

## **DRAFT**

### **TESTIMONY BEFORE COMMITTEE ON FINANCIAL SERVICES U. S. HOUSE OF REPRESENTATIVES**

**By Howard Schmidt  
Vice President and Chief Information Security Officer  
eBay Corporation**

#### **Introduction**

Chairwoman Kelly, members of the Committee, my name is Howard 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 each day. But, I come before you today primarily as an individual who has 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. I assisted in the formation of some of the first collaborative efforts in the law enforcement community to address cyber crime in local law enforcement and the FBI and I helped lead the creation of the Information Technology Information Sharing and Analysis Center (IT-ASAC) and had the honor of serving as its first president. I also had the privilege of being appointed by the President to serve this great nation while leading, with Richard Clarke, 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 body and the American public.

My remarks today will focus primarily on the transformation underway within both business and government to create the level of information sharing and collaboration necessary to safeguard computing and communications. The events of the late summer served to deepen our appreciation for the interdependency between the Internet and the critical infrastructure of commerce, as perfect storm emerged among the confluence of two major worms and viruses and the blackout.

This past year has again shown us dependencies we have on the various parts of the power and telecommunications infrastructure and how interrelated they both are. The power blackout of the Northeast this past summer was a unwelcome reminder of how inextricably the physical world and the "cyber" world are connected.

As if the power outage was not proof enough, the forces of nature again showed us the impact that a catastrophic event could have on our IT infrastructure and the systems they support.

In a public report by the North American Emergency Organization, they estimate that over 50% of businesses do not reopen their doors after a prolonged outage as we have seen this past year. Those that do face tremendous rebuilding cost as well as lost business.

One of the key things that help to reduce the impact of these disruptive events is the ability to share information, across sectors and across competitive lines. The same fundamental principals that have applied in cyber security information sharing apply in the cases of disasters as we have recently seen. During the events of this summer it is estimated that the online industry saw a 10-15% reduction of activity during the power outage and the hurricane. In a published report, a division of Eagle Rock Alliance outlined the financial impact of system failure by various industries and the estimated losses by hour based on system failures. In the financial services industry they cite that credit card/sales authorizations cost \$2.6 Million per hour, brokerage operations at a rate of \$6.45 Million per hour and home shopping \$113,000 per hour. As we can see by this report, the longer the duration of the event the more costly it becomes.

Although there is little we can do to stop a hurricane or other natural disasters we can do much to prepare for events such as these as insure the impact is of minimal duration by taking the same basic measures we would to prepare for a cyber security event. We must share best practices, identify threats and vulnerabilities and create an environment where information sharing becomes the rule, not the exception.

The use of increasingly sophisticated attack tools, with automated attacks penetrating the Internet in seconds, collaboration across industry and government is essential. The events of the late summer clearly highlighted the vulnerabilities and the challenges we face, but I also believe they illustrated the significant progress that has been made in creating an infrastructure for information sharing and collaboration.

Without committed companies working together and with government, I am convinced that the impacts of these events would have been far more severe. Recent initiatives by the Department of Homeland Security to implement the President's Strategy to Protect Cyber Space hold the potential to significantly enhance the momentum created by this increased collaboration. This will further reduce our risks to disruption of our critical infrastructure.

### **The Problem --- Building an Infrastructure for Cyber Security Protection Capable of Operating At Internet Speed**

Today, the Internet connects over 170 million computers and an estimated 680 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. In one sense eBay offers an enhanced mechanism for transactions between buyers and sellers. More fundamentally, the success and popularity of eBay reflects the power of the Internet to extend and enhance the global marketplace.

More pointedly, the Internet has become a fundamental component of business processes--enhancing productivity by speeding connectivity between remote locations or across functional operations. The Internet is deeply ingrained in managing power, producing chemicals, designing and manufacturing cars, managing money and delivering government services ranging from human services to environmental permitting. The flip side of these productivity-enhancing applications is an increase in vulnerabilities.

The BLASTER and Sobig "worm" incidents and the blackout demonstrated the effect of these vulnerabilities. BLASTER and Sobig impacted operations ranging from major rail freight services to charter schools and local government operations. The impact of the blackout reached far beyond the affected region -- services such as home sale closings were delayed because of lost work days in major financial centers.

In assessing our ability to meet the challenges of these events and prevent their reoccurrence, it is essential to note that, in many ways, we have been racing to craft a infrastructure for cyber warning and response that is as dynamic as the Internet itself. Until very recently much of the formal governmental infrastructure for warning and response had changed little from the days when the Internet was used by a relatively small group of trusted users, sending generally non-confidential information to a small set of U.S. destinations very slowly. It was an infrastructure built to address attacks that took days to develop. This legacy warning and response network was still in part a vestige of a time when the private security industry was only in its infancy.

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 also now 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 measured in seconds, not days.

The challenge is to craft a warning and response infrastructure that reflects the dynamics of today's Internet.

It must be an infrastructure that reaches across and engages the sectors and communities that utilize the Internet. It must harness, engage and empower the private security industry right at the heart of its operations. It must prove to be as nimble and flexible as those who attack the Internet. For example, as the focus of attacks shift in real time to particular categories of users, as we witnessed in BLASTER, the focus of our response must be capable of shifting.

The times also demand a response capability that can be a bridge between efforts to identify threats and vulnerabilities and build partnerships to reduce them ---much the way the treatment of symptoms of new biological viruses are synergistically and seamlessly connected to the resources committed to rapidly creating vaccines. In short, it must be faster, more collaborative and broader in its reach in order to shift the frontier from response and warning to prevention.

There will be no silver bullets in meeting these challenges. The creation of a dynamic warning and response infrastructure certainly involves new technologies that both speed response and, ultimately, protect systems from attacks. But the heart of the system will always be collaboration---real information sharing and coordination to identify, reduce and respond to threats and vulnerabilities within and across industries and with the government -- the very type of communication and information exchange that enabled some of our brightest minds in companies and response organizations to reverse engineer and mitigate the impact of the Sobig attack.

### Emerging Solutions---Growing Collaboration in the Creation of a Cyber Security Infrastructure

Two of the earliest examples of private-public cooperation for “Cyber Crime/Cyber Security” were the formation of the High Tech Crime Investigators Association (HTCIA) and the Information Systems Security Association (ISSA). Both organizations date back to the mid/late 80’s and are dedicated to sharing of information on cyber crime and information security. They still exist today and their membership and value have increased significantly over the years.

The growth and evolution of private sector collaboration in information sharing, threat assessment, and incident mitigation has increased significantly by major private sector developments over the past few years: (1) Sector Coordinators; and (2) Information Sharing and Analysis Centers (ISACs), created by PDD 63 in 1998. These developments strike decisively at the issues of concern to this committee and continued progress in this area holds the greatest promise to secure cyber space.

**Sector Coordinators:** This is for each of the major sectors of our economy that are attractive to potential terrorist attack -- the federal government, designated lead agencies and DHS. 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 infrastructure protection issues. The sector coordinator can be an individual or an institution from a private entity. Sector coordinators may also identify a representative(s) at the working level for day-to-day activities.

These 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.

Other functions of the sector coordinator include:

- Coordinate a national plan for infrastructure protection for its sector
- Facilitate outreach and awareness to support infrastructure protection plan implementation;
- Perform or coordinate risk assessment methodology and implementation for the sector, including interdependencies;
- Identify requirements for research and development necessary to meet the special needs of the sector;
- Help oversee the development of an information sharing mechanism (e.g., ISAC) for the sector, tailored to the special needs of the sector and infrastructure protection;
- Help develop or support requirements for sector wide guidelines/standards/useful/effective practices on infrastructure protection, training and education and implementation, metrics for success of infrastructure protection activities; and
- Identify and communicate obstacles or impediments to an effective infrastructure protection program that contains all elements of above;
- Serve as the coordination point for the sector’s owners and operators in discussions with other sectors as needed (particularly to identify interdependencies, address common issues, and share effective practices); and
- Act as the coordination point of contact for the sector with the federal government at various infrastructure protection meetings, and the strategic communication point back into the sector and its members from the federal government.

Some sectors’ diverse interests may make choosing a single sector coordinator challenging. Industry and the lead agency may explore innovative solutions, such as a coordination body or “virtual coordinator” based on existing networked resources, by designating separate sector coordinators to represent key sub-sectors who can, in turn, work together to represent the entire sector. The intention is for sector liaisons and coordinators to have a close working relationship and communication.

Second, of Information Sharing and Analysis Centers (ISAC): An ISAC is an operational mechanism to enable members to share information about vulnerabilities, threats, and incidents (cyber and physical). The sector coordinator develops these Centers with support from the sector liaison. 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.

Presidential documents, such as the *National Strategy for Homeland Security*, continue to encourage information sharing and identify ISACs as an information-sharing model. Many of the ISACs, particularly since the events on September 11, 2001, incorporate more information on physical security.

An ISAC's purpose is to gather, analyze, and disseminate to its members an integrated view of information system and other infrastructure vulnerabilities, threats, and incidents that are relevant to the sector. An ISAC includes the following characteristics:

- 24 x 7 indications and warnings within the sector;
- Information sharing with government and other ISACs as desired;
- Receive alerts and warnings of threats and incidents for dissemination to sector from government and other sources;
- Receive vulnerabilities or remediation information for dissemination to sector from government and other sources; and

The information which ISACs commonly work with provide warnings, establish trends in types and severity of attacks, and share threats and solutions among the ISAC membership and other appropriate organizations, including the federal government.

Thus, Sector Coordinators and the ISACs essentially form a dynamic intersection among Internet users, vendors and public and private response communities.

Recent action taken by the Department of Homeland Security (DHS) to create the US CERT at Carnegie Mellon University has the potential to significantly enhance the continued growth and evolution of ISACs. The US CERT is designed to serve as a focal point for building partnerships based cyber security response network.

The goal for US CERT is to ensure that there is on average no less than a 30 minute response to any attack within one year. No surprises and faster response. The very specific nature of this goal is designed to deliberately focus the US CERT on building broad participation by ISACs and response organizations and 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 development of response and warning technologies.
- Forge partnerships to improve incident prevention methods and technologies.

An immediate focus of the US CERT is to more fully engage and truly serve the ISACs--to ensure that they are right in the front lines of warning and incident communication. The new incident and vulnerability reporting protocols will include more responsive and

immediate engagement of the ISACs and the US CERT is designed to facilitate more immediate interaction with ISACs and among ISACs during major incidents.

## **FUTURE CHALLENGES**

The creation of the US CERT will, for the first time link public and private response capabilities and facilitate communication on cyber security across all infrastructure sectors. Together with increased collaboration and coordination of cyber crime and forensics activities and the growth and evolution of Sector Coordinators and ISACs, the US CERT has the potential to create the national response network envisioned in the President's strategy.

But we can also be certain that as increased collaboration continues to enhance our protection and responsiveness, the nature and sophistication of attacks will also evolve. There are clear challenges we must address.

First, we must develop a clear strategy for the long-term growth and operation of the ISACs. No clear model exists for their long-term support. To what degree should these critical operations be privately financed? What degree of public support is appropriate given their essential role in safeguarding the lifeblood of our physical infrastructure? We must dedicate ourselves to addressing these growth issues immediately.

Second, we must renew our commitment to enhance consumer awareness of basic cyber security practices. The recent attacks demonstrate that home users can be an effective pathway to launch attacks. We need to build on the public/private initiatives to promote cyber security with a focused and aggressive outreach effort.

Third, 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 potentially decisively transform our cyber security challenges. Self-healing computers, embedded technologies that enable devices to recognize and defend against attacks and devices which enhance both security and privacy are within reach of 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.

I don't want to close without mentioning my expectation that many of these challenges will be addressed, and indeed met head-on, with tangible commitments and deliverables through the upcoming National Cyber Security Summit December 2 and 3. This Summit

will be co-hosted by the Information Technology Association of America, the U.S. Chamber of Commerce, TechNet and the Business Software Alliance, with the support of the Department of Homeland Security. I will have the honor to serve at that summit, as will many of the brightest minds and most innovative companies across all sectors of the economy.

The work of this summit won't take place over just the two days it is scheduled December 2 and 3, but through task force work programs that will drive toward solutions in intense work before during and beyond the Summit. We expect that many of these deliverable will be forwarded to DHS early next year, after which we can measure progress on an ongoing basis. We expect this to be an all-hands-on-deck effort where we bring together, distill and integrate many of the outstanding work products from many groups regarding cyber security metrics, software development and maintenance, public outreach initiatives, and, of course, public-private partnerships in information sharing and early warning systems.

Chairwoman, Kelly, this concludes my prepared remarks and I thank you for the opportunity to come before this committee and welcome any questions that you may have.