

Appropriate Response: More Questions Than Answers

Chris Loomis 2001-11-28

Appropriate Response: More Questions Than Answers

by *Chris Loomis*

last updated November 28, 2001

So, just how far should security administrators go to protect their systems? What is an appropriate response to a detected security incident? Ask ten security professionals that question and you will most likely get ten different answers. Ask them more specific questions – such as, how do you handle active intrusions? Denial of service attacks? Probes? - and eventually you will be able to piece together their response set, a collection of reactions tailored to particular attacks or threats.

And once the "response" has been determined, how do we decide what makes a particular response "appropriate" or not? Who decides this? If you ask those same ten security professionals directly, each of them will consider their own responses to be, of course, appropriate. Given this, it should come as no surprise that there is no universally agreed upon set of appropriate responses within the security community. The discussion has been contentious - with two major camps emerging from the crowd - the first I will refer to as the Defenders, and the second, the Digilantes.

Defenders are guided by their organization's written security policy. As the name implies, their primary emphasis is on preventing breaches in the first place. If there is an intrusion, a Defender focuses on containing and eradicating the problem, plugging the security hole and getting back to business. While they may consider notifying the ISPs of attackers or perhaps calling in law enforcement, they will not engage in retaliatory actions directly against attackers for a variety of legal and ethical reasons.

Digilantes, or digital vigilantes, on the other hand, have no qualms about striking back against attackers. While they do everything they can to prevent successful attacks, in the event that one does occur they won't even think about reporting it to the authorities. Instead, they prefer to handle things "in house". To them, virtually all responses can be considered appropriate - as long as they don't get caught. Examples of a digilante response may include a denial of service attack, breaking into the attacking machine and neutralizing it, using a variety of techniques to trace an attack back to its point of origin and, in very extreme cases (which may in most cases

just be cyber-folklore), visiting that physical location to have a "chat" with the suspected attacker.

Causes of the Schism

So, why the striking divergence of attitudes and approaches? Throughout history, vigilante behavior has emerged to fill a real or perceived inability of conventional law enforcement agencies to adequately and effectively enforce the law. Today this void is, unfortunately, quite real. The inability of law enforcement to successfully combat cybercrime is well documented. The U.S. General Accounting Office recently released a scathing report on the NIPC (National Infrastructure Protection Center), the government's lead cybercrime-fighting agency. While the GAO found too many deficiencies to mention, the general conclusion of the report was that the NIPC has "been impeded by the lack of a comprehensive, government-wide data collection framework for identifying imminent computer-based attacks. Further, the NIPC faces other barriers in issuing timely warnings, including a shortage of skilled staff, avoiding undue alarm for insignificant incidents, and ensuring that sensitive information is protected" (see "[Significant Challenges in Developing National Capabilities](#)".)

Governmental cybercrime-fighters won't find a lot of fans amongst the private sector security community either. A recent CIO Magazine poll of 450 chief information officers reveals that only six percent of them believe that existing law enforcement divisions (local and state police, FBI, Secret Service, etc.) are equipped to manage cybercrime (see "[CIOs Say Law Enforcement Can't Hack It When It Comes To Hackers](#)".)

Law enforcement is not entirely to blame for the sad state of cybersecurity. After all, they can only enforce the laws that are on the books. Because of our rapid transformation into an interconnected world, the established body of case law pertaining to cybercrime is still rather sparse. Judges are forced to try to apply outdated precedents to contemporary cases since lawmakers, discouraged by the sheer complexity of the issues, have been hesitant to jump into the fray and pass new laws. Instead, those lawmakers are content to stand back and do little, waiting (and waiting...) until the "dueling experts" are able to achieve something resembling consensus on the key issues.

From the point of view of law enforcement, part of the blame may also lie with the private sector itself. Law enforcement agencies need the cooperation and case referrals from the companies they are meant to protect. However, companies are reluctant to enlist the aid of law

enforcement for several reasons: they lose control of the investigation, expose themselves to a potential public relations nightmare and, in the case of publicly traded companies, invoke the wrath of their shareholders. The bottom line is that the private sector needs to be able to trust law enforcement - but law enforcement needs to earn that trust. This may take some time.

Digilantes

Digilantes are tired of waiting. To them, we are years away from a legitimate cybersecurity effort. Law enforcement is simply out of its depth. Agencies are overworked, understaffed and underfunded. In addition, until the government can compete with the private sector in terms of compensation, they will not be able to attract the kind of expertise necessary in order to effectively combat cybercrime. Because of this, Digilantes feel compelled to take matters into their own hands. They contend that you can't reason with attackers and you can't coddle them - the only language they understand is force. Attackers search for weak victims. Digilantes feel that if you make it clear to them that you are a formidable foe, the attackers will look elsewhere. This approach can backfire, however, if an admin gets into a shooting match with an attacker who is determined to make it clear that he is the formidable foe.

One of the strongest criticisms of the Digilante approach is that innocent bystanders may get caught in the crossfire, stressing that, "when you strike back - you don't really know who you are hitting." However, Digilantes feel that on the Internet there is no such thing as innocent bystanders - just ignorant bystanders. Digilantes feel that they have a right to defend themselves from whoever is attacking them. If you are going to put a system on the Net without properly securing it and that system ends up being compromised and used in an attack, too bad if you get caught in the crossfire. You have a fundamental responsibility to ensure that your system isn't used to attack others.

Perhaps the biggest problem with digilantism is that it is *usually illegal*. I say usually because the security community has received mixed signals from law enforcement regarding what is and isn't acceptable - and what laws will and won't be enforced. Winn Schwartau, President of Interpact and founder of Web security service [Infowar.com](http://infowar.com), points out an interesting dichotomy. "If you ask (a law enforcement officer) what the official position of their agency is concerning vigilante behavior, their response will be that they will investigate, pursue and prosecute it as they would any other crime". Off the record, however, they don't object to digilantism as long as you "make sure that you have the right guy, have deniability and don't put their agency in a situation where they have to enforce the official position". However, this

should not be construed to mean that people who are caught committing illegal acts are somehow above the law: an illegal act is an illegal act, whether perpetrated by a criminal or in the name of vigilante justice.

How prevalent is Digilante behavior? This is difficult to gauge, considering that it's not something that an organization usually wants to discuss. There have been some studies done in an attempt to quantify the attitudes of security professionals (see Schwartau's book - Cybershock). Even so, it is difficult to discern if organizations are actually engaging in digilantism or are just talking tough in an effort to deter attacks. Regardless of what the numbers are, digilantism will continue to exist as a viable option for many in the security community until they can get some legal clarification, some ethical guidance and until law enforcement improves on its dismal record in cyberspace.

Defenders

It's not that Defenders don't understand or experience the same frustrations that Digilantes do; it's just that they don't think that retaliation is a particularly effective approach - especially if we are looking for long-term solutions. There isn't any evidence that digilantism has any appreciable deterrent effect. Take out an attacker's zombies and he'll get more. Take out an attacker and he'll be back - and more determined. Computer security professionals have an obligation to uphold the highest ethical and legal standards - digilantism is neither ethical nor legal. Also, when you attack an attacker, you are assuming a risk for your organization that you are most likely not authorized to assume. Defenders repeatedly assert that they have yet to see one written security policy that advocates digilantism as a viable incident response option. (Perhaps this is an unfair argument - for it would obviously be foolish for an organization to put such a policy in writing.)

Defenders don't get mired down in ethical or legal grey areas; for them, the emphasis is on securing their systems and educating the users of those systems. This is a sound strategy regardless of where you fall along the appropriate response spectrum. With threats of legal action against those that fail to adequately protect their systems on the horizon, organizations need to commit the resources necessary to get their systems secured before claims of negligence and failure to perform due diligence start flying.

Defenders are not naïve, they are well aware that all is not well in the security field. Stephen Northcutt, Director of the SANS GIAC Training Program, understands the shortcomings of our

current approaches. "Clearly we lost a lot of ground to attackers in 2001. One way that I can see for us to stem the tide is to apply deterrence. One possibility is to increase the number of civil suits - when you get attacked, sue the individual". Obviously, the major roadblock with this approach is determining the actual source of the attacks.

Circle Group Internet was able to do just that after discovering that an attacker had sent over four million pornographic spam e-mails from their systems. Their investigative team was able to track the offender back through several layers of ISPs and servers. Once they had successfully identified the culprit, they sued the attacker and were able to collect a monetary settlement. Not every organization is able to muster the resources necessary to pull off this type of investigation and civil action. An attractive alternative may be to contract out the investigation to a private computer security firm. Once all of the evidence is gathered and analyzed by the firm, the victim organization can decide what they want to do next.

Before any attacks occur, it is critical that an organization map out its response strategy. This includes defining the specific policies and procedures it will employ to counter any anticipated types of attack. However, they need to know their limitations. Tom Perrine, Security Manager for the San Diego Supercomputer Center, points out that organizations need to find a balance between going it alone and calling in the cavalry. "It is important to follow your own policies and do, at least, the beginnings of your own investigations. But in many cases, you will need to bring in law enforcement. Anything else is not being a good Net citizen."

Striking the Balance

So where do you stand? If you're like most people, you find yourself somewhere between the extremes of the Defender and the Digilante. There is no definitive answer – organizations will need to evaluate their particular situation and make their own decisions accordingly. For a moment, though, let's get back to basics. Whether you're talking about defensive actions or offensive actions, computer security is, at its heart, about managing risks. Failure to properly manage those risks may have adverse and unintended consequences.

I am optimistic that law enforcement efforts will eventually come around, but the security community shouldn't kid itself into believing that when that happens then our all of cybersecurity problems will be solved. While the Defender vs. Digilante debate is an important one; we must recognize that each approach is borne out of a much greater concern. Inadequate computer security is a systemic, multi-dimensional problem. Therefore, we need systemic,

multi-dimensional answers (I know, easy for me to say).

While I admit that this article poses more questions than it delivers answers, its true intent is to generate discussion. But not just amongst security professionals. If we are serious about this, then we will need to get all of the players involved - industry leaders, software vendors, ISPs, law enforcement, government, etc. Then, and only then, will we be able to formulate and implement the kinds of solutions that truly address the root causes of our security problems.

[Privacy Statement](#)

Copyright 2006, SecurityFocus