Global Information Assurance Certification Paper

Finding the Fine Line – Taking an Active Defense Posture in Cyberspace without Breaking the Law or Ruining an Enterprise's Reputation

GIAC (GLEG) Gold Certification

Author: Christopher Jarko, csjarko@yahoo.com
Advisor: Manuel Santander
Accepted: February 6, 2016

Template Version September 2014

Abstract

Active cyber defense, referred to in this paper simply as active defense, has become more common in recent years. The definition and legality of active defense varies, ranging from non-intrusive means such as using deception to make a potential attacker believe the network is not worth exploiting, to "hacking back," i.e., direct counterattack against the attacker's computer or network. Before taking an active defense posture, network owners would be well served by engaging in a broader discussion on the legal and policy implications of active defense. Enterprise leaders must assess whether or not the security gained by active defense measures is worth the potential risks, which could include not only legal repercussions but also political risks, as well as negative public perception of the enterprise. Defenders may gain some legal protection by posting warning banners, but this is not a guarantee of safety from legal troubles or bad public relations. With the number of high-profile data breaches seemingly increasing without end, most enterprises can benefit from some degree of active defense while staying within the bounds of the law and on the favorable side of public opinion if they take a deliberate, reasoned approach to the matter.

1. Introduction – Why Active Defense?

The issues discussed in this paper will include the legal and ethical questions raised by the use of active defense to protect computer networks. This begs a very important question: If active defense could be considered illegal or unethical, why use it in the first place? To answer this, the problem must be framed in the context of not using active defense.

1.1. Breaches continue to happen – with increasing frequency

A cursory comparison of the three most recent Verizon Data Breach Investigations Reports shows that the number of confirmed data breaches is climbing at an alarming rate; 622 in 2012, 1,367 in 2013, and 2,122 in 2014 (Verizon Enterprise Services, 2013, 2014, 2015). Other sources tend to confirm the trend shown by Verizon – and give little cause for optimism (Identity Theft Resource Center, 2015). The victims of these breaches are enterprises with dedicated, professional information security staffs, and while it is easy to second-guess their actions with the benefit of hindsight, the vast number of breaches in and of itself reveals how difficult it is to successfully ward off an attack.

1.2. Traditional technical defensive measures have a significant probability of failure

Many of the primary technical security controls used today, such as anti-malware software and intrusion detection systems are highly dependent on signatures, i.e., known characteristics of malicious activity, to detect or prevent an attack. So-called "zero-day" attacks exploit previously unknown weaknesses to attack a target, and therefore no signatures have been developed for these attacks (FireEye, Incorporated, 2016). While broader adoption of secure coding practices would reduce the number of zero-day vulnerabilities, simple human fallibility makes it unlikely they will ever be completely eliminated. A single vulnerability coded into an otherwise secure application is all that is required for an attacker to gain a foothold in a victim's computer or network.

Christopher Jarko, csjarko@yahoo.com

1.3. Senior executives are starting to pay the price for failing to protect critical data

Throughout the vast and growing number of high-profile data breaches reported thus far, there has been surprisingly little in the way of consequences for high-ranking officials at the hands of the shareholders and customers. There have been exceptions, perhaps the most notable being the CEO and CIO of Target following that company's massive breach in 2014 (Hsu, 2014). Nonetheless, boardrooms are starting to demand accountability following costly and embarrassing breaches, and a company (referred to in this paper generically as "the enterprise") may find its financial, legal, and public relations interests better protected by taking a more proactive approach to network security.

1.4. Approaches to Network Defense

1.4.1. Defense in Depth

Perhaps the most widely recommended approach to network defense is *defense in depth*. In his book *Network Security Bible, 2nd Edition,* Dr. Eric Cole defines defense in depth as, "having multiple mechanisms protecting a site." For example, this means not relying exclusively on a firewall or Network Intrusion Detection System (NIDS) to protect the network, but instead having both of these means, most likely in addition to other defenses, such as two-factor authentication and sound security policies like *separation of duties* and *least privilege* (Cole, 2009).

1.4.2. Active Defense

Another approach to network defense is *active defense.* The term active defense (or active cyber defense) lacks a universally accepted definition. The 2011 *Department of Defense Strategy for Operating in Cyberspace* offered the following:

> Active cyber defense is [the Department of Defense's (DoD's)] synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities. It builds on traditional approaches to defending DoD networks and systems, supplementing best practices with new operating concepts. It operates at network speed by using sensors, software, and intelligence to detect and stop malicious activity before it can affect DoD networks and systems. As

> intrusions may not always be stopped at the network boundary, DoD will continue to operate and improve upon its advanced sensors to detect, discover, map, and mitigate malicious activity on DoD networks. (U.S. Department of Defense, 2011)

As lengthy as the above definition is, it is also vague; a threat can be mitigated in any number of ways, such as by updating antivirus malware definitions, or in the case of a government's defense department or ministry, by using kinetic force during time of armed conflict to physically destroy an enemy hacker's infrastructure or even kill the hacker himself. In spite of the fact that commercial enterprises cannot take active defense to the same extreme, many cybersecurity analysts and writers tend to frame active defense in very aggressive terms. Performing a Boolean search on the Internet for "active cyber defense AND hacking back" produces no shortage of responses. For that matter, the term "hacking back" is not clearly defined, either. Beyond the context of "ethical hacking" where network attacks are conducted with the explicit permission of the network owner, such as during a penetration test, "hacking" typically violates state and federal laws, several of which will be discussed later in this paper. (For the purposes of this paper, the term "hacker" refers to *black-hat* hackers, who attack computer networks and systems without permission, usually for personal gain, political motivation, or social status within the black-hat community.)

2. Active Defense - a Spectrum of Assertiveness

This paper will use the three categories of active defense activities (annoyance, attribution, and attack) as defined by John Strand and Paul Asadoorian in their 2013 book *Offensive Countermeasures: The Art of Active Defense*. These categories are not necessarily sequential, but they are increasingly more aggressive, and will be shown to typically have progressively more severe adverse consequences for the enterprise if not undertaken with due care.

Figure 1: Assertiveness Spectrum

2.1. Annoyance

Annoyance activities can be fairly simple, and can be restricted to within the perimeter of the enterprise. Annoyance can be implemented in such a way as to be entirely benign, requiring no specific IT knowledge, or it can be quite elaborate and labor intensive. An example of each follows below.

2.1.1. Annoyance techniques

An enterprise can structure their website uniform resource locators ("URLs") using only numbers to identify subdirectories. While this might seem pointless to the outside observer, it would make a hacker's job of scanning and enumeration more difficult since the web pages most likely to contain valuable data (e.g., the admin login page) would only be represented by a series of numbers ("www.enterprise-website.com/33829/78332") instead of the more customary "www.enterprise-website.com/internal/admin/." Admittedly, this would be a minor annoyance (at best) for most hackers, but it may raise the enterprise's security posture just enough to make it less attractive than some other target. Also, this method comes with no legal risk to the enterprise, since a company can use any naming scheme it chooses for its websites. It could also be implemented in such a way as to be transparent to the website's legitimate visitors, who have no need to access admin pages.

A more disruptive method of annoyance would be to set up a *honeynet* Wi-Fi access point with weak encryption such as Wired Equivalent Privacy (WEP) on a separate and isolated subnet populated with *honeypots*, that is, information systems used to attract attackers, thus giving the network defenders a better opportunity to prevent, detect, or respond to an attack (Cole, 2009). WEP encryption can be defeated very quickly with readily available open source tools such as Aircrack-ng (Aircrack-ng

project, 2015). Annoyance can be brought into play by setting up the access point such that once connected, the hacker is redirected away from valuable information. This can be done by establishing a static route for all traffic leaving the honeypot IP, either to a bogus IP address inside the enterprise, which would quickly be discovered by the attacker, or to an address outside the enterprise's network.

2.1.2. Annoyance benefits to the enterprise

As stated before, annoyance raises the enterprise's overall security posture, making it less of a "low hanging fruit" for a would-be hacker, and encouraging them to look elsewhere for their next victim. Also, of all the principles of active defense, annoyance is probably the easiest to implement, and typically has the least impact on other users' computers. That being the case, it carries the least risk of the three principles, but it is not risk free, as explained below.

2.1.3. Potential problems caused by engaging in annoyance

The honeynet and redirection may protect the enterprise's critical information, but it could also cause problems for the enterprise as well as other networks. These problems could manifest themselves as monetary liability for damages suffered by a third party. Taking the redirection example further, if the hacker then attacks the website he was redirected to by the honeynet, the enterprise could be held liable for hosting the *hop point* used to attack the innocent website. Since the access point was a honeynet, which by definition was set up for the express purpose of attracting hackers, it would be difficult for the enterprise to claim it did not know a hacker would use the access point, or that there was no foreseeable chance a hacker might use the access point to attack another network.

Civil liability is not the only possible negative effect for the enterprise; there is also the possibility of damage to the enterprise's brand. In all likelihood, the redirection tactic in the scenario above would not sit well with the public, either. After all, the website that was eventually hacked was an innocent bystander and only became the hacker's target as a direct result of the first enterprise's WEP access point and redirection. While the desire to deflect a hacker's efforts is understandable, the

enterprise's attitude could be easily interpreted by the public as "Better you than me," which has a decidedly unsympathetic ring to it.

2.1.4. Reducing the likelihood of problems caused by engaging in annoyance

On the other hand, the enterprise can take steps to avoid these problems in the first place. Establishing the honeynet in such a way as to ensure would-be attackers are not automatically set upon someone else's network or website would clearly show the public or any law enforcement authorities that the enterprise is appreciative of its place in the Internet and intends no harm to its neighbors. Also, the enterprise can post warning banners at its network boundaries advising users that accessing their network resources makes them subject to monitoring, deception, redirection, or any number of other reasonable defensive measures. While it is extremely unlikely such a banner will deter attempts at unauthorized access, warning banners are a manifestation of transparency by the enterprise.

Another means of avoiding civil liability and brand damage is to consider *proportionality* when engaging in any aspect of active defense, to include annoyance. This means that the effect on the attacker's system must be proportional to the effect desired by the enterprise. For example, if the enterprise wants to set up a honeynet to trap and redirect an attacker, the redirection should be done in such a way as not to cause harm to a third party.

Finally, the enterprise can reduce liability and brand damage through extensive documentation of its active defense. Documentation can be used by the enterprise to show the intent behind the use of active defense, and to provide a sense of transparency with regards to its actions. Documentation and transparency are critical when using any active defense measures, and will be discussed in greater detail throughout the remainder of this paper.

2.2. Attribution

Attribution refers to the identification of the party or parties responsible for a specific action. In cyberspace, attribution can be very difficult; since hacking is illegal, hackers typically use various means to obscure the origination point of their activities. At

the strategic level, hackers are backed by the resources of a nation-state (commonly referred to as advanced persistent threats, or "APTs"), and attribution is typically made based on commonality of tactics, techniques, and procedures (TTPs). Attacks by APTs are not tied to a specific individual, but rather to so-called "threat actors," who are grouped under a code name such as "The Darkhotel Group" (Kaspersky Lab, 2014).

That being said, most enterprises are not targeted by APTs, and at this lower level, sometimes the attribution takes care of itself when the attacker's ego gets the better of him. There have been cases where hackers have executed a technically skillful attack, only to be caught because they bragged about it in a chat room or other forum that was being monitored by law enforcement authorities (Fogarty, 2011). On most occasions, however, attribution only comes after extensive cyber forensics, if at all.

2.2.1. Attribution techniques

Attribution typically requires either extensive observation to determine the attacker's behavior profile, or the use of technical means to trace the attack back to the point of origin. Attribution through behavior profiling is beyond the means of most enterprises (Strand & Asadoorian, 2013). Technical means for attribution often involves using network traffic analysis to watch the data flow from the enterprise in order to try to determine the ultimate source of the attack. Network defenders can use tools like Wireshark to map the path between computer hosts and conduct packet analysis of the data traversing the network perimeter. Wireshark has a highly customizable graphical user interface (GUI) which can be set up to filter specific conversations and IP addresses, allowing security analysts to quickly identify traffic leaving the network towards suspicious IP addresses (Chappell, 2013). A new tool for attribution is available that can turn a document or file into a form of honeypot: *web bugs*, special code embedded in a file that "beacons" its location back to its point of origin (Strand & Asadoorian, 2013).

2.2.2. Attribution benefits

So why should an enterprise bother with attribution in the first place? For some enterprises, it may not be worth the effort (or within their means) to conduct an in-depth forensic investigation themselves. Rather, once the incident handling is complete, the enterprise can turn over the evidence they obtained during the incident handling process

to the authorities, and let law enforcement deal with it. This is fine, assuming the local authorities have the capability and capacity to investigate the incident to the point of attribution, which may not be a valid assumption. If the authorities are incapable of attributing the attack (whether due to a shortage of requisite skills or an excess of higher priority cases such as child pornography), the enterprise may still have interest in learning the source of the attack in order to pursue legal action in civil court. Accordingly, the burden of attribution must then fall back upon the resources of the enterprise.

Some enterprises inherently have a greater interest in attribution. One example of this is when the data breach involves the theft of intellectual property such as *trade secrets,* which for some enterprises may represent the majority of their critical data. A trade secret is information that derives independent economic value from not being generally known to other persons who can obtain economic value from its disclosure or use, and is the subject of reasonable efforts to keep it secret (Uniform Law Commission, 1985). Trade secrets are not the same as *patents* (which protect an inventor's right to make, use, sell, or offer to sell an invention) or *copyrights* (which protect an author's particular expression of an idea), but are still widely protected, at least within the United States. The Uniform Trade Secrets Act (UTSA) was drafted by the Uniform Law Commission in 1979 and amended in 1985. As of December, 2015, the UTSA has been adopted in 47 states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands (Uniform Law Commission, 2015). Going back to the issue of active defense, legal protection is of little help unless the source of the trade secret theft can be attributed to a specific actor, giving the enterprise a target for civil suit.

2.2.3. Potential problems caused by engaging in attribution

But can the enterprise conduct attribution without exposing itself and its leadership to civil and criminal liability as well as damage to its brand? It appears the answer is "no," at least to some extent. As stated earlier, attribution typically involves using technical means to monitor the attacker's transmissions. Enterprises need to exercise caution here. First, use of these technical means may be a violation of the Acceptable Use Policy (AUP) established by their Internet Service Provider (ISP). Violating the AUP can have very negative consequences for the enterprise should the ISP

detect the violation. For at least one major ISP, these consequences can include immediate disconnection or suspension of Internet services (Cox Communications, Inc., 2012). For an enterprise dependent upon Internet connectivity for its revenue, the cost can potentially be higher than if the attack had simply been allowed to happen in the first place.

From a legal perspective, the actions taken by the enterprise to attribute the attack may violate various laws, perhaps the most relevant being the Wiretap Act. The Wiretap Act (18 U.S.C. §§ 2510-22, also known as "The Act," or "Title III of the Omnibus Crime Control and Safe Streets Act of 1968") was written before the advent of the Internet, and was amended to include electronic communications in 1986 under the Electronic Communications Privacy Act (ECPA). The Wiretap Act is a complex law that sets the minimum privacy protections in the United States; state laws may give greater protection than the Wiretap Act, but not less. In general terms, The Act prohibits unlawful interception of wire, oral, or electronic communications. Unfortunately, The Act is not clear on exactly what constitutes unlawful interception within the context of active defense. The Act prohibits "nonconsensual" interception, but only one party's consent is required (U.S. Department of Justice, 2013). This would tend to relieve the enterprise of legal liability, but then the various state laws come into play. As discussed above, states may be more restrictive than the federal law, and some states (such as Pennsylvania) have done just that. In Pennsylvania, with certain exceptions made for law enforcement, *both parties* must give consent to the interception. Since the hacker presumably would not be willing to do so, interception and monitoring would put the enterprise in violation of the law, at least at the state level (Pennsylvania General Assembly, 1978).

Civil liability to the enterprise is very unlikely since a hacker probably would not sue, but there could be criminal liability against the enterprise (and perhaps those individuals who authorized the interception). Also, evidence obtained illegally is typically inadmissible in court, thereby making it much more difficult for the enterprise to sue the hacker, if the attribution activities were ruled illegal by the court. Since the enterprise would not know initially where the hacker is located, the enterprise accepts risk with its actions.

Christopher Jarko, csjarko@yahoo.com

The last consideration for enterprises considering attribution activities is how their activities might appear to the public, particularly with regards to transparency. While the term transparency usually refers to openness on the part of the party initiating communication, it also presumes understanding on the part of the party receiving the communication. This is important when taking into consideration the technical means for attribution. To any observer not familiar with network operations or how data moves across the Internet, these actions can all appear quite sinister, despite the fact that with the exception of web bugs, they are all routine operations for network administrators and security analysts. Unfortunately, most of the public at large is unfamiliar with computer networking and how data moves across the Internet. With the exception of IT industry journalists, the news media who would report the story is probably no better educated than the general public. In all likelihood, the public would be suspicious and mistrustful of the enterprise's actions, which they do not understand; this impression would not be helped by media sensationalizing alleged "hacking" by a white-hat enterprise.

2.2.4. Reducing the likelihood of problems caused by engaging in attribution

Before engaging in attribution, enterprises should start by reviewing their ISP's AUP and other policies as applicable. If the tools and techniques the enterprise would use are not permitted by the policy, the enterprise should engage the ISP in order to find a solution. If the enterprise can show a credible threat or evidence of previous breach attempts, the ISP may be willing to work with the enterprise to either allow attribution or to conduct the attribution themselves. After all, the ISP must also consider its own reputation and responsibility. If it later becomes known that the ISP prevented one of their customers from taking reasonable defensive actions, the ISP's public image would certainly suffer.

Once the path has been cleared with the ISP, a thorough review of federal and state law is in order. Obviously, the enterprise cannot predict where the next attack will come from, but a general survey conducted with the help of their legal counsel can help shape the methods and procedures used for attribution. An understanding of applicable international law is useful here as well. Again, there is no way to predict which foreign

country will be involved, and it is impossible to have a thorough understanding of every foreign counter surveillance statute, but the enterprise could limit its study to nations most likely to be the source of the attack, as reported by threat intelligence companies or government agencies.

Once the enterprise decides to use attribution as part of its active defense posture, it should be thoroughly documented in information security policy. This policy should be used to guide all attribution activities before they happen, and can be used later in court as evidence of transparency should the enterprise face legal action.

Another benefit of codifying and following a written policy is to ensure attribution does not evolve into attack, which carries greater risk and may not be what the enterprise intended. If the enterprise uses software that actually transits into the hacker's computer, the enterprise must ensure access to the hacker's computer is limited to the minimum amount needed to attribute the source of the attack and no more. This keeps the enterprise's actions in line with its policies.

If an enterprise detects an attempted or successful breach and attributes the attack to a specific source, the enterprise must use discretion as to what to do with the information gained by the attribution. Regardless of how confident the enterprise is in its attribution, public "shaming" of alleged hackers should be avoided, as this publicity does nothing to further the security of the enterprise's information, and may bring into play a host of other laws concerning defamation of character and violation of privacy. Moreover, a large enterprise singling out an individual hacker may find itself portrayed as a bully by the media. Should such an issue become public, the enterprise should engage the public through the media – not to point a finger at a specific individual, but rather to explain the reasoning behind conducting attribution in the first place – to protect its critical information.

2.3. Attack

Attack, as the name implies, refers to causing adverse effects on a hacker's computer. By nearly any definition of active defense, this is truly "hacking back." Attacking a hacker is a very risky proposition for the enterprise, since there is little in the way of case law to support an enterprise's right to take such actions. Even staunch

advocates for active defense such as Strand and Asadoorian urge caution and consultation with lawyers prior to attacking a hacker's computer or network (2013). The ability to conduct attack requires precise and correct attribution; if the enterprise intentionally causes harm to a party later determined to be innocent, there will be little to no protection from civil or criminal liability for the enterprise, and the enterprise's actions almost certainly will not sit well with the public.

2.3.1. Attack techniques

Attack techniques within the context of active defense come in many forms. For example, if a data breach is conducted with the intent of publicizing embarrassing or sensitive data, the enterprise could conduct a Denial of Service (DoS) or Distributed Denial of Service (DDoS) attack on the server hosting the website where the data is being dumped. Some sources have alleged that Sony Pictures did just this in 2014 following its massive breach in November of that year (Murphy, 2014).

Other means are more technically sophisticated, and may be perceived as more sinister by law enforcement agencies and the public at large. One such means would be to modify a piece of software used for beaconing and attribution such that it causes damage to the hacker's computer or exfiltrates data unrelated to the original attack on the enterprise. Another means would be to access the hacker's computer using traditional hacking techniques, such as phishing or exploiting other known vulnerabilities in the hacker's system.

2.3.2. Attack benefits

Attacking a hacker's computer would probably give a feeling of satisfaction or even justice to the enterprise that had just been breached, but this feeling of righteousness does nothing for the security of the enterprise's data, and therefore should not be used as justification. On the other hand, preventing the public release of sensitive information by conducting a DDoS against the appropriate server, does in fact protect the enterprise's data from release to individuals not authorized to receive it. In a more extreme example, if an enterprise's infrastructure is used not to move information, but rather to operate industrial control systems such as a hydroelectric dam, a hacker could do much worse than steal credit card information or disclose embarrassing E-mails. In theory, the hacker

could cause billions of dollars in damage or even the loss of life due to a massive flood. If such a scenario is plausible, what options does the enterprise have? Actions taken after the flood will mean little to those impacted, and yet that enterprise has nowhere else to turn for support during an imminent crisis. The enterprise must weigh the risk of relying upon defense in depth against the myriad risks of attacking another computer, even if the attribution was correct.

2.3.3. Potential problems caused by attacking a hacker

As with attribution, the enterprise's problems may begin with consequences for violating their ISP's AUP. The acceptable use policies of Cox Communications, Centurylink/Qwest, Time Warner, and Verizon all prohibit activities which violate or circumvent the security or function of other computers or networks (2016). To date, ISPs are generally not liable for the actions of their subscribers, but a recent court ruling may indicate be the start of a new trend. On December 17, 2015, a federal jury in Virginia ordered Cox Communications to pay $25 million to BMG Rights Management for digital media piracy allegedly conducted by some of Cox's Internet service subscribers (BMG Rights Management (US) LLC v. Cox Communications, Inc., and Coxcom, LLC, 2015). In court, Cox had sought protection under a "safe harbor" of the Digital Millennium Copyright Act (DMCA), specifically where the ISP is merely the conduit for data transmission and does not otherwise contribute to the copyright infringement. In a separate memorandum opinion handed down two days prior to the jury verdict, the judge ruled against Cox on the grounds that it had not met the conditions necessary to claim safe harbor.

In his ruling, Judge Liam O'Connor found that Cox had failed to adopt and reasonably implement a policy whereby repeat copyright infringers' Internet service is terminated (BMG Rights Management (US) LLC, and Round Hill Music LP v. Cox Communications, Inc., and Coxcom LLC, 2015). Judge O'Connor's ruling was largely based on internal Cox E-mails documenting that enterprise's reinstatement of subscribers known to be engaged in media piracy. In one instance, Jason Zabek, Cox's Manager of Customer Abuse Operations addressed the reinstatement of a subscriber terminated *twice in one year* for copyright infringement, telling a Cox representative, "It is fine. We need

the customers." In another E-mail, Zabek wrote, "DMCA does not hurt the network like DOS attack, spam or hacking. It is not something we advertise however" (Mullin, 2015).

While the Cox case revolves around copyright infringement and not hacking *per se*, it is worth watching to see if this truly is the beginning of a trend where ISPs are much more sensitive to the possibility of a hefty monetary judgment against them as a result of their subscribers' actions. As a side note, Cox offers an important lesson for any enterprise with regards to the operation of their networks: If you have a documented policy, enforce it, especially if that policy pertains to the rights or property of others.

Of course, doing so makes active defense more difficult for the enterprise, or at least the attack aspect of active defense. That being said, an enterprise engaged in attacking its hacker will likely have bigger problems than an AUP violation. Attacking a computer is typically a violation of section 1030 of Title 18 of the United States Code (18 U.S.C. § 1030, *et seq.*), also known as The Computer Fraud and Abuse Act (CFAA). The CFAA imposes civil and criminal liability, and its prohibitions include using a computer to commit fraud, unauthorized access, exceeding authorized access, or intentionally causing unauthorized damage to a protected computer. The CFAA's definition of "protected computer" is extremely broad, including any computer "used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States" (Government Publishing Office, 1986). In effect, this encompasses nearly every computer (including smartphones) used to connect to the Internet. In fact, the 2010 Department of Justice manual for prosecuting computer crimes advises U.S. Attorneys that "the statute does not require proof that the defendant also used the Internet to access the computer or used the computer to access the Internet" (U.S. Department of Justice, 2010). The penalties under the CFAA are severe, including hefty fines and up to 10 years imprisonment per count for first offenses (up to 20 years per count for subsequent offenses). It is important to note that there are no provisions in the CFAA granting exceptions for self-defense.

As previously stated, the act of attacking a hacker presupposes attribution, which places the enterprise at risk for violating other federal laws such as the Wiretap Act,

which carry their own penalties in addition to those of the CFAA. And those are just the *federal* laws; many states have enacted their own versions of the CFAA. For example, the Nebraska Computer Crimes Act (Nebraska Revised Statute 28-1341 *et seq.*) imposes criminal penalties for many of the acts covered under the CFAA, albeit with less severity (a maximum of four years imprisonment and two years post-release supervision or twenty-five thousand dollars fine, or both) (Nebraska Legislature, 1991). Like the CFAA, the Nebraska law reveals no provisions for self-defense.

Then there are the laws of other nations. The Internet is inherently global in nature. An enterprise that conducts attack (or perhaps even attribution) activities against a computer or network outside the U.S. will find itself subject to the laws of that country, which could be more strict than American laws. In the case of criminal charges, the question of extradition would have to be resolved based on whether or not the U.S. has an extradition treaty with the country, whether or not the act is considered a crime in the U.S., and ultimately whether or not the U.S. court deems it appropriate (Rubino, 2015). That last condition is significant, as it places the fate of the enterprise (or at least certain enterprise employees) at the mercy of politics. Hypothetically speaking, if political leaders in the U.S. are publicly calling for a crackdown on illegal computer activity (a common event at the time of this writing), it would not bode well for a U.S. enterprise to be accused of criminally attacking a computer in another country, as that would make the U.S. susceptible to accusations of hypocrisy should the request for extradition be denied. Courts are meant to be above politics, but the power of political pressure should be not discounted by any enterprise.

While this paper assumes and strongly recommends that the enterprise will respect the rule of law regardless of a law's country of origin, in point of fact, the enterprise could choose to ignore foreign charges. Extradition for criminal charges seems unlikely. Online searches for relevant case law do not reveal a history in the U.S. of prosecuting enterprises for active defense under the CFAA, making it implausible that a U.S. court would be willing to extradite U.S. citizens to face criminal charges in another country. Still, ignoring the charges brings risk. A U.S. citizen charged or convicted *in absentia* in another country could potentially be arrested years later should they enter that

country, or depending on the circumstances, even certain third-party countries (Fair Trials International, 2013).

With regards to a potential civil action, defending the enterprise from a suit brought in another country could become very complicated. According to the Digital Media Law Project, in order to respond to a foreign claim, an individual [or enterprise] must either "handle the situation yourself, find non-profit legal help, or hire a lawyer in that country" (Digital Media Law Project, 2011). As with foreign criminal charges, ignoring the action *is* an option, provided the enterprise has no assets, employees, or other interests in the country where the suit is filed. Under U.S. law, a judgment handed down by a foreign court cannot be enforced in the U.S. unless the plaintiff also files suit in the United States (U.S. Department of State). Of course, the plaintiff *could* do so, provided they have the financial means. If the plaintiff does file a lawsuit in the U.S. in an attempt to enforce the foreign judgment, the court may look unfavorably upon the enterprise for having ignored the matter overseas, perhaps imputing some degree of arrogance or dishonesty on the enterprise.

The appearance of arrogance or wrongdoing is arguably the greatest risk faced by any enterprise engaging in active defense, especially for an enterprise that goes to the extreme of attacking and damaging a perceived hacker's system. An enterprise that does not appear to be transparent and acting in good faith (not only for itself, but also with regards to its Internet neighbors) will likely pay the price in the form of reduced revenues. If the enterprise is a publicly held corporation, reduced revenues will typically trigger a loss of confidence among its shareholders, which usually leads to lower stock values. Public corporations are also more susceptible to public pressure, as their actions attract more media attention (and therefore provide politicians greater opportunity to be seen taking a stand on cybersecurity). The problem with political pressure is that it often applied publicly, as was the case when the Texas Attorney General upbraided Sony for using spyware to aggressively enforce digital rights management (Texas Attorney General's Office, 2005). Such grandstanding further contributes to a negative public opinion held by a largely uninformed public and amplified by a mostly uninformed media. This leads to a drop in revenues, and the downward spiral gets tighter. All of these factors can be considered as damage to the enterprise's brand. Worst of all, these

public tirades can now be posted on social media sites such as YouTube, where they may remain indefinitely.

Perceptions matter in court, as well. Enterprises that act in such a way as to call their motives into question are likely to be viewed unsympathetically by courts. Given the vagueness of laws such as the CFAA, any enterprise facing a judge or jury is at greater risk if viewed in a negative light. Judges must explain the reasoning behind their decisions, but juries do not; a defendant who is unsympathetic compared to the plaintiff risks being on the wrong side of a verdict with a large monetary award (Manakides & Edmonds, 2015).

2.3.4. Reducing the likelihood of problems caused by attacking a hacker

Since attribution must precede attack, all liabilities listed above for attribution must be mitigated prior to including attack as part of the enterprise's active defense posture. Also, before carrying out an attack, the enterprise must ensure without a doubt that the attribution is correct. If the original hack is attributed to the wrong individual or group and the enterprise subsequently attacks, the enterprise becomes just another hacker.

In addition to the need for certainty with regards to who to attack, proportionality is critical. For clarity's sake, an explanation of proportionality is useful here, and this paper will use one very similar to that of the Law of Armed Conflict. A proportional attack is one that does not cause incidental damage that is excessive in comparison to the intended damage or advantage gained (International Committee of the Red Cross, 2016). In an active defense context, this might mean an enterprise could render a hacker's computer incapable of viewing the particular file type (presumably the files stolen by the hacker). On the other hand, if the enterprise were to destroy the hard drive of every computer host in the same subnet as the hacker, the enterprise's actions would not be proportional.

When moving further along the spectrum from attribution to attack, laws such as the CFAA tend to appear less ambiguous. While the CFAA does not cover beaconing, it does cover DDoS attacks, since DDoS impairs the availability of data (Government Publishing Office, 1986). At this point, the letter of the CFAA puts an enterprise conducting a DDoS to prevent public release of data in the same category as any other

hacker conducting a DDoS. Therefore that enterprise must trust that the court will look favorably upon its intent in conducting the DDoS and weigh that against the perceived intent of the CFAA. Unfortunately, there is no way an enterprise can predict the outcome of that event, and therefore, the enterprise cannot fully mitigate this risk.

With regards to demonstrating intent in such a court case, the enterprise should thoroughly document its policies and plans regarding the use of attack as part of its active defense portfolio. This documentation should include guidance on when to terminate the attack (preferably as soon as the threat of breach is stopped). This shows the court (and possibly the public) that the enterprise is using discretion in the application of potentially destructive cyber force.

Finally, and perhaps most importantly, the enterprise can mitigate the risks of attacking a hacker by having a clear understanding of what constitutes sufficient justification. This justification should use objective means to the maximum extent possible. Is it loss of life? Is it a set amount of financial loss? Is it only to protect the interests of its customers, as opposed to the interests of the employees of the enterprise itself? There are no easy answers to these questions, and the answers will vary from enterprise to enterprise. One thing is certain: an enterprise caught attacking its hacker must be prepared to explain its actions repeatedly.

2.4. Other considerations

2.4.1. Ethics

In addition to legal, political, and brand damage risks, some critics of active defense claim that certain activities are inherently unethical and violate certain standards of professional conduct. In the article, "Cyber Security Active Defense: Playing with Fire or Sound Risk Management," Sean L. Harrington discusses the perceived deceptive qualities of active defense. Since deception is contrary to the Rules of Professional Conduct for attorneys (and perhaps for other professions as well), individuals who authorize active defense on behalf of the enterprise may expose themselves to professional sanctions (Harrington, 2014). If so, this cannot be ignored, but it also begs the question as to whether or not attorneys should be the ones authorizing active defense in the first place. In any use of active defense, coordination with qualified legal

professionals is essential given the extensive risks already laid out in this paper. By definition, lawyers are experts in the law, but network defense should be entrusted to the foremost expert in information security at that particular enterprise. In some instances, that may be a lawyer, and if so, the enterprise should not put that lawyer in a position to compromise the ethical standards of their profession. Otherwise, information security should be informed by expert legal advice, but not necessarily guided exclusively by it.

2.4.2. Escalation

Harrington also makes the claim that active defense invites escalation by the hacker (Harrington, 2014). This may be true; the hacker may either become angered by the enterprise's tactics, or he might decide to rise to the challenge created by the active defense. If so, the enterprise does risk greater harm from the hacker than if active defense had not been used. If the enterprise views this as likely, then they must simply accept the risk that their defensive posture is sufficient.

On the other hand, active defense may have the opposite effect. What if, instead of increasing the intensity of his attack, the hacker looks for an easier target? Unless the original attack was motivated by personal or political factors, the hacker would likely achieve his aims (usually financial gain) by going elsewhere. Also, the hacker reduces his own risk by avoiding enterprises using active defense, since accurate attribution by the enterprise can land the hacker in jail.

Hackers exploit weakness to steal money or other valuables or to humiliate their victims. People who do this on the street are called bullies. There are many potential responses to a bully. One could submit to their demands, flee, respond with violence, or report the incident to the authorities. Each of these responses has been tried, both successfully and unsuccessfully countless times. Ultimately, each enterprise must decide for itself which response is in line with its core beliefs and what is in the best interests of itself and its customers.

2.5. Recommendation

In spite of the risks outlined in this paper, many enterprises can benefit from employing certain aspects of active defense. The choice of how far to take an

enterprise's active defense posture must be accompanied by other actions taken to protect the enterprise's legal status and public reputation.

2.5.1. Words matter – use precise language

Enterprises desiring to employ active defense – and for that matter, the larger information security community – should strive to eliminate the phrase "hacking back" in association with active defense, with the specific exception of attack actions as described above. From an effects standpoint, there is a significant difference between using beaconing to attribute an attack and using a logic bomb or other malware to cause physical or logical damage to an attacker's computer. Is it technically difficult for an enterprise to go from the former to the latter? Perhaps not, but as long as the net result remains different, the terminology used to describe them should be different as well.

Precise language will also be very important should an enterprise's use of active defense become public knowledge, whether as a result of legal action or as a result of public disclosure following a successful or attempted breach. Enterprises engaging in active defense must be ready to conduct active public communications in order to establish the enterprise's intentions as legitimate and to educate the public on active defense.

Using precise language after the fact may not be sufficient to prove the legitimacy of one's intentions. The intent to use active defense must be well documented in advance. This should be done not only with warning banners as described above, but even in company IT policy. For example, an enterprise could have a written policy on active defense scoped for management personnel responsible for defining the enterprise's security posture as well as the IT professionals responsible for implementing the policy. Such a policy could contain language like the following:

Hypergolic Reactions, LLC strives to protect its critical data with an active defense posture. We define active defense as:

Actions taken *in the spirit of transparency* by the enterprise against an attacker for any or all of the following three specific purposes:

1. Strengthening the network and protecting the enterprise's critical data.

2. Attributing the source of an attack to aid law enforcement or other authorities, or to support future legal actions by the enterprise against an attacker.
3. Deterring or preventing repeated attacks by a given attacker in the future.

For the purposes of this policy, our active defense also *specifically excludes* the following:

1. Actions taken for the *sole purpose* of punishing an attacker, whether by publicly "shaming" them or by causing physical damage to their personal property.
2. Actions taken to gather information on an attacker's online activities which do not strengthen the enterprise's network, attribute the source of an attack against the enterprise, or deter or prevent a repeat attack in the future.
3. Actions taken without regard to potential damage to innocent persons or enterprises.
4. Actions taken in deliberate violation of the law.
5. Actions taken which can be reasonably expected to impede law enforcement or other authorities in the performance of their duties.

This policy language not only serves as confirmation of the enterprise's intent prior to the use of active defense, but also can be made public. For example, the web banner warning potential hackers of active defense actions could link to a public facing web page containing the policy language. Also, the enterprise could feature the above policy language prominently on their public website. This could be especially beneficial for enterprises entrusted with a great deal of their customers' sensitive data as many customers may take some degree of reassurance in knowing the steps being taken to protect that data. (On the other hand, some may be put off by such a revelation.)

Christopher Jarko, csjarko@yahoo.com

2.5.2. The spirit of transparency

The sample policy language above makes reference to the "spirit of transparency." As used here, the spirit of transparency does not refer to a complete absence of deception on the part of the enterprise. In fact, many tools and techniques used in active defense such as honeypots are designed to deceive an attacker (Shadowserver Foundation, 2015). Rather, transparency refers to the enterprise's full disclosure of its intentions towards attackers, usually through the use of warning banners.

2.5.3. Use active defense constraints and restraints to stay on the right side of the law and public opinion

The definition above contains three explicit purposes (strengthening the network, attributing attacks, and deterring or preventing future attacks) and five explicit prohibitions (punishing or shaming the attacker, excessive surveillance, disregard for the innocent, breaking the law, and interfering with law enforcement). In military planning terms, the three purposes of active defense can be thought of as *constraints* (things the organization *must* do), while the five prohibitions can be thought of as *restraints* (things the enterprise *must not* do) (U.S. Department of Defense, 2015). The constraints and restraints serve to help keep the enterprise's active defense tactics and techniques within the bounds of the law and on the favorable side of public opinion. This is critical, and difficult, since clear legal boundaries are as lacking as a universally accepted definition of active defense itself. When undertaken with transparency, the three constraints channel the enterprise's activities into areas where laws such as the Copyright Act may lend support to a more aggressive defensive posture (U.S. Copyright Office, 1976). The five restraints, on the other hand, help the enterprise refrain from engaging in activities that are (or could appear to be) malicious or vengeful, whether in the eyes of the court or the public. Intent (either real or apparent) matters; in practical terms, John Strand and Paul Asadoorian admonish enterprises with a simple, yet apt statement: "Don't be evil" (Strand & Asadoorian, 2013).

2.5.4. Work with legal counsel, ISP and law enforcement before an incident happens, and engage the public vigorously afterwards

As demonstrated throughout this paper, taking an active defense posture carries significant risks for any enterprise. Obtaining a complete understanding of those risks is easier if the enterprise engages qualified experts from its own legal department as well as local and federal law enforcement. Working with the ISP can not only help the enterprise understand the limitations placed on active defense, but it may also reveal additional resources to prevent a breach from happening in the first place.

If an enterprise uses active defense to prevent or respond to a breach and it becomes public knowledge, the enterprise should not be bashful about explaining its actions and intentions to the public. An uninformed public may be more likely to accept the first explanation it hears. The enterprise is best served by getting its side of the story out first.

2.5.5. Know thyself

Enterprises are made up of people, each with their own beliefs and values. Any policy, whether related to network defense or not, should be in line with the beliefs and values of the company that enacts it. Beliefs such as the right to self-defense and values such as being a good neighbor must all be taken into consideration and are every bit as important as risks to the company's brand or civil liability.

If the enterprise chooses to engage in active defense, it should understand what its "red lines" are, that is, what actions by a hacker are sufficient to justify an active response. Once these red lines are understood, they should be documented, but not publicly released. One risk of a publicized red line is that it tells the adversary exactly how far they can go without fear of repercussion.

2.5.6. Remember that discretion is the better part of valor

Of all the benefits and hazards to the enterprise that have been presented in this paper, attacking the hacker outright will provide comparatively few benefits compared to the significant chance of civil and criminal liability for the enterprise's leadership. Given that few enterprises will find themselves in a life-or-death situation as a result of a network compromise, it is difficult to see what circumstances would justify causing harm

to another network. To further complicate matters, attribution is difficult, yet it must be perfect in order to conduct the attack. When in doubt, enterprises should avoid attacking their hacker and should instead rely upon well thought out annoyance to prevent further attacks, and attribution to support criminal and civil action against the hacker.

3. Conclusion

Ultimately, traditional network defense is very difficult and has a high likelihood of failure. At this time, law enforcement authorities generally lack the capability and capacity to protect the public from malicious cyber activity. After such a failure, there is often little that can be done to repair the damage. Another approach to defending critical information is active defense, consisting of activities to annoy the hacker, attribute the source of an attack, or attack the hacker's own system. Each of these carries increasingly greater risks ranging from public embarrassment to significant criminal and civil liability. The choice to engage in active defense must be made after careful deliberation by the enterprise with regards to liabilities versus benefits, and ultimately the enterprises' core beliefs and values.

Christopher Jarko, csjarko@yahoo.com

References

Aircrack-ng project. (2015, December 15). Aircrack-ng. Retrieved from Aircrack-ng Web site: http://www.aircrack-ng.org/

BMG Rights Management (US) LLC v. Cox Communications, Inc., and Coxcom, LLC, 1:14-cv-1611 (LO/JFA) (U.S. District Court, Eastern District of Virginia, Alexandria Division December 17, 2015).

BMG Rights Management (US) LLC, and Round Hill Music LP v. Cox Communications, Inc., and Coxcom LLC, 1:14-cv-1611 (U.S. District Court for the Eastern District of Virginia December 15, 2015).

Centurylink/Quest. (2016, January 2). *Qwest's Acceptable Use Policy*. Retrieved from Centurylink Web site: http://www.centurylink.com/aboutus/legal/acceptableuseqwest.html

Chappell, L. (2013). Wireshark 101. San Jose: Protocol Analysis Institute, Inc.

Cole, E. (2009). Network Security Bible, 2nd Edition. Indianapolis: Wiley Publishing, Inc.

Cox Communications, Inc. (2012, October 1). *Cox Business Acceptable Use Policy*. Retrieved from Cox Communications Web site: https://www.cox.com/aboutus/policies/business-acceptable-use-policy.html

Digital Media Law Project. (2011, April 5). *Dealing with Foreign Legal Threats*. Retrieved from Digital Media Law Project Legal Guide: http://www.dmlp.org/legal-guide/dealing-foreign-legal-threats

Fair Trials International. (2013, February). *European Arrest Warrant.* Retrieved from Fair Trials International Web site: https://www.fairtrials.org/wp-content/uploads/EAW-advice-note.pdf

FireEye, Incorporated. (2016, February 2). *What is a Zero-Day Exploit*. Retrieved from FireEye Web site: https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html

Fogarty, K. (2011, October 24). *Core IT*. Retrieved from ITWorld.com: http://www.itworld.com/article/2735940/security/how-hackers-get-caught.html

Government Publishing Office. (1986). 18 U.S.C.§ 1030. Retrieved from Cornell University Law School: https://www.law.cornell.edu/uscode/text/18/1030

Christopher Jarko, csjarko@yahoo.com

Harrington, S. (2014). Cyber Security Active Defense: Playing with Fire or Sound Risk Management. *Richmond Journal of Law and Technology*.

Hsu, T. (2014, May 5). *Target CEO Resigns as Fallout from Data Breach Continues*. Retrieved from Los Angeles Times Web site: http://www.latimes.com/business/la-fi-target-ceo-20140506-story.html

Identity Theft Resource Center. (2015, Dec 26). *Data Breaches*. Retrieved from Identity Theft Resource Center: http://www.idtheftcenter.org/id-theft/data-breaches.html

International Committee of the Red Cross. (2016, January 5). *Rule 14. Proportionality in Attack*. Retrieved from ICRC Customary International Humanitarian Law Web site: https://www.icrc.org/customary-ihl/eng/docs/v1_cha_chapter4_rule14

Kaspersky Lab. (2014, December 11). *Emerging threats in the APT World: Predictions for 2015*. Retrieved from Kaspersky Lab Web Site: http://www.kaspersky.com/about/news/virus/2014/Emerging-Threats-in-the-APT-World-Predictions-for-2015

Manakides, T., & Edmonds, J. (2015). *Curtailing Retroactive Liability Should Fall To Courts.* Retrieved from Gibson Dunn & Crutcher, LLP Web site: http://www.gibsondunn.com/publications/Documents/Manakides-Edmonds-Curtailing-Retroactive-Liability-Should-Fall-To-Courts-Law360-10-20-2015.pdf

Mullin, J. (2015, December 17). *Rightscorp Wins Landmark Ruling, Cox Hit with $25M Verdict in Copyright Case*. Retrieved from Ars Technica: http://arstechnica.com/tech-policy/2015/12/rightscorp-wins-landmark-ruling-cox-hit-with-25m-verdict-in-copyright-case/

Murphy, D. (2014, December 11). *Report: Sony Pictures Attacks Sites Hosting Stolen Data*. Retrieved from PC Mag web site: http://www.pcmag.com/article2/0,2817,2473514,00.asp

Nebraska Legislature. (1991). Nebraska Revised Statute 28-1341 et seq., Nebraska Computer Crimes Act. Nebraska Revised Statutes.

Pennsylvania General Assembly. (1978, October 4). Title 18, Chapter 57, Wiretapping and Electronic Surveillance. Pennsylvania Consolidated Statutes. Harrisburg, Pennsylvania: Pennsylvania.

Christopher Jarko, csjarko@yahoo.com

Rubino, F. E. (2015). *Frequently Asked Questions About International Crime*. Retrieved from Frank A. Rubino, Esq. Web site.

Shadowserver Foundation. (2015, December 25). *What is a Honeypot?* Retrieved from Shadowserver Foundation Web Site: https://www.shadowserver.org/wiki/pmwiki.php/Information/Honeypots

Strand, J., & Asadoorian, P. (2013). *Offensive Countermeasures: The Art of Active Defense.* Rapid City: CreateSpace Independent Publishing Platform; 2 edition.

Texas Attorney General's Office. (2005, November 21). *Attorney General Abbott Brings First Enforcement Action In Nation Against Sony BMG For Spyware Violations*. Retrieved from The Attorney General of Texas - Ken Paxton: https://www.texasattorneygeneral.gov/oagnews/release.php?id=1266

Time Warner Cable Enterprises. (2016, January 2). *Acceptable Use Policy*. Retrieved from Time Warner Cable Enterprises Web site: http://help.twcable.com/twc_misp_aup.html

U.S. Copyright Office. (1976). 17 U.S.C. Washington, D.C.: U.S. Copyright Office.

U.S. Department of Defense. (2011). *Department of Defense Strategy for Operating in Cyberspace.* Washington, D.C.: United States Government.

U.S. Department of Defense. (2015). *Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms.* Washington, D.C.: United States Government.

U.S. Department of Justice. (2010). *Prosecuting Computer Crimes.* Retrieved from U.S. Department of Justice Computer Crime and Intellectual Property Section: http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf

U.S. Department of Justice. (2013, September 19). Title III of The Omnibus Crime Control and Safe Streets Act of 1968 (Wiretap Act). Retrieved from Justice Information Sharing: https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1284

U.S. Department of State. (n.d.). *Enforcement of Judgments*. Retrieved January 3, 2016, from U.S. State Department Bureau of Consular Affairs Web site: http://travel.state.gov/content/travel/en/legal-considerations/judicial/enforcement-of-judgments.html#headerandtext_0

Christopher Jarko, csjarko@yahoo.com

Uniform Law Commission. (1985, August). Uniform Trade Secrets Act (with 1985 Amendments). Minneapolis, Minnesota.

Uniform Law Commission. (2015, December 25). *Legislative Fact Sheet - Trade Secrets Act*. Retrieved from Uniform Law Commission Web site: http://www.uniformlaws.org/LegislativeFactSheet.aspx?title=Trade%20Secrets%20Act

Verizon Enterprise Services. (2013). *2013 Data Breach Investigations Report.* New York City: Verizon Enterprise Services.

Verizon Enterprise Services. (2014). *2014 Data Breach Investigations Report.* New York City: Verizon Enterprise Services.

Verizon Enterprise Services. (2015). *2015 Data Breach Investigations Report.* New York City: Verizon Enterprise Services.

Verizon Enterprise Services. (2016, January 2). *Acceptable Use Policy.* Retrieved from Verizon Enterprise Services Web site: http://www.verizonenterprise.com/terms/aup/

Christopher Jarko, csjarko@yahoo.com