Testimony of

Mr. Howard Schmidt

February 24, 2004

TESTIMONY BEFORE THE
JUDICIARY COMMITTEE ON CYBER TERRORISOM
U.S. SENATE

By Howard A. Schmidt
Vice President and Chief Information Security Officer
eBay Inc.

Introduction

Senator Kyl, Senator Feinstein, distinguished members of the Committee; my name is Howard A. Schmidt. I am the Vice President and Chief Information Security Officer for eBay, where I lead a team responsible for ensuring the trustworthiness and security of the services that bring so many global citizens together in a vast global marketplace each day. I would like to thank you for the opportunity to come before this Committee as well as your continued leadership on this very important issue. Prior to my current position at eBay, I had the privilege of being appointed by President Bush, along with Richard Clarke, to lead the President's Critical Infrastructure Protection Board, which represented one part of the overall governmental response to the threat of cyber security attacks in the wake of September 11. I retired from 31 years of public service after completing and publishing the "National Strategy to Defend Cyberspace," working with a team of dedicated public servants, this distinguished body and the American public.

I have had the privilege of working with committed individuals in the private sector, law enforcement, and government to forge the collaboration and cooperation that is so essential to safeguard cyber space for everyone, from inexperienced home users to large well-run corporate enterprises. I assisted in the formation of some of the first collaborative efforts in the law enforcement community to address cyber crime with local law enforcement, the FBI, Secret Service and the dedicated military criminal investigators. I also helped lead the creation of the Information Technology Information Sharing and Analysis Center (IT-ISAC) and had the honor of serving as its first President.

I continue to proudly serve in the U.S. Army Reserves, assigned to the 701st MP Group, (CID) as a Special Agent with the computer crime unit at CID headquarters. I also serve on the Board of Directors for ISC2, the body that oversees certification of security professionals through the CISSP certification. And, I serve on the Information Security Privacy Advisory Board, appointed by the Secretary of Commerce to advise NIST, CSD and OMB.

My remarks today will focus primarily on the cyber security threats that we find within business and government; some insights into public-private cyber security partnerships and their

effectiveness; and finally, some recommendations of things that we can do to further improve security for consumers, enterprises of all sizes, educational institutions and government systems.

Today, it is estimated that the Internet connects over 840 million users, with an estimated growth to 904 million by the end of 2004. From major data operations conducting large-scale financial transactions, to wireless devices keeping families connected, the Internet touches virtually all aspects of our economy and quality of life. eBay is a prime example of how deeply ingrained the Internet is in American life. Every day on eBay, millions of Americans, along with millions of people in countries around the world, come together to buy and sell all types of goods and services. Business relationships and, often, deep friendships are formed on the basis of commerce and shared interests. The eBay marketplace reflects the enormous power of the Internet to unite humanity at a crucial moment in history.

More pointedly, the Internet has become a fundamental component of business processes by enhancing productivity through faster connectivity between remote locations or across functional operations. The Internet is deeply embedded in managing power, producing chemicals, designing and manufacturing automobiles, managing money and delivering government services ranging from passport services to environmental permits. Tragically, the flip side of these productivity-enhancing applications is an increase in attacks against the online community.

Today, the Internet is utilized by hundreds of millions of users all across the globe sending information ranging from homework assignments and simple greetings to the most sensitive financial and operational data of government and industry, all at the speed of light. The Internet landscape includes a private sector security industry that has grown to an estimated $17 billion per year in goods and services. And, as we are all painfully aware, attack speeds today are now measured in seconds, not days.

Threats:

During the Cold War many of the threats we identified surrounded nation states, foreign doctrine and intelligence. Threat data was often based on movements of troops and supplies, development of weapons systems that required procurement of goods and materials that provided telltale information of intent and capabilities. The threats against Critical Information Infrastructure are much different. We do not have early warning systems, or see electronic movement that indicates that some system or systems have been targeted; we do not have a single hardened point that we can secure and say we are protected. Often when we do see something it is too late.

I am often asked about the use of the term "cyber-terrorism" and I refrain from using such a term. To many of us in the "cyber security" business, it makes no difference if the attack comes from the Midwest or the Middle East, Eastern Europe or northern Arizona, so long as it is disruptive to the smooth and reliable operation of our Critical Information Infrastructure.

The threats we do see manifest themselves in various formats: Denial of Service attacks (DoS); hacking; "phreaking"; authentication attacks; identity theft; "phishing" and malicious code (virus, Trojans, worms etc.). To try to articulate a specific threat at any given time is almost impossible - the attacks come from nowhere with no warning. What we do know and what we can identify are

the vulnerabilities. Reducing vulnerabilities must be our focus. We once had vulnerability identification and remediation done on an annual basis, then semi-annual and we now have reached a point where vulnerability identification and remediation needs to be done "on demand" at a near real-time basis. The technology currently exists to facilitate this through web-based services. The Department of Defense, who has long been a leader in the public sector in cyber security, had shown that over 98% of successful incursions into DoD systems COULD have been prevented by eliminating known vulnerabilities.

We also have a new category of threats that exploit a single machine now connected to the wonderful broadband capabilities that cable modems and DSL connectivity provide us. The criminals that exploit these single system attacks can harness resources formerly found only in massive enterprises. These single system attacks use automated tools to allow them to take over tens of thousands of broadband machines and have a greater affect than the major Distributed Denial of Service (DDoS) attacks we all suffered in February 2000. DDoS attacks continue to be a favor target of worms, Trojans and viruses.

The ability to use strong authentication and encryption when logging into systems and even doing simple daily tasks like sending email provides yet another vector of vulnerabilities that can be exploited. One of the common ways to takeover a system is to use common hacking tools to "hijack" someone's electronic identity and become an insider. Once inside these people use other tools to identify other vulnerabilities to give themselves greater privileges until succeed in controlling the system. None of us would intentionally send sensitive information through the mail system on the back of a postcard but effectively we do that every day using email. Although easy-to-use technologies such as PKI ("Public Key Infrastructure") are available to protect sensitive data, they are mostly ignored..

The concept of "zero-day vulnerabilities" is closer to reality then ever before. In the recent past as vulnerabilities were made public, it often took months before the ability to exploit the vulnerability was available. The window between vulnerability and exploitation is closing rapidly, from weeks to hours. Formerly, the technical skills to create an exploit were limited to the "elite," but we now see exploit tools to write viruses, Trojans and worms that can be easily modified by novices, often referred to as "script kiddies."

The last point on threats is the new creation of what we call "blended threats," a malicious program that seeks out not just one vulnerability but also any one of a number of potential vulnerabilities and looks to exploit each one in turn. Two of the most virulent of these were called "Code Red" and "NIMDA," neither of which have we identified the criminals that launched these attacks nor the motives behind these attacks. NIMDA is especially troubling since it was launched one week after the September 11th attacks.

PRIVATE PUBLIC PARTNERSHIPS:

During the formulation of the National Strategy to Defend Cyber Space, we at the White House held a series of town hall meetings with private-sector partners. These town hall meetings were open to the public and well-attended, with speakers ranging from CEOs of major financial institutions and exchanges, to subject-matter experts in cyber security. Many of these town hall

meetings were webcast so those that could not attend in person could participate over the Internet.

Private sector companies have also held free seminars around the country to increase awareness of citizens. Many of the sessions focused on informing the elderly, one of the segments of our society that has received great benefit from the online world. Just this past holiday shopping season there was mass media campaigns to educate consumers on how to safely and securely enjoy the richness and robustness of the online e-commerce world.

In the category of formal education, the National Security Agency (NSA) has a program identifying universities to be designated as centers of academic excellence in information security. This NSA program not only ensures the education of the next generation of information security professionals, but also guarantees that each university has sound cyber security practices in place. The academic excellence program provides awareness education for students, who make up a large number of online users and consumers. The NSA also administers the Cyber Corp program with the National Science Foundation and OPM, providing scholarships for students in cyber security.

Another major improvement in the past two years is the way security enhancements are now standard parts of software and hardware. One very visible example is the hardware provided to use wireless technology. Broadband technology (Cable modem, DSL, satellites etc.) has given us capabilities and speeds that were before only available to corporations. We now see firewalls and the ability to download anti-virus software being built into wireless modems. More importantly, firewalls and encryption are now turned on by default rather than waiting for users to install these protections.

The major computer operating systems now have auto-update features and will soon be turned on by default in future versions. Some products that have services that can be exploited are now being shipped with these vulnerable services turned off by default, and thus, making them more secure. Many online email services block potentially malicious code and do a much better job of blocking Spam that contains malicious functions.

Anti-virus vendors have done an amazing job in speeding up the detection, analysis and updates for many of the viruses that are found in the "wild." Many of them even provide free online virus scans as a public service to assist consumers.

There have been a number of government actions that have taken place; most notably the creation of the President's Critical Infrastructure Protection Board and the release of the National Strategy to Defend Cyberspace. This critical document provides a framework for many of our successful private-public partnerships, including home users and small/medium enterprises.

I would also contend that the consolidation of cyber security-related organizations into the Department of Homeland Security (DHS) under the Infrastructure Protection Director has been a positive action. Bringing together the NIPC (FBI), Fed-CIRC (GSA), CIAO (Commerce), Energy Information Assurance Division (DoE) and the National Communications System (DoD) has created a center of excellence that, with the help of focused leadership, will move to

implement our national strategy. This new organization is called the National Cyber Security Division.

Recent action taken by DHS to create the US CERT at Carnegie Mellon University has the potential to significantly enhance security for all users. The US CERT is designed as a focal point for a cyber security response network and providing a notification network as threats and vulnerabilities are discovered.

The goal of US CERT is to ensure that there is an average response time of no more than 30 minutes in the case of any attack. The very specific nature of this goal is designed to deliberately focus the US CERT on building broad participation by the private sector.

The US CERT will undertake the following major initiatives:

? Develop common incident and vulnerability reporting protocols to accelerate information sharing across the public and private response communities;

? Develop initiatives to enhance and promote the creation of response and warning technologies; and

? Forge partnerships to improve incident prevention methods and technologies.

The Department of Justice (DoJ), the U.S. Secret Service and the FBI have significantly decreased their response times and increased the priority of cyber crime investigation. FBI Director Mueller has placed cyber crime as a top five priorities of the FBI, and the Secret Service has added a number of electronic crime task forces to investigate and prosecute cyber criminals. All of DoD's criminal investigative organizations are leaders in investigating cyber crimes and include among their ranks some of the best investigators in the world. DoJ, through its Computer Crime and Intellectual Property Section, has chaired the G-8 Subcommittee on cyber crime and has been a significant driving force in combating cyber crime worldwide.

Since there are no borders when it comes to cyber space, and criminal attacks on consumers can come from all corners of the world, the State Department has conducted bilateral and multilateral discussions to ensure that there is international cooperation in cyber security.

I have had the distinct pleasure of working with Commissioner Orson Swindle of the Federal Trade Commission, who has been a beacon of light for the protection of consumers' privacy and security. With his help in the creation of the FTC's "Dewey" program and his tireless support for town hall meetings, he has truly created a "culture of security" globally.

While there will be no silver bullets in enhancing cyber security, the private sector continues to grow its capabilities and make solid improvement in securing their part of cyberspace. Two of the earliest examples of private-public cooperation for "Cyber Crime/Cyber Security" were the High Tech Crime Investigators Association (HTCIA) and the Information Systems Security Association (ISSA). Both organizations date back to the 80's and are dedicated to sharing information on cyber crime and information security. They still exist today and their membership and value have increased significantly over the years.

Most recently, the private sector has created a coalition that I see as an excellent example of efforts to enhance consumer cyber security. As you are undoubtedly aware, identity theft is a major problem. While the vast majority of ID theft occurs in the physical world, we have seen an increase in the activities of criminals to commit the same types of crime online. The most recent method is what we call "phishing" or "spoofed" emails. The criminals will send out thousands of emails telling people that there is an error with their online account and ask them to fill in an "update form" or their account will be closed. This form has the look and feel of major e-commerce sites - there was even a fake email from someone pretending to be the FBI and the FDIC asking unsuspecting users to enter personal information into a fake web site or their bank account would be closed.

To combat this many of the major players in the e-commerce space banded together to create the Anti-Online ID Theft Coalition. The Coalition boasts many private sector members, with the Information Technology Association of America providing support as the executive director. The Coalition has four major goals: 1) to build technology to reduce the likelihood of these mails ever reaching their intended victim; 2) to provide awareness training to consumers so they can more readily identify these criminal acts; 3) to share information on new scams amongst the various security teams; and, 4) to insure accountability by working with law enforcement to identify and prosecute these bad actors.

In a larger perspective with the federal government, Sector Coordinators representing each of the major sectors of our economy have been appointed to fight potential cyber attack. A Sector Coordinator is an individual in the private sector identified by the sector lead agency to coordinate their sector, acting as an honest broker to organize and bring the sector together to work cooperatively on sector cyber security protection issues. The Sector Coordinator can be an individual or an institution from a private entity. These private sector leaders provide the central conduit to the federal government for the information needed to develop an accurate understanding of what is going on throughout the nation's infrastructures on a strategic level with regards to critical infrastructure protection activities. The Sector Coordinators and the various sector members were key to the creation of the National Strategy to Defend Cyber Space.

In addition, there have been a number of new private sector Information Sharing and Analysis Centers (ISACs). An ISAC is an operational mechanism that enables its members to share information about vulnerabilities, threats, and incidents (cyber and physical). In some cases, an ISAC Manager may be designated, who is responsible for the day-to-day operations of the ISAC, to work with the Sector Coordinator or the sector coordinating body with support from DHS and the lead federal agencies.

Despite these security enhancements, we can be certain that the nature and sophistication of attacks will evolve. There are clear challenges we must continue to address.

First, we must renew our commitment to enhance consumer awareness of basic cyber security practices. The most recent attacks demonstrate that home users can be used as an effective pathway to launch attacks, or as a gateway into large enterprises. We need to build on the public/ private initiatives to promote cyber security with a focused and aggressive outreach effort to all consumers.

Second, while we build an effective response network we must not lose sight of the innovation frontier. Technologies on the horizon hold the potential to dramatically and decisively transform our cyber security challenges. Self-healing computers, embedded technologies that enable devices to recognize and defend against attacks, and devices that enhance both security and privacy are within our reach with an aggressive technology development agenda. This effort must be industry-led in collaboration with our best Universities. Most importantly, it must be synergistically linked with our response initiatives.

Finally, we must recognize that cyber security is no longer merely about products, services and strategies to protect key operations. What is at stake in the effective implementation of advanced cyber security technologies and strategies is nothing less than the ability to unleash the next wave of information technology-led growth in jobs and productivity. Cyber security is an essential enabler to the advent of the next generation Internet and all it holds for how we work, live, and learn.

In the early part of December 2003 the private sector held the first national security summit in Silicon Valley. In attendance were private sector and public sector leaders including DHS Secretary Tom Ridge. This Summit was co-hosted by the ITAA, the U.S. Chamber of Commerce, TechNet and the Business Software Alliance, with the support of DHS.

The work of this summit has continued through the creation of task force work programs that will drive toward solutions to secure and defend cyber space. I am happy to report that much progress has been made and when the results of the various task forces are announced in early March we will again see the progress being made. The task forces bring together, distill, and integrate expertise regarding cyber security metrics, software development and maintenance, public outreach initiatives, and, of course, public-private partnerships in information sharing and early warning systems.

RECOMMENDATIONS:

While much good work has been done over the years, there is still work that needs to be done. My recommendations today fall into three major categories: 1) Cyber Crime investigations; 2) identity management; and, 3) vulnerability remediation.

Cyber Crime Investigations

For the past three years, we have seen a significant increase in the number of cyber crime investigations undertaken by all levels of law enforcement, federal, state, local and international. Although we have had success in a number of investigations, I would recommend to the Committee to look again at the federal agencies and their coordination and investigative responsibilities.

I am often asked by my private sector counterparts who to call to report cyber crimes. At one point, there were pretty clear guidelines of which federal agencies handled intrusions, frauds, financial crimes, denial of service, child exploitation, etc. Today, some federal agencies handle all or some parts of all of these investigations with varying levels of success. When agencies are

asked who should be contacted, one of the answers has been "wherever you get the best service," this puts the private sector and the law enforcement agencies in somewhat of a competitive position which could result in investigative information not being shared broadly and not linking key information that could potentially solve some of these crimes. I would hate to see a hearing some day to identify why agencies did not "connect the dots" in a cyber attack because we do not have a centralized clearing house to analyze, correlate and disseminate information relative to cyber attacks. The creation of a centralized responsibility would go a long way to facilitate solving of these events.

Identity Management

In the area of identity management, static user ids and passwords are no longer sufficient to provide strong ("2-factor") authentication for identity. We have created a system where we must use complex passwords to login to various systems. We also have to change those passwords frequently creating another challenge for mere human beings to remember these complex passwords. This is made even worse by the need to use different passwords for different systems that few people voluntarily choose to do. This is a known weakness often exploited by criminal hackers. As we make identity management secure in the physical world it is not a stretch to presume organized crime and terrorists will then resort to online identity theft to evade detection and apprehension. The government can be a leader in accelerating the creation of digital identity management that would work just for government services and online e-commerce. The nation could be well served to have 2-factor authentication in place by the end of 2004. The form factor to be used can be smart cards, USB "dongles," credit cards and ID cards with Smart Chips built into them or one-time passwords found with some secure ID devices currently in use by some. The DoD has incorporated digital identity on the military ID card called the Combination Access Card (CAC)

Vulnerability Remediation

My last recommendation is in the area of vulnerability identification and remediation. As I mentioned earlier, annual security audits are not sufficient anymore, we need to implement a program where we have an ongoing vulnerability assessment that reports in real time the status of the "state of security" and provides this information in a format that is actionable and comprehensive. Many of us are looking to the development of a "security dashboard" that provides this information to executives so we can prioritize our resources and operationalize security into daily IT operations. Requiring government agencies to develop a program such as this will provide a baseline by which the private sector can develop similar efforts.

The remediation of these vulnerabilities also requires a comprehensive patch management program that so that enterprise-wide programs are not left vulnerable to many system-wide types of attacks.

Reduction and remediation of vulnerabilities will better provide a Critical Information Infrastructure that is more robust and resilient from whatever threats come our way.

Senator Kyl, Senator Feinstein, this concludes my prepared remarks. I thank you again for the opportunity to come before this Committee and welcome any questions that you and the Committee members may have.

Biography of Howard A. Schmidt

Howard A. Schmidt joined eBay Inc. as Vice President and Chief Information Security Officer in May of 2003. He retired from the federal government after 31 years of public service. He was appointed by President Bush as the Vice Chair of the President's Critical Infrastructure Protection Board and as the Special Adviser for Cyberspace Security for the White House in December 2001. He assumed the role as the Chair in January 2003, until his retirement in May 2003.
Prior to the White House, Howard was chief security officer for Microsoft Corp., where his duties included CISO, CSO and forming and directing the Trustworthy Computing Security Strategies Group.
Before Microsoft, Mr. Schmidt was a supervisory special agent and director of the Air Force Office of Special Investigations (AFOSI), Computer Forensic Lab and Computer Crime and Information Warfare Division. While there, he established the first dedicated computer forensic lab in the government.
Before AFOSI, Mr. Schmidt was with the FBI at the National Drug Intelligence Center, where he headed the Computer Exploitation Team. He is recognized as one of the pioneers in the field of computer forensics and computer evidence collection. Before working at the FBI, Mr. Schmidt was a city police officer from 1983 to 1994 for the Chandler Police Department in Arizona..
Mr. Schmidt served with the U.S. Air Force in various roles from 1967 to 1983, both in active duty and in the civil service. He had served in the Arizona Air National Guard from 1989 until 1998 when he transferred to the U.S. Army Reserves as a Special Agent, Criminal Investigation Division. He has testified as an expert witness in federal and military courts in the areas of computer crime, computer forensics and Internet crime.
Mr. Schmidt had also served as the international president of the Information Systems Security Association (ISSA) and the Information Technology Information Sharing and Analysis Center (IT-ISAC). He is a former executive board member of the International Organization of Computer Evidence, and served as the co-chairman of the Federal Computer Investigations Committee. He is a member of the American Academy of Forensic Scientists. He serves as an advisory board member for the Technical Research Institute of the National White Collar Crime Center, and is a distinguished special lecturer at the University of New Haven, Conn., teaching a graduate certificate course in forensic computing.
He served as an augmented member to the President's Committee of Advisors on Science and Technology in the formation of an Institute for Information Infrastructure Protection. He has testified before congressional committees on computer security and cyber crime, and has been instrumental in the creation of public and private partnerships and information-sharing initiatives.
Mr. Schmidt has been appointed to the Information Security Privacy Advisory Board (ISPAB) to advise the National Institute of Standards and Technology (NIST), the Secretary of Commerce and the Director of the Office of Management and Budget on information security and privacy

issues pertaining to Federal Government information systems, including thorough review of proposed standards and guidelines developed by NIST.
Mr. Schmidt holds a bachelor's degree in business administration (BSBA) and a master's degree in organizational management (MAOM) from the University of Phoenix. He also holds an Honorary Doctorate in Humane Letters