# Testimony of Alan Paller
# Director of Research, The SANS Institute

Before the
Committee on Governmental Affairs
United States Senate
Hearing on
"Securing Our Infrastructure: Private/Public Information Sharing"
May 8, 2002

## Introduction

Chairman Lieberman and Members of the Committee, thank you for inviting me to testify today on information sharing for improved security. I am deeply honored. My name is Alan Paller. I am Director of Research for the SANS Institute. SANS is the primary training organization for the technologists who battle every day to protect the computer systems and networks in the global infrastructure. SANS alumni, more than 28,000 in all, are the intrusion detection analysts, security managers, security auditors, firewall analysts, system and network administrators, incident handlers, forensic analysts, and law enforcement officers who are responsible for building, maintaining, and auditing their organizations' cyber defenses, fending off attackers, and, when attackers succeed, investigating the crime and tracking down the criminals. SANS sees itself as not only the provider of formal education and training but also as a source of continuing education to these technologists on the front-line of protecting our critical infrastructure. Each week, more than one hundred and fifty thousand individuals receive SANS *NewsBites* and SANS *Security Alert Consensus* to keep them up to date on new developments in information security and new threats. We see information sharing as an essential element of what we do.

These technologists, the computer security professionals, are the front-line warriors in a constant fight against cybercrime. Every day, they are forced to engage the criminals who seek to use the Internet for financial gain or to disrupt commerce and government. The prize to the winners is control of the systems that operate our economy and provide the essential services on which we all depend. In my testimony today, I hope to illuminate the chain of nine primary stages in the battle and the consequences of losing at each stage. Then I'll show how sharing of five specific types of information, both from industry to government and from government to industry, can affect the outcome of the battle – perhaps changing in some measure the balance of power between the attackers and the defenders.

The fight against cybercrime resembles an arms race where each time the defenders build a new wall, the attackers create new tools to scale the wall. What is particularly important in this analogy is that, unlike conventional warfare where deployment takes time and money and is quite visible, in the cyber world, when the attackers find a new weapon, they can attack millions of computers, and successfully infect hundreds of thousands, in a few hours or days, and remain completely hidden. The Code Red attacks last summer were perfect examples as is the current scourge sweeping through the Internet – the Klez worm.

One important objective of any sharing activities, therefore, should be to shorten the time it takes for the defenders to respond to new attacks. That requires not only strong computer security technical skills but also sharing of knowledge among the "good guys and gals" that is at least as effective as the sharing that goes on among those who would do us harm. To help us understand the nature of the battle and how information sharing makes a difference, I have constructed a model that shows what we see as nine stages of the cyber battle.

## Nine Stages in the Fight to Prevent Successful Cyber Attacks

Stage 1. *Finding the vulnerabilities.* In the first stage defenders and attackers search for new vulnerabilities (called "zero-day vulnerabilities") that can be used to gain control of a system, remotely. When the defenders lose, as they do many times each year, attackers have an open door to any vulnerable system. However, so far, attackers who discover new vulnerabilities seem to use them narrowly to attack specific enemies. If they used them widely, some intrusion detection analysts would likely discover the attacks and spread the alarm. Discovery and publication would immediately shift the battle to other areas and tend to reduce the effectiveness of the attacks over time.

The most common examples of this type of vulnerability are called buffer overflows that are usually caused by programmers who did not check their programs for errors before releasing them to the public. A buffer overflow allows an attacker to send a command to a machine that does not belong to him, and force the machine to execute the command.

Five types of organizations and people are actively engaged in the process of finding and closing new vulnerabilities:
(1) The software development companies that create vulnerable systems test them; some hire outside hackers to test them, as well.
(2) Customers who deploy systems, especially those in major organizations engaged in electronic commerce, often hire penetration testing firms to try to "think like hackers" and find ways to compromise the security of their systems.
(3) Independent security researchers vie for the notoriety of being the first to point out a vulnerability.
(4) Military cyber researchers and their contractors search for vulnerabilities to be used either for offensive or defensive information warfare purposes.
(5) The criminals and their supporters search for vulnerabilities to exploit.

Stage 2. *Creating patches* The second stage begins when a critical vulnerability is discovered and made known to the system vendor. System vendors try to create and post patches to their systems before the hacker community posts attack scripts that anyone can use to exploit the vulnerability. Once those attack scripts are released, the number and impact of damaging attacks quickly mount. The vendors often win this stage, but their users lose anyway because they don't win the next battle.

Stage 3. *Distributing and installing patches* Once a patch is available for a critical vulnerability, the third stage begins. It is the race to protect large numbers of systems by persuading system administrators to install patches before attackers launch automated programs that scan the Internet for unpatched systems or systematically attack all e-commerce sites (or others groups of interest) looking for systems that have not been patched. There is ample evidence – the Code Red and Nimda worms are examples – that hundreds of thousands of Windows systems were still unprotected more than a month after a critical vulnerability was found, a patch built and posted, and announcements made that the patch needed to be applied immediately. That means that worms and other automated programs can take advantage of these vulnerable systems long after the vendor has released a patch.

Stage 4. *Finding and stopping worms.* During the past fourteen months, a series of worms have spread through the Internet. Worms use recently discovered vulnerabilities to take control of vulnerable systems. A worm as we use the term in cyber security, is a particularly insidious form of parasite that not only infects the machine that it has attacked, but also immediately puts every new victim system to work searching for more victims. That's why worms like Code Red and Nimda spread so fast. Worms can exploit hundreds of thousands of systems in just a few days. Some worms do a great deal of damage. The Lion worm (March 2001) stole thousands of password files and sent them to China.com. Once a password file has been stolen and cracked, every account on that system (and on other connected systems where the same account names and passwords are used) is open to exploitation. So when a worm is launched, the fourth stage begins. In this battle, the defenders try to find new worms that have been unleashed on the Internet and block their most damaging impacts before all vulnerable systems have been exploited.

This is an area in which a private/public partnership has emerged and prospered. SANS operates the Internet Storm Center. It collects data from hundreds of sensors around the world and has been able to put out early warnings of new worms spreading on the Internet. Immediately upon discovering any indication that a worm is loose, SANS informs law enforcement and DoD personnel as well as a council of very smart security practitioners around the globe who have proven capable of breaking these worms. Storm Center was responsible for finding both the Lion and Leaves worms last year. In the case of Leaves, which had taken over more than 20,000 systems and had complete control of them, Dick Clarke's staff at the White House and officials of the National Infrastructure Protection Center convened a joint public/private technical response team and together they broke the code of the worm and caught the criminal who had started it.

Stage 5. *Updating minimum security benchmarks.* Months, even years after vulnerabilities have been discovered and patches have been posted, huge numbers of people continue to connect unpatched systems to the Internet, so the fifth battle is to establish consensus agreement on minimum benchmarks for safe configurations that can help every user know what needs to be done to use their systems safely. This stage is important and it is often misunderstood. What we are talking about here is the equivalent of standards for aircraft maintenance and configuration. If anyone ever sits before this Committee and tries to persuade you that it would be bad policy to set standards for securing information systems, I hope you will ask them whether they also think it is bad policy to set standards for configuration and maintenance of passenger aircraft. Without standards for secure configuration, only the most security-savvy users have the knowledge needed to keep their systems safe. With standards, users can not only buy systems that are well protected but also automate the process of keeping them protected. Time is of the essence here. Every day additional applications are being developed using unsafe configurations. When agencies or companies buy such unsafe applications, they often have to reduce the security settings on their current systems to install and use the applications, obviously a backward step in security.

Before going on to describe the next stage, I would like to take a moment to tell you about an important public/private partnership and the work it has done. The National Security Agency and the National Institutes of Standards and Technology, in cooperation with the Center for Internet Security and the SANS Institute, with substantial help from Microsoft, have reached initial agreement on a benchmark for securing Windows 2000 computers – by far the most popular type of system being deployed as servers in government and in the commercial world. Their joint action will lead to testing of applications to be sure they work correctly on securely configured systems and do not force users to reduce security. Their effort will lead to automation of security configuration and testing, and it will lead to procurement language that allows federal agencies and commercial organizations to order securely configured versions of Windows 2000. The group is also making rapid progress on security benchmarks for Cisco systems and Sun Solaris systems. Benchmarks for several other operating systems are in the pipeline.

Stage 6. *Finding victims and fixing their systems.* The sixth stage happens because attackers do not use their own systems for the majority of attacks. Instead they take over other people's vulnerable systems and use those victim systems to scan for additional victims. In this stage, the defenders try to find exploited and infected machines and persuade their owners to fix them, before those systems exploit more victims and before they are used by attackers in large scale, distributed denial of service attacks. This race should be easy for the defenders to win because networks of sensors in the Internet Storm Center and at UUNET and other organizations are constantly identifying systems being used in attacks. However, when the Internet service providers (ISPs) that connect these attacking systems to the Internet are informed of the problem, many of them ignore the warnings. Government and the private sector could do more to solve this problem by working together to raise the visibility of the systems being used for broad based attacks.

Stage 7. *Deflecting or stopping distributed denial of service (DDoS) attacks.* In the seventh stage, victims being subjected to distributed denial of service attacks try to get the attack stopped before their business deteriorates irretrievably. Innovations by UUNET (WorldCom) have helped improve the defenders' chances, but for many types of DDoS attacks, there is little the defenders can do other than wait until the attackers tire of the game.

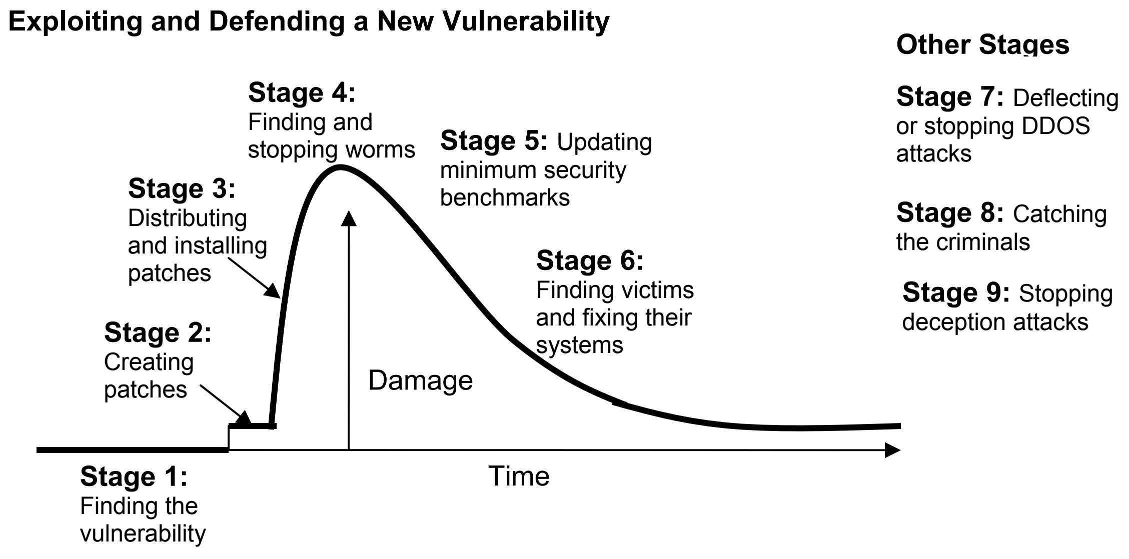
Stage 8. *Catching the criminals.* In the eighth stage, law enforcement people work with technical experts from the victim organizations and other helpers to track down the successful hackers before they do more damage. Of all the stages of the battle, this is the one that should make us all feel pretty good. The FBI has done an extraordinary job of tracking down cyber criminals and deserves our great appreciation for increasing the risk faced by attackers. I would prefer to prevent attacks, but some will always succeed. It is gratifying to see the international cooperation and deep technical expertise the FBI has developed paying off in convictions.

Stage 9. *Stopping deception attacks.* While the defenders are trying to block attackers who probe and exploit vulnerabilities in the systems and software, other attackers are making a mockery of the defenses by persuading gullible users to open up back doors that allow attackers to control systems inside the otherwise secure perimeter. They send an instant message or forge an email or create a web site that persuades users to download and run programs. The programs seem helpful – some even masquerade as "critical" security patches - but when the user executes the downloaded program, it installs a back door and, more recently, opens a connection through the firewall to another system controlled by the attacker. And once the attacker controls one trusted system, he can often gain control of many other systems inside the organization. The ninth stage, then, is to get the users educated so they know how attackers get in and what to do to stop them, before the attackers take advantage of their naiveté.

And in the spirit with which this hearing is being called, to help protect the infrastructure, I should add that security awareness is an important undertaking for every user organization. If someone wanted to take control of the computers Senate staff members use to conduct business with each other or to interact with the press or key constituents, they would most likely use one of the approaches I outlined in stage 9, because deception attacks often elude computer-based cyber defenses.

Chart 1, below, illustrates how the nine stages in the battle correspond with first a rise and later a fall in the damage attackers can cause using a new vulnerability. As the chart tries to make clear, catching attacks at the earlier stages will significantly reduce the damage that they do.

**Chart 1: Cyber Attack Stages**


Exploiting and Defending a New Vulnerability
Other Stages
Stage 4: Finding and stopping worms
Stage 5: Updating minimum security benchmarks
Stage 3: Distributing and installing patches
Stage 6: Finding victims and fixing their systems
Stage 2: Creating patches
Damage
Stage 1: Finding the vulnerability
Time
Stage 7: Deflecting or stopping DDOS attacks
Stage 8: Catching the criminals
Stage 9: Stopping deception attacks

Let's move on to information sharing that can help the defenders win more of those battles.

## How Information Sharing Can Help Defenders Protect the Infrastructure

Sharing five types of information can help win the war against attackers.

**Type I. Data on vulnerabilities and information technology assets with potential vulnerabilities.**

This type covers two sets of information: the inventory of information technology assets and the actual vulnerabilities found in that inventory. Inventory data is of particular interest in critical infrastructures such as power production and distribution, telecommunications, and air traffic control, because some of the key systems used in those sectors are unique to each sector and are often found throughout the sector. If a major threat to one of those shared technologies is discovered, how can you protect the infrastructure in that sector if you do not know where in that sector the vulnerable technology is being used? Sharing inventory data helps the defenders distribute and deploy security patches quickly (Stage 3).

Another opportunity for sharing arises when one organization finds vulnerability in a key system. The vendor that built that system may not act immediately to create a patch (Stage 2). If the user can share the discovery with other users and government, these groups can act together to bring substantial additional pressure to bear on the vendor to produce a new patch. We saw a great example of this during the SNMP threat late last fall when ISPs and government acted together, but outside the public view, to pressure router vendors to develop a patch that protected their customers from the single packet denial of service attack made possible by the SNMP vulnerability.

A third opportunity for sharing data on vulnerabilities is one in which the US General Services Administration has made enormous progress. GSA recently established a single common source of information for all federal agencies answering three key questions: (1) What new vulnerabilities have been discovered? (2) How much control can an attacker gain and how easy is it for an attacker to exploit each new vulnerability? and (3) Where can the user find the patch that corrects each of them? The GSA service will launch June 24th. It would be wonderful if this free distribution were not limited to the Federal government. Just as the federally funded National Weather Service provides information to all citizens on severity of hurricanes, so federal sharing of information about the criticality of new computer security vulnerabilities could help all users of vulnerable computers. For now, however, GSA's offering is the best we have seen. This type of sharing is a great help in distributing and installing security patches (Stage 3) and forms much of the basis for updating minimum security benchmarks (Stage 5), as well.

Just knowing that vulnerabilities exist is not entirely sufficient. To craft an appropriate national response to a major threat, one also needs to know that a vulnerability is being actively exploited. For that you need some or all of the next three categories of data

**Type II. Data on attempted (unsuccessful) attacks**

Millions of unwanted communications hit large companies and government agencies every day, and their firewalls and screening routers block nearly all of them. The unwanted data is being sent by hackers and by programs the hackers launch or by incorrectly configured systems somewhere on the network. Hidden in that flow of bits across the Internet is information that can tell us a new worm has been launched, and as I mentioned before, Storm Center – a cooperative effort among private and public organizations – is already and sharing this data. Storm Center has discovered two major worms and helped stop their damage in one case and led to the arrest of the hacker in the second. The Center is a free public service, and many companies willingly send the data from their firewalls to Storm Center, in part because the Center enables them to remove identifying data from their submissions. Storm Center can be much better than it is and we are investing heavily to improve its precision and speed.

Sharing data on attempted but unsuccessful attacks helps in two ways. First, it helps find and stop worms (Stage 4). Second, it helps find systems that have already been exploited and are being used in untargeted attacks (Stage 6).

However, Storm Center's sensors are far too sparsely distributed in Internet space to find attacks focusing on specific industries or critical sectors such as telecommunications or electric power. For this service to be helpful in more targeted attacks, Storm Center would need to be replicated in each sector. To encourage that type of sharing, SANS has offered to make the Storm Center software available at no cost to any

Information Sharing and Analysis Center (ISAC)* that wants to have a public or private collection and analysis system.

Although data on unsuccessful attacks is extremely useful in illuminating broad attacks such as worms, it is not the answer for rapid response to targeted attacks on the infrastructure. For that you need data in the next category.

**Type III. Data on successful attacks as they are first discovered.**

Data on successful attacks as they are happening is likely to be the most valuable information that can be shared and could help enormously in distributing and deploying security patches (Stage 3), updating minimum security benchmarks (Stage 5) and catching the criminals (Stage 8). Rapid sharing of information on ongoing attacks could improve the chances that organizations most likely to be the next target would act quickly to defend themselves and even set up honey pots to help catch the culprits. Sadly this data is the least likely to be shared. Anecdotal evidence suggests that those who have been attacked successfully are reluctant to share information about the attack – or even admit that they were attacked – for two reasons. They fear that public disclosure could embarrass the organization and possibly cause their customers to abandon them. That's a "bet your company" risk. Further, the experience of the ISACs shows that when an organization is under attack, its technical employees are so busy that they don't even think of telling anyone outside about the problem – unless they want help from consultants in cleaning up or help from law enforcement to catch the culprits.

Those last exceptions – where companies want help from consultants or law enforcement people -- offer two small windows through which real-time attack data can be shared. When the organization that runs the ISAC also contracts with individual ISAC members to provide rapid response forensics and clean-up services when those members are being attacked, the ISAC can be an extremely effective means of getting patches installed quickly (Stage 3). Law enforcement can also offer valuable information on actual attacks, and I'll talk about that in the discussion of the final type of information.

Discussion with officials at the General Services Administration, which operates the
Federal Computer Incident Response Center (FedCIRC)**, suggest that Federal agencies are equally unlikely to report incidents very rapidly for the same reasons, fear of embarrassment and preoccupation with dealing with the immediate problem.

**Type IV. Analyses of the cause and impact of attacks**

When attacks are understood and information about how they were conducted is shared, organizations focus on eliminating the risk because both their senior managers and technicians know the risk is real and know how to avoid it. Thus sharing attack analyses can help in distributing and deploying security patches (Stage 3), updating minimum security benchmarks (Stage 5) and, when the attack involves taking advantage of overly trusting users, can also help with stopping deception attacks (Stage 9).

Companies are just as reluctant after the attack as they are during the attack, to take the chance that information about their security breach would be made public. They act as if experiencing a security breach is similar to contracting a social disease.

Sharing after-attack analysis data is an area in which consultants and law enforcement can and have helped. Consultants and law enforcement agencies can be filters that pass data to other potential victims without identifying the current victims. A great example of the value of this type of sharing took place last spring

* ISACs have been established in financial services, information technology, energy, telecommunications, and electrical utilities, and others are under development. They are private organizations that promote the exchange of information on security threats and breaches among their members.

** FEDCIRC is the central coordination and analysis facility dealing with computer security related issues affecting the civilian agencies and departments of the Federal Government (www.fedcirc.gov).

when the FBI’s National Infrastructure Protection Center revealed that organized crime groups were targeting ecommerce and ebanking companies for extortion. The criminals systematically exploited a pair of web server vulnerabilities in hundreds of ecommerce companies, stealing credit card information and other private customer data. Then they threatened the e-commerce companies saying they would publish the private customer information on the Internet if the company did not pay 100,000 Pounds Sterling. Although the FBI had many ongoing cases, and disclosure could have compromised the investigations, the NIPC told the world about the crimes and exactly which vulnerabilities were being exploited. Their announcement persuaded many e-commerce and e-banking organizations to act quickly to protect themselves, and told them exactly how to do it.. More sharing of that nature could do a great deal of good in Stage 3.

**Type V: Safe Configuration Benchmarks**

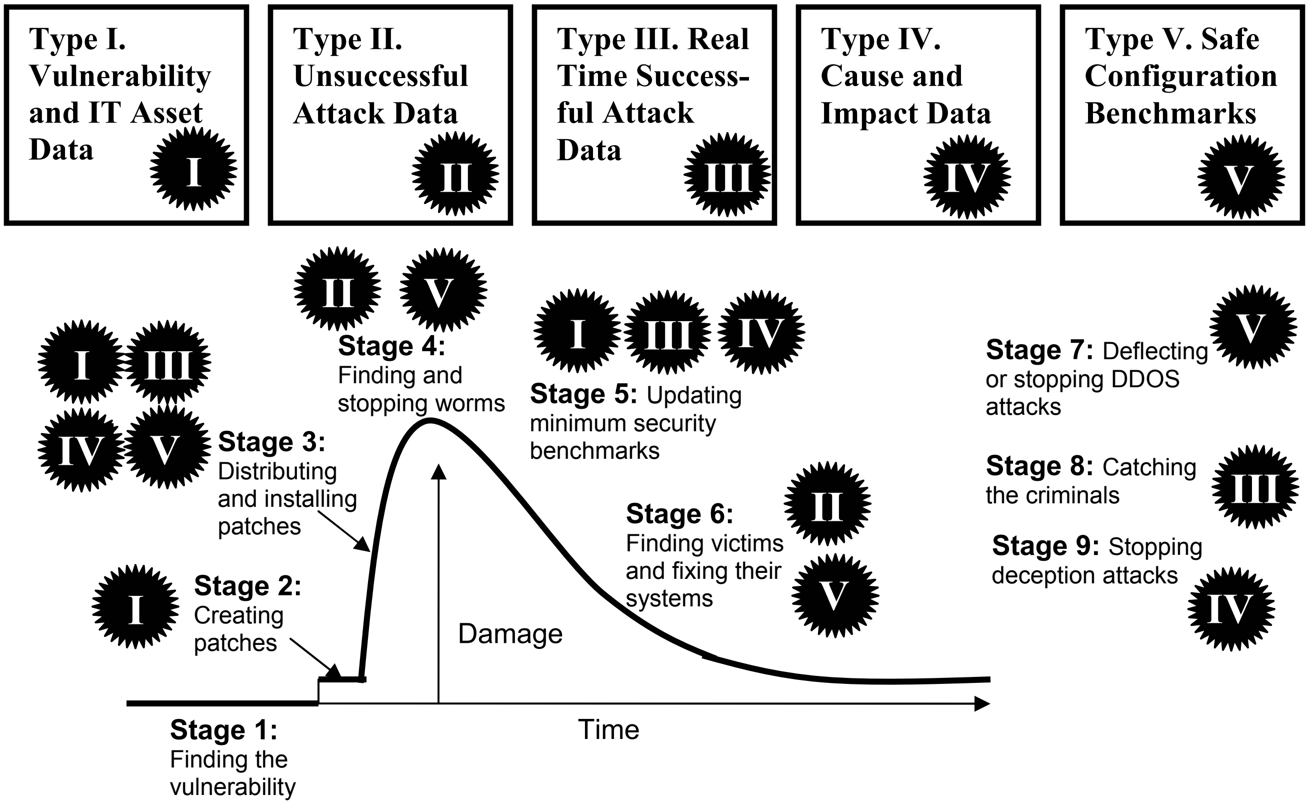
Safe configuration benchmarks are the synthesis of data from the other four categories. They bring together knowledge about vulnerabilities, successful and unsuccessful attacks, and the best methods to block attacks. Few organizations are large enough or have sufficient access to private law enforcement information to build effective configuration benchmarks alone. They lack a complete picture of the risks they face and the actions they should take to eliminate those risks. On the other hand, many experts believe that more than 80% of the successful attacks of the past two years could have been stopped if the organizations had taken specific minimum steps to secure their systems. Therefore, one area of great opportunity to prevent attacks, thereby helping win several stages of the cyber security war, is to share a set of minimum benchmarks for securing common operating systems.

The initiative I spoke about earlier is central to this sharing effort. NIST, NSA and the Center for Internet Security came to agreement on a benchmark for securing Windows 2000 and are nearing agreement on other popular systems. Once these benchmarks are shared, and tools are available to test systems, four stages in the battle will be much easier for defenders to win: stage 3 (distributing patches), stage 4 (stopping worms), stage 6 (getting infected systems fixed – because there will be fewer of them), and stage 7 (stopping DDoS attacks because there will be fewer victims to use for DDoS).

If this Committee can help ensure that federal agencies use their purchasing power to acquire safer systems from the vendors using the consensus benchmarks, you will have an enormous effect on federal cyber security. In addition, the private sector will quickly follow the federal leadership. One easy way to encourage such action would be to add to the reauthorization of your Government Information Security Reform Act, a few words requiring federal agencies to report to NIST or OMB the specific configuration benchmarks they are using to test security of the systems they are deploying.

The chart below illustrates the stages of the battle that can be helped by sharing each type of data.

# Information Sharing Can Help In All Stages



**Type I. Vulnerability and IT Asset Data** I

**Type II. Unsuccessful Attack Data** II

**Type III. Real Time Successful Attack Data** III

**Type IV. Cause and Impact Data** IV

**Type V. Safe Configuration Benchmarks** V

**Stage 1:** Finding the vulnerability

**Stage 2:** Creating patches — I

**Stage 3:** Distributing and installing patches — I, III, IV, V

**Stage 4:** Finding and stopping worms — II, V

**Stage 5:** Updating minimum security benchmarks — I, III, IV

**Stage 6:** Finding victims and fixing their systems — II, V

**Stage 7:** Deflecting or stopping DDOS attacks — V

**Stage 8:** Catching the criminals — III

**Stage 9:** Stopping deception attacks — IV

**Conclusions on Information Sharing**

As the Internet grows in importance over time, Internet security will increasingly coincide with economic security. But computer security is hard, and it is made even harder when each user must act alone because he doesn't have access to critical information from other users. You can help in four ways: (1) by removing barriers that keep the private sector from sharing data with government, (2) by encouraging the federal government to share data it has on vulnerabilities and attacks with the private sector, (3) by requiring federal agencies to lead by example by testing all their systems against security benchmarks, and (4) by asking that all newly acquired federal systems meet minimum security benchmarks except where such a requirement would disable a mission-critical system.

Mr. Chairman, I hope that this framework is helpful as the Committee examines the important role that timely sharing of information plays in preventing, detecting, and recovering from cyber attacks. Clearly, greater and timelier sharing of all of the types of information outlined above can significantly reduce the damage being done by those who would exploit our technology infrastructure whether for financial gain or to terrorize us. The impediments to sharing, some of which I have enumerated above, are complex. One alleged impediment, which I am not able to evaluate, is a concern that, in reporting to government, companies will give up control over proprietary information and that such information might ultimately even be made public. In that regard, it is interesting to note the experience of private ISACs, where no such threat exists, who report similar problems with under-reporting. If a case is made for broader guarantees of confidentiality, and existing restrictions for certain national security, trade secret or law enforcement information are deemed to be insufficient, I would urge the Committee to draw any new restriction on public access as narrowly as possible by defining the categories of information that would be kept confidential quite precisely. To do otherwise, could very well create a new impediment to the sharing of cyber security information so vital in the war we are waging where the government might be unable to pass warnings along because of FOIA restrictions. The enemy - and make no mistake about it -- he or she is an enemy – uses the Internet to great effect to share information. We need to be at least as effective.

We at the SANS Institute and, I believe, the entire community of SANS alumni, will continue to work every day to do our part to turn the tide against cyber attacks.

Thank you very much for this opportunity to share my views with the Committee, and I look forward to your questions.