Global Information Assurance Certification Paper

Alec Nisbet
SANS Security Essentials Practical
May 24, 2001

When Abuse Becomes Criminal: An Analysis of the Security Professional's Responsibilities in Dealing With Cyber Problems of Various Severities

Introduction

If you have an email address, you have seen Unsolicited Commercial Email, or SPAM. If you have been online, particularly if you have been using an always-on connection like a Digital Subscriber Line, you have been port scanned. These statements are generalizations, and while it is possible that neither applies to you despite how many email addresses you have or how much time you spend online the point is that these events occur with blinding frequency. So frequent are they, in fact, that these two examples of network abuse are simply expected, and no security professional can either completely eliminate them or spend all of his time trying. The pursuit of the perpetrators of such nuisances seems especially inconvenient in light of the most devastating attacks and the resources necessary to guard against them.

So while the online theft of a credit card number and the ensuing use or sale of that number by unauthorized parties is clearly a crime, and the receipt of an unsolicited email is clearly not, a good number of common exploits can be considered invasive but fall within a gray area between legal and illegal. Where should the security professional devote his limited time and resources? In which instances should action be escalated to law enforcement? What laws and precedents exist that might protect the individual and the organization, and, conversely, what laws and precedents may implicate the individual and the organization? These are some of the questions that the security professional must ask when designing and maintaining a security policy in the face of a wide range of risks representing a wide range of potential damage.

This paper will attempt to outline the range of these risks and provide examples of how different security policies handle them differently. In different contexts, security may very likely prioritize differently; what one organization views as a threat, regardless of it being a legally prosecutable offense, may not pose the same risk for another organization with a different business model. In any case, the security policy must walk a delicate line between protecting itself from viable threats while still preserving the privacy of the individuals involved. From here the paper will break down the factors that the security professional must consider by legal context and precedent. Under each context different business models will be considered along with the priority that each will have for the respective threat and security policy guidelines will be suggested accordingly.

Security Considerations in Regard to Network Abuse and Network Crime

For clarity and simplicity, the discussion will assume the existence of three hypothetical private institutions, each with a different function and business model, but all inextricably linked to the Internet. The goal of each institution is to develop business by making full use of online technologies and protecting the private information of its users at a minimal cost to the availability of information. As a greatly exaggerated cross-section of online institutions we will examine Acme Savings and Trust (a bank), Acme Online (an Internet service provider), and Acme College (a university). A synopsis of different security risks in each case from SPAM to outright theft will be considered with respect to applicable law. From there the security professional will have a better idea of how aggressive he should be in his policy toward the given issue. As a general trend we will see that the bank is under more pressure than the other two to secure its network, although this is not true in all cases.

Malicious Code

Worms and viruses present a threat to every computer user who has a connection to the Internet. Once incubated within a system, a virus can cause untold destruction to the host computer and its trusted peers. To this end, security administrators should insist on current anti-virus software installed locally on every machine on the network. In a related category, Trojans, engineered for the purpose of establishing unauthorized remote access on a given machine, can be equally devastating to the particular infected host. All reasonable precautions should be taken to guard against the propagation of malicious code. More regulated environments, such as the bank, should consider blocking .exe email file attachments at the firewall, thus shutting down a common means for the spread of a virus at relatively little inconvenience to the user.

The ISP and the University, given their open environments compared to that of the bank, could not likely impose such a measure without cost to their operations. At very least these organizations should educate their users about the spread of viruses and post advisories in response to CERT announcements and make current patches and anti-virus software available. Furthermore, because of the likelihood that these types of institutions will not impose a regulation such as that by the bank and thereby leave themselves more open to virus propagation, they highlight a dynamic to which the security professional must be sensitive: liability. As incomplete as cyberspace law is, it can work just as easily for the security organization as against it, and the failure to take due diligence against the propagation of viruses is a clear example.

User Confidentiality

This subject is of enormous importance to the information security professional in ever context. Law suites seem to lurk at every turn when it comes to deciding on company policy about employee and end user privacy. As always, an elaborate, clearly-stated policy is the best defense in such instances, but the following dynamics are to be considered when drafting that policy:

Email

While it is tempting to promote a secure, trusting corporate environment by stating boldly that employee email communications are not monitored, an organization such as Acme Savings and Trust might find itself in legal difficulty should it have to renege on that policy. As a practical matter, monitoring email is a means of measuring employee efficiency. Should the bank decide that a certain employee may not be producing as expected, it might find tallying that employee's personal emails an effective measure for building a case for the ultimate dismissal of that employee. Furthermore, the content of emails sourced from inside the organization may include sensitive materials that ought to be monitored. The bank will not want to ensure employee privacy to the point that members of the organization will cheerfully distribute delicate financial information to unauthorized parties from company IP space.

The ISP, with regard to employee privacy, has a broader scope to define. That is to say, it is equally important that the ISP develop a reasonable policy as to the privacy of its internal employees as well as a policy about the privacy of its related end users. Law enforcement will often begin the investigation of all types of computer crime with the upstream service provider, and it is crucial that that organization have a firm policy about handling subpoenas and the release of end user account information. It is generally a good idea for the ISP to take a content-neutral stance about the online activity of end users, and leave the judgement of activities to the proper legal authorities. This is a situation that highlights the ambiguous nature of cyberlaw in the definition of what abuse constitutes crime. Frequently the ISP will find itself in the middle of legal issues involving harassment, copyright infringement, death threats, and fraud. The implications of each of these cases are discussed below.

Acme College also will likely want to tailor its security policy around cooperation with law enforcement. The university by definition sets a context in which to encourage experimentation and the flow of ideas, and their policy toward network abuse should reflect that reality. As far as monitoring email, the university, like the other two institutions, will not want to trap itself into a declaration of absolutes when it comes to reading personal emails, but it should be aware that such activity will only very randomly be necessary. Again, here the responsibility of such an organization concentrates on the education of its associated users. The security officers in this situation should make great effort to stress to the rest of the organization the risks associated with sending email across the Internet in plain text and perhaps design a policy around the university's mission statement in regard to acceptable email content.

The Release of User Information

This is a broad category that covers personal information given to an organization by a private party under the assumption that such information will not be redistributed without permission. This is information such as social security numbers, credit card numbers, and bank account information. All of these organizations that find themselves privy to trusted information may be held legally responsible for improperly distributing it. As a general rule of thumb, the ISP and the university should not release any user

information without a subpoena, and that holds true both for cases of relatively minor network abuse as well as much more serious criminal activity.

The ISP should expect to work with law enforcement frequently in the process of investigating and prosecuting computer related crime. The ISP will also work with other ISPs and the general public toward the common goal of promoting general Internet security and eradicating unauthorized activity. However, the ISP must maintain a strict security policy regarding the release of account information and user identity that reflects the elaborate privacy clauses stated in their contracts. They must also attempt to distinguish relatively harmless scans and probes from more serious, and sometimes life threatening network abuse related situations. By maintaining a content-neutral policy, the ISP relieves itself of the responsibility and legal liability of judging what material on the Internet qualifies as a high-severity incident. There are legal definitions of what constitutes libel, harassment, and death threats, and the ISP should not take it upon itself to investigate claims of any of these offenses unless served with a subpoena for customer information. Being too aggressive in the release of information may land the ISP in a law suite over breach of contract.

Non-criminal Abusive Activity

As mentioned earlier, Unsolicited Email and port scanning are two of the most common forms of network abuse. Neither qualifies as criminal activity and neither is covered by formal legislation or legal precedent. However, both constitute annoying drains on an organizations bandwidth and resources, and online service providers have a responsibility to promote efficient, productive use of the Internet and, to the best of their collective ability, to limit the misuse of shared resources. Furthermore, SPAM, taken to an extreme, can result in crashed mail servers and denial of service attacks, and port scanning and OS fingerprinting is a common precursor to more elaborate attacks. However, while the bank can and should establish a strict policy concerning such activity launched by take firm and decisive action against employees who violate it, the university and the ISP, given their respective business models, face a more complex situation.

Network security testing is an important complement to every security policy and yields invaluable information to the security professional. In a relatively isolated environment, such as a bank, where there is no reason for employees to be running scans and intrusion attempts into the host network or outside networks, the company policy can universally condemn such activity and use violations as grounds for the dismissal of an employee. As always, when conducting legitimate tests of company security, the administrator of the test should have written permission from the responsible authority. End users online through the ISP or the university, however, are likely to experiment with such technology as port scanning, and it seems inappropriate to take drastic measures in response to such activity especially if it is only sporadic, isolated instances.

This is a clear example where an institution's security policy must establish an appropriate response to activity which is almost universally condemned by the Internet community, but is not forbidden by law or any formal legislation. At the same time, a

service provider may ultimately end up liable for lack of action taken should an instance of scanning result in a much more serious exploit. To this end, the security team at this institution must keep accurate records of the instances of abuse and strictly enforce their official Terms Of Service or Acceptable Use Policy as grounds to deactivate repeat offenders. In more serious cases of abuse the service provider must have solid guidelines for working with law enforcement toward the goal of efficiently prosecuting such common crimes as fraud, identity theft, and copyright violations. It is a delicate balance that the ISP must maintain in order to comply with outside legal obligations without compromising their customers' privacy.

Current Regulations

Even while the realm of network abuse is not highly regulated, there are currently a handful of laws on the books of which the information security professional must be aware in order to establish a well-prioritized policy. It is important not only to understand the exact implications of the laws themselves, but also to consider the trends that they represent. This is to say that the Internet exists today because of a spirit of cooperation and the free exchange of ideas among a number of dedicated engineers. It is difficult to begin to regulate such a project without compromising those basic objectives. However, it was inevitable that such a means of communication would be compromised by individuals with less noble intentions. Therefore these laws exist not to deter further exploration of Internet technology but to protect users from elaborate criminal activity that takes advantage of that same technology.

One of the most formally regulated sectors of Internet activity is currently that of customer privacy in relation to financial institutions. The Gramm Leach Bliley Act of 1999 has set forth general criteria to which a bank's security policy must apply in order to take all reasonable measures to safeguard customer information. The act defines a number of guidelines on structuring policy across a number of areas including the testing of their information security infrastructure, employee training, and requirements for the upstream ISP. It is thus imperative that the security professional involved in the financial sector, even if he works for the upstream provider and not the bank directly, be intricately familiar with this legislation.

Another law with which the security professional must be familiar is the Computer Fraud and Abuse Act which provides some guidelines for distinguishing between abuse and crime. The information security professional should use this documentation to identify which aspects of the organization will be most at risk for what type of potential crime and how the law will subsequently treat the incident. It is a very useful tool for insight into how the legal community views information technology, and it offers perhaps an opportunity to see trends develop as more laws come into existence surrounding the Internet.

Conclusion

The involvement of the legal community in the handling of computer incidents is still in its infancy and there still exist many gray areas. It is vitally important, however,

that an organization take the time to draft a security policy that reflects an awareness of the trends in law enforcement. The information security professional must be aware that ignoring the legal reality in the industry may lead not only to the inability to prosecute effectively the responsible party after an attack, but also to proactive lawsuits directed at the organization by end users, customers, or employees.

References

Brewer, Wendy. "More Snooping to Come." PC Advisor. 18 May 2001, URL: www.pcadvisor.co.uk/news/display_news.cfm?NewsID=1124

Johnson, David R. "Taking Cyberspace Seriously: Dealing with Obnoxious Messages On the Net." Electronic Frontier Foundation. URL: www.eff.org/pub/Legal/content_regulation_johnson.artic

Foster, Ed. "When Should the Burden of Informing Customers of a Hacker Break-in Begin?" InfoWorld. URL: www.idg.net/ic_530272_1794_9-10000.htm

Frankel, Cathy J. "Perfection of Security Interests in Copyrights." FindLaw. June 1997, URL: http://library.lp.findlaw.com/scripts/getfile.pl?file=/articles_old/msllp/msllp000009.html

Garfinkel, Simson L. "An Introduction to Computer Security for Lawyers." Electronic Frontier Foundation. URL: www.eff.org/pub/Legal/comp_security_legal.artic

Godwin, Mike. "The Law of the Net: Problems and Prospects." Internet World. October 1993, URL: www.eff.org/pub/Legal/law_of_the_net_godwin.artic

Green, Kristine. "How Hard Does the Hack Have to Hurt? An Analysis of the Damage Requirement of the Computer Fraud and Abuse Act, 18 U.S.C. Section 1030." SANS Institute. 9 March 2001, URL: www.sans.org/infosecFAQ/legal/act.htm

Hadden, Arter and Lewis, John B. "Cyberspace Privacy in the Workplace." FindLaw. Summer 2000, URL: http://library.lp.findlaw.com/scripts/getfile.pl?file=/firms/ah/ah000016.htm

Lang, Marion. "Gramm Leach Bliley Act of 1999: What Information Security Professionals Need to Know." 4 April 2001, URL: www.sans.org/infosecFAQ/legal/gramm.htm

Silverglate, Harvey. "The Electronic Frontier and the Bill of Rights." Electronic Frontier Foundation. URL: www.eff.org/pub/Legal/bill_of_rights_online.paper

Staggs, Jimmy. "Computer Security and the Law." SANS Institute. 1 December 2000, URL: www.sans.org/infosecFAQ/legal/law.htm

USA Today Staff. "Hot on the Trail of Virus Writers." USA Today. 7 May 2001, URL: http://www.newsbytes.com/news/01/165374.html

Vijayan, Jaikumar. "IT Security Destined for the Courtroom." ComputerWorld. 21 May 2001, URL: www.computerworld.com/cwi/story/0,1199,NAV47_STO60729,00.htm

Wendt, Carla. "Identity Theft." SANS Institute. 3 May 2000, URL: www.sans.org/infosecFAQ/legal/identity_theft.htm