TESTIMONY OF DR. WILLIAM HANCOCK
Chairman, Internet Security Alliance
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

Thank you Mr. Chairman. My name is Dr. William Hancock. I am Vice President of Security and Chief Security Officer of Cable & Wireless, a large multinational telecommunications and hosting company. I am Chairman of the National Reliability and Interoperability Council (NRIC) Focus Group 1B, Cybersecurity, a federally authorized council of advisors to the FCC. I am also the Chairman of the Board of the Internet Security Alliance. I appear here today on behalf of the nearly 60 member companies of the Internet Security Alliance.

The Internet Security Alliance was created in April of 2001, six months prior to 9/11 as a collaboration of the Computer Emergency Response Team Coordination Center (CERT/CC) at Carnegie Mellon University and the Electronic Industries Alliance as well as founding membership of well known international companies with high interest in security issues related to Internet commerce.

I am pleased to note that four of the five witnesses before you this morning are members of the IS Alliance. This doesn't surprise me since members of the Alliance engage in a broad range of activities designed to enhance information security not just for themselves but for all of us who make up the world-wide Internet community.

We are an international, inter-industry group of companies dedicated to expanding cyber security through information sharing, best practices, standards development, education and training, public policy development, international outreach to trusted partners and the creation of market-based incentive programs to improve information security.

Among the core beliefs of the IS Alliance are the following:

1. The Internet is primarily owned and operated by private organizations and therefore it is the private sector's responsibility to aggressively secure the Internet.
2. Information security on the Internet is grossly inadequate.
3. A great deal of security enhancements can occur through application of basic technologies and through enhanced education and security awareness.
4. Technology, while critical to security, will not be enough to provide a safe and secure Internet environment.

5. To improve overall cyber security, creative structures, thought and incentives may need to evolve to provide continued security assurance from the home PC to the large corporate network environments.
6. Government is a critical partner, but, ultimately, the industry must shoulder a substantial responsibility and demonstrate leadership in this field if we are to eventually succeed.

As what we in the security business call a "grey beard," I have been a technical expert, "insider" and leader in the development and deployment of networking and security technologies for over 30 years. While such a span of time might tend to make one wax philosophical about viruses and worms, I tend to have a reality-based perspective as an active practitioner of security on one of the largest network infrastructures in the world. When worms and viruses hit infrastructures, to me it's not a statistic where some other company was taken to the pavement: it's often one of my customers where I and my security teams are expected to leap into action and solve the crisis at hand.

As a security practitioner, I saw the technical games that were the genesis of modern computer viral infections. A computer virus is a man-made code component that attacks computer software and causes a variety of debilitating conditions. Most folks in the security community attribute initial virus development as part of a technical game at Bell Labs in the late 1960's called "CPU Wars," where developers of operating systems would deliberately create infestation code and place it on each other's machines. This action typically resulted in machine disruptions, funny messages on screens and other types of computing interruptions. There were strict rules, however – infestations had to be non-propagative, they could not cause destruction, stop applications from executing and they could not execute during normal hours of operations. Infestations had to be removable on demand. The initial purpose of such games and pranks were to learn, creatively, about how operating systems and computers worked and to share discoveries and ideas in a creative way.

Such is not the case today.

Viruses are a main staple of the hacking community as a method of disrupting programs and systems for a variety of purposes. Some virus-writing efforts are for personal motivations to hurt a specific company, product or service. Some are written by skilled programmers with serious social development or emotional problems as a means of self-expression. Other viruses are written by "gangs" of programmers who have a specific political agenda or by those who have a need to express social will. Still other viruses are written by nation-states as part of their cyberwarfare development efforts to debilitate infrastructure in today's modern technology-dependent warfare environments. There are entities that write viruses under contract to attack competitors and their infrastructure. There are disgruntled employees who seek revenge on their former corporate masters. Viruses are written for a wide variety of reasons but are broadly categorized as being written for social dysfunctional reasons or for the purposes of economic disruption.

Viruses do not self-propagate. They attack whatever system upon which they are activated and perform their damage on that system. Some virus writers have gotten creative with the explosive use of email and have devised ways for viruses to be propagated by email programs and systems. While it appears that a virus "moves," the technical reality is that the virus does not self-propagate – it needs assistance from an external program such as e-mail or from a file transfer action to move from system to system. With the worldwide proliferation of email in the last five years, this makes movement of viruses from one system to another painfully trivial.

Viruses have a variety of effects on businesses. Some are just annoying, such as one of the early viruses called "giggle," which caused a PC to play a giggling voice continually through the PC's speakers for hours upon end. Other viruses destroy software at great corporate cost. One disgruntled employee case I worked on some years ago with the FBI involved an individual who was fired for hacking into the human resources system and changing his salary. After being fired, he went home, downloaded a piece of malicious code from an Internet underground hacking site and created a small program that would delete all contents of a user's hard drive. He then created a fake email account on a popular public email site and emailed the virus to all the staff at the company with a notation that the file contained a speech from the company's president and that it was being sent so that employees could hear it. Upon "playing" the file, the virus wiped out the hard drive. 1279 employees were sent the virus – 710 ran the program and their entire systems had to be rebuilt. The overall cost to correct the damage caused by this one virus at this company was almost one million dollars. You can imagine the horrific cost to repair such damage at a large defense contractor, financial institution or manufacturing concern.

Many more malicious and wide-spread viruses are seen "in the wild" on the Internet on a daily basis. Many are written with Russian, Chinese and other languages in comments in their code. Some have direct ties to organized crime, especially outside the US. Many are propagated from commonly known havens for virus writers where there is no fear of legal prosecution or where the technical skills of the government to prosecute are minimal or non-existent. Some estimates are as many as 100 or more computer viruses or their variants are released world-wide on a monthly basis. The costs to protect against viruses and contain them when they hit can easily be quantified world-wide in the billions of dollars.

In 1988, at the genesis of commercial use of the Internet, I was working at NASA's Langley facility as a consultant when the now-famous Morris worm hit the Internet. We all scratched our heads and initially thought there was a network infrastructure problem. What we did not know was that a young student at Cornell University had created a self-replicating program which would move, very rapidly, from computer to computer, attempting to replicate itself as fast as possible throughout all connected computers. Back then, the Internet was small enough that all the major network control area personnel knew each other personally. We could all get on a conference call and discuss what was going on and coordinate a response. It caused such a serious outage of the Internet that many organizations, to include CERT/CC

(represented here today), were founded to serve as an early-warning and solutions service for what was recognized as a new security threat with explosive growth potential. Needless to say, with the estimated 655 million worldwide users of Internet, getting together on a worm attack conference call has become rather problematic.

A worm is typically an autonomous self-propagating program which travels from machine to machine, executing its payload. They do not need the assistance of other standard programs, such as email servers, and can move from system to system using an exploit in a program or protocol. A worm typically consists of a "movement" component, a propagation component and a payload, which may contain nothing at all, self-executing code or a malicious viral infection. Payloads seen in the last couple of years have consisted of a system subversion methodology called a "root kit," where a hacker may later take total control of a system, using standard "known" viruses or defacement tools for automatically defacing websites. For instance, in May 2001, a hacking group that called themselves the Honkers Union of China defaced several hundred thousand websites using a worm that defaced the victim's website with a banner containing the hacker's name. The worm would then rapidly attempt to propagate itself to other sites.

Most worms in today's environment propagate from system to system using known vulnerabilities and attempting to exploit a system based upon those vulnerabilities. In many cases, proper patching against known vulnerabilities or disabling technical components that are not needed for operations would prevent the attack and subsequent propagation of many worms. For instance, on January 25th of this year, a worm called "Slammer" attacked Internet systems via a known vulnerability in a popular database program – one for which the corrective patch had existed for over 7 months. Sites that were patched simply were not affected. Sites that blocked all network entry points for all programs, except those that were open for production programs, with technologies such as firewalls were similarly not affected. Unfortunately, much of the Internet community using the database had not properly applied those patches and they were severely debilitated for almost three days as a result of such negligence.

Some worms have been written to attempt to hurt specific Internet addresses such as whitehouse.gov and software manufacturing companies. Studies of the various types of worms seen in the last two years suggest that some are being used to probe, experiment and test methods in which to infiltrate infrastructures throughout the world. Having reviewed many of them and examined the code personally, it is readily apparent to me that some were written by very professional, highly trained programmers who could have easily done substantially more damage than they did – if they wanted to. When professionally written worms appear, they gain extra attention from within the security community as it usually is an indication that someone very serious about their efforts is setting something up for later use in a more destructive way.

The use of worm-based techniques of propagation, combined with virus development techniques, is causing new problems for companies and consumers alike. A good example is the recent and continuing propagation of the SoBig worm/virus technology that was and is still used by SPAMmers. SoBig and its variants are commonly

used by SPAMmers to distribute a compact email server system to computers which previously did not have such capability. The unwitting victims, such as a broadband cable-connected home PC, are favorite targets of SPAMmers. By doing this, the numbers of email servers capable of sending SPAM to users on any given day has jumped from a couple of hundred thousand or so to several million. This type of technological approach to SPAMming has resulted in an exponential jump in SPAM emails, bandwidth consumption, and overhead (congestion) throughout the Internet.

While most of the uses of viruses and worms are typically malicious or at least inconvenient in today's environment, this will change over time. Worm technologies are currently being viewed as a potential method to distribute critical security patches to systems on networks. Viruses can be used to distribute applications on some modern operating systems. Some countries have introduced legislation to outlaw all use of viruses and worms in all forms. This is a short-sighted and a simplex application of laws to a complex issue as the same technologies are being looked at, very seriously, for use in good – not evil.

With the conditions for development of viruses and worms remaining as-is, I expect the following situations to develop in the near future:

- Infestations of "invisible" infrastructures. Most of us don't think about the software inside a cell phone, automotive electronic system, DVD player, radio frequency ID tag systems, parking lot gate attendant systems, toll booths, wireless luggage bag-to-passenger matching systems, point of sale terminals, automatic door openers, letter sorters, printing presses and many others. As these technologies become more sophisticated, so do their connectivity methods and operating environments. Companies that produce such products migrate towards general-use commercial off-the-shelf (COTS) technologies, which allow greater opportunities for attack.
- Worm, virus and hybrid attacks against communications infrastructures due to lack of security controls in base networking protocols and "building block" protocols such as Abstract Syntax Notation.1 (ASN.1). Much of the communications infrastructure of the world is built on protocol security concepts developed in the 1970's which do not translate well into today's technical security needs.
- Use of viruses and worms by terrorist organizations as a way to deteriorate, disrupt and disable economic and social support systems in use by countries dedicated to anti-terrorist efforts. As horrible and malicious as the various physical attacks have been by terrorists against the United States, those effects are minimal compared to a debilitating attack by a worm against our financial, transport or utility infrastructures.
- Accelerated sponsorship by hostile nation-states where the use of cyber attack is a rapid method of furthering a country's political and economic goals (cyber warfare and information operations methodologies).
- Worms/viruses that "jump" between operating environments and applications. Some have shown this capability already and it's a rapidly growing trend.

While there are many disturbing trends in virus and worm development, there are certain issues which IS Alliance is particularly concerned about:

1. Companies that provide critical services, such as utilities, transport and petrochemical entities are interconnecting historically isolated networks with Internet facilities. This results in such networks being attacked and infested with viruses and worms that cause the networks to become disabled and this can critically affect infrastructure.
2. Home consumer PCs are being increasingly targeted by viruses, worms and hybrids harnessed for use as part of world-wide malicious "chains" of attack systems (known as Zombies) to effect Distributed Denial of Service (DDoS) and worm attacks against Internet connected entities
3. Research and development into new security encodings and methods in base network protocols needs to be accelerated to help offset the continued development of malicious code used to attack infrastructure
4. Lack of law enforcement actions, globally, in the prosecution and arrest of virus and worm developers. An extremely low number of persons involved in the development and distribution of malicious code are ever identified or prosecuted due to a lack of technical tools, skills and personnel in most law enforcement organizations.
5. Inclusion of basic system and application protection methodologies by developers of same. Basic technologies such as polymorphic checksums and cryptographic signature methods are well known and available. Such technologies could be used by all manner of developers to stop infestations and propagation of these malicious code segments.
6. Lack of senior corporate management to act properly, responsibly, rationally and quickly in the deployment of security technologies to prevent infestations and propagation of malicious code. Too many companies still do not invest in the basics.
7. Acknowledgement that viruses and worms are truly a multinational problem. While leadership by technologically advanced countries is crucial, introduction of viruses and worms into network infrastructure is easily done by the "weakest link" in connectivity – a small country with no laws on cybercrime, no assets to protect, and no national will or means to prosecute perpetrators becomes the entry point for the world to be attacked. Remember that access to a small country's infrastructure does not require a physical presence – even a dial-up connection from anywhere on the planet will do just fine.

The "cure" for infestations is a long way off and will require partnership with industry and government to solve. Base research in network security improvements, deployment of security technologies, legislative efforts to prevent criminal use of worms and viruses, improvement in operating systems to stop infestations, application-level security technologies, law enforcement prosecution of cyber criminals involved in the creation and distribution of virus and worm technologies, improvement in base critical

infrastructure and education and training through all levels of corporations, government and society will need to be combined to come up with effective eradication solutions.

Perhaps the most ironic aspect of viruses and worms is not just the cost to repair or prevent infestation - it's not like biological, chemical or nuclear terrorism where thousands or millions of dollars are required to make such an attack happen. It's just the entry cost necessary to create and distribute worms and viruses:

A PC with an Internet connection.

With this, Mr. Chairman, ladies and gentlemen, I conclude my opening remarks. Thank you for your efforts and your leadership in this important topic.