Prepared testimony of
Paul B. Kurtz
Executive Director
The Cyber Security Industry Alliance

Before the House Small Business Committee
Subcommittee on Regulatory Reform and Oversight
"Data Protection and the Consumer: Who Loses When Your Data Takes a Hike?"
2360 Rayburn House Office Building
Tuesday, May 23, 2006
10:00 AM

Introduction

Chairman Akin, Ranking Member Bordallo and other members of the Subcommittee, thank you for the opportunity to testify today before the House Small Business Subcommittee on Regulatory Reform and Oversight. My name is Paul Kurtz and I am the Executive Director at the Cyber Security Industry Alliance (CSIA). I will cover several areas in my testimony: the importance of data security to small businesses and steps small business, industry, and the Federal government can take to improve security.

Before I begin my comments, I would like to thank Chairman Akin and Ranking Member Bordallo for emphasizing the important role information security plays with small businesses through hearings such as this, and outreach efforts to discuss security with small business owners and their supporting entities. And to Chairman Akin in particular, CSIA was pleased to have representatives from three of our member companies participate in a Town Hall discussion you held last month in St. Louis. CSIA also worked with the National Cyber Security Alliance (NCSA) to produce a tip card for small businesses that was distributed at that event, and can be found on NCSA's website StaySafeOnline.org. We appreciate, and are supportive of your efforts to increase information security awareness, both here in DC and at home.

CSIA is the only advocacy group dedicated to ensuring the privacy, reliability and integrity of information systems through public policy, technology, education, and awareness. The organization is led by CEOs from the world's top security providers who offer the technical expertise, depth and focus needed to encourage a better understanding of security issues. It is our belief that a comprehensive approach to ensuring the security and resilience of information systems is fundamental to global protection, national security, and economic stability.

Why Securing Data within Small Businesses is Important

Small businesses are the backbone of the American and international economy, as nearly 99 percent of all U.S. businesses are small or medium-sized,[1] and they represent 97 percent of all U.S. exporters.[2] The Internet has enabled small businesses to compete with large enterprise because of the accessibility and ease of communication the Internet offers; but this accessibility

[1] 2003 County Business Patterns. http://www.census.gov
[2] http://www.sba.gov/aboutsba/sbastats.html

has also created new challenges by increasing threats such as those caused by system vulnerabilities and exploitation by bad actors. As you know from the Subcommittee's hearing in March on "The State of Small Business Security in a Cyber Economy," Symantec Corporation found in its semi-annual Internet Security Threat Report that small businesses have consistently been one of the top three most targeted groups for cyber attacks over the past year.[3] Organizations with weaker security infrastructures - often small businesses with more limited resources – are exploited by cyber criminals in greater numbers.

Although small businesses have increasingly been targeted recently by cyber criminals, data security has been a front-page news story for well over a year now. Since February, 2005, when it was revealed that a major data broker disclosed personal data to criminals posing as legitimate businesses, more than 55 million records of Americans' private personal information – an average of 120,000 per day – have been hacked into, lost, stolen or otherwise compromised from digital databases.[4] In fact, more than 60 new major incidents have been reported since January 1, 2006. These security breaches are increasingly eroding public confidence in the security of private personal information. According to a survey CSIA recently released, 50 percent of Internet users avoid making purchases on the Internet because they are afraid their financial information may be stolen. This lack of consumer confidence inhibits e-commerce across the board, but the problem for small businesses is disproportionately greater. This is so because in the absence of reliable assurances that reasonable security measures are in place, consumers will assume, rightly or wrongly, that larger, better-recognized businesses will offer their customers more protective avenues of recourse in the event of a problem, while smaller businesses with little brand-recognition would offer no such intangible comfort level.

There are other important reasons why small businesses must take data protection seriously. For many small businesses that are part of the integrated supply chains of larger government and private sector organizations, their customers will be looking for the assurance that their small business partners are operating consistently with their own data protection policies and procedures.

What Small Businesses Can Do to Protect Themselves

Companies looking to strengthen information security practices should consider a three-prong risk management approach that uses a combination of policies, technology and people to address data protection. In the summer of 2003, the U.S. Federal Trade Commission held a two-part workshop on the current and potential role of technology in protecting consumer information. Workshop participants concluded that while technology can play a key role in protecting personal information, effective data protection requires a comprehensive approach that also addresses the critical roles that people and policies play in addition to technology.[5]

---

[3] http://wwwc.house.gov/smbiz/hearings/databaseDrivenHearingsSystem/displayTestimony.asp?hearingIdDateFormat=060316&testimonyId=483

[4] http://www.privacyrights.org/

[5] Federal Trade Commission Staff Workshop Report: Technologies for Protecting Personal Information, http://www.ftc.gov/bcp/workshops/technology/finalreport.pdf

This holds true for small and large enterprises alike. In general, the complexity of information security increases with the size of the organization. In this sense, small businesses may have an advantage. However, small businesses do not have the same resources as large enterprises. For example, many small businesses cannot afford to hire experienced information security staff. As the FTC observed, security-enhancing technologies must be properly installed and maintained, and knowledgeable IT security professionals able to perform these functions today are in short supply.

Small business should begin by establishing a security policy. Several sources of guidance exist today, including the U.S. Chamber of Commerce's Common Sense Guide to Security for Small Business[6] as well as NCSA's tips. In addition, practical advice is available through the National Institute of Standard and Technology's SecureBiz workshops dedicated to small business.[7] These workshops are co-sponsorship with the Small Business Administration (SBA) and the Federal Bureau of Investigation (FBI), and they are especially designed for small businesses and not-for-profit organizations. Attendees have the opportunity to explore practical tools and techniques that can help them to assess, enhance, and maintain the security of their systems and information. Also under the Federal Information Security Management Act (FISMA), NIST has published several publications designed to assist with computer security, in particular its 500 and 800 series publications which are available on line.[8] This guidance was developed for Federal agencies, however the principles contained are applicable to small businesses. For example, NIST has issued guidance on categorizing systems based upon risk in order to help an entity more efficiently deploy scarce resources.

Steps the Information Security Industry is Taking to Improve Security

Improvements in technology have made basic security measures more available and affordable for small businesses. Systems are now being designed with security built-in, relieving end-users of the confusion and costliness of add-ons. Many security firms have developed products specifically designed for small businesses. A typical suite of security technologies includes: authentication, encryption, intrusion prevention, vulnerability testing, and monitoring technologies. Many of these capabilities are now bundled together or can be outsourced to managed security service providers. Other online services are available now free of charge to provide consumers with real-time advice on potentially dangerous sites which may contain spyware or generate unwanted e-mail. One example is a security add-on for web browsers called SiteAdvisor by McAfee. This service identifies web sites linked to spyware, adware, spam, viruses, browser-based attacks, phishing, or other online fraud. This free service has surveyed and tested 95% of the most frequently accessed web sites and notifies consumers of online "neighborhoods" that may pose more risk to their personal and financial information. Consistent with the FTC's principles and recent statements, technology such as McAfee SiteAdvisor has a role to play in protecting consumers online and can be applied without posing a heavy burden on owners of small businesses.

[6] U.S. Chamber of Commerce, Common Sense Guide to Security for Small Business, (September 2004); http://www.uschamber.com/publications/reports/0409_hs_cybersecurity.htm
[7] National Institute of Standards and Technology, (http://csrc.nist.gov/securebiz/)
[8] NIST, see: http://csrc.nist.gov/publications/

The financial services industry, in particular the payment card industry, is seeking to improve information security among merchants through its Payment Card Industry (PCI) Data Security Standard. The PCI includes Visa, MasterCard International. They realize consumers must have confidence in conducting a secure electronic transaction from the point-of-sale. The PCI Data Security Standard, which went into effect last year, has 12 basic requirements that focus on using secure systems. The rules include installing a firewall, changing default passwords, protecting stored data, using antivirus software and encrypting transmissions of cardholder data across public networks. This top-down approach forces a common standard among merchants.

However, small businesses are beginning to face a new challenge in the growth of state legislation requiring the notification of consumers in the case of a breach of sensitive personal information. Some 29 states have passed data breach notification laws in 2005 and 2006 since California passed its law in 2003. The borderless nature of the Internet means that a small business must comply with all of the state laws. For example, if your business is based in Missouri and your database contains the name of California residents, you must notify those residents in case of a breach. While there is some similarity among the state laws, they set different thresholds for when a consumer must be notified, and the contents and means of notification vary from state to state. Local governments are also beginning to legislate in the area of security. Westchester County in New York has mandated security for wireless devices for business that deploy public Wi-Fi networks and required that they secure sensitive personal information.

The patchwork quilt of laws and regulations to address data security is beginning to look ugly. The laws and regulations place a burden on small businesses. There is an urgent need for Congress to pass legislation to create one standard by which all organizations will comply. Small businesses have limited legal and technical resources; therefore, they find the task of complying with different and potentially conflicting state statutes very difficult. Of all the segments of the business community, small businesses may have the greatest stake in the rapid adoption of a nationally pre-emptive data security law: any further delay by Congress leaves small businesses in an impossible legal situation. This is further complicated by the fact that small businesses must also contend with such laws as Sarbanes-Oxley. The SEC recently upheld that small businesses must comply with Sarbanes-Oxley despite intense pressure from various stakeholders.

Consumers too are also growing wary of the current situation, and are losing confidence in the information infrastructure. For example, CSIA's "Digital Confidence Index" showed a one point drop since December. The DCI is designed to measure the confidence of citizens in the security of the Internet. According to a survey CSIA commissioned in April by Pineda Consulting, half of the respondents avoided making purchases on line because of fear over identity theft or fraud. In addition, only 19 percent of respondents polled believe that existing laws are enough to protect their privacy.

Federal Government Action

There are several actions Congress and the Executive Branch can take to improve information security among small businesses, including passing a national data security law, greater leadership by the Small Business Administration and bolstering outreach efforts.

Implications of National Data Security Legislation for Small Businesses

As stated earlier, small businesses must enhance their data security capabilities in order to remain competitive with larger entities and to comply with existing state laws. The key is how to do so in ways that maximize protections without undue cost or burdens. One key answer is to enact a federal law that reflects this balance. CSIA believes that there are several provisions in pending legislation that are particularly important for small businesses:

Scope. Most state data breach laws apply to all organizations that hold sensitive personal data. Therefore, to ensure effective pre-emption, it is important that federal legislation apply to any agency or person who owns or licenses computerized data containing sensitive personal information; it should not be limited to "data brokers." Security breaches have occurred in a variety of industry sectors, and national legislation should be broader to include such groups and organizations as data brokers, banks, hospitals, educational institutions and large employers. This is important for small businesses because it assures consumers – the customers of small businesses – that their information will be protected regardless of where it is held or used. A more fragmented or limited approach will simply not enhance consumer confidence in doing business online.

Reasonable Security Practices. Legislation should set forth reasonable security measures based on widely-accepted industry standards, best practices or, where appropriate, existing Federal law, such as Gramm-Leach-Bliley (GLB) and the Fair Credit Reporting Act (FCRA). This is extremely important for small businesses because it sets forth a consistent, predictable national approach that gives clear guidance to small businesses that may otherwise struggle to determine on their own what reasonable standards are or how or when to apply them.

Notification Requirements. Small businesses will benefit from legislation that makes clear when notification is required, and that minimizes the need for notification when the likelihood of harm is low. In this context, a Federal law should include a "safe harbor" provision that would exempt companies from the obligation to notify in the event of a data breach when the data is encrypted. All state laws passed to date contain a similar provision. Such a provision may be useful to small businesses by encouraging the use of inexpensive and widely used methodology that can minimize costs associated with notification, lost reputation, and potential liability under the law.

Pre-emption. One strong federal law that pre-empts existing state laws would alleviate the compliance complexities small businesses currently face. As indicated earlier, this is a critical point and one we believe would make passage of a federal law attractive to small businesses.

Enforcement. Federal data security legislation does little to enhance consumer confidence absent strong and effective enforcement mechanisms. To this end, two specific provisions will be of particular importance to small businesses, as follows:

- **The Insider Threat.** The increasing threat presented by a malevolent or dissatisfied insider is an unfortunate reality for the entire business community, but for small businesses with limited detection and investigative resources, the implications can be particularly devastating. Legislation must ensure that provisions requiring reasonable security standards are enforceable so that consumers can be assured that actions by rogue employees or other insiders can be prosecuted. Inclusion of an enforcement requirement would bring data security legislation in line with other statutes (FISMA, HIPAA, GLBA) and provide a more uniform data protection regime.

- **Adequate resources for Federal enforcement.** The agency or agencies with enforcement authority should be granted adequate resources to properly and effectively enforce the law. This includes adequate funding, personnel, and tools to conduct thorough investigations, and prosecute and penalize offenders. The enforcing agency should also utilize existing standards wherever possible, rather than creating a new standard.

Executive Branch Leadership

Small business would benefit from more consistent leadership from the Federal government on the information security issues they face. Given the importance of IT as an enabler to small business, SBA should give information security far greater attention than it has to date. It should begin by establishing an office within the agency dedicated to the information assurance needs of small business, developing a comprehensive suite of programs. The SBA should also create an advisory committee comprised of small business community and technology leaders to advise the agency on programs specifically tuned to the challenges faced by small business.

Programs would be useful in several areas:

Information Assurance Survey. SBA should undertake a survey targeting small business to ascertain the specific challenges they face in securing networks. The Department of Homeland Security and Department of Justice have commissioned a survey targeted at larger businesses. Such a survey would provide for confidential results, but enable SBA to understand the types of attacks or disruptions small business are encountering and the associated costs. The results of the survey could inform SBA on key gaps requiring attention.

Tap InfraGard. SBA outreach should be expanded beyond SecureBiz. SBA should partner more consistently with InfraGard, a grass roots effort focused on critical infrastructure protection in tens of cities across the U.S. sponsored by the FBI. InfraGard brings together small and large business to share information and receive briefings on protection strategies. For example, InfraGard chapter members in San Francisco last week where briefed on the PCI Data Security Standard. The SBA need not create a new

network—one exists today. Within the context of InfraGard, SBA could sponsor regional or local information assurance small business awards recognizing innovation and leadership in information assurance.

NIST Guidance for Small Business. SBA should fund a NIST effort to publish guidance for small business. With appropriate funding, based upon guidance from an SBA advisory committee and the survey, NIST could publish information assurance guidance for small business.

Summary of Recommendations

CSIA offers the following recommendations for the Committee's consideration:

Create an Information Security Office within SBA. The office would serve as the Federal government's "go-to" organization for small business on information assurance. The office would act as a portal for receiving and dispensing educational information security tools and resources for small and medium-sized businesses. The office would chair the advisory committee, survey small businesses, and determine whether government programs and services are sufficient to serve the specific information assurance challenges they face.

Support national data security legislation. Small businesses have fewer resources and funding at their disposal to ensure they are in compliance with the laws of every state their businesses touch. A comprehensive, strong federal law will simplify the compliance process. Congress has introduced several bills, indicating its understanding of the importance of such legislation, and CSIA urges rapid enactment this year.

Take the message beyond the beltway. Reaching out to owners of small businesses on a local level is a more effective way to make known the resources and assistance available to small businesses. The NIST workshops I referenced earlier in addition to an expanded effort with InfraGard are examples of valuable local efforts. SBA leadership should draw from the existing network of programs already available to small businesses and conduct a broader outreach campaign.

A consistent approach to data security levels the playing field that is the online marketplace and enables small businesses to compete effectively for clients and customers with much larger businesses like no other time in the past.

I appreciate the opportunity to testify today, and I am pleased to answer any questions you may have.