TESTIMONY OF KEN SILVA
VeriSign, Inc.
before the
HOUSE COMMITTEE ON ENERGY AND COMMERCE
SUBCOMMITTEE ON TELECOMMUNICATIONS AND THE INTERNET
Hearing on "Computer Viruses: The Disease, the Detection, and the Prescription for Protection"
November 6, 2003

Good morning Mr. Chairman and distinguished members of the Subcommittee. My name is Ken Silva and I am Vice President for Networks and Security of VeriSign, headquartered in Mountain View, California.

We at VeriSign are honored to have the opportunity to provide our views on the very important subject of Computer Viruses and how we detect them proliferating across the internet by watching our information networks.

VeriSign is uniquely situated to observe the continuing assaults on our information infrastructure. Our company provides industry-leading technologies in three relatively distinct - yet interrelated - lines of business. Each of the three serves an important role in the rapidly converging infrastructures that support communication and electronic commerce around the globe.

VeriSign's security organization provides encryption, authentication, secure credit card processing, fraud protection and detection, managed network security services and a range of other services that enable e-commerce, e-government and the over-all secure Internet experience that hundreds of millions of users around the globe have come to rely on.

VeriSign's second line of business is our Telecommunications Services group provides the essential signaling and switching services that make today's digital telephony - both wired and cellular - possible. This includes features like call waiting and forwarding, wireless roaming and the soon-to-be available wireless number portability.

Our third major line of business is now known as "naming and directory services," and includes VeriSign's computer infrastructure dedicated to the management of the Domain Name system of the Internet, including our stewardship of the A- and J- root servers - two of the thirteen computers around the globe that represent the top of the pyramid of the Internet's dispersed

hierarchy. This is the part of the infrastructure of the Internet that allows each one of you as you type in www.house.gov into your web browser and be instantly connected to one unique computer from among the hundreds of millions on the network. VeriSign also manages the .COM and .NET top-level domains that for many have come to symbolize the essence of the Internet.

Since 2000, I have had the privilege of serving both Network Solutions and now VeriSign as manager of the resources dedicated to maintaining the security of these complex technology assets. On behalf of VeriSign, I also have the privilege of serving in a number of industry leadership capacities, including representing the company on working groups of the President's National Security Telecommunications Advisory Committee - the "NSTAC", working groups of the NRIC, which advises the Federal Communications Commission, and as a board member of both the Internet Security Alliance and the "IT ISAC" - the Information Technology sector's Information Sharing and Analysis Center.

The proliferation of worms and viruses is costing our nation's companies billions of dollars. Some examples of worm costs are; Klez - $9.5 Billion, Love Bug - $9 billion, Code Red - $2.5 billion, Slammer - $1 Billion, and Sobig.F and Blaster combined were anywhere from $3.5-7 Billion in August alone. This coupled with increasingly costly regulatory compliance is a tremendous burden on our economy and the strength of our industry.

In discussing this topic of the proliferation of worms, viruses and hacking attacks, I want to address three key cyber security myths that exist today. But before I discuss these myths, I'd like to begin first with a picture of what we are seeing on the network from our unique perspective as one of the Internet's stewards.

Today, despite widespread perceptions that Internet-related activity has slowed since the "bubble" burst in March 2000, Internet usage has, in fact, continued to grow at impressive rates. This is best illustrated by the growth in Internet Domain Name Systems' resolutions. VeriSign's data show hat Domain Name resolutions grew by an average 51% between August 2002 and August 2003. Domain Name resolutions for e-mail grew by 245% in the same time period. Currently, VeriSign processes over 10 billion Internet Domain Name queries a day on average, which is more than 3 times the daily volume in 2000.

This growth in Internet usage has been outpaced by increased security and fraud threats, which increasing both in number and complexity. The number of security events per device managed by VeriSign grew on average by 99% just

between May 2003 and August 2003. From a geographical perspective, the United States continued to be the leading source of threats to the internet, accounting for nearly 81% of security events.

The Sobig.F email worm, released in August 2003, provides a clear example of the increase in complexity of security threats. This worm was hard-coded to access the Domain Name System root servers, bypassing the Domain Name servers run by enterprises. As a result, VeriSign recorded a 25-fold increase in peak e-mail related DNS traffic on its roots servers when the worm was active.

We are also seeing that Internet fraud is growing rapidly as well. Data from VeriSign's fraud prevention systems indicate that 6.2% of e-commerce transactions in the United States were potential fraud attempts. Over 52% of fraud attempts originate from outside the United States.

There is increasing evidence of overlap between perpetrators of Internet fraud and security attacks. Analysis of VeriSign's data shows extremely high correlation (47%) between sources of fraud and sources of other security attacks. Attackers who gain control of Internet host machines are using these compromised hosts for both security attacks and fraudulent e-commerce transactions. Let me now explain how there are three myths in our current state of cyber security that must be addressed.

· Myth #1: The real problem on our networks is a proliferation of worms, virus attacks, identity theft or even Spam.

Let me explain this point. The proliferation of worms, viruses, ID theft or even Spam is not the problem. All of these - while each extremely serious - are only symptoms of a much larger problem that we have today of a highly attractive vulnerability across our computer networks. Identity thieves, corporate saboteurs, spammers, and mischievous hackers exploit this vulnerability. That vulnerability must be addressed through changed behaviors, both by users and by Internet infrastructure stewards.

Simply put, we all have a shared responsibility as users to uniformly deploy better security hygiene. Whether we are a large e-commerce dependent business or individuals, we can and should do more. At the most basic level, every individual user can contribute to improve security by taking basic steps toward improved security. These prescriptions are well known and widely distributed - yet far too few actually engage even in the most simple, low-cost and no cost measures such as: using passwords and changing them regularly; using anti-virus software and updating it regularly; patching operating systems;

getting firewalls and using them; and if you have an always on network connection, turn it off when not using it.

These simple, low cost measures are not a prescription for guaranteed network security. But they are easy steps every user can take to increase their own security posture. By doing so, we improve the overall resilience of the network to attacks. Such measures will strengthen the networks weakest links and those exploited by hackers. When taken, these steps to reduce the population of targeted computers a virus can successfully invade.

· MYTH #2: The solution to this problem is to require more rigorous software design to protect individual systems.

Many are tempted today to demonize software vendors and other members of the network community for viruses, worms and attacks. We believe we must resist this temptation. The idea that somehow if only Microsoft made bulletproof operating systems and applications all Internet security problems would evaporate is purely fiction. This type of finger pointing is often misplaced and in most cases does more harm than good. It is all too simple to blame the operating system manufacturer for flawed code or the network providers for not securing their networks. Many of the worm attack not only popular operating systems, but open source software as well.

This second myth of software user culpability is another area of user responsibility at the consumer and commercial level. This area involves what is called "patch management" - a catch phrase to describe the very important act of maintaining current release levels of software and installing and configuring them appropriately. Only in this way with the benefits of discovered, reported and fixed vulnerabilities that have been addressed through software research and development be put to use on the network.

For the networks stewards such as VeriSign, this area is a crucial aspect of an overall cyber security strategy. Over the past few years in a down economy, we have invested tens of millions of dollars in equipment to provide the massive headroom of servers and storage to withstand unexpected attacks of untold dimensions. At the same time, we also have a strong commitment to fundamental innovations that will bring improved, increasingly secure tools to the broad community of network users.

· MYTH #3: The objective is a network so secure that it can withstand the evolving and ever more sophisticated assaults.

The need to achieve an impenetrable network belies the fact that even if we succeed in scaring away many of the most opportunistic exploiters by better and broader deployment of enhanced security tools; there is still the likelihood that some attacks will succeed. To this point, we must heed the words of Julia Allen and other colleagues at the Carnegie Mellon's Software Engineering Institute: the point is not to prevent every attack but is to make sure that no attack succeeds in bringing down the institution. The point is not to be blindly secure, but rather to be thoughtfully survivable.

In the final analysis, all of us must strive for a system of operating principles that means that no attack will succeed in disabling the user or its institution.

We must stop believing that firewalls, intrusion detection systems and log monitoring is adequate security. These are only tools of security. A comprehensive approach that entails those tools, as well as network intelligence on impending or immenent attacks is the only viable solution for success. If we consider this a war on cyber attacks, then we must treat it as such. No military commander would suggest that his troops simply wait in foxholes and return fire when fired upon. They would insist on early warning systems and detailed intelligence about their targets and movements. This is the direction we must head in the war on cyber attacks.

In conclusion, the solutions to our cyber security challenge require three commitments.

First, we must provide incentives to all users to make the investments in hygiene-practices and tools necessary and appropriate to their status on the Internet.

Second, we must provide incentives to infrastructure custodians, such as VeriSign, to maintain the investments in research and development to provide the innovative tools that meet the ever-evolving threat to our networks from the many sources we have heard about today.

Last, we must provide government at the national and international levels with both forensic tools and investigative training and powers to reach those who are attacking our networks, and through those attacks seek to impact our way of life and our opportunity to contribute to better lives around the world.

VeriSign believes that these actions will improve the overall health and well being of the Internet, but none are magic solutions or silver bullets. True long term health and well being of our information systems will take time and

everyone's efforts. Again, this is as much a responsibility of people as it is of technology.

Thank you Mr. Chairman and members of the committee for the opportunity to testify before you today.