Before the
DEPARTMENT OF COMMERCE
Internet Policy Task Force

	)	
	)	
In the Matter of	)	
	)	
Cybersecurity, Innovation	)	Docket No. 100721305-0305-01
	)	
and the Internet Economy	)	
	)	
	)	
	)	

COMMENTS OF VeriSign, Inc

Joe Waldron
Director, Product Management
VeriSign, Inc
21345 Ridgetop Circle,
Dulles, VA 20166

September 13, 2010

Overview

VeriSign's role as a critical Internet infrastructure provider for the world's largest Top Level Domains (TLDs) provides VeriSign with an opportunity to offer new and valuable insight into the cybersecurity threats that face our nation - now and into the future. VeriSign is pleased to share this insight through its response to the Department of Commerce's Notice of Inquiry "*Cybersecurity, Innovation and the Internet Economy Docket* #100721305-0305-01)".

1. Quantifying the Economic Impact

Challenges to implementing a data gathering and analysis system to measure the impact of cyber security incidents:

Data gathering impediments to cooperation and information sharing are no clear division of responsibility for incidents, differences in the security cultures of the relevant parties, lack of trust relationships between partners and no common information sharing model.

Incidents that cross international boundaries create an additional layer of confusion on what information to share, and with whom to share it. What responsibility/authority do US companies or non-US companies have when incidents are not restricted to a specific jurisdiction?

Various privacy and data protection laws can also deter information sharing due to concerns that broad definitions of what constitutes personally identifiable information (or broad interpretations of such terms) may cover critical data (*i.e.*, IP addresses, Device IDs). This creates potential liability for the accidental release of such data by the sharing program. Creating safe harbors exceptions for the sharing of data for these purposes would increase the value and utilization of such sharing programs.

The appropriate entity to perform collection and analysis of the data:

A clear definition is needed of what should be reported, who should receive the reports, and the use of the data. Currently a number of agencies gather data for a variety of reasons. For example:

- The Cyber Intelligence Section (CIS) of the Secret Service was founded in 2005 to combat trends in fraud and identify theft. The CIS serves as a central repository for the collection of data generated through the agency's field investigations, open source Internet content and a variety of information obtained thru financial and private industry partnerships as it relates to identify theft, credit card fraud, bank fraud and telecommunications fraud.
- The Financial Services Information Sharing and Analysis Center (FS-ISAC) was established by the financial services sector in response to 1998's Presidential Directive 63. That directive - later updated by 2003's Homeland Security Presidential Directive 7 - mandated that the public and private sectors share information about physical and cyber security threats and vulnerabilities to help protect the U.S. critical infrastructure.
- The National Cyber-Forensics and Training Alliance (NCFTA) combines the FBI, United States Postal Inspection Service, industry and academia in several initiatives to share information to diminish securities fraud, pharmaceutical fraud, and malware used for fraud
- The United States Computer Emergency Readiness Team (US-CERT) is the intended focal point for identifying and responding to computer security incidents in the United States (not

just e-commerce incidents). The primary mission of US-CERT is to coordinate previously dispersed efforts to counter threats from all forms of cybercrime.

It would be desirable to develop an overall framework of information sharing, with a single authority for gathering information on cyber crime incidents for e-commerce. Currently the various Information Sharing and Analysis Centers (ISACs) do operate to serve this function for specific groups. One option would be to create an e-commerce ISAC, as none of the other 17 ISACs specifically serve the e-commerce community.

Another consideration is to develop APIs for use in the collection point which will sanitize the data so that it contains no information that would enable one to ascertain a client's identity. There are studies currently that do provide excellent security metrics and analysis but contain no information that would enable one to ascertain a client's identity.[1]

Other data that would determine if the nation's information and communication systems are adequately protected:

Real world data breaches follow 3 major phases that also closely align to a typical incident response process: point of entry to compromise, compromise to discovery and discovery to containment. The issue for e-commerce is less data/money is lost if the breach is found and mitigated quickly. However, the statistics are not encouraging.

- Compromise to discovery. Over the last 2 years, the most damage occurred between the time of the compromise of data and the discovery of the breach. Between 44% and 65% of breaches remain undiscovered for months or more. Over half of all breaches go uncontained for weeks or more after they have been discovered. Proper planning and testing of incident response is critical but can pose contractual problems.[2] For example: how do you manage security incidents for assets that are hosted by a third party?[3]
- Third party fraud detection is still the most common way breach victims become aware of the breach. In fact, 35% of these breaches were discovered by 3rd party fraud detection while only 12% were reported by law enforcement.[4]

Adding metrics for these data points would help assess how quickly data breaches are found and addressed, and would likely correlate to the overall loss of investment.

Gathering data from information and communications systems providers related to the following would also provide insight into whether the current information and communications systems are adequately protected:

- Presence of an Information Security Policy.
- Definition of best practices related to identity management, network security, application security, business continuity planning and physical security.

Another recommendation is to expand analysis activities on the impact of specific malicious activity to include the supply chain. For example, when was a specific piece of malware developed, how was it distributed, what command and control is used to manage it, and who are the victims infected by

[1] 2010 Data Breach Investigations Report, Verizon RISK team and United State Secret Service
[2] 2010 Data Brach Investigations Report, Verizon RISK team in cooperation with United States Secret Service
[3] Ibid.
[4] Ibid.

it? This would enable a concerted response to remove the C&C, disrupt the distribution channel(s), and clean the victim's websites.

2. Raising Awareness

Awareness of information sharing programs:

As stated above, a number of government organizations have information sharing programs. There is confusion on where information should be shared, what information should be shared, and a lack of trust as to how and for what the information will be used

Designating a single point of accountability within the federal government with over-arching responsibility for commercial interests would be ideal. The data would need to be aggregated and sanitized, to protect company identifies. An incentive could be to provide the aggregated report information to companies who participate in the data sharing program.

3. Web Site and Component Security

Government and private sector collaboration on third-party verification of Web site and component security to reduce the presence of malware:

VeriSign supports collaboration between government and the private sector to develop a means of third party verification of web sites. Innovation by the private sector has introduced a wide range of tools to mitigate the threat presented by malware – including url blocking and anti-virus implementations down to the consumer level.

The issue requires more than just monitoring or auditing for security. Over the last few years, the number of application vulnerabilities has surpassed the number of vulnerabilities discovered in operating systems. Specifically, users download commonly used client side files in applications such as Adobe Acrobat and infect their systems inadvertently. On average, major organizations take at least twice as long to patch client-side vulnerabilities as they take to patch operating system vulnerabilities according to a recent study by the SANS Institute (http://www.sans.org/top-cyber-security-risks/summary.php). As a result, more exploitation attempts are recorded on application programs. For e-commerce, this presents a hurdle for new application innovation, greatly increases the amount of cyber crime events and consequently threatens consumer confidence in online transactions. The following examples of application or client-side vulnerabilities present serious challenges to the future of ecommerce:

- Web applications are the most used path of intrusion. Attack pathways by percent of breaches are 54%, remotes access and control services are 34%, and backdoor or control channel are 23%[5].

[5] Ibid.

- Services and application were compromised more than any other asset and comprise 98% of the total records compromised. Breach involving end user devices nearly doubled from last year. Much of this growth is attributed to credential capturing malware.[6]
- Web application attacks often occur without the web site owner's knowledge. Web site attacks often involve exploiting vulnerabilities in the web server to execute malware on the web site visitor's client.

> For example, two common avenues for exploiting and compromising web servers: brute force password guessing attacks and web application attacks. Microsoft SQL, FTP, and SSH servers are popular targets for password guessing attacks because of the access that is gained if a valid username/password pair is identified. SQL Injection, Cross-site Scripting and PHP File attacks continue to be the three most popular techniques used for compromising web sites.
>
> Automated tools target custom web application vulnerabilities and make it easy to discover and infect several thousand web sites that, in turn, infect website visitors. These attacks install a large variety of malware ranging from information-stealing Trojans and spyware. The major mass SQL injection attacks in 2009 - Gumblar.cn, Martuz.cn, Beladen.net and Nine-ball - delivered exploits and utilized a high number of intermediary domains.

An area to address is the actual development of controls into the web site applications. For example, in August of 2009, the Center for Strategic and International Studies formed a consortium made up of cross-agency and private sector information security experts. This team of experts published a report, entitled "Twenty Critical Controls for Effective Cyber Defense Consensus Audit Guidelines". This document represents successful collaboration across public and private sectors to mitigate risks on the Internet. The controls outlined in this document span a wide range of security threats including, but not limited to:

Threat	Security Controls
HTTP Server Threats	Control 7 (Application Software Security) Application developers should ensure that all input received from remote sources is sanitized of data meaningful to backend database systems. Control 5 (Boundary Defenses) can ensure that the appropriate layered protections are in place to prevent/detect attacks aimed at your web servers. Control 2 (Inventory of Software) Control 3 (Secure Configurations) Control 10 (Vulnerability Assessment and Remediation) can ensure that vulnerable applications are accounted for, identified for defensive

[6] Ibid.

	planning, and remediated in a timely manner. [7]
Prevention of exploitation that grants the attacker the ability to put malicious code on the server and attempt to compromise all clients that browse that server.	Control 6 (Audit Logs) can assist in identifying when someone has compromised your web server. Control 18 (Incident Response Capability) can help mitigate the impact of, and assist in recovery from, attacks against vulnerable applications.

Source: "Twenty Critical Controls for Effective Cyber Defense Consensus Audit Guidelines"

4. Authentication/Identity (ID) Management

Adequacy of the authentication and/or identity management controls employed by commercial organizations or business sectors:

Based upon the information reported in the commercial and business sectors, the current implementations for authentication and identity management are not adequate. While the use of stolen credentials is widely prevalent with the proliferation of password-gathering malware like Zeus, internal agents now comprise 48% of the data breaches.[8] Abuse of system access and privileges involves 46% of data breaches caused by misusing organizational resources or privileges.[9]

Attacks from external actors are not necessarily difficult to prevent. Attack scenarios are most effectively and efficiently prevented before the adversary owns the box.

More incentives for development of multi-level authentication technology would help to prevent entry to the system. Also education programs developed for use by small/medium size companies to educate their employees on the dangers of Social Engineering attacks, and their use to provide entry into a system.

7. Research and Development

Cybersecurity disciplines that require more research and development resources:

Expanded research and development into active detection mechanisms would improve the security posture and reduce incident response times. Active detection mechanisms are not broadly deployed currently. Those active detection mechanisms that are broadly deployed led to only 4% of the data breaches reported in the *2010 Data Breach Report.* Yet, 86% of the victims of data breaches usually have evidence of the attack in their log files. Increased financial incentives for research and development of these tools (like the DARPA-BAA-10-84) would greatly improve the performance and adoption of these tools.

[7] 20 Critical Controls, Center for Strategic and International Studies

[8] 2010 Data Breach Investigations Report; Verizon RISK Team and US Secret Service.

[9] Ibid.

Another concern that could be addressed is the convergence of traditional telecommunications and internet infrastructure. What needs to be monitored to ensure adequate levels of protection have been applied to the underlying infrastructure?

8. An Incentives Framework for Evolving Cyber-Risk Options and Cybersecurity Best Practices.

Merits of providing legal safe harbors to those individuals and commercial entities that meet a specified and minimum security level

While the creation of legal safe harbors are generally desirable in that they provide value by establishing a level of legal certainty and spurring investment in desirable security measures, developing appropriate safe harbors may be difficult as there may be a need to establish different minimum security standards and best practices for different businesses and industries. Furthermore, due to the constantly evolving nature of cyber threats, there is also the risk that such standards will quickly become outdated Unless safe harbors are carefully designed to avoid becoming outdated and are tailored to the specific needs and risks of different businesses and industries, compliance with such safe harbors could result in wasted or misdirected investment in unnecessary and/or outdated security measures as well as a false sense of security.

9. Additional Comments

Challenge: Surface area to defend is huge. Need to scope the current defensive efforts focus on addressing standards, training, and incentives on infrastructure and platform solutions, as well as the applications and Operating Systems.

State of the industry on platform and infrastructure hacking:

- **Cloud Computing** presents a wide range of potential security threats both from outside the cloud and among the multiple tenants who share the resources in the cloud. However, cloud computing also provides an opportunity to create more secure environments with consistent, standard security controls that are centrally managed by security experts.

    1. VeriSign's iDefense team has cataloged hackers using legitimate cloud computing services and illegitimate bulletproof hosting services to store illicit material. Specifically, hackers have adapted the protocols of many social networking sites such as Twitter, Google groups and URL shortening services to send action messages to zombie computers.[10]

    2. New Command &Control channels using cloud technologies and other public services are not a surprise given the use of compromised Web servers, which attackers still use frequently to perform similar tasks. Using public services to issue commands are more reliable, given the inability o f administrators, Internet

[10] iDefense2010 Cyber Threats and Trends, Dec. 18, 2009.

service providers and blacklist services to label the domains as malicious. Attackers will continue to deliver commands through these media, as it is easier and less risky for fraudster to deal with legitimate services than to engage with other fraudsters.

- DNS supply chain organizations impacted by DNS-based attacks include registrars, operators, domain name owners, Internet Service Providers (ISPs) and Internet application developers. Forms of DNS-based attacks include:
    1. Distributed Denial-of-Service (DDOS) attacks;
    2. Man-in-the-middle attacks;
    3. Compromise of a DNS server to house false binding information;
    4. DNS cache poisoning; and
    5. Hacked host files.

  Mitigating these DNS-based attacks typically consumes 1-5 man days.

- Forrester research on DNSSEC finds half of the organizations surveyed have seen DNS-based attacks, DDOS and man-in-the-middle attacks have been the two most commonly seen attacks.
    1. eCommerce and ISPs top the industry that are concerned about DNS security. 93% have some existing measures to protect DNS servers yet 88% are ready to invest in additional DNSSEC security mechanisms. The community wants training and best practice knowledge to aid DNSSEC implementation. ISPs and application developers viewed as key for adoption.