neither personal, nor illegal use, is permitted.
4. … provide explicit examples of (but not limited to) inappropriate usage. For example, that pornographic material and harassing e-mails are not permitted.
5. … inform employees that the employer may engage in electronic auditing and monitoring. The employee implicitly and explicitly consents to this monitoring as a course of their employment and use of employer resources. All systems and networks may be monitored at all times. The language from US v. Simons provides a starting point here.
6. … inform employees that warrantless searches may be conducted in the course of an investigation to determine if policy was violated. Explicit explanation of what can be searched and how it can be searched should also be noted.
7. … be coordinated with other existing policies governing personal use of other systems (phone, copying machine) and other facets of communication (e-mail).

The Department of Justice (USDoJ) also provides some examples of "Sample Network Banner Language" to aid computer security professionals in securing their respective networks. Echoing the above seven points, USDoJ noted that for non-government networks, banners should make clear that the system administrator may consent to a law enforcement search. In addition, consequences for unauthorized activities must be spelled out and that discovery of unauthorized activities may be referred to law enforcement or management, as appropriate.

Once the policy for the network and users has been established, now it is up to the computer security professional to construct the monitoring and auditing tools within the network. Before taking the plunge for a five or six figure service, the security professional must accurately evaluate what system is most appropriate for their infrastructure. There are a number of corporate and private entities that offer their product on a trial or limited fee-based service for evaluation and testing. Cornell University, in a student assignment, provided the following [adapted] partial brainstorm for guiding such and evaluation:

- What does the service cover – the Web, e-mail, chat, etc?
- How does the service work?
- Does the service monitor, alert, and block inappropriate sites from being viewed (or just one of the three)?
- Does the service rely on client-side techniques (listing of sites or keywords), some other technique, or some server-side system?
- Who determines what sites or words are blocked (client or vendor)? Is an addition automatically added or does it need a vendor review? Who is authorized to submit additions (client or vendor)?
- Are the services modifiable by administrators (usually good) or by users (bad if a user wants to defeat the system)?
- How effective does the service appear to be? Can the security professional test the system to see if inappropriate sites are allowed to pass through or if appropriate sites are being incorrectly blocked?

While most of these systems outlined below initially focus on small networks (home, small business), their products can be adapted to handle fifty or more computers or servers depending on an organization's physical architecture. Here are a few of the more popular titles.

- Cyber Patrol <http://www.cyberpatrol.com>
- Sentian <http://www.securecomputing.com>
- Net Nanny <http://www.netnanny.com>
- Surf Control <http://www.surfcontrol.com>
- Internet Filter <http://research.internetfilter.com>
- Cyber Sentinal <http://www.securitysoft.com>

Now, for the sake of argument, the policy that has been written meets legal muster and has now been disseminated to all users. Tomorrow morning, one of the junior network analysts is at the office door and there is a problem. During a review of the security and system logs, files with sexually explicit names (possibly child pornography) were transferred across the network. What should be the first step in addressing the incident?

If the first thought is to panic; it's time to step out of the lab and take a walk around the block until cooler heads prevail. If the first thought is to start shutting down all or parts of the network; take that walk around the block in the opposite direction. While each organization's procedures will and should be different, there are some common themes that can be applied to incident response.

There are six steps to incident handling: preparation, identification, containment, eradication, recovery, and lessons learned (SANS). The first step of incident handling is to not wait until an incident occurs before developing a plan. This paper has addressed part of planning with the implementation of the Internet policy. A second facet of this step is to identify team members and support

components who will aid throughout the entire process. These team members may include technical specialists, interviewing specialists, management support, and legal counsel.

Among these team members that may be most crucial is legal counsel. Coordinating with counsel at the first instance may be the decision that not only saves the investigation from being dismissed in court, but may even save one's job. An important question to answer very early on in the process of both preparation and identification is whether or not an organization's investigation into an incident needs to cease when there is a violation of law discovered. In evaluating this question, John Gasiorowski, Deputy Inspector General for the City of Chicago, noted "maintaining the investigating office's focus on the work-related nature of the investigation will go a long way to ensure [the legal standards] will be applied by a court in determining whether the evidence obtained during a search conducted pursuant to an investigation of an employee is admissible [in that court]."

As for retaining one's position, there have been instances where well meaning IT security professionals have been the subjects of retribution and retaliation. In 2002 during routine troubleshooting, Dorothea Perry and Robert Gross discovered thumbnail images of naked children on the workplace computer of New York Law School Professor Edward Samuels. While Samuels was arrested and sentenced to six months in jail, Perry and Gross were put on probation and fired four months after their discovery. The contracting firm that fired them claims there were performance issues, but those claims in this case have been evaluated by journalists as dubious (Foley).

In identifying the incident, a large part of that has been done by the lead reporter (network analyst) in this case. However, recognizing the difference between a standard event and an incident that has the potential to do harm to the organization is key in the *correct* identification of an incident. Maintenance of logs and backups will provide a baseline showing what events are unusual occurrences and need further investigation. This paper will consider some tools commercially available to aid in incident identification in a later section.

There are two avenues to consider in making sure that the security incident is contained. The first area is to handle the computer media that has been contaminated. Again, using logs and adding a forensic and physical inspection, determine what, if any, other media may have been used to transport or store the offensive content.

The second avenue in containing the incident comes from a personnel side. By analysis of logs, e-mail, and other communication methods, one can determine if this is an issue isolated to one trusted insider or if there is a ring of this activity going on within the network. As referenced above, an organization need not wait until all legal action is completed before executing a disciplinary action.

Provided that the discipline is consistent with organization policy and that will not upset legal equities, management should address the issue as transparently as possible to show its staff that the organization takes information security seriously.

Continuing with the SANS model, the fourth and fifth steps are eradication and recovery. Dependent on the vulnerability created or exploited by the incident, this could be one of the longest and most deliberate steps undertaken. The problem must be fixed and secured before the system can be restored to its original working order. With the example proposed in this paper, the issue of eradication is more of a bureaucratic exercise than technical one. For the bureaucratic, the organization must be sure that all deletion efforts are coordinated with any law enforcement entity so as not to jeopardize evidence to be used in a criminal or civil proceeding. From the technical perspective, any deletion or wiping of the affected machines should be validated and tested so that no trace of the offensive materials can resurface or be passed on to other users. This, in itself, would be a new crime. Once the tests are successful and the vulnerabilities have been corrected, the system can be restored and recovered.

Finally, all processes should be finished up with a review of what parts went well and what parts could be improved upon. Throughout the event and investigation, keep a running list of changes or successes, as it will be a helpful memory aid. When the members of the incident response team and all other liaisons to the team can meet to debrief the incident, the group should arrive at some implementable recommendations that can be forwarded to the appropriate management divisions. By acting on these recommendations, there is the opportunity to save additional time and financial resources should a similar incident occur again.

Network Analysis Tool

In order to identify that a problem exists, an organization needs to set up its network infrastructure in such a way that can accurately capture network activity. However, there are many points that a network analysis tool and activity capturing tool (sniffer) can be placed to achieve this goal. Each organization needs to determine within their operation whether or not it is appropriate to capture only the activity that links the firm with the outside world (Internet) or all traffic that occurs within the Intranet as well.

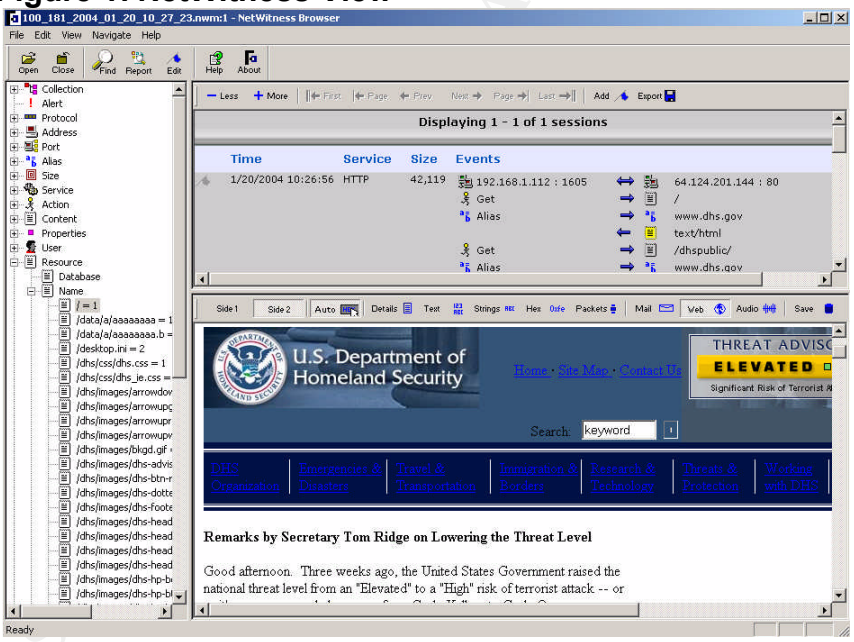
When the organization knows where to put the sniffer, the decision of what tool to employ must be made. One of the tools that have been receiving increasing levels of interest is called NetWitness, developed by Forensic Explorers. Developed in conjunction with US Government agencies nearly ten years ago, this system has been the primary choice of these agencies for identifying and

resolving not only external threats, but internal threats as well.

As the paper has outlined above, internal threats can often be more damaging and prevalent than attacks from the outside world. A 1999 FBI study reported that over 60% of network vandalism and attacks come from within a company (Rand). Though an employee may be granted approval to access sensitive information, without ways to detect potential abuse of that access, the organization is a substantial risk.

With regard to the topic of pornography, the NetWitness system not only records the domain name of the site being viewed, but it extracts key information from sessions of network activity and displays them in a visual interface for lay interpretation. Websites that are viewed appear within the NetWitness tool as websites, not lines on logs. Additionally, as websites within the pornography industry update and change frequently, investigations can be based on the information viewed by the insider, not on what information is displayed on the website at the time of the investigation.

Figure 1: NetWitness View



Finally, the NetWitness tool allows isolation of suspect network activity by multiple factors: what protocol was used, IP address, port, DNS resolution, size of the traffic, content, user, and others. Say Mr. Smith was at an IP address ending in 201.144 from noon to 1 PM. By isolating that address, the investigator can inspect the network activity to and from that machine for that time. Within this activity will expose identities (userids for multiple programs), passwords, images viewed (by content), websites requested, and much more. It is a difficult process for security professionals to explain such information to lay individuals who do not interact with security logs and network traffic on a routine basis

without having visual evidence that they can quickly and correctly interpret and present.

This paper is not intended to be an advertisement for this product at the exclusion of any others. However, when considering a system to use for monitoring one's networks, strong consideration should be given to the use by non-IT individuals. Cases involving disciplinary action against trusted insiders often require lay individuals' involvement.

Conclusion

This issue of pornography in the office place is not likely to go away soon. Neither is risk from a trusted insider doing harm to an organization from this and other activities. By addressing this issue with policy and effective use of network monitoring systems, the security professional has a greater probability of staving off more damaging and nefarious attacks from these insiders in the future. This paper has outlined the issue that presents itself in the workplace, examples of how that issue has manifested itself, the vulnerabilities of pornography in the workplace, the professional's role in combating this problem and protecting the organization, and some of the tools to prevent and investigate this activity.

Through constant vigilance and leadership, the organization and country will be better able to thrive through effective and appropriate use of this computing medium to which the security professional works hard to maintain.

Works Cited

Associated Press. "Probe Finds IRS Workers Misuse Internet on Agency Time." *USATODAY.com*. 20 June 2003. <http://www.usatoday.com/tech/news/techpolicy/2003-06-20-irs-workers-surf-too_x.htm> (05 Mar. 2005).

BBC News. "Internet Abuse Costs Big Money." *Technology*. 01 Nov. 2002. <http://news.bbc.co.uk/1/hi/technology/2381123.stm> (17 Jan. 2005).

Cornell University. "Porn Lab." *Filtering Software Against Online Pornography*. 06 Nov. 2002. <http://instruct1.cit.cornell.edu/courses/comm240/labs/porn/> (27 Feb. 2005).

Cyber Patrol. *Internet Filtering Software*. 2005. <http://www.cyberpatrol.com> (27 Feb. 2005).

Foley, John. "Work/Life: When Things Go Wrong." *Information Week*. 16 Aug. 2004. <http://www.informationweek.com/story/showArticle.jhtml?articleID=28700222> (17 Jan. 2005).

Forensic Explorers. *Net Witness*. 2005. <http://www.forensicexplorers.com> (12 Mar. 2005).

Gasiorowski, John A. "Regarding the Law: Probable Cause/Reasonableness Standard/Criminal Conduct." *Association of Inspectors General*. Spring 2003: 1+.

Greenspan, Robyn. "P2P = Porn2Peer?" *Internet News*. 26 Mar. 2003. <http://www.internetnews.com/stats/article.php/2170451> (21 Feb. 2005).

Hogge, Raymond L. "Recent Developments in Privacy Rights in the Public Sector Workplace Related to Electronic Communications." *Virginia Labor Law*. 24 Jan. 2001. <http://www.virginialaborlaw.com/library/e-law/outline-publicsectore-privacy2001-01-24.pdf> (26 Feb. 2005).

Johnson, Dennis K. "Controlling User Abuse." SANS GSEC Practical Assignment Version 1.4b. 21 Feb. 2004.

Lawson, Jen. "Man Kept Child Porn at County Job, Police Say." *Las Vegas Sun*. 07 Jan. 2004.

<http://www.lasvegassun.com/sunbin/stories/text/2004/jan/07/516135702.html> (17 Jan. 2005).

Net Nanny. "Products List." *Internet Filter, Family-Safe Search Toolbar, Chat Monitor, and Ad Blocker*. 2004. <http://www.netnanny.com/products/index.html> (27 Feb. 2005).

NW Tech Inc. "NetSpective: Numbers Count." *NetSpective*. 2003. <http://www.nwtechusa.com/netspective_numbers.html> (17 Jan. 2005).

Rand, Len. *Security Policy Enforcement for Networks*. 1999. <http://www.itsecurity.com/papers/policyenf.htm> (13 Mar. 2005).

Roberts, Barry S. and Richard A. Mann. "Sexual Harassment in the Workplace: A Primer." *Akron Law* Review 29.2 (1996): 269-290.

Rockwell, Lilly. "Task Force Considers Porn Filters." *The Daily Texan*. 20 Apr. 2004. <http://www.dailytexanonline.com/news/2004/04/20/TopStories/Task-Force.Considers.Porn.Filters-665343.shtml> (17 Jan. 2005).

SANS Institute. *Defense-in-Depth*. Bethesda, MD: SANS Institute, September 2004.

Secure Computing. "Enterprise-Class Filtering Software." *Sentian Web URL Filtering and Reporting*. 2005. <http://www.securecomputing.com> (27 Feb. 2005).

Security Software Systems. *Internet Monitoring, Filtering and Blocking Software*. 2005. <http://www.securitysoft.com> (27 Feb. 2005).

Stone, Beth. "Barnstable Town Official Indicted on Child Pornography." *Massachusetts Attorney General*. 11 June 2002. <http://www.ago.state.ma.us/sp/.cfm?pageid=986&id=747> (05 Mar. 2005).

Sumerlin, Terry L. "Sex, Sex Everywhere." *Selfgrowth.com*. 2004. <http://www.selfgrowth.com/articles/Sumerlin18.html> (21 Feb. 2005).

Surf Control. "SurfControl Web Filtering Solutions." *Products*. 2005. <http://www.surfcontrol.com> (27 Feb. 2005).

Turner and Sons Production Inc. "Research." *The Internet Filter*. 2005. <http://research.internetfilter.com> (27 Feb. 2005).

United States v. Simons. No. 99-4238, 206 F.3d 392 (4th Cir. 28 Feb. 2000).

United States Department of Justice. "Appendix A: Sample Network Banner Language." *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*. 2002. <http://www,cybercrime.gov/s&sappendix2002.htm> (17 Jan. 2005).

University of Nebraska at Omaha. "The Facts." *The Power of Porn*. 2004. <http://www.whatdoyouthinkaboutporn.com/pop/facts.htm> (26 Feb. 2005).