Information Systems Management in Government: Ongoing Issues and Approaches

Young B. Choi*, Augusta Hayward, Sara J. Forkey, and Roy Griffin
Department of Business, Leadership, and Information Systems
College of Arts & Sciences
Regent University
1000 Regent University Drive
Virginia Beach, VA 23464-9800
USA
*E-mail: ychoi {at} regent.edu

Abstract --- We will identify how Information Systems (IS) are managed in the United States government. Furthermore we will discuss diverse approaches to developing and maintaining a secure IS and various ongoing issues and resolutions to this conflict.

Keywords-Information Systems Management, Government, FISMA, NIST, Defense-in-Depth, Cyber Threats, Information Systems Security

I. INTRODUCTION

Information Systems have taken over as the latest and greatest system of record keeping. IS can store a large amount of data in quite a small space. It is not only a more cost effective measure, but it is also much easier for the end user to utilize rather than working on a paper based system. The United States government stores most of its data on its IS and this data is sensitive and vulnerable to many different kinds of attacks and infiltrations. The management of IS in United States government is a daunting task and one that requires a great skill set and knowledge.

In this paper, we will address currently outstanding security issues in government and federal government management responsibilities. Based on the Information Systems security compliance of FISMA and NIST standards, the ways of federal government Information Systems protection will be suggested.

II. SECURITY ISSUES IN GOVERNMENT

This section introduces currently outstanding security issues in government briefly in the aspects of Web, email, authentication, encryption, digital signature, VPN (Virtual Private Network), and fault tolerance.

A. Web Security

There are many security issues arising from technology advancement. It is important to realize the direction of where we are heading.- When dealing with management of personalized services within our government, there are many threats that could evolve very quickly including viruses, works, Trojan horses, packet sniffers, stolen identity, and much more. In order for them to protect the services offered, they must know what they are up against.

Plug-ins for government sites that might be required could play a role in the performance of the program being offered at the time. If there are errors or conflict between plug-in and browsers/software then the task at hand might fail and cost the government millions of dollars. Services offered to individuals are very important considering so many Americans rely on government aid.

Client authorization for users trying to log on to a service at hand might need to have a specific type of answer key to obtain their information considering the government has so much information stored on so many people. This prevents identity theft and much more. The key distribution allows for the individual to decode a message that they are trying to receive. The IRS (Internal Revenue Service) or other government sites that apply to individuals require some sort of encryption or password to identify who you are. "Agencies must set service standards and use customer feedback to improve the customer experience. Agencies that provide significant services directly to the public are required to identify and survey their customers, establish service standards and track performance against those standards, and benchmark customer service performance against the best in business [3]."

Deploying and managing web-based solutions are important to the upkeep and maintenance of a site. There are many examples of this issue, but the most recent one I can come to think of is the Obama Care website. Julie Bataille, a CMS (Centers for Medicare & Medical Services) spokeswoman, said Monday that CMS had fixed "one bug" that was responsible for about 80% of the 834 enrollment errors. The bug, she said, prevented a Social Security Number from being included in the form [1]." It continued to have many issues while people tried to just obtain information. For this, a fix was needed extremely fast considering many people trying to obtain some sort of knowledge on the subject. Since this directly dealt with personalized services towards people, there should have been test runs of the site before deployment of the final product.

A comprehensive readiness assessment framework for identity theft safeguards in Web-based electronic government information systems was proposed by Ryoo, Oh, Shin, and Choi [10] and a multi-dimensional classification framework for developing context-specific Wireless LAN (WLAN) security attack taxonomies was suggested by Ryoo, Choi, Oh, and Corbin [11].

B. Email Security

Inside the government, most individuals rely on email for communication between one another. Snail mail (surface mail) is becoming obsolete whereas email is taking over and has become a more efficient and reliable way of sending a message. There are four different elements that make up an email. The first one is MUA (Mail User Agent), which deals with sending and receiving messages. The second one is MTA (Mail Transport Agent) has to do with a server based transfer between machines. The third component of the individuals email is MDA (Mail Delivery Agent), which goes back and forth between MTA's. The last type is a MRA (Mail Retrieval Agent) gathers messages from other inboxes.

Since the government and everyone else rely on email so much, there is a standard of components put in place. A header section is for information use which allows a person to see details of the message. The email includes a date of which the email has been sent, a "To" section which shows who the email is going to, a "From" section providing information on who sent the email, and a "Subject" section allowing the user to give a brief view of the email is about. There is also a carbon copy (Cc) area to allow a person to add other recipients. Last there is a blind carbon copy (Bcc) area where you can send a message to others without anyone else knowing who else is receiving the message.

With all the information being sent back and forth between individuals, there should be some type of encryption. Some parts of the government actually have users use a free service that is called PGP (Pretty Good Privacy). This encrypts email, allows for verification of the user, and compresses any data files one might need to include. This produces the amount of privacy needed between users to secure a message without decryption occurring from any outside sources.

One of the biggest security risks with email for individuals within the government or outside is spam. This is a junk email that gets sent to individuals that usually contains advertisements. There are some that might contain other threats if opened such as viruses. Other threats for email-based programs include phishing, which deals with stealing someone's password, and snarfing where someone intercepts an email message stealing anything of value.

C. Authentication, Encryption, and Digital Signature

Other than email, people user multiple types of services or workstations for work or personal use. In order to gain proper access, one must need the right credentials allowing for authentication of their identity. Usually a username and password is required. Many times, a system requires specific types of requirements when creating an individual password. There are also access cards used within the government for individuals to obtain clearance to certain areas. This is a security feature that allows information and sensitive data to be kept private from outside users. Another form of authentication is retina scanning.

Encryption of data for personalized services is of extreme importance. Without this, personal information could be stolen very easily resulting in identity theft. There are two major types of computer encryptions, which is symmetric-key encryption and public-key encryption. Our government and many other businesses focus on the use of firewalls, which blocks any unwanted data from entering the database. Another way to encrypt data is hashing. This is good for keeping records confidential because it creates a type of ciphertext that cannot be decrypted without a correct key.

A digital certificate is a good way to keep data secure because it provides asymmetric key pairs to a specific person. This is done through a third party who holds the proper credentials. Digital signatures can also give users a secure experience. These work of public-key infrastructure deals with electronic messages being sent back and forth. "The interest in e-signature technology and digital signatures continues to swell among government agencies of all sizes because it delivers a big impact. This makes e-signatures particularly intriguing for the approximately 75 percent of government budgets – at all levels – that are stabilizing or increasing, according to Gartner Research [2]."

D. Virtual Private Networks

Individuals using services that include Wi-Fi in public areas may still need to relay private information to each other. When this happens, a good type of connection is a VPN (Virtual Private Network), which allows for a secure connection between the source and the remote location the user is trying to access. It allows for tunneling to occur. This combines the data into packets of secure protocols, which allows for the proper encryption to occur for exchange information without a possible interception of information.

VPNs contain hash secure which ensures the transfer of data engulfed with encryption. The secure transaction allows for the user to keep their privacy along with the assurance and confidence of secure data transactions. This also authenticates the majority of types of data being sent through the tunnel of a virtual private network. The connection used for these individuals when linked up with a VPN are SSH (Secure Shell) and PPP (Point-to-Point Protocol). These tend to not have as many issues when connected to dynamic IP addresses.

Only people with proper authorization can actually access the VPN. This helps with keeping the level of security on track. As users enter their credentials, you can see who is registering any data to the system and can track their individual accesses.

E. Creating Fault Tolerance

Using networks and workstations within the government and really any work type of environment has to prepare for some degree of fault tolerance. This is where even when a system messes up, you can still recover and strive to have a workarounds until the equipment is backed up and running properly. It all depends on how long they are willing to wait. One of the easiest ways to solve a workstation problem is to use the procedure of process of elimination. If someone cannot fix the problem, replace the workstation with an extra one set aside for emergencies like this.

The reasons for failure of equipment to occur might happen simply because of user error. This of course might not always be the case unfortunately. There are viruses and worms that can cause a massive outbreak on a network. There are also acts of sabotage and terrorism on the extreme side. The other one besides user error most likely to occur would be natural disasters.

One preventive measure that the government takes for managing the personalized services is keeping proper backups of all the data at remote locations. This option comes in hand in case of a system crash or some kind of natural disaster. Another preventive measure performed is archive marking. This allows for privileged users to see if any of the files have been modified by any way. Generators always seem to come in handy as well. This allows for enough backup power so the machines would not shut off and cause damage to the files stored on the hard drives. Taking secure measures also means putting up secure walls and advanced security systems to prevent any unauthorized use by gaining physical access to the network.

Deployment testing is another way to ensure individual users are getting the most and best experience of their personalized services. Performing these tasks gives the developer an idea if there will be any bugs between one Operating Systems (OS) or another. It prevents users from experiencing issues with the program being brought forth and creates as little errors as possible for the final developed product.

F. Incident Response

The types of incidents that can happen to a network including individual workstations include natural disasters, hackers, and the loss of power. Once again, you have to be ready for all of these situations at all times. There are many incidents that fall under the above categories such as confidentiality, reconnaissance attacks, repudiation, harassments, extortion, pornography, organized crime, and hoaxes.

The key is to know whom you report a situation to. This simplifies things keeping a bare minimum to the chaos that is probably going on around the incident at hand. The best response that someone could do first is to report this to personnel who include security coordinators, CSIRT (Computer Security Incident Response Team), FedCIRC (Federal Computer Incident Response Center), and the police. Each branch has their own step-by-step procedures that they follow and who they report to.

In order to recover any drastic situations, response teams may need to work longer hours to fix the devastation and the complications for which an area might be experiencing. Tracking charts allow them to keep proper information on an incident that has occurred. The record on file allows people to see how previous situations were handled. It could help out a great deal if a difficult decision is put on the table.

Usually in these cases most places have put a CSIRT in place. This group ensures the proper format is taken in to action. They are aware of the correct way to handle situations because they create the plans for such situations. When having a CSRIRT team in-house, everything is run smoother because they know the policies that can be carried out.

III. FDERAL GOVERNMENT MANAGEMENT RESPONSIBILITIES AND CYBER THREATS

A. Federal Government Management Threats

The federal government has been, and is continuing to be, a major user of information technology since the development of first generation technology. The nation is heading towards a “paperless” society and as an end result we need more security on our computers and databases. IT is vital to the public, to agency missions, and the functioning of the government as a whole. “The security of these systems and data is essential to protecting national and economic security, and public health and safety. Safeguarding federal computer systems and the systems that support critical infrastructures—referred to as cyber Critical Infrastructure Protection (cyber CIP)—is a continuing concern [9].“ IS management consists of many different components such as planning, procurement, information trends, implementation and congressional policy. As a result of IS requiring such a high level of protection this has given a rise to a theft of information via computer systems called computer crime. Computer crimes have reinforced the fact that IS having a great many vulnerabilities. So with this in mind, effective information security cannot be independent of the other aspects of information management, but has to incorporate all aspects as a whole.

B. Cyber Threats

"Cyber threats and incidents are increasingly prevalent. Threats to systems supporting critical infrastructure and government information systems are evolving and growing. These threats come from a variety of sources and vary in terms of the types and capabilities of the actors, their willingness to act, and their motives [9]." These threats are real, they are serious, and the trend is on the rise. These types of threats can occur at any time of day and can affect one computer system, multiple systems, or even servers, at any given time making their detection a difficult challenge. With such vulnerable and sensitive information to protect, the federal government has gone to great lengths to protect their IS from cybercrime. This includes monitoring the IS, tracking the data that is found, and addressing situations at hand and ways to combat the attacks. "GAO and agency inspector general reports have identified challenges in a number of key areas of the government's approach to cybersecurity, including those related to protecting the nation's critical infrastructure. While actions have been taken to address aspects of these challenges, issues remain in each of following areas [9]." These areas include, "Designing and implementing risk-based cybersecurity programs at federal agencies; Establishing and identifying standards for critical infrastructures; Detecting, responding to, and mitigating cyber incidents; Promoting education, awareness, and workforce planning; Promoting research and development (R&D). Managing risks to the global information technology supply chain and addressing international cybersecurity challenges [9]." With the government issuance of such "strategy-related documents" the administration has taken forward moving steps to enhance many cybersecurity vulnerabilities that have emerged over the course of many years.

IV. INFORMATION SYSTEMS SECURITY COMPLIANCE: FISMA AND NIST STANDARDS

A. Information Systems Security Compliance to FISMA Standard

As security threats known and unknown continue to grow, industry leaders are requiring organizations both public, local and state governments to implement safeguards that comply with the security standards as defined by NIST (National Institute of Standards and Technology) Federal Information Risk Management Framework. "The major focus of NIST activities in IT is developing tests, measurements, proofs of concept, reference data and other technical tools to support the development of pivotal, forward-looking technology [6]." There are specific requirements for information security that were designed by Federal Information Security Management Act of 2002 (FISMA) to decrease vulnerability in computer systems, but these requirements did not give much instruction on how to implement these security guidelines. This recommendation is to create a subjective risk assessment approach coupled with a quantitative metric that will measure, manage and track the status of IS compliance with FISMA. Using a risk based approach will help determine the level of risk, the likelihood of the threat exploiting an existing vulnerability. According to Hulitt, & Vaughn, "The managed risk approach is recognized as the best way to achieve good information security [4]." As the federal government takes the lead in establishing guidelines, NIST was tasked with creation of standards and policies that governs the implementation of the Risk Management Framework (RMF).

B. NIST Compliance Regulation

Secure management in IS is difficult enough for any corporation to handle let alone a large business such as the government. There are many questions that come to mind when primarily addressing the management of secure IS and how to find commonality with the security framework for all government systems. One place to start is the NIST. "Founded in 1901 and now part of the U.S. Department of Commerce, NIST is one of the nation's oldest physical science laboratories [8]." NIST helps to regulate and standardize instruments that professionals use on a daily basis and also have updated their guidelines for establishing risk assessment in federal IS. "Under the Federal Information Security Management Act, NIST is responsible for developing guidelines, standards and specifications for IT security, but the FISMA requirements do not apply to the .mil domain or to national security IT systems. That split has resulted in separate but overlapping security programs for the different sectors of government. Civilian, military and intelligence agencies have been cooperating for four years to bring their information security policies in line with one another's under the Joint Task Force Transformation Initiative [7]." All government systems need to have a common baseline security framework to function. With the new revisions of NIST the government is working towards a common security framework for the government as a whole. This is a challenge, but with the assistance of a set of more stringent standards such as NIST this goal is more achievable to reach and covers a more broad range of agencies than just the older FISMA requirements.

V. FEDERAL GOVERNMENT INFORMATION SYSTEMS PROTECTION

In this section, how federal government information systems are protected with the principle of Defense-in-Depth and various available security technologies.

A. Protecting Federal Government Information Systems

The federal government has a major role in protecting sensitive information; however this role is not just in managing its information but also protecting the IS of the citizens, federal, and state level agencies. Jordan states, "United States federal government agencies, whether civilian or military, are a regular target of cyber-attacks from a variety of sources. These sources range from amateur to experienced hackers, hostile nation states, or even agency personnel.

Agencies are good targets for cyber-criminals because their IS hold a treasure trove of data [5]. To manage and protect information, the government agencies have to abide by legal statues and regulations instituted of Congress and oversight bodies who govern their IS. Also, there is a certain amount of information that is disclosed by the federal agencies over the Internet, so the government has to ensure that sensitive information is not improperly disclosed or remains confidential as needed.

Without proper security, the government opens itself up to spy activity and risk harm to the military troops, including possible exposure of citizens to cybercrime. The federal government also has defined Information Security as, defined by 44 U.S.C Section 3542 is "the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destructions in order to provide confidentially, integrity and availability (CIA) [5]." The government realizes that processes, standards and technology go hand in hand in creating a layered defense against intrusions, and unauthorized access to information systems and data. Information Security and Computer Security are used interchangeably, but Computer Security implies the security of everything associated with it, such as the building, terminal, printers, cabling, disks and tapes [5].

B. Federal Government Defense-in-Depth

The Federal government strategizes on how to provide and maintain confidentiality, integrity and availability to federal IS and cyber-based critical infrastructures by employing the regulations enacted by NIST to protect their data and they strongly encourage all other agencies and departments to do the same. There are several federal organizations that have regulatory supervision of U.S. civilian agencies, for instance, “All U.S. civilian government agencies are bound by legal statutes enacted by the US Congress and regulations from oversight agencies (e.g., General Accounting Office, NIST, and Office of Management and Budget) in the way information security and information systems are managed [5].” And some of the agencies also have reporting requirements to the US House of Representatives as it relates to Homeland Security.

Most officials were concerned about attacks from individuals and groups that may have malicious intent such as criminals, terrorists, and foreign nations including information warfare, hackers, virus writers, and disgruntled employees and contractors (Jordan 2012). There are outside threats that have their concern like espionage (foreign governments damaging IS for political or economic gain) and spear-phishing (emails crafted to gain unauthorized access to confidential data held by the agency). If the federal government suffers any of the above threats, or malicious acts, the impacts could be severe, for example, “Resources, such as federal payments and collections, could be lost or stolen sensitive information, such as national security information, taxpayer data, social security records, medical records and proprietary business information could be inappropriately accessed and used for identity theft or espionage [5].”

C. Approaches to Federal Government Security Protection

It does not matter whether an organization is a government or private sector implementing industry based best practices to secure their data and network is good strategy though there may be several approaches to doing so. Stacy Jordan recommends that a defense-in-depth that incorporates hardware protection via hard disk encryption; Software protection using McAfee E-Policy Orchestrator and other Windows based equipment and using role based information security policies [5]. There are different techniques utilized by federal government IS. First and foremost building a secure network based on industry best practices in hardware, software and policy represents a sound strategy. This is the groundwork for building defense-in-depth. According to Stacy, hardware protection is mentioned as “Hardware protection devices include firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Host Intrusion Protection System (HIPS) and biometric devices (e.g., retinal scanning, secure token devices, etc.) [5].”

This approach boasts some of the more advanced techniques to information security in terms of biometrics. In terms of software protection, Stacy reports, “All agency equipment is registered with the master ePO (McAfee ePolicy Orchestrator) server and Information Security Officers (ISOs) receive an email when a device is suspected with some type of malicious software. Patch management for all Windows based equipment is done through a combination of Microsoft System Center Configuration Management (SCCM) and IBM's Tivoli Endpoint Manager (BigFix) [5].” Maintaining a standard desktop while keeping the software updated from one central location is also key to security improvements. In addition to running patches on off peak hours, reports are run to show compliance, system vulnerability, encryption and operating system. Most importantly, the agency uses Public Key Infrastructure to protect email messages that contains sensitive data. Stacy reports, “Agency personnel and partners can obtain certificates in order to properly secure messages that contain information like social security number, medical conditions, bank account number or employee performance rating [5].” The federal government also encourages mandatory training for security policies so that employees will know what is appropriate in protecting sensitive information. In fact, “Agency use software protective measures to enforce agency-wide security policies (e.g., prohibited use of non-encrypted and non-agency issued flash drives, using bandwidth intensive applications, downloading unauthorized software) as a means to decrease exposure to malicious software [5].”

VI. CONCLUSION

Information Systems, due to their vast number of vulnerabilities, needs to be properly managed and maintained. Even though the United States government has seen some recent trials and tribulations with the security of their IS, they have ultimately been extremely adept at accepting new technologies and deploying their usage. This not only aids the United States government in ensuring proper deployment of resources, but it also ensures that its citizen’s data is properly safe and secure from malicious attacks whether it is from a physical attack or a cyber-based attack.

REFERENCES

[1] LOGIURATO, B. (2013). *Politics*. From Business Insider: http://www.businessinsider.com/obamacare-website-back-end-issues-834-healthcare-gov-2013-12

[2] Power, M.-E. (2013). *Digital Signatures Push Success of Business Priorities for Governments of All Sizes*. From silanis: http://www.silanis.com/blog/archives/digital-signatures-push-success-of-business-priorities-for-governments-of-all-sizes/

[3] *Requirements and Best Practices Checklists*. (2013). From HowTo.gov: http://www.howto.gov/web-content/requirements-and-best-practices/checklist

[4] Hulitt, E., & Vaughn, R. B. (2010). *Information system security compliance to FISMA standard: a quantitative measure.* Telecommunication Systems, 45(2/3), 139-152. doi:10.1007/s11235-009-9248-8

[5] Jordan, Stacy. (2012). *Defense in Depth: Employing a Layered Approach for Protecting Federal Government Information Systems.*Retrieved From: https://www.sans.org/reading-room/whitepapers/bestprac/defense-depth-employing-layered-approach-protecting-federal-government-information-system-34047

[6] NIST (2013). *Federal Information Processing Standards Publications (FIPS PUBS).*Retrieved on 01 December 2013 from http://www.nist.gov/itl/fips.cfm

[7] Jackson, William. (2012) *Common IT Security Framework for Government Gets a Step Closer*. GNC. Media, Inc. Retrieved on 07December2013 from http://gcn.com/Articles/2012/09/21/NIST-Risk-Assessment-Guide.aspx?Page=1

[8] NIST Public and Business Affairs. (2013). *About NIST*. Retrieved on 07December2013 from http://www.nist.gov/public_affairs/nandyou.cfm

[9] U.S. Government Accountability Office. (2013). *Protecting the Federal Government’s Information Systems and Nation’s Cyber Critical Infrastructures.* Retrieved on 07December2013 from http://www.gao.gov/highrisk/protecting_the_federal_government_information_systems/why_did_study#t=1

[10] “A Comprehensive Readiness Assessment Framework for Identity Theft Safeguards in Web-based Electronic Government Systems.” with Jungwoo Ryoo, Tae Hwan Oh, and Seungjae Shin. The Electronic Government: An International Journal, pp. 19-40, Vol. 6, No. 1, 2009.

[11] “A Multi-Dimensional Classification Framework for Developing Context-Specific Wireless LAN Security Attack Taxonomies.” with Jungwoo Ryoo, Tae H. Oh, and Gregory Corbin. The International Journal of Mobile Communications (IJMC), pp. 253-267, Vol. 7, No. 2, 2009.