U.S. House of Representatives

Committee on the Judiciary

Subcommittee on Intellectual Property, Competition and the Internet

&

Subcommittee on Crime, Terrorism and Homeland Security

Hearing on "Cybersecurity: Innovative Solutions to Challenging Problems"

Testimony of Robert W. Holleyman II
President & CEO, Business Software Alliance

Wednesday May 25, 2011

Chairman Goodlatte, Chairman Sensenbrenner, Ranking Member Watt, Ranking Member Scott, thank you for holding this hearing today and for inviting me to testify. My name is Robert Holleyman. I am the President and CEO of the Business Software Alliance (BSA.) BSA is an association of the world's leading software and hardware companies. BSA's members create approximately 90% of the office productivity software in use in the U.S. and around the world.[1]

Over the last 20 years, consumers, businesses and governments around the world have moved online to conduct business, and access and share information. This shift to a digital world has revolutionized personal interactions, education, commerce, government, healthcare, communications, science, entertainment and the arts, etc. It has delivered unprecedented efficiencies and considerable cost savings and it will continue to produce immense benefits to our global society.

However, this revolution has brought with it a number of risks. We all face a variety of online threats, which can undermine trust in the digital environment – the single greatest platform for commerce and sharing information.

BSA has greatly appreciated the opportunity to work with the members of this Committee over the years to address some of the challenges we face in cyberspace, including the continuing problem of software piracy and the threats to cybersecurity. Indeed, the two issues are connected: the use of illegal software is often an entry point for computer malware that jeopardize not only the security of that particular computer but the security of the networks to which that computer is connected.

1. The Size and Nature of the Threats

The gravity and nature of the threats to cybersecurity are significant. These threats fall into four categories according to their motives:

1. Cybercrime—For several years now, cybercrime has been overwhelmingly fueled by profit, employing sophisticated technologies capable of highly targeted attacks that increasingly emanate from organized crime.
2. Espionage targeting corporations—Cyber attacks against the computers, servers and networks on which companies depend have reached unprecedented levels of sophistication, with the aim of committing extortion or stealing intellectual property and other trade secrets for the benefit of competitors;
3. Espionage targeting governments—Governments have become as reliant on information technology as corporations have; as a result, advanced persistent threats that penetrate government computers, servers and networks can produce significant intelligence;

[1] The Business Software Alliance (www.bsa.org) is the world's foremost advocate for the software industry, working in 80 countries to expand software markets and create conditions for innovation and growth. Governments and industry partners look to BSA for thoughtful approaches to key policy and legal issues, recognizing that software plays a critical role in driving economic and social progress in all nations. BSA's member companies invest billions of dollars a year in local economies, good jobs, and next-generation solutions that will help people around the world be more productive, connected, and secure. BSA members include Adobe, Apple, Autodesk, AVEVA, AVG, Bentley Systems, CA Technologies, Cadence, CNC/Mastercam, Compuware, Corel, Dassault Systèmes SolidWorks Corporation, Dell, Intel, Intuit, Kaspersky Lab, McAfee, Microsoft, Minitab, PTC, Progress Software, Quark, Quest Software, Rosetta Stone, Siemens, Sybase, Symantec, and The MathWorks.

4. Cyber warfare—The dependence of a Nation on cyber resources can be exploited by another to electronically disable its critical infrastructure, essential governmental services and military capabilities.[2]

Some of the major attack trends that Symantec detailed in its latest Internet Security Threat Report include:[3]

- Targeted attacks—attackers increasingly identify specific targets and develop sophisticated plans for compromising their computers. They have learned "that the easiest vulnerability to exploit is our trust of friends and colleagues."
- Social networking—linked to the first trend is the exploitation of online social networks which "provide rich research for tailoring an attack" allowing hackers to "learn our interests, gain our trust, and convincingly masquerade as friends."
- Stealth—Once inside an organization, a targeted attack attempts to avoid detection until its objective is met. Exploiting zero-day vulnerabilities[4] and using rootkits[5] are two effective ways of evading detection.
- Attack kits—the sophisticated stealth attacks mentioned above are not exclusive to a few elite cyber attackers. They are packaged and traded as easy to use attack kits in a vast underground economy.

Another way to gauge the cyber threats we face is to look at a simple and compelling number: McAfee reports that in 2010, they detected an average of 60,000 new pieces of malware – i.e. malicious software – *each day*.[6]

This testimony addresses several aspects of our collective response to this challenge, including the role that Congress needs to play. Recently, the Administration made a number of legislative proposals, many of which we could support with appropriate modifications. It is clear that the Judiciary Committee has an essential role to play in strengthening the hand of law enforcement and prosecutors as they battle cybercriminals, and in providing appropriate incentives for private sector entities to further improve their cybersecurity and to share information that allows us to improve our collective cybersecurity posture.

2. The technology industry's response to the challenge

Protecting cyberspace is a shared responsibility. No single entity or group of stakeholders can address the problem by itself – and no individual or group is without responsibility for playing a part in cybersecurity. The technology industry, consumers, businesses and governments must all take steps to secure their own systems and to collaborate with each other to define and implement comprehensive cybersecurity policies and technologies.

---

[2] See http://blogs.technet.com/b/microsoft_on_the_issues/archive/2010/05/03/the-cyber-threat-deconstructing-the-problem-to-promote-comprehensive-dialogue-and-action.aspx

[3] Symantec Corp., Internet Security Threat Report, Vol. 16: http://www.symantec.com/business/threatreport/index.jsp

[4] Zero-day vulnerabilities are previously unknown, and therefore still unpatched, software vulnerabilities.

[5] A rootkit is malicious software that provides an attacker with privileged and undetected access to a computer.

[6] "A Good Decade for Cybercrime – McAfee's Look Back at Ten Years of Cybercrime", http://www.mcafee.com/us/resources/reports/rp-good-decade-for-cybercrime.pdf

The technology industry's responsibilities in the face of cybersecurity challenges are fourfold.

First, each and every day our members focus on the trustworthiness of the information technology products, systems and services. Since governments, critical infrastructure providers, businesses and consumers worldwide depend upon these technologies for their daily operations and business processes, our members have undertaken significant efforts to reduce vulnerabilities, improve resistance to attack and protect the integrity of the technologies they provide.

Users can expose themselves to cybersecurity risks when they use counterfeit or unlicensed technologies. Users of counterfeit hardware or software have no assurance of their trustworthiness, and in many cases intentional vulnerabilities – i.e. malware –are found in counterfeits.[7] In fact, most PC users seem to understand this risk: in a survey of 15,000 PC users in 32 countries, conducted by the respected research firm Ipsos Public Affairs as part of the 2010 BSA Global Software Piracy Study, eighty-one percent of respondents say that fully licensed software is better than pirated software in providing protection against computer viruses or hackers. Eighty-six percent of respondents also say that protection against computer viruses or hackers is an important factor in determining which software to use.[8] That is why our industry consistently advocates that technology users – whether consumers, businesses or government agencies – purchase only from authorized dealers and resellers and use commercial anti-piracy and anti-counterfeiting technologies and processes.

Indeed, in order to better protect themselves, BSA has advocated that organizations adopt Software Asset Management (SAM.) SAM is the people, processes and technology necessary for the effective management, control and protection of the software assets within an organization, from acquisition to retirement. SAM enables organizations of all sizes to realize the full potential of, and value from, their software investments, such as: controlling license compliance, ensuring ongoing software cost-efficiency, and meeting IT governance requirements. The International Organization for Standardization (ISO) developed the ISO/IEC 19770-1 SAM standard to enable organizations to demonstrate that they are managing their software assets to a standard sufficient to satisfy corporate governance requirements and ensure effective support for IT service management overall. BSA developed an online course and certification, SAM Advantage, to allow IT professionals to learn how to effectively manage software assets in their organization.[9]

Second, our members work diligently to develop security technologies to defend against evolving threats. Users of technology rely on BSA members for innovative solutions that provide layered defenses – from protection at the data and document level to the network and perimeter level – that are adapted to the threats they face and the value of the assets they need to protect.

Third, our members are leaders in educating and raising public awareness of cyber risks and how users can protect themselves. Many of our members have developed their own substantial programs to convey these messages, and many offer free security checkup tools. In addition, several BSA members

---

[7] See for example the 2006 IDC White Paper on "The Risks of Obtaining and Using Pirated Software." It showed that 25% of the Web sites that were reviewed for the study that offered counterfeit product keys, pirated software, key generators or "crack" tools attempted to install either malicious or potentially unwanted software. It also showed that 11% of the key generators and crack tools downloaded from Web sites and 59% of the key generators and crack tools downloaded from peer-to-peer networks contained either malicious or potentially unwanted software.

[8] http://portal.bsa.org/globalpiracy2010/

[9] More information about SAM is available at http://samadvantage.bsa.org/

play a leading role in the National Cyber Security Alliance (NCSA),[10] a non-profit organization supported by public and private sector partners. NCSA's mission is to educate and therefore empower a digital society to use the Internet safely and securely at home, work, and school, protecting the technology individuals' use, the networks they connect to, and our shared digital assets. In 2010, NCSA and the Anti-Phishing Working Group (APWG),[11] launched the "Stop | Think | Connect" campaign, the first-ever coordinated message to help all digital citizens stay safer and more secure online. The hope is that "Stop | Think | Connect" will achieve for online safety awareness what "Smokey Bear" did for forest fire safety and "Click It or Ticket" did for seatbelt safety.[12]

Finally, our members partner with the government to develop and implement policy, share information about threats, and respond to incidents. Given the complexity and interconnected nature of information systems and networks, as well as an ever-evolving and sophisticated threat environment, no one organization or entity can address U.S. national cybersecurity alone. Industry entities work together, government entities harmonize their approaches to protecting critical infrastructure, and government and industry work together to address common concerns and build collaborative solutions. The public-private partnership on critical infrastructure protection and cybersecurity, currently organized under the framework of the National Infrastructure Protection Plan (NIPP), is sound, widely accepted, and one in which both government and industry are heavily invested.

3. The Judiciary Committee's role in improving cybersecurity

Cybersecurity is a major challenge. While industry takes its responsibilities seriously and devotes considerable time, energy and resources to the fight, we believe legislation in several areas within the Judiciary Committee's jurisdiction would be extremely helpful.

We believe that this Committee has the opportunity to improve cybersecurity in a way that strengthens the hand of law enforcement and prosecutors, provides incentives to companies to improve cybersecurity, rewards industry leadership and furthers collaboration between the public and private sectors. We make five recommendations towards that goal.

a. Criminal laws

For several years now, cybercrime has been overwhelmingly fueled by profit, employing sophisticated technologies capable of highly personalized attacks increasingly emanating from organized crime. Thus BSA has long championed the need to equip investigators and prosecutors with the tools they need to effectively fight cybercriminals.

We thank this Committee for the leading role it played in securing the enactment in 2008 of the Identity Theft Enforcement and Restitution Act. This law, which was the most significant modernization of the Computer Fraud and Abuse Act (18 USC 1030) in a decade, resulted from remarkable bipartisan

[10] http://www.staysafeonline.org
[11] http://www.apwg.org
[12] http://www.stopthinkconnect.org/

cooperation within and among this Committee, the Senate Judiciary Committee and the U.S. Department of Justice.

We cannot stop there. As cybercriminals continue to adapt, so must our laws. BSA broadly supports the Administration's law enforcement legislative proposals, which strengthen penalties and expand the scope of offenses.

We would like to recommend however an important modification to the Administration's law enforcement proposals, to avoid unwarranted treble damages.

Part 2 of the bill adds cybercrime to the list of offenses that can be prosecuted under the Racketeering Influenced and Corrupt Organizations Act (RICO, 18 USC 1961(1).) Cybercrime has often become an organized criminal activity. We therefore believe it is appropriate to allow *criminal prosecution* of cybercrime as an organized crime, with the effective tools of the RICO statute. However, the proposal does not consider the risk that this creates for legitimate businesses on the *civil liability* side. Listing an offense in 18 USC 1961 opens the way for a civil plaintiff to seek treble damages, as well as the cost of the lawsuit including a reasonable attorney's fee, under 18 USC 1964(c). While legitimate businesses do not participate in organized crime, any attorney could create a very effective threat just by filing for discovery, seeking treble damages and exposing a company to the considerable reputational damage of being branded an "organized criminal enterprise." This would often be sufficient for legitimate businesses to agree to an out-of-court settlement, however undeserved by the plaintiff.

We therefore urge that Congress follow the reasonable and legitimate precedent it has already set with regard to securities fraud, by excluding cybercrime from 18 USC 1964(c). We believe this would have no effect on prosecutorial authority against cybercrime under RICO.

b. Data security and data breach notification

BSA supports efforts to enact a federal law requiring that organizations secure the sensitive personal information that they hold, and notify individuals when that security has been breached.

Consumers' trust in the security and confidentiality of their sensitive personal data is eroding. Over the past several years, the number of significant database security breaches has increased dramatically. The stakes are high and getting higher all the time. According to the non-partisan *Privacy Rights Clearinghouse*, data breaches have affected a staggering 533 million records containing sensitive personal information since 2005.[13] For example recent intrusions into Sony's PlayStation Network led to the theft of sensitive personal information related to 77 million accounts.

BSA believes that federal legislation that requires organizations to secure the sensitive personal information that they hold, and notify individuals when that security has been breached can effectively help restore consumers' trust. Such data breach notification legislation should be based on the following criteria.

[13] http://www.privacyrights.org/data-breach

Establish a uniform national standard that preempts state laws

The National Conference of State Legislatures (NCSL) indicated that, as of October 2010, forty-six States, as well as the District of Columbia, Puerto Rico and the U.S. Virgin Islands had enacted data breach notification laws.[14] This patchwork of state laws has created a compliance nightmare for businesses. Importantly, it can also create confusion for consumers who receive notices from a multiplicity of sources. Federal legislation establishing a uniform national framework would therefore benefit businesses and consumers alike. Section 109 of the Administration's data breach notification legislative proposal also would preempt state laws, but we recommend that legislation preempt state requirements that breach notices include information regarding victim protection assistance provided by that State.

Prevent excessive notification

Not all breaches are of equal importance. Some create great risks of harm to consumers from identity theft and fraud, while other breaches create little to no risk. Currently, most state data breach laws require notification in all instances, even when no risk results from the breach. Over notification is likely to numb consumers, who will then fail to take appropriate action when they are truly at risk. A more effective notification provision would include language that would require notification only in those instances where an unauthorized disclosure presents a significant risk of material harm.

Section 101(a) of the Administration's data breach notification legislative proposal requires that the breach creates a risk of harm or fraud. While this is a step in the right direction, we recommend that the threshold be raised from "*reasonable risk*" to "*significant risk,*" to ensure that only genuine risk is notified.

Exclude data that has been rendered unusable, unreadable, or indecipherable

BSA believes that data security can be much enhanced, without a significant and difficult-to-enforce regulatory system, simply by using a market-based incentive for the adoption of strong data security measures. This can be done through an exception to the proposed obligation to notify security breaches in cases where the data is protected, so that even if it "*gets out*" the information cannot be used.

BSA believes this can be achieved if the measure in question satisfies two conditions:

1. It must render data unusable, unreadable, or indecipherable to any party that gains unauthorized access.
2. It must also be widely accepted as an effective industry practice or an industry standard. Examples of such measures include, but are not limited to, encryption, redaction, or access controls.

Under these two conditions, the data that has been accessed cannot actually be used to defraud or inflict harm on data subjects. A breach would not pose a risk to the data subjects. Therefore, the apparent breach should not require notification.

[14] http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx

In this regard, the Administration's proposal got it right. Section 102(b)(1)(A) of the Administration's data breach notification legislative proposal provides such a market-based incentive for the adoption of strong data security measures. We are particularly supportive of the fact that this incentive is technology neutral, in other words that it does not favor any specific technology. This ensures that innovators will continue to develop new techniques and methods, and organizations will continue to adopt them, without feeling that legislation has favored one type of measure over another. It is also demanding enough to provide a high degree of protection for consumers, today and tomorrow.

Include data security safeguards

Requiring breach notification is fair to consumers who need to know they are at risk, but we believe we should do more to prevent breaches from happening in the first place. We support the inclusion in federal legislation of provisions requiring organizations that hold sensitive personal information to establish and implement reasonable and appropriate data security policies and procedures. Such a requirement should be flexible, by providing that these policies and procedures should take into account the size, scope and nature of the organization's activities and the cost of implementing safeguards. These requirements should also avoid prescribing the use of specific security technologies or methods, and rather ensure that the organization selects those technologies and methods that are most appropriate to their circumstances and risk profile.

Such preventative security requirements have been included in every bill discussed in Congress in the last several years.

Appropriate enforcement

Whether this enforcement authority rests with the U.S. Attorney General or the Federal Trade Commission (as the Administration proposes) what is needed is vigorous action to defend consumers against businesses that fail to provide fair protection of sensitive personal data, without interfering with legitimate businesses. We also support the inclusion, in section 108 of the Administration's proposal, of state Attorneys General (AGs) as enforcers, when federal authorities have not acted. The FTC has limited resources and as a result appropriately focuses on large or precedent-setting cases, while state AGs can supplement the FTC in other cases worthy of enforcement.

We believe however that state AGs should be required to bring their civil actions under the bill in federal, rather than state, court. Federal jurisdiction would ensure that this federal legislation is applied consistently throughout the country.

BSA believes it is also important to prevent excessive litigation. Allowing private lawsuits as a result of the occurrence of a data breach would create the risk that some data custodians refrain from notifying consumers in case of breaches, for fear of opening themselves to lawsuits. Section 108(f) of the Administration proposal also clarifies that their bill does not establish a private cause of action.

c. Incentives for information sharing

Sharing information about threats and vulnerabilities and their consequences greatly contributes to more effective collective risk mitigation, and thus improves cybersecurity.

Many private sector companies, in particular in the information technology sector, have invested important resources into information sharing, in particular by dedicating personnel to gathering and analyzing the data and to participating in collaborative information sharing mechanisms such as the IT Information Sharing and Analysis Center (IT ISAC.)

We believe legislation can make an important contribution to improving information sharing, by removing some of the legal barriers that have been identified. In this respect, the Administration has made two useful proposals.

First, section 245 of the Administration's legislative proposal on the cybersecurity authorities of the Department of Homeland Security (DHS) authorizes companies that lawfully intercept, acquire, or otherwise obtain or possess any communication, record or other information to disclose that information to DHS for the purpose of protecting the cybersecurity of an information system. This is appropriate because current law authorizes the collection, use, and disclosure of information for self-defense purposes, but does not provide explicit authority to do the same for the defense of others. We note that this proposal contains useful privacy safeguards, such as requiring that reasonable efforts be undertaken to remove information that can be used to identify specific persons unrelated to the cybersecurity threat before any disclosure, and that further disclosures and use of the information that was shared be subject to a number of restrictions.

Second, section 246 of the Administration's legislative proposal on the cybersecurity authorities of DHS prohibits a civil or criminal cause of action against a company that lawfully intercepts, acquires, or otherwise obtains or possesses any communication, record or other information and discloses that information to DHS for the purpose of protecting the cybersecurity of an information system. This is needed because the fear of liability has long been known to inhibit information sharing.

We would encourage you to consider an additional market-based incentive for sharing information. We believe it would be appropriate to create a safe harbor from liability, so that information that is shared about an incident cannot be used to seek damages against the company that experienced the incident. Again, we believe that, with the right privacy protections in place, encouraging companies to share information about threats and vulnerabilities without fear of exposing themselves to liability can significantly contribute to improved cybersecurity.

d. <u>Incentives for the cybersecurity of critical infrastructure</u>

We believe this Committee can make an important contribution to cybersecurity by providing liability protection to companies identified as critical infrastructure.

These incentives would be provided to companies operating systems or assets designated as critical infrastructure when these companies are complying with the cybersecurity requirements of DHS, or when they are taking reasonable and appropriate steps to mitigate risks identified by DHS but for which DHS has not approved best practices. Under such conditions, these companies should be protected from related liability, whether for direct, indirect, economic, non-economic or punitive damages.

Other Committees have been, and we hope will remain, interested in the issue of liability protection as it is part of the regulatory framework they have proposed for critical infrastructure. We have other recommendations, which we highlight in the last section of this testimony, about the rest of that

regulatory framework, and we need to make sure they are addressed before that framework is adopted by Congress.

However, we bring this specific aspect of the proposed regulatory framework to the attention of the Judiciary Committee, separately from the rest of that framework, for three reasons. First, because issues of liability protection are relevant to the jurisdiction of the Judiciary Committee. Second, because providing incentives in the form of liability protection strengthens the public-private partnership model that has been successful in improving our Nation's cybersecurity. And third, because this approach will not strain the organizational or budgetary resources of the government, which we recognize is an important consideration in the current fiscal climate.

e. Require that federal contractors use licensed software

Finally, the Obama Administration is considering issuing an Executive Order to require Federal contractors to use licensed technologies, including software. This follows an Executive Order issued some ten years ago requiring government agencies to use licensed software.

We urge this Committee to express its support for this new Executive Order. Using licensed software is not only required by our copyright and patent laws, but as noted above is essential to maintaining security and avoiding the malware that is often bundled with pirated software.

4. Congressional action should also be guided by the following objectives

In addition to the above recommendations, which we think are of most relevance to the Judiciary Committee, other Committees and the Administration have signaled that they want to address a host of other cybersecurity issues. In fact, their proposals contain a number of very useful provisions, although some important improvements are needed. We would like to highlight a few significant considerations.

a. Reforming the Federal Information Security Management Act

Federal agencies are under regular and persistent cyber threats from criminals and hostile nations. The enactment in 2002 of the Federal Information Security Management Act (FISMA) was an important milestone, but its implementation has not improved information security as much as it was hoped. Agencies can comply with FISMA and yet still have significant gaps in their actual security.

We will continue to work with the Administration, the House of Representatives and the Senate towards enactment of effective FISMA reform and to providing the corresponding funding, to ensure that agencies have the authority, resources and obligation to identify and mitigate the cyber risks they actually face.

b. The scope of critical infrastructure

The security of critical infrastructure has been a major focus of cybersecurity legislation. The Administration's legislative proposal and the comprehensive bill currently being developed in the Senate both create a regulatory framework for critical infrastructure.

The scope of what is critical infrastructure is particularly important. We must define "critical infrastructure" in a manner that is not excessively broad, to avoid overstretching the resources of DHS and imposing a potentially cumbersome set of obligations on non-genuinely critical companies.

BSA will continue to work with Congress and the Administration to narrow the criteria that have been proposed to designate critical infrastructure, and to improve the proposed designation process so that it involves industry more and provides more guarantees of due process.

c. Obligations put on critical infrastructure

We must preserve flexibility and technological innovation, which are critical to our ability to respond to cyber threats. This requires that cybersecurity obligations imposed by the government on critical infrastructure do not mandate the use of any specific technological solutions or products and, to the greatest extent possible, permit the use of off-the-shelf commercially developed information security technologies. We will continue to work with Congress to make sure that legislation prevents the government from mandating compliance with standards that require the use by critical infrastructure companies of specific technological solutions or products.

We also must leverage recognized, internationally accepted standards developed through public and private participation, which spur the development and use of ever more secure technologies. Imposing country-specific cybersecurity standards, in particular standards developed by government agencies, would weaken cybersecurity by requiring compliance with standards that would be less flexible, less frequently updated and less adapted to each company's own cybersecurity challenges. Importantly, if the US imposes government-created, country-specific standards, we invite other countries to do the same, which would wall-off foreign markets to American companies and products. Indeed, we already face such threats in various countries.

d. Supply chain security

The development and integration of trustworthy information technology products, systems and services is one of our industry's most important responsibilities in the fight against cyber threats, and our members take it very seriously.

At this time, we do not have sufficiently detailed information to comment on the supply chain security provisions of the comprehensive bill that has been developed by the Senate. We will continue to work constructively with Congress to ensure that any legislation strengthens cybersecurity as well as our industry's global competitiveness.

e. Information sharing

Sharing information about threats and vulnerabilities and their consequences greatly contributes to more effective risk mitigation, and thus improves cybersecurity.

To date, sharing of information about threats, vulnerabilities and consequences has largely been one-way: industry shares a lot of information with the government, but relatively little of the information government gathers through its intelligence collection and investigative capabilities is shared in return.

We believe Congress should ensure that the government shares more information with the private sector. We understand that this will require overcoming persistent resistance among certain government agencies. This will not happen without engagement from government's most senior leaders, and sustained congressional oversight. The government agencies taking part in this information sharing will need appropriate direction, legal authority, and resources. Existing structures between government and industry may need to be adapted to share information in a trusted environment, but those structures provide a foundation from which to build.