Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Attack of the 50-Pixel (Naked) Woman

Porn exists in cyberspace- what does that have to do with security? Good question. From an organizational standpoint, pornographic IT forays pose several threats. The risky nature of downloading untrusted data, sexual harassment issues in the workplace, time wasted by unproductive employees, and simple bandwidth loss are all tangible concerns with associated real financial costs. Add to this the slightly-amorphous and downright-intangible reasons that your clientele might also harbor: moral and ethical concerns, embarr...

Copyright SANS Institute
Author Retains Full Rights

AD
nitrosecurity Log Management

ATTACK OF THE 50-PIXEL (NAKED) WOMAN

OR

THE QUESTIONS OF WEB PORNOGRAPHY: BALANCING SECURITY AND PRIVACY

WARNING: CONTENT HEREIN CONCERNS MATURE THEMES AND SUBJECT MATTER, AND CONTAINS ADULT LANGUAGE - DO NOT CONTINUE IF THIS OFFENDS YOU.

Do you, as a security professional, have an obligation to know something about pornography? Is the world's greatest high-tech threat couched in a form of coitus? Or, conversely, is pornography just an anxiety-laden red herring in the security realm?

This essay purports the latter is true.

ESTABLISHMENT: A CASE FOR CASES

Unless you're exceptionally lucky, at some point in your career as an information technology (IT) security specialist, a client will ask you to deal with pornography in some manner. This could be a request to implement Internet browsing filters, or investigate a user suspected of downloading adult material, or craft a policy protecting the client organization from litigation involving obscene exposure (so to speak). Familiarization with the dilemmas inherent to such activity is advised, yet somewhat difficult.

For the most part, nobody likes to talk about porn. Except, of course, pornographers.

The American cultural perspective concerning porn is rife with hypocrisy. For some reason too vast for the scope of this study, we view the purchase, viewing, or other use of pornographic media as something to be hidden, shunned, and the basis for guilt. Porn, it would seem, is something other people buy- probably people we wouldn't like to associate with or even know. And yet, the numbers don't bear out this assumption: as far back as 1981, a *U.S. News and World Report* article estimated domestic gross revenue of adult-oriented goods and services at $4 billion[1], a 1998 *Toronto Star* piece evaluated U.S. wholesale receipts for videotape **alone** to be $819 million[2], and some industry insiders claim that current annual income for the entire "adult market" is $8 billion[3]. That's far too much money to be dismissed solely as purchases by perverts in trenchcoats and horny teenagers. Using the arguably-high estimate of $8 billion per annum for means of comparison, that's more than American women spend on cosmetics each year, and only somewhat less than the U.S. illicit drug trade revenues. The volume of adult-oriented Internet traffic alone is staggering: according to her website, as of December of last year, Danni Ashe's image was downloaded over one billion times[4]; *Harper's* magazine declares that NakedNews.com (in which news anchors strip during webcast) has an average monthly viewership of six million people[5].

So, quite obviously, Americans, no matter what they say, like porn. With those numbers, it's safe to say that you, the reader, at some point or another, have partaken in pornography to some degree, whether that entails indulging in the prurient interest of your choice via the 'net in

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

the privacy of your own home, purchasing adult films/magazines/objects, or researching a scholarly work for a security certification.

Of course, anecdotal evidence more than bears this out: anyone who has spent any time whatsoever on the Internet, from web-neophyte to hardened hackmaster, knows porn is out there. While cataloging content of websites (and, an even more difficult decision discussed later in this study, distinguishing between “porn” and “non-porn”) is a Sisyphisian task at best, some indicative data is available, such as the claim made by web-filtering vendor Websense that “The No. 1 search term used at search engine sites is the word "sex."”[6] *The Wall Street Journal* even touted the efficacy of on-line pornography purveyors as other e-commerce ventures lagged[7]. Such assertions and assumptions are not hard to believe: for every sexual kink, fetish, bent, and predilection, there seem to be enough websites to not just proffer satiation, but competition for your purchasing power.

If one considers that, in a free-market economy, citizens vote with their dollars, then the reason that porn exists in the United States and on the Internet as a whole is because, whatever else we might say, we *want* it to.

THE GIST

Great, says you, the security professional, porn exists in cyberspace- what does that have to do with security? Good question.

From an organizational standpoint, pornographic IT forays pose several threats. The risky nature of downloading untrusted data, sexual harassment issues in the workplace, time wasted by unproductive employees, and simple bandwidth loss are all tangible concerns with associated real financial costs. Add to this the slightly-amorphous and downright-intangible reasons that your clientele might also harbor: moral and ethical concerns, embarrassment to the organization, etc. Unfortunately, unlike other risk-mitigation, assessment, and cost-benefit analyses, those involving pornography tend to become less rational and more emotional; this, for you, is dangerous territory.

Let’s examine each of the threats in turn, both tangible and intangible.

Dubious Downloads

Even the Security Administration, Networking, and Security (SANS) Institute warns of the perils associated with seemingly-pornographic sites and downloads offered therein in the Security Essentials coursework. Viruses, worms, and Trojan horses have to initially be distributed by some means, so enterprising cybervillains have made the intuitive leap to appeal to users’ baser instincts; porn seems an excellent avenue for launching malware. “Anna Kournikova,” “Naked_wife,” etc., may just as easily have been accepted by naive users if they were otherwise-named...then again, they may not.

Add to this (largely-e-mail-borne threat) mass-exchange resources such as peer-to-peer file sharing applications, and the likelihood of unintentional infection from external sources increases exponentially.

Of course, the real issue involved in this aspect of IT pornography is not actually the nature of the material exchanged, but the unsafe practices of the exchange itself. Pornography, then, might not be the threat at all, but more a means of exploiting a vulnerability (users with Internet access); an incentive, if you will. This being the case, many organizations attempt to

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

stamp out access to pornography (more on this later), when, strangely enough, it might be argued that a suitable alternative would be to train the users to download porn safely. While this suggestion is more than slightly facetious, it makes a point by demonstrating the irrationality of the concern.

An associated comparison: an organization blaming porn for introduction of malicious code could just as well blame desserts for excessive use of sick days; more health hazards -and the costs associated with them- come from obesity than anywhere else, but there are few employers who ban sweets in the workplace.

Harassment Harangues

Pornography, viewed by those who do not express a specific desire to do so, can contribute to the legal definition of a hostile workplace environment. Any management structure that does not take this threat seriously is just as negligent as one that fails to introduce fire safety measures. As a special case, however, pornography poses no more threat than any other personal memorabilia kept or viewed in an employee's workspace. Odd, but true.

Harassment, from a legal perspective, is ill-defined, as it assumes a "reasonable person" qualification, with the stipulation that the harassing item/person/stimulus be delineated by the harassed, i.e., someone can say they are offended by anything, and the burden of proof is on the harasser/organization to prove that a reasonable person would feel otherwise. Organizations run into conflict almost as often in defining what is **not** acceptable in the workplace as they do by being overindulgent of possibly-offensive material. Any organization trying, for instance, to ban employees from wearing yarmulkes in the workplace have been roundly trounced by the courts for discrimination.

The true test of this dichotomy then, will be when someone is accused of harassment, management will intervene to abrogate the harassing material, and the alleged harasser will claim the item has religious significance. Extreme cases could be easily dismissed; however, an employee offended by, say, a semi-clad deity portrayed on a crucifix could pose a fascinating legal quandary.

Again, porn, as an organizational concern in terms of harassment, should not merit any more consideration than any other item of media that might (and can) be found offensive. The most common problem here is not management's neglect, but an overabundance of attention and effort placed on porn, to the detriment of sense, logic, and pragmatism. Granting an overabundance of concern to a threat can be just as negligent as not granting any.

Time's a-Wasting

Some organizations blame porn for employees' seeming-inability to stay focused on productive behavior. This is, in fact, not entirely ludicrous; the human sexual drive is far more powerful than, say, the evolutionary impetus to shop for automotive accessories. If propagation of the species is a fundamental aspect of life, and porn is directly linked to the sexual act, it stands to reason that the inclination of personnel to gravitate towards porn sites is vast and nigh-overwhelming.

It might be true that, if porn were completely and totally removed from employees' grasp altogether, unproductive web surfing would decrease drastically, or might be eliminated completely. It might be true. It might not.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Indeed, the assessment of an employee's malingering should really not be based on what the person was doing in the stead of gainful activity, but the simple fact that work was being shirked. Whether the person was surfing porn or reading sports trivia in the bathroom or exchanging crocheting tips with colleagues or talking to family members on the telephone is irrelevant (unless any of those activities constitutes that employee's duties)- the fact is that work is not taking place, which is a human resources or management concern, not a security concern.

Moreover, if, indeed, porn is such a malignant force that employees are inexorably drawn to it, then any organizational efforts to stem such behavior will only increase the level of effort by employees to access porn. This is a threat unto itself- more on that later.

Bandwidth Bamboozlement

With IT resources a premium concern (and premium cost) for many organizations, the loss of IT capabilities due to overwhelming usage of those precious resources to search out, access, and collect pornography is a viable fear. But again, the threat is not due to the nature of the media, but the media itself; any large files exchanged by misappropriating organizational resources will clog the electronic arterials, not just porn. If there is some substantiation to the claim that without porn there would be no wasteful trading of photographic and/or video images, this researcher has yet to see it. The link between porn and bandwidth choking is one of correlation, not causality: people like porn the most, so porn is most often what congests e-traffic, but it is not safe to assume that if in the absence of porn there would be no such congestion.

Moral and Ethical

Organizations attempting to impose constraints on employee behavior based on whether something is "right" or "wrong" face danger by running afoul of a host of problems, many of which, ironically, are the very anxieties attributed to porn. Earlier in this essay, there was mention of the difficulty in distinguishing between "porn" and "non-porn," and this is where the difficulty arises: who makes that decision for the organization? Porn, like beauty and offensive imagery, is in the eye of the beholder. A completely arbitrary decision is legally shaky and lends itself and the organization to attack, while codifying porn is a patently absurd and ridiculously naive undertaking.

One person's porn is another's fine art.

This is especially tricky when one realizes that all organizations are not simply legal constructs, but actually *do* things, other than spend time in litigious battles. What does your organization, or your client organization, do? A university with any sort of history program might find it difficult to outlaw porn if they want their students to view works by Michelangelo or DaVinci. A publisher would find it impossible to keep from seeing scantily-clad or bare-breasted women if they were dealing with fashion in any way. The permutations are endlessly mind-boggling.

For instance, in a vain attempt to stem e-mail spamming, Microsoft Outlook offers a function where the recipient can block future missives from an undesirable sender by adding the sender's e-mail address to one of two lists: "Adult Content" or "Junk Mail." Which is which? A note offering the sale of Viagra- adult content or junk mail? A sales pitch for refinancing your home- minors aren't eligible, so is it adult content? In this case, an individual gets to delineate,

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

and the only person affected by that choice is the individual choosing, so the risks associated with the policy are minute. Anything other than this, and the risks escalate drastically.

Organizational Embarrassment

From a management perspective, public knowledge that organizational personnel are indulging in porn in the workplace is one of the least-discussed and yet most anxiety-laden concerns. This seems to be an outgrowth of individual shame regarding pornography; getting "caught" is cause for tribulation, and requires the use of stealth.

There may be realistic basis for this concern: public organizations might feel the displeasure of the taxpayers who support them, and private organizations might feel the wrath of the marketplace, in the form of decreased share value or boycotts. Yet, while this seems a viable threat, the evidence does not bear it out: organizations that have caught employees (or had their employees caught) surfing or trading porn have not suffered overwhelmingly deleterious impact because of it. Indeed, even the White House fell victim to just such an event in August, 2000[8], yet no massive public outcry resulted (the argument might be made, however, that people had become inured to sexually-oriented shenanigans in the White House at that point).

Of course, it might be suggested that only the drastic unilateral action of the organizations themselves, in efforts towards very-publicized self-policing, stemmed such public furor in pre-emptive strikes, such as Dow[9], General Dynamics, and the CIA[10] disciplining or terminating groups of employees in attempts to stave off outside influences. This philosophy has yet to be truly tested though: while employees have sued their organizations for a myriad of IT-related matters, none has yet challenged dismissal for abuse of IT resources on the basis anti-porn or anti-adult policies are capricious and overbroad. While this will make an interesting case, finding a sympathetic court will be difficult at the moment, so it may not take place for a few more years.

BIGGER TROUBLES

The real quandary, then, for the IT security professional, is creating an environment that dovetails management's concerns with operational parameters and legal constraints; a dicey proposition, at best. What do you do to please the client while avoiding other pitfalls? The answer to this question has opened other dangerous doors most organizations have failed to consider.

Some workplace entities have opted for commercial web-censoring products, thereby placing the onus of filtering material well outside the organization itself, in an effort to abrogate culpability for any ramifications. This is also somewhat more cost-effective than having internal personnel find, evaluate, and block each offensive site on the Internet; organizational policy can then be generalized to "Employees may visit sites not blocked by our filtering product," instead of "Employees will not visit the following sites....".

This approach is almost comically naive and foolhardy. Third-party products currently available rely on the same detect, analyze, and block model purchasers want to avoid, and are therefore susceptible to various problems. Who is paid to make the distinction between "good" and "bad" sites? In an ideal world, it would be personnel with the very same mindset as the purchasing organization's leadership, but, realistically, it is usually overworked and underpaid graduate students carrying this burden. Can they find everything pornographic on the Internet?

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Never. New sites (and old sites with new addresses) are constantly created. Is every decision they make in line with management's policies? Unlikely- the companies who provide such products, and the personnel they employ, necessarily have their own biases and beliefs, which may conflict with the policies, ideals, and actual operational needs of the client's organization.

Organizations, like parents, need to realize, and quite soon, that they cannot prevent all "disagreeable" sites from being viewed on equipment under their purview simply by buying a tool that claims to provide just such a service.

ADVERSITY AND ADVERSARIES

Finally, the most important and completely-overlooked truism is that if people want something, they will get it, and, if they want it badly enough, they will get it no matter what is done to prevent them. Therefore, organizational efforts to keep employees from accessing porn may, in fact, *harm* the security posture of the organization.

Simply stated: employees (read: users) are a necessary element of IT security; if the organization creates an environment of distrust and prohibition wherein the users are alienated from taking part in the process, security decreases. Furthermore, if users take steps to broach the hindrances placed on IT usage, in an effort to gain access to pornographic material, the security measures become obsolete or irrelevant. Instead of a cooperative effort involving all members of the workplace, the organization has created an adversarial relationship between management and employees, a sure detriment to overall security.

Technology cannot solve this problem, as every development for securing systems brings with it the need to create a countermeasure; SafeWeb (www.safeweb.com) and TriangleBoy are fine examples of this concept applied to web-monitoring products.

THE END OF THE MATTER

This essay is not to be taken as a defense of inappropriate use of IT resources by organizational personnel, or, for that matter, of pornography, which are both wholly other subjects. It is also not meant as a tirade for personal freedom. It is hoped, instead, to be a launching-point for rational, balanced discussion of the actual position of pornography in the security realm, something that heretofore has been drastically lacking.

Organizations, both public and private, as well as interest groups and even the American community at large, continue to view pornography on the Internet as a bastion of illicit and fear-inducing legal quagmires. Hysteria is, in no way, conducive to security practices; porn has thus far created a disproportionate concern in the security field (granted, mainly from customers), a trend that is detrimental to a truly secure environment. Even granting that porn creates some security problems does not excuse overburdening security efforts and resources to stem threats no more or less important or pervasive than others.

As security and IT professionals, proper discussion and dissection of this topic is necessary to further efforts to provide real service to our clientele, not just assuage ungrounded or overarching paranoiac concerns. With pornography, this effort is hampered more so than with other security matters, as adult discussion causes discomfort. That, then, is the real threat from porn, and the real challenge.

It's time, then, that we grew up enough to be able to overcome that challenge.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

[1] Thornton, Jeannye. "Sex Business Booms Despite Cleanup Drive," *U.S. News & World Report*, March 16, 1981.
[2] Considine, J.D. "Porn Stars Get More Exposure In Mainstream Movies," *The Toronto Star*, December 31, 1998.
[3] Serenity, personal interview, 1998.
http://www.lasvegasweekly.com/departments/12_02_98/thirddegree_serenity.html
[4] http://www.billiondownloadwoman.com/images/ff_03.jpg
[5] "Harper's Index," *Harper's*, July, 2001.
[6] http://www.websense.com/products/why/stats.cfm
[7] Weber, Thomas. "For Those Who Scoff at Internet Commerce, Here's a Hot Market," *The Wall Street Journal*, May 20, 1997.
[8] Sperry, Paul. "Web-porn Scandal Rocks White House," *WorldNetDaily.com*, August 9, 2000.
http://www.warroom.com/Whitehouse/pornscandal.htm
[9] Associated Press, "Dow Fires 50 Over E-mail Abuse," *USAToday.com*, July 28, 2000.
http://www.usatoday.com/life/cyber/tech/cti298.htm
[10] "CIA Probes Employees' Computer Use," Excite News, November 12, 2000.

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 22nd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**