Cyber Security: A National Effort to Improve

John Malgeri
Kennesaw State University
678.521.4136
jmalgeri@students.kennesaw.edu

ABSTRACT
New and advanced combinations of cyber security threats are being introduced into the online world. Malware authors are forced to create more efficient software with the advancement of network security systems. Recent governmental legislation offers support to companies that operate through the use of sensitive consumer information. Governmental agencies also promote consumer education about law enforcement actions under way. The reporting mechanism for information security incidents needs to be centralized to eliminate confusion amount agencies.

Categories and Subject Descriptors
K.6.5 [**Computers in Society**]: Security and Protection

General Terms
Management, Security, Legal Aspects.

Keywords
Cyber security, information security,

1. INTRODUCTION
To effectively manage against cyber security threats one must first fully understand them. The sophistication and effectiveness of cyber attacks are progressively moving forward. Attacks centered on manipulation and fraud of financial markets is one of the top cyber security threats in 2009. Other cyber security threats such as exploitation of social networks and damage created by disgruntled employees are rising dramatically [2]. Spam, phishing, spyware, and various other malware have become more prominent in today's online driven world. Although spam, phishing, and spyware were once seen as isolated challenges for organizations, hackers are now creating hybrid threats that can even infiltrate federal systems. The federal government has taken steps to help protect the private sector and themselves, but efforts must be made as a collective to improve cyber security reporting.

Spam, the distribution of unsolicited commercial e-mail, has become a nuisance for people at home and for organizations alike. The Anti-Spam Technical Alliance states that, in recent years, spam annoyance has become significantly worse in both quantity and quality. Spam makes up over sixty percent of all e-mail. This is becoming a worsening security problem for networks because of the potential loss of confidentiality, integrity, and availability of information systems that become distributers of cyber security threats. Many denial-of-service attacks have also been linked to spam. Most importantly for organizations is that the sheer volume of spam over a network slows down productivity, requires technical support, and consumes the operating bandwidth. Spam causes many organizations to allocate additional resources for the management of risk, which includes anti-spam software and increased storage space [3].

Spam can be boiled down to two fundamental issues. First, spam is a profitable business. Not only is sending spam inexpensive, but a percentage of people who are exposed to spam end up opening the messages and actually buying the products or services offered. Secondly, recipients of spam have a hard time determining if the message is legitimate or fake due to the lack of reliable information presented. Because of this, spammers can forge e-mail headers that appear to have originated from a source that is somehow connected to the recipient. Recent advances in anti-spam measures have forced spammers to become more intelligent about their methods for bypassing detection and filtration. Some of these methods are the use of alternate spellings, using various characters that look like letters, disguising the addresses in emails, and inserting the text as an image so that filters cannot read it properly. Spammers also become difficult to track because compromised computer systems delivery forty percent of all spam. This means that when someone is tracking a spammer they can be led back to an innocent user's computer instead of the true culprit. With recent potential for financial profitability, spammers, malware writers, and hackers have been merging methods into more advanced attacks [3]. Ryan Naraine of Kaspersky Lab believes that there will be an increase in malware detections by tenfold from 2008 to 2009.

Another high technology scam is phishing, which more often than not uses spam or pop-up messages to deceive people into divulging sensitive information such as Social Security numbers, credit card numbers, bank account information, and passwords. Phishers typically attack through e-mails that claim to be from a business that the target deals with on a routine basis, such as Internet service providers, banks, online payment services, or governmental agencies. These messages will ask users to update their account information and will typically use threats of time-sensitive consequences to put the user on the spot and further goad them into action. The user is then directed to a Web site that is constructed to look identical to the real Web site. This type of scam has caused thousands of people to have their identity stolen [3].

Phishing works through a carefully planned mixture of social engineering and technical skills to convince users that they are in contact with authorized individuals. Social engineering relies on

InfoSecCD '09, September 25-26, 2009, Kennesaw, GA, USA.

an attacker's ability to obtain information regarding businesses computer systems. Then through their technical skills, a phisher creates Web sites and e-mails that appear legitimate by easily copying images and layouts used by the original, legitimate organization. Phishers use knowledge of scripting languages to position what looks like the real address of the organization over the fake one. They can even forge the closed lock icon in the corners of browsers to convince users that the site is protecting their sensitive data through encryption. Through social engineering, an attacker can sometimes convince a target to open specific e-mail attachments or visit Web sites from which malware is then downloaded to the target's computer. Once this malware is installed, it has the capability of monitoring all information on the resident computer. For example, if the target were to visit an online banking website, the malware would capture valuable account information and passwords and forward it to the phishers [3].

Two main types of phishing have emerged based on their threats and victims. The first is employee targeted phishing that is received by employees of agencies. The second is agency exploiting phishing that mimics the identity of an agency to assist a phishing scam. Phishing is a very serious threat that doesn't only affect individuals but can also have huge impacts on major organizations. Phishing scams have exploited online financial and auction sites such as US Bank, Citibank, eBay, and PayPal. Some scams have infiltrated such federal agencies as the Federal Bureau of Investigation, the Internal Revenue Service, and the Federal Deposit Insurance Corporation. Phishing scams that result in the acquisition of user access information of such organizations as the FBI, IRS, and FDIC can have extremely damaging effects on the trust of E-government services. Gartner Inc. reported that direct phishing related losses to U.S. banks and credit card companies were estimated at $1.2 billion in 2003. Other areas that were affected – such as customer service expenses, account replacement costs, and higher expenses due to customers' decreased use of online services – caused indirect losses to be significantly higher than direct losses. In general, researchers have noted the potential for phishing scams to disrupt the growth of electronic commerce. Just as spammers have teamed up with other malware writers, some phishing scams have been known to install spyware, showing the evolution of more sophisticated online crimes [3].

Unlike spam and phishing, spyware does not have a widely accepted definition. Instead, there have been multiple definitions proposed by security experts and software vendors, evidenced by the varying interpretations of spyware in proposed legislation. Factors such as the type of information collected, the nature and extent of the harm caused, and whether the user consented to the downloading of the software all attribute to spyware's ambiguous definition. Though spyware is difficult to define, it can be broken down into two primary purposes: advertising and surveillance. Most of the time spyware can be found delivering advertisements to users in exchange for the free use of an application or service. Information is collected about the user such as their Internet Protocol address, online buying habits, e-mail address, Web surfing history, and software and hardware specifications. Then, based on the Web surfing history and buying habits, the end user will be targeted with pop-up advertisements for the products and services that interest them. Spyware has been known to go as far as changing browser domain name settings to redirect users to alternate search sites packed with more advertisements. Surveillance spyware is more malicious in that it's designed specifically to steal information or monitor information access. Key logging software stores the movements of every single move made on a system and transmits the information back to a database. Although both methods can be used illegally, they both can also be used for legitimate reasons. The previously mentioned surveillance applications can be used by organizations to monitor employee movements around sensitive company information. The Federal Trade Commission defines spyware as "software that gathers information about a person or an organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over computers without the consumer's knowledge." At first glance this definition can seem extremely negative for spyware, but one has to remember that there are a few instances, like employee monitoring, where spyware serves a useful purpose [3].

Just like phishing experts, spyware authors use social engineering techniques to lure users into installing their creations. The main technique used to dupe someone involves the creation of a pop-up window that informs the user that their computer is being affected by spyware, and that by downloading the software being offered they will rid their systems of the infections. In fact, the downloading of the proposed anti-spyware software will not safeguard the user's system, but open it up to many possible threats. Security experts have even noticed that no matter what choice the user makes they may still allow spyware to enter their system. Peer-to-peer file sharers must be on the offensive when it comes to spyware prevention. Often, spyware descriptions are offered in end user license agreements, but many people just click accept without reading all the terms of the agreement. While the spyware previously mentioned tricks users into installing its packages, some spyware spreads by exploiting system weaknesses. These weaknesses, such as low security settings in e-mail and Web browsers, allow malicious scripts to easily infiltrate their network and install spyware. One thing that separates spyware from other cyber security threats is the level of difficulty it takes to detect. The National Cyber Security Alliance and America Online found that 89% of users who were found to have spyware on their systems didn't even know it was affecting them. Many times people noticed a change to their operating systems but didn't consider themselves at risk and therefore continued to use infected systems. In these cases, users need not only to detect against future spyware, but also to remove the spyware already hidden on their computers. Because spyware doesn't come with its own uninstall feature, it forces users to manually remove it or be forced to use a separate tool. Once a spyware file has been removed, the user needs to recheck the entire system due to the fact that some spyware installs multiple copies of itself, and will repopulate if not entirely removed. Antivirus, antispyware, and firewalls must be rechecked after deleting spyware because some applications may have been turned off by the intruding software [3].

Similar to phishing, spyware can have a major impact on federal information systems by compromising their confidentiality, integrity, and availability through its ability to capture and release sensitive data, make unauthorized changes to systems, decrease system performance, and create new system vulnerabilities. Both types of spyware mentioned have the ability to collect any type of information on someone that is stored on their computer. Some advanced administration tools can even activate a computer's

Webcam and microphone to capture private information. Spyware can change a Website's appearance and forward users to specific sites with questionable content, therefore causing liability risks inside companies. Some applications have even been known to assist phishing scams by redirecting users to the fake Websites previously mentioned. Major new security concerns have emerged due to the ability of malicious users to remotely control a machine through spyware. Once a system's configuration is changed without detection, the system will become even more vulnerable to future attacks from other outside threats [3].

Botnets are quickly moving up the list of worst cyber security threats. A botnet is a computer that is infected with malicious code that allows some outside user to control that machines actions. Georgia Tech's Information Security Center predicted that in 2008 10% of online computers were part of botnets, and that by the end of 2009 that number may reach as high as 15%. One reason that botnets are quickly becoming so dangerous are that they can infect a computer through unavoidable means such as simple browsing or loading up of legitimate Web sites. Various other types of malware like Trojan horses have also been known to deliver botnets to a host. One very tricky aspect of botnets is that they can get past firewalls and other detection systems by looking like normal internet traffic and using accepted ports. Multiple botnets acting together are known as bot armies. These bot armies can general massive amounts of computing power, and this computing power can be used for data theft like social security and credit card numbers, denial of service attacks, spam delivery, and spoofing. While spam, phishing, spyware, and botnets are major cyber security issues, other threats like worms and viruses are still prevalent in the information security world [1].

Security experts have noted that the time between a system released vulnerability and an exploitation of that vulnerability is decreasing. These kinds of events are happening because the technology being used for the internet was not originally intended to be highly secure. The internet was primarily thought to be used only by scientists, but now years later has exploded to include millions of user's world-wide. Some people even believe that the internet will never be secure unless the underlying architecture is changed [4]. In 2004, the average exploitation code emerged within 5.8 days and more than 10,000 new viruses were identified in that year. This type of security evolution is forcing agencies to identify and correct newly released systems or patches in only a few days. Other advanced threats such as polymorphic, metamorphic, and entry point obscuring viruses are reducing the effectiveness of traditional antivirus software. Polymorphic viruses are encrypted and make use of a small decoder which decrypts the virus' main body right before execution. Metamorphic viruses actually change their code every time they replicate, resulting in very unique patterns that go undetected by basic antivirus software. Entry point obscuring viruses make detection more difficult by placing the malicious code in an unspecified location on the target's computer. Once one of these threats enters a computer system, the computer's risk for further criminal activity greatly increases. Users must make sure that they remain diligent in maintaining antivirus software because they put their entire organization in jeopardy when their computers become exposed. Through the blending of different types of malicious code like viruses, worms, Trojan horses, and spyware, criminals have created a versatility that allows them to get around organizations' security measures. Since the spring of 2007 the Secretary of Defense and The National Defense University had to take their email systems offline due to hackers, both the Republican and Democratic presidential campaigns were hacked, the Department of Homeland Security and the Department of Defense were attacked by outside threats, and many other instances have occurred to that show that cyber security disasters occur all the time [4]. These blended threats can cause massive damage by infecting a large number of systems in a short period of time with little human interaction. Some threats can simultaneously overload system resources and destroy bandwidth [3].

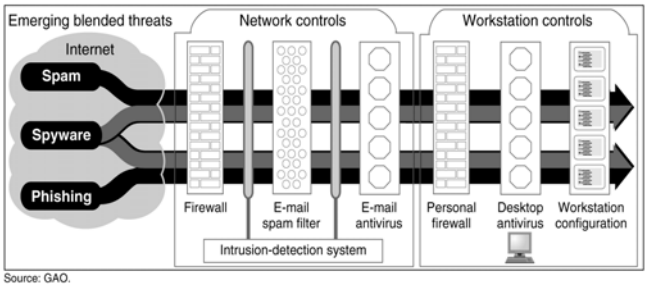

Figure 1: Blended Threats May Bypass Traditional Security Controls

Depicted above are just a few examples of how cyber security threats can team up and attack a system. Eight different types of system security measures are shown above. As can be seen, the combination of spam, spyware, and phishing may have no problem getting through all of them. Sobig is an example of one of the many dangerous blended threats out there. After Sobig infects a computer, it downloads spyware which contains a key logger program. The key logger monitors the computer for financial activity and user information, sending the information back to the authors. On top of that, Sobig downloads an unlicensed copy of the Wingate proxy server which allows spammers to anonymously send unsolicited e-mails. Spam will decrease the capability of technical resources while delivering dangerous mechanisms to others. Employees can become victims of phishing scams which in turn puts companies at risk. Additionally, spyware puts confidentiality, integrity, and availability of organizations systems at high risk. Many agencies face significant risks as new and improved cyber security threats surface [3].

Even with such strong proof to the dangers of cyber security threats, many companies do not take advantage of practices that could greatly enhance their protection. The Federal Information Security Management Act even requires such practices as performing periodic risk assessments, implementing security controls equal with the identified risk, ensuring security awareness training for personnel, and implementing procedures for detecting, reporting, and responding to security incidents. Due to companies' perceptions of risk and their effects, some of these requirements have not been met. In a study involving the 24 Chief Financial Officers Act agencies, 14 of the 24 agencies reported that spam took up network bandwidth and disk storages space which resulted in losses for the company. Only one of these agencies identified the possible risk of spam delivering phishing, spyware, and other major network threats to employees. This lack of knowledge could be very detrimental to a company, especially to one that doesn't even understand the potential risks their networks face. In a similar study, only 5 of the 24 agencies

reported that spyware had minimal to no effect on their operations. This means that 19 agencies believed that spyware had some kind of negative effect on the company such as loss of productivity, increased use of company support personnel, and network connection issues. Many companies are blind to the full effect of phishing scams. They believe that phishing scams are a personal risk to their employees, but not the company overall. When companies think foolishly like this and don't perform risk assessments, they become vulnerable to unauthorized access, disclosure, modification, or destruction of information systems that support the agencies operations. Listed below are major agencies that have been exploited by phishing scams [3].

Table 1: Federal Entities Exploited by Emerging Cybersecurity Threats

Entity	Exploit
Immigration and Customs Enforcement (ICE) (DHS)	E-mail claiming to be from an ICE agent referred users to ICE's official Web site in an effort to steal money from relatives of U.S. soldiers killed in Iraq.
FBI (Department of Justice)	Spoofed e-mail claiming to be from the FBI requested users to verify their information to avoid further investigation. The Web address contained in the e-mail was deceptive and led to a fraudulent Web site.
FDIC	Spoofed e-mail forwarded users to a fraudulent Web site that used FDIC's logos, fonts, and colors to request users to submit bank account information, as well as credit card and Social Security numbers.
IRS (Department of the Treasury)	Spoofed e-mail claiming to be from the IRS and an official-looking Web site were used in an attempt to trick recipients into disclosing their personal and financial data.
Bureau of the Public Debt (Department of the Treasury)	Spoofed e-mail from what appeared to be Public Debt e-mail addresses contained links to rogue Web sites. These sites claimed to be legitimate private commercial banking Web sites and attempted to obtain financial information from individuals.
Operators of the regulations.gov Web site: Environmental Protection Agency, Food and Drug Administration, Government Printing Office, and National Archives and Records Administration/Office of the Federal Register	Regulations.gov is a Web site where consumers can participate in government rulemaking by submitting comments. The e-mail included a link to a Web site that mimics regulations.gov and asked readers to provide their personal and financial information.
State Department	Spoofed e-mail claiming to be from security-abroad@state.gov and maintained by the department's Bureau of Public Affairs attempted to dupe recipients into clicking a link to download an executable file that would change access to specific folders and files.

In an effort to help companies with risk management, the National Institute for Standards and Technology created the *Risk Management Guide for Information Technology Systems.* This document breaks risk management down into identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. This guide will help any company form a foundation for mitigating risks associated with Information Technology Systems. Companies are taught to evaluate the current status of their information systems and to then establish a target for improvement [3].

Companies believe that issues such as unreliability and limited technical controls plague the information security arena. Most agencies (20 of 24) have reported the implementation of agency-wide anti-spam tools. Anti-spam tools scan, inspect, filter, and quarantine incoming messages that are flagged as potentially unsolicited e-mail. Spam filtering can be accomplished through many techniques such as whitelists, blacklists, and content analysis to name a few. The whitelist technique accepts any mail from users previously designated by the administrator. One issue here is that e-mail messages that exhibit characteristics of spam will be let through the filter. Similarly, blacklists prevent e-mail from specific IP addresses, domains, or individuals. Content analysis is a little more advanced in that it scans the subject line, header, or body of an e-mail for specific words identified with spam and then filters them accordingly. A company's largest concern with spam filters is the level of reliability. Users place a high priority on receiving every single legitimate e-mail and therefore will not accept a system that loses messages as a result of defective filtering [3].

In terms of stopping phishing scams that affect employees, companies feel like only limited technical controls are available. One company in particular wanted a way to control the many ways in which employees browse the Internet without restricting access to the point that job performance is affected. The first thing an agency can do is to take advantage of any enterprise anti-spam tools on the market to lessen the risk of employee targeted phishing. However, these anti-spam tools are not enough to guarantee a company's safety. For most anti-spam software, a person must review each quarantined message and either delete or keep the message. This type of approach can be hard to implement for someone not technologically savvy. The next step for a company is to actively search the Internet for ill-use of their trademarks, logos, and names. Not only does this method help discover phishing scams, but it also has been known to discover cases of trademark or copyright infringement. One very important method of operation for a company is to establish clear communication practices with customers. Clear communication practices help reduce phishing scam success rates. Letting a customer know that an e-mail will never ask for sensitive information protects the customer and the company. Phishers are excellent at exposing vulnerabilities in code. Properly secured services could reduce any company's risk of attack. Lastly, a company must respond quickly and effectively to a phishing scam once it strikes. The typical phishing scam will come from outside the agency's network. This means Internet Service Providers should be contacted to organize a cooperative effort to shut down the Website and preserve possible evidence for prosecution. Anyone that believes they are subject to a phishing scam should immediately contact the authorities to reduce the potential damage that can ensue [3].

Companies feel that the same immaturity that exists in phishing protection software also exists in antispyware programs. Antispyware programs work by scanning a system for known unwanted programs. Some tools use something called real-time detection, which continuously scans active processes in the memory. These real-time detection programs can prove to be very useful since most antispyware is detected after it has already installed itself on a host network. Approaches such as antivirus applications and firewalls can offer only limited spyware protection. The main functions of firewalls are to protect a network from unauthorized access. Sometimes firewalls have a difficult time distinguishing normal Web traffic from spyware traffic. Firewalls also have the ability to detect spyware when it tries to request access to the Internet. The NIST recommends that people use multiple antispyware tools because different technologies have different capabilities. Since no one spyware tool can detect all threats, having multiple options can reduce networks odds of infection. Tracking the true amount of spyware incidents is extremely difficult because spyware transmits using the same communications path as legitimate Web traffic. Software vendors have recently focused on the need for enterprise antispyware applications. New enterprise software allows companies to detect and block known spyware from centralized locations. This type of centralized administration provides updates for individual clients and schedules for system scans, monitors newly found spyware, and determines if detected spyware has been removed. The largest drawback for antispyware tools is that spyware can only be detected if the tool has prior knowledge of its existence. This means that all antispyware tools must be constantly updated for new information [3].

The United States government has implemented several laws aimed at improving the nation's cyber security stance. Federal networks and systems are in a constant battle with outside threats trying to obtain sensitive information. As technology evolves more every day the United States is slowly acquiring a competitive disadvantage against cyber criminals. Criminals that

have no boundaries and that are finding ways to steal personal and financial information [5]. At the forefront of these laws is The Federal Information Security Management Act of 2002 (FISMA), which calls on federal agencies to maintain the confidentiality, integrity, and availability of their information. Within FISMA, the Office of Management and Budget (OMB) is given specific information security responsibilities. The Director of the OMB is charged with providing guidance to agencies on detecting and reporting incidents. In August of 2004, the OMB and FISMA issued instructions which established yearly reporting of security controls to maintain acceptable levels of security. FISMA requires agencies with national security implications to provide information regarding their information security practices. A periodic assessment of risk and the magnitude of harm that could result from the loss of sensitive information must be implemented. Based up risk, policies and procedures must cost-effectively reduce information security. Back up plans that contain a certain level of necessary information about networks, facilities, and systems must be created. Anyone involved in the use of information systems must pass a security awareness training program. Corrective action must be taken against any information security deficiencies. Agencies involved with information security must also have a set strategy for detecting, reporting, and responding to security incidents. All of these steps implemented by FISMA have an extremely positive impact on agencies. One of the problems with FISMA is the avenues through which companies are expected to report. FISMA makes every agency report annually to the OMB, various congressional committees, and the Comptroller General. These agencies are supposedly held accountable for compliance with the aforementioned FISMA requirements [3].

The affects of FISMA were also extended out to the NIST to provide guidance on the protection of information security programs. The NIST has published many documents in efforts to assist agencies in protecting their systems from modern cyber security threats. One such publication is *Computer Security Incident Handling Guide*, aimed at establishing incident response protocols for a company. The NIST's *Guidelines on Electronic Mail Security* explains multiple practices that can be implemented to help secure a mail server and its surrounding infrastructure. The first step is to create an information systems security policy that is implemented organization wide. Various other steps include risk assessment and management, standardizing software configurations, security awareness and training, and contingency planning. The NIST has provided dozens of special publications for the public to take advantage of to further protect themselves from imminent threats [3].

The Homeland Security Act of 2002 enabled the Department of Homeland Security to have a critical role in cyber security prevention. Minor influences of The Homeland Security Act brought about the increase in penalties for fraud and computer related criminal activities. The Department of Homeland Security's main efforts were put towards developing a national plan, analyzing ways to protect critical infrastructures, and the collection of information for both government and private sector entities in response to terrorist activity. The Department of Homeland Security was also put in charge of providing vulnerability analysis to governmental and private entities that operate critical infrastructure. Part of this vulnerability analysis includes crisis management support in relation to critical information systems. Technical assistance is also provided in response to major information system failures [3].

In another attempt to reach out to both governmental agencies and the private sector, The President's National Strategy to Secure Cyberspace was issued on February 14, 2003. This strategy called forth specific recommendations for the DHS to improve analysis awareness and threat reduction. Specifications were narrowed by asking for a better defined approach on which vulnerabilities were disclosed. The DHS needed to create universal test beds for commonly used applications to help in the reduction of redundancy. A best practices strategy needed to be formed for areas like training, patch management, and analysis of attacks. Part of the collective effort included development of national response to cyber incidents. This helped reduce wide area damage by alerting the proper authorities who could then alert other agencies nationwide. The Department of Homeland Security became even more involved after the passing of Homeland Security Presidential Directives. These Directives added to the responsibilities of the Secretary of Homeland Security, which ranged from the creation of a new National Response Plan to the coordination of efforts with the Department of Defense over incident response [3].

The Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003 was designed specifically to attack the rising threat of spam, phishing, and spyware. CAN-SPAM is the first federal law that specifically targets the transmission of commercial electronic messages. Unfortunately this act did not outright ban the distribution of unsolicited e-mail, it just created a set of parameters for which the process of distribution could operate. The federal government established a strong anti-spam stance here by prohibiting the use of deceptive or misleading information in the header or text of the e-mail. Spammers could no longer send e-mails to accounts that were acquired through illegal activity. Strict guidelines were also established in regard to the spreading of sexually oriented material. Under CAN-SPAM, people found in violation of this act are subject to civil and criminal penalties of fines up to $6 million and a maximum prison sentence of five years. Over time the CAN-SPAM Act has received heightened criticism for its supposed lack of enforceability. However, the act has succeeded in bringing about multiple prosecutions at the federal and state levels. The first wireless spammer, along with other criminals, has been convicted under the CAN-SPAM Act. State legislatures have also created their own laws extending the influence of the CAN-SPAM Act [3].

The government has done a good job of providing legislation that prosecutes individuals for their criminal activity. Now the goal of both the federal government and the private sector is to raise education and awareness levels of major cyber security threats. As stated earlier many organizations do not fully comprehend the implications of security vulnerability. A program to educate both Federal leaders and members of the workforce would go a long way in raising the cyber security mind set [5]. In the fall of 2003, The Anti-Phishing Working Group was established to combat the increased threat of phishing. As an industry focused association, The Anti-Phishing Working Group created forums for discussion of any topic related to phishing and the eradication of this problem. The Phish Report Network's focus is to help rebuild consumer confidence in e-commerce by creating a united defense against modern phishing efforts. This united front is created through a sender and receiver network interaction. Any company

that falls victim to a phishing attack can securely report phishing sites to a database. Then, Internet service providers or other interested organizations can join the network and receive the information and block the reported sites. Governmental agencies such as the FDIC believe the best way to fight phishing is through end-user education. The FDIC maintains a telephone service in which callers can ask questions about messages that they have received claiming to be from the FDIC. These types of efforts help prevent many people from being duped by phishing scams [3]. The main issue is that as a whole, the United States is too dependent upon cyberspace, and being the wealthiest economy, cyberspace criminals target here first [4].

After all the proposed legislation, lawsuits, and consumer education about cyber security threats, the federal government has an extremely inconsistent manner in which to report incidents. Agencies such as the Department of Homeland Security, the Office of Management and Budget, and the Federal Information Security Management Act all supposedly have the responsibility of identifying and taking action against cyber security incidents. No consistency exists between how and to whom reports should be sent. Organizations have realized that there is no central federal agency that exists to completely cover all their needs. The government needs to establish clearly defined roles and responsibilities for cyber security protection. Harry In a 2009 address to a governmental subcommittee, Harry Raduege stated the need for "a properly structured and resourced organization that leverages and integrates the capabilities of the private sector, civilian government, law enforcement, military, intelligence community, and our nation's international allies to address incidents against critical cyber infrastructure, systems, and functions, is essential." FISMA declared that the OMB be responsible for a federal information security center. The OMB then specified that operations for this center have been transferred to the DHS's United States Computer Emergency Readiness Team (US-CERT). Many agencies have claimed to report incidents to US-CERT, law enforcement agencies, or keep incident reports internal. US-CERT officials have stated that report consistency is rare, and even if they receive information on an attack, the level of detail is minimal. On top of lackluster reporting methods, many agencies see multiple copies of incidents because organizations forward the same reports between themselves. Agencies attribute this institutional confusion to the federal government's inability to assign specific responsibilities and processes and then to uphold these decisions. Many people believe the government also needs to define a clear framework for the roles and responsibilities of institutions that collect issue occurrence reports. The last known efforts to establish consistent incident reports was stated by the DHS, in that US-CERT is working closely with OMB to meet current needs. This lack of coordinated effort can potentially nullify all the previous hard work, because of muddled end-user specifications [3].

Information Security Curriculum Development Conference 2009, September 25-26, 2009, Kennesaw, GA, USA.

2. CONCLUSIONS

Cyber security threats such as spam, phishing, spyware, and botnets each present a unique challenge to companies trying to protect sensitive information. Modern authors of malware have begun to realize that past methods are no longer as effective as they used to be. As a result these authors have created new blended threats to counteract advances made in information system security. These blended threats produce the capability of bypassing system firewalls, workstation configurations, and various other intrusion-detection systems.

Government bodies have made huge advances in cyber security legislation to help protect private sector consumers and themselves. Some legislative efforts focus on the creation of governmental entities that will provide support against systems attacks. The Federal Information Security Management Act of 2002 is one such act that establishes clear criteria to improve cyber security programs. Other agencies such as the Office of Management and Budget and the Department of Homeland Security help with the reporting and analysis of cyber security incidents. Some governmental legislation was created to deal with the prosecution of criminals in an effort to deter criminal activity. CAN-SPAM was the first federal law that addressed the transmission of unsolicited electronic messages. CAN-SPAM established a new electronic precedence which saw the trial of many malware authors.

Several of the positive steps forward made by governmental agencies are negated when companies must report information systems incidents. Legislation did a good job of laying the groundwork for anti-malware detection, analysis, and internal prevention. Agencies though have never been given a centralized location for which to report problems to. This can cause problems for other agencies that don't know about some of the current threats that exist. If an organization ever does receive an incident report, the report typically leaves out pertinent information about the security threat.

To effectively manage against cyber security threats an organization must be involved from process start to process end. A company must be knowledgeable about the current threats in existence and the ways in which to help protect against those threats. They must also be up to date on legislative proceedings that could affect the manner in which they conduct business. Finally a business must know where and to whom to report information security risks.

3. ACKNOLWEDGEMENTS

Thanks to Andy Ogden for all the useful input.

4. REFERENCES

[1] Ahamad, M. (October 2008). Emerging Cyber Threats Report for 2009. Retrieved July 15, 2009, From http://www.gtisc.gatech.edu/pdf/CyberThreatsReport2009.pdf

[2] Bass, T. (January 2009). The Top Ten Cybersecurity Threats for 2009. Retrieved July 15, 2009, From http://www.thecepblog.com/2009/01/05/the-top-ten-cybersecurity-threats-for-2009-draft-for-comments/

[3] Nicholas, J. P. (May 2005). Information Security: Emerging Cybersecurity Issues Threaten Federal Information Systems.

Retrieved June 9, 2009, from http://www.gao.gov/new.items/d05231.pdf

[4] Lewis, J. A. (May 2009). Cybersecurity: Emerging Threats, Vulnerabilities and Challenges in Securing Federal Information Systems. Retreived July 15, 2009, from http://governmentmanagement.oversight.house.gov/story.asp?ID=2421

[5] Raduege, H. D. (May 2009). Cybersecurity: Emerging Threats, Vulnerabilities and Challenges in Securing Federal Information Systems. Retrieved July 15, 2009, from http://governmentmanagement.oversight.house.gov/story.asp?ID=2421