Written Testimony on

Proposed Amendments to the Sentencing Guidelines for The Identity Theft Enforcement and Restitution Act of 2008

Presented by:

Vincent Weafer
Vice President, Security Response

Symantec Corporation
900 Corporate Point
Culver City, CA 90230

Before the:

United States Sentencing Commission

March 17, 2009

INTRODUCTION

Mr. Chairman, members of the Commission, I would like to thank the United States Sentencing Commission for the opportunity to testify today on behalf of Symantec regarding the implementation of Subtitle II of Public Law 110-326, the Identity Theft Enforcement and Restitution Act of 2008.

I commend the Commission for holding this hearing on an issue that is very important to Symantec Corporation. Symantec is the global leader in information security. We provide solutions that assure the security, availability and integrity of our customers' information. Headquartered in Cupertino, California, Symantec employs over 17,000 professionals and has operations in more than 40 countries.

Symantec welcomes the opportunity to provide comments as the Commission continues its important efforts to review and update its sentencing guidelines for identity theft and other serious cyber crime offenses as required by section 209 of the Identity Theft Enforcement and Restitution Act of 2008.

We strongly encourage the Commission to adopt enhanced cyber crime sentencing guidelines and stricter penalties in order to:

1. account for and combat the latest escalating organized cyber crime threat landscape which increasingly includes sophisticated techniques such as the creation of malicious code that targets specific organizations for information that can be used for financial gain; and

2. to help more effectively deter the underlying threat of harm incurred by such data theft and data leakage of personally identifiable information as well as intellectual property;

3. Finally, the majority of internet users continue to be unprotected and more must be done at a legislative and judicial level to provide deterrents and punish offenders in order to encourage more citizens and businesses to engage in online commerce in a trusted environment.

My testimony today will first summarize Symantec's views on defining cyber crimes and our efforts to combat such activities. Second, I will brief you on Symantec's latest assessment of the cyber crime threat landscape. Third, I will highlight the particular findings from Symantec's recent Under Ground Economy Network which describes an online underground economy that has matured into an efficient, global marketplace in which stolen goods and fraud-related services are regularly bought and sold. Fourth, I will outline some of the challenges posed in extending the rule of law into cyberspace as a critical step to create a trustworthy environment for people and businesses. Finally, my testimony concludes with Symantec's recommendations on strengthening cyber crime sentencing guidelines.

SYMANTEC'S BACKGROUND FIGHTING CYBER CRIME

As Vice President of Security Response, I'm responsible for the Symantec Security Response global research teams who research and provide rapid response to the latest Internet security attacks. Our "Global Intelligence Network" consists of over 40,000 sensors monitoring computer activity in 180 countries worldwide. We operate four Security Operations Centers worldwide – in the United States; England; Germany; and Australia. Each provides pre-emptive, managed protection to potential cyber threats 24 hours a day, 365 days a year.

In short, if there is a class of threat on the Internet Symantec knows about it.

We hear about cybercrime, but what exactly is it? The simple answer is complicated! Like traditional crime, cybercrime can take many shapes and can occur nearly anytime or anyplace. Criminals commit cybercrime use a number of methods, depending on their skill-set and their goal. This should not be surprising: cybercrime is, after all, simply 'crime' with some sort of 'computer' or 'cyber' aspect.

The Council of Europe's Cybercrime Treaty uses the term 'cybercrime' to refer to offenses ranging from criminal activity against data to content and copyright infringement [Krone, 2005]. However, others [Zeviar-Geese, 1997-98] suggest that the definition is broader, including activities such as fraud, unauthorized access, child pornography, and cyber stalking. The United Nations Manual on the Prevention and Control of Computer Related Crime includes fraud, forgery, and unauthorized access [United Nations, 1995] in its cybercrime definition.

As you can see from these definitions, cybercrime can cover a very wide range of attacks. Understanding this wide variation in types of cybercrime is important as different types of cybercrime require different approaches to improving your computer safety.

Symantec draws from the many definitions of cybercrime and defines it concisely as *any crime that is committed using a computer or network, or hardware device*. The computer or device may be the agent of the crime, the facilitator of the crime, or the target of the crime. The crime may take place on the computer alone or in addition to other locations. The broad range of cybercrime can be better understood by dividing it into two overall categories, defined for the purpose of Symantec's research as Type I and Type II cybercrime.

Type I cybercrime has the following characteristics:

- It is generally a single event *from the perspective of the victim*. For example, the victim unknowingly downloads a Trojan horse which installs a keystroke logger on his or her machine. Alternatively, the victim might receive an e-mail containing what claims to be a link to known entity, but in reality is a link to a hostile website.

- The introduction of the malicious code or user exploit is generally a single event, but the theft of their identify can be a long drawn out multi stage process, taking hours, weeks, or even years.

  - It is often facilitated by crimeware programs such as keystroke loggers, viruses, rootkits or Trojan horses.

  - Software flaws or vulnerabilities, social engineering sites or scams often provide the foothold for the attacker. For example, criminals controlling a website may take advantage of vulnerability in a Web browser to place a Trojan horse on the victim's computer.

Examples of this type of cybercrime include but are not limited to phishing, theft or manipulation of data or services via hacking or viruses, identity theft, and bank or e-commerce fraud.

Type II cybercrime, at the other end of the spectrum, includes, but is not limited to activities such as cyberstalking and harassment, child predation, extortion, blackmail, stock market manipulation,

complex corporate espionage, and planning or carrying out terrorist activities. The characteristics of Type II cybercrime are:

- It is generally an on-going series of events, involving repeated interactions with the target. For example, the target is contacted in a chat room by someone who, over time, attempts to establish a relationship. Eventually, the criminal exploits the relationship to commit a crime. Or, members of a terrorist cell or criminal organization may use hidden messages to communicate in a public forum to plan activities or discuss money laundering locations, for example.

- It is generally facilitated by programs that do *not* fit into under the classification crimeware. For example, conversations may take place using IM (instant messaging) clients or files may be transferred using FTP.

The technology vendors and security experts also recognize their part in closing the security holes and strengthening the critical infrastructure. Symantec believes the industry has reached an inflection point where more new malicious programs are being created than good programs and is developing a three-pronged approach to the malicious code problem including continuing to use blacklisting to identify high-prevalence malware programs, building a massive white list to identify popular, legitimate programs and allow them to run unhindered, and deploying a novel reputation-based software rating system that can accurately categorize less popular legitimate and malicious files.

Symantec has found a way to harvest reputation information about Web sites and applications from millions of users who opt into the service. The reputation process is completely automated and has been shipping for more than a year to 18 million users' machines.

TODAY'S CYBER CRIME THREAT LANDSCAPE

Over the last two years, an ominous notable change has swept across the Internet. The threat landscape once dominated by the worms and viruses unleashed by irresponsible hackers is now ruled by a new breed of cybercriminals. Cybercrime is motivated by fraud, typified by the bogus emails sent by "phishes" that aim to steal personal information. The tools driving their attacks and fueling the black market are crimeware - bots, Trojan horses, and spyware.

We've made significant headway in containing these sorts of threats but the very nature of the risks we face has also changed. Cybercrime is now the dominating security threat we're seeing today. In the past, cyber attacks were largely designed to destroy data or gain notoriety, but today's attacks are increasingly designed to silently steal data for profit or advantage. Fraud, intelligence gathering and gaining access to vulnerable systems are the motivation behind today's attacks.

How do most of these threats arrive on a consumer's computer? A lot do so through botnets – programs that provide attackers unauthorized and secret control of a computer. Botnets are the engine that drives most of the criminal activity, as they get used by to distribute Spam, Phishing messages, malicious code as well as storage for illegal material. Many of these botnets are created on systems owned by home users, small businesses and even some large corporations.

Symantec releases a bi-annual Internet Security Threat Report or "ISTR" which includes a worldwide analysis of Internet attacks with a review of known threats, vulnerabilities, and security risks.

Symantec's ISTR findings consistently reveal:

- The theft or loss of computers and data-storage devices continues to be the leading cause of data breaches that could lead to identity theft;

- A strong growth in "crimeware," software built with the purpose of committing online scams and stealing information; it includes bots, keystroke loggers, spyware, backdoors, and Trojan horses. 60% of all currently detected malicious codes threats were detected in 2008 and indicates that malicious code is reaching epidemic proportions

- Attackers are focusing not just on the end users systems via exploitable browser vulnerabilities, but also on weaknesses in the web servers and web applications. The majority of vulnerabilities continue to be easily exploitable and require little or no advanced skills for an attacker to take advantage of;

- The majority of brands used in phishing attacks continues to target financial services which also accounts for the highest volume of phishing lures indicating that the cybercriminals are attempting to leverage the current economic crisis;

- Bots are also contributing to the rise in cybercrime threats with the United States having the highest percentage of bot command-and-control servers worldwide. The daily average of active bot infected computers rose nearly thirty-one percent in 2008 and botnets were responsible for the vast majority of spam being distributed;

- There has been an increase in modular malicious code, which initially possesses limited functionality but is designed to update itself with new, more damaging capabilities. The majority of these threats are threats to confidential information which in turn are sold on the Underground Economy. Stolen credit card information continues to be the most advertised item for sale on the Underground Economy.

A BOOMING UNDER GROUND ECONOMY

If confusion still lingers about the health of the online underground economy, a new Symantec report should dispel it. The Symantec Report on the Underground Economy, released in November 2008, characterizes this illicit economy as "booming," adding that it "has matured into an efficient, global marketplace in which stolen goods and fraud-related services are regularly bought and sold, and where the estimated value of goods offered by individual traders is measured in millions of dollars."

The potential value of advertised goods observed by Symantec between July 1, 2007 and June 30, 2008 on underground economy servers was more than $276 million. That figure was determined using the advertised prices of the goods and services, and it indicates how much advertisers would make if they liquidated their inventory.

The Symantec Report on the Underground Economy looks at some of the more notable groups involved in cybercrime activity and examines the major advertisers and most popular goods and services

available. It also includes an overview of the servers and channels that have been identified as hosts for trading, and provides a snapshot of software piracy.

- **Groups and organizations.** Numerous groups and organizations are active in the trade of fraudulent goods and services in the underground economy. The majority of these groups function through Web-based forums devoted to online fraud. And as the report observes, "considerable evidence exists that organized crime is involved in many cases." Although a wide variety of individuals and groups are active in the underground economy, there appears to be some correlation between the level of organization and specific regions. For example, various arrests and indictments of underground economy participants suggest that groups in Russia and Eastern Europe are more organized in their operations, with greater ability to mass-produce physical credit and debit cards. In contrast, groups operating out of North America tend to be loosely organized, often made up of acquaintances who have met in online forums and/or Internet relay chat (IRC) channels and who have chosen to associate with each other.

- **Advertisers on underground economy servers.** During the reporting period, Symantec observed 69,130 distinct active advertisers and 44,321,095 total messages posted to underground forums. The potential value of the total advertised goods for the top 10 most active advertisers was $16.3 million for credit cards and $2 million for bank accounts. Furthermore, the potential worth of the goods advertised by the single most active advertiser identified during the study period was $6.4 million.

- **Goods and services advertised.** Of the categories of goods and services advertised on underground economy servers observed by Symantec, credit card information ranked highest during this reporting period, with 31% of the total. Symantec speculates that credit card information is in such demand because using credit card data fraudulently is relatively easy. Often an online purchase requires only the credit card information. The second most common category advertised was financial accounts at 20% of the total. (While stolen bank account information sells for between $10 and $1,000, the average advertised stolen bank account balance is nearly $40,000.) The third most common category of advertised goods and services for sale was spam and phishing information, with 19% of the total.

- **Value of total advertised goods.** Symantec estimates the value of total advertised goods on observed underground economy servers at over $276 million for the reporting period, with credit card information accounting for 59% of that total. (That's not surprising given that credit card information was the highest priced good in the underground economy.) Symantec researchers add: "Although law enforcement agencies have been concentrating their efforts on arresting and indicting those involved in fraud and identity theft, the global nature of these criminal enterprises increases the difficulty of locating their operations and shutting them down."

- **Servers and channels.** Due to the inherent illegality of the underground economy, the lifespan of its servers is, not surprisingly, relatively brief. According to the report, 98% of underground economy servers have a lifespan of less than six months. North America had the largest number of these servers, hosting 46% of the total.

- **Malicious tools.** Malicious tools enable attackers to gain access to a variety of valuable resources such as identities, credentials, hacked hosts, and other goods and services. Some

malicious tools and services are designed to counter security measures such as antivirus software to increase the lifespan of a malicious code sample in the wild. As the report explains, "The result is a cycle whereby malicious tools must be continuously developed and used to produce other goods and services." The highest priced attack tool during this reporting period was a botnet, which sold for an average of $225. On average, binders were the most expensive malicious code-related good advertised in the underground economy, with an average price of $27. Often called joiners, binders are programs that allow multiple executables to be combined into a single executable file.

- **Pirated software.** During this reporting period, desktop computer games were the most pirated software by a significant margin, accounting for 49% of all file instances observed. As the report observed, "Given the steadily increasing popularity of electronics games, this is not surprising. Retail sales of desktop games reached $9.5 billion in the United States alone in 2007, a 28% increase from 2006. In comparison, retail sales in the United States of software other than games were an estimated $3.3 billion in 2007." The second highest category was for utility applications, while third place was claimed by multimedia productivity applications (such as photo editors, 3D animation editors, HTML editors, etc.).

WHY NEW CYBER CRIME LAWS ARE NEEDED

The growing danger from crimes committed against computers, or against information on computers, is beginning to claim attention by governments worldwide. Undeterred by the prospect of arrest or prosecution, cyber criminals around the world lurk online as an omnipresent menace to the financial health of businesses, to the trust of their customers, and as an emerging threat to nations' security.

Cyber crimes—harmful acts committed from or against a computer or network—differ from most terrestrial crimes in four ways. They are easy to learn how to commit; they require few resources relative to the potential damage caused; they can be committed in a jurisdiction without being physically present in it; and they are often not clearly illegal.

The laws of most countries do not clearly prohibit cyber crimes. Existing terrestrial laws against physical acts of trespass or breaking and entering often do not cover their "virtual" counterparts. Web pages such as the e-commerce sites sometimes hit by widespread, distributed denial of service attacks may not be covered by outdated laws as protected forms of property. New kinds of crimes can fall between the cracks, as the Philippines learned when it attempted to prosecute the perpetrator of the May 2000 Love Bug virus, which caused billions of dollars of damage worldwide

Effective law enforcement is complicated by the transnational nature of cyberspace. Mechanisms of cooperation across national borders to solve and prosecute crimes are complex and slow. Cyber criminals can defy the conventional jurisdictional realms of sovereign nations, originating an attack from almost any computer in the world, passing it across multiple national boundaries, or designing attacks that appear to be originating from foreign sources. Such techniques dramatically increase both the technical and legal complexities of investigating and prosecuting cyber crimes.

Symantec asks the Commission that as you revise cyber crime sentencing guidelines to also take under consideration a behavioral approach that focuses on punishing bad behavior vs. regulating the technology. For example, penalties should criminalize the act of intentionally accessing a computer

without authorization, or intentionally obtaining or transmitting personal information with the intent of injuring or defrauding a person or damaging a computer. Laws should also criminalize activity to intentionally impair the security protections of a computer.

Stronger penalties are needed to punish and deter bad actors who seek to capture information from a users' computer without authorization. We fully support strengthening enforcement measures to go after these increasingly emboldened bad actors. Strengthening enforcement mechanisms is preferable in an environment where hackers and criminals are constantly changing their means of attack.

Penalties in criminal law must also account for innocent unsuspecting users whose computers are sometimes unknowingly taken over by cyber criminals and used as a platform to orchestrate cyber crime on other users' computers which is often the case in botnet herding.

A botnet, or robot network, is a group of networked computers — sometimes called zombies — that have been commandeered, in some instances by criminals, to perpetrate all kinds of online fraud and abuse. Typically a 'bot' is installed on a machine usually through some form of malicious code such as a trojan, an insidious program that can find its way into an insufficiently protected computer in a variety of ways, such as when a user clicks on a link to an infected web page or e-mail message, views an infected document, or runs an infected program. Once the bot has made itself at home, it "opens the doors" of its new host computer to its master, who can instruct the machine to engage in various nefarious activities such as sending out spam and phishing e-mails, or launching the distributed denial of service or DDOS attacks like the kind that almost brought down the internet.

In some cases, these bots can steal personal data and return it to a central site to be used for identity theft purposes. However, in the past few years bots and botnets have been turned into mechanisms that have made web criminals much more efficient — and dangerous.

Bots began to get more sophisticated towards the end of the nineties. People started creating special purpose bots, and selling them to spammers and others. Unfortunately, some abused bots to extort money from websites by launching attacks, for example, against online gambling sites. Back in 2001 and 2002, computer 'worms' were spreading and compromising hundreds of thousands of machines. But back then, the attacker had no control over how the worm behaved once it was released. The main difference between worms and bots is that bots offer a communication channel, and the attacker can send commands, which are then obeyed by all the bots.

By monitoring bot sales on Internet Relay Chat (IRC), we're able to see credit card, bank account and other information going that's been picked up off of these infected machines. Programs like this are becoming increasingly common, because they're extremely lucrative for criminals. Symantec reports that in the last six months of 2007, 68 percent of the Top 50 Malicious Code samples causing potential infections were threats to confidential information. The bottom line is that malicious code, bots and the trade in stolen confidential information has become so pervasive that anyone with a computer and an internet connection is at risk.

Symantec strongly supported the Identity Theft Enforcement and Restitution Act of 2008 in order to combat the pervasive spread of malicious code (bots, keystroke loggers, etc.), which has exploded. Expedited action is particularly needed now because the use of the web as not only a source for attacks but also utilized by criminals for the hosting of malicious code now means that cybercriminals have never had it so better in terms of their ability to have direct access to pools of unsuspecting victims.

Federal statute needs to keep pace with the latest cyber criminal techniques. We believe the Identity Theft and Restitution Act will **a**llow prosecutors to pursue racketeering charges against cybercriminal groups, would expand sentencing guidelines for cybercrime by allowing the forfeiture of property used to commit the crime, and add needed funding to federal agencies efforts to combat cybercrime.

STRONGER AND UPDATED CYBER CRIME SENTENCES ARE NOW REQUIRED

Symantec believes that many Internet users are still unprotected and more must be done at a government level to provide deterrents and punish offenders in order to encourage more citizens and businesses to engage online. It is unconscionable that cyber crime is going unpunished to the degree that it is around the world and governments worldwide must come to grips with the escalating threats.

Governments must have a rule to protect and serve in the digital world. We need to have uniformity, not just in terms of what the laws are but what the punishments are.

Consistently calculating losses from computer intrusions is a difficult endeavor because security incidents are characterized by intangible harms like interference with system availability and interference with the integrity of data. These harms can be difficult to translate into monetary terms. More easily measured are labor and hardware costs associated with repairing and restoring compromised systems, if there is a methodology in place for tracking these expenditures of time and money. Computer crime sentencing should have an accurate method for assessing the cost of attacks develops, since the most important factor in computer crime sentencing under the Federal Sentencing Guidelines is the harm caused by the intruder. Hundreds of computer crime cases are adjudicated in the courts every year, and in each one loss valuation factors into the disposition of the case.

However, criminal law has failed to develop a useful methodology for the accurate and consistent valuation of intrusion losses across incidents and across victims. The statute clearly contemplates that intrusions cause intangible harm by interfering with system and data integrity, but requires courts to define that damage in monetary terms without giving any guidance for how to accomplish that task.

Since the labor costs for investigation and remediation are more readily measured, and specifically mentioned by statute, prosecutors and courts rely on these expenses to prove a federal crime and to sentence. Still, courts must look closely at labor costs, and not take victim assessments at face value. The legal definition of investigation and remediation expenses excludes the forensic activities first responders are taught to take following a computer intrusion. Since the burden of proof for sentencing only requires courts to decide whether the preponderance of evidence shows that the victim has made a reasonable assessment of damages, courts are not motivated to look seriously and critically at victim loss assertions.

For these and other reasons, computer crime adjudications are highly irregular in damage assessment and in offender sentencing. The statute fails to discriminate well between harmful and trivial attacks. This undermines the goals of sentencing, specifically that courts should impose fair, just sentences that reflect the seriousness of the offense and treat like offenders equally.

There are several legal approaches we could adopt to mitigate this problem. However, the question of how to remedy intrusions will remain so long as there is no legal consensus on the nature of the rights and property interests implicated by computer attacks. The Department of Justice is now charging

people by adding up all the potential breaches of the stolen accounts and using that calculate the impact of the crime, so 10,000 accounts at an average of $10k per account is $100m in stolen goods. We encourage the Commission to explore an equivalent way of measuring the impact of compromised identifies and assets i.e. cleanup of an infected computer or network.

RECOMMENDATIONS

Reliance on terrestrial laws is an untested approach. Despite the progress being made in many countries, most countries still rely on standard terrestrial law to prosecute cyber crimes. Many countries are relying on archaic statutes that predate the birth of cyberspace and have not yet been tested in court.

Weak penalties limit deterrence. The weak penalties in most updated criminal statutes provide limited deterrence for crimes that can have large-scale economic and social effects. Tougher fines and criminal sentences are needed to combat today's sophisticated cyber criminal.

Self-protection remains the first line of defense. The general weakness of statutes increases the importance of private sector efforts to develop and adopt strong and efficient technical solutions and management practices for information security.

A global patchwork of laws creates little certainty. Little consensus exists among countries regarding exactly which crimes need to be legislated against. Gaps remain, even in countries that have already taken steps to address cyber crimes. In the networked world, no island is an island. Unless crimes are defined in a similar manner across jurisdictions, coordinated efforts by law enforcement officials to combat cyber crime will be complicated. A globally harmonized framework of legislation against e-crime is needed. Governments around the work need to agree on the definitions of e-crime and of phishing so that attackers from all jurisdictions can be aggressively pursued in the criminal justice system.

A model approach is needed. Most countries, particularly those in the developing world, are seeking a model to follow. These countries recognize the importance of outlawing malicious computer-related acts in a timely manner in order to promote a secure environment for e-commerce. But few have the legal and technical resources necessary to address the complexities of adapting terrestrial criminal statutes to cyberspace. A coordinated, public-private partnership to produce a model approach can help eliminate the potential danger from the inadvertent creation of cyber crime havens.

Thank you for taking our views into consideration.