**Case Study #2: Can We Ensure Digital Government Services Are Secure?**

**Meg Crouch**

**CSIA-360**

**4 April 2016**

**Overview of Digital Government**

            With the growing range of electronic devices, social media communication, and cloud-computing, there is an increasing need for the Federal Government to serve the American people through the use of technology and fast-paced communication. This kind of need pertains directly with cybersecurity and efforts to maintain secure information. Cybersecurity represents the ability to protect information in communication systems from damage, exploitation, or unauthorized use (NICCS, n.d.). In order to regulate how information is digitally presented, President Barack Obama issued a large statement regarding Digital Government and how it allows Americans to have digital information readily available at any given time or place, on any device (Obama, n.d).

Currently, there are policies in place that require federal agencies to provide specific information and services to the public. Some of these policies include:

* Using web APIs to release information to audiences
* Complying with federal guidelines when applying metadata tags
* All agencies must follow the same standards on how to present information and make it available in multiple formats
* Ensuring employees and citizens can efficiently find what they need when using government services and information
* Office of Management and Budget (OMB) must work with agencies to publish an open data policy that regulates how standards, practices, and regulations will be coordinated
* Requirements for new IT systems to be designed to provide the information in a secure and timely manner in order to provide easy access for agencies and the public
* Requiring agencies to evaluate information before posting it machine-readable to agency.gov/developer

(Obama, n.d.)

**Overview of Information & Services**

            Information is described as knowledge acquired from study, research, instruction, or investigation that includes facts or data (Merriam-Webster, n.d.). When a source of information, such as a scholarly website, provides useful information for the public or agencies, it becomes a service because it is a helpful act. These types of services help the public gain knowledge in particular areas, and offer agencies collectible data for necessary business or continuity.

**Available Information & Services**

            Along with these websites, Ready.gov is an example of a service which provides helpful information for those who could possibly endure disastrous events or impacts, whether in businesses, homes, or communities. This website, created by the Department of Homeland Security, delivers information that is easily available to the public by communicating through social media, online sources, and publications. Some of the services offered by Ready.gov include:

* Preparing for natural disasters
	+ Includes: earthquakes, tornadoes, wildfires, winter storms, hurricanes, floods, drought, etc.
* Preparing for terrorist attacks
	+ Includes: bomb threats, explosions, nuclear threats, cyber threats, etc.
* Creating emergency plans
	+ Includes: elderly, evacuation, animals, infants, first responders, school campuses, military, etc.
* Business continuity planning

This kind of information can greatly reduce the potential vulnerabilities and can help to prepare for a disaster or emergency situation. By providing such resources to the public and businesses, individuals can be well-informed of unexpected situations they may endure.

**Intended Audience**

Those who are looking for ways to prepare themselves from natural disasters, threats, and/or attacks should seek guidance or knowledge from this website. Anyone ranging from children to adults can benefit from this website because it is targeted towards those who need preparation or help on how to use emergency plans. As stated from Ready.gov, their mission is to educate Americans to be ready to respond to emergency situations and increase preparedness amongst the nation (Ready, n.d.).

**Sensitivity Level**

            Organizations and federal agencies must be categorized in the Federal Information Processing Standards Publication (FIPS) 199. This publication categorizes based on the potential impacts that may jeopardize certain information that is needed by the agency to perform or protect necessary duties and information (NIST, n.d.). Assessments are conducted which analyze the vulnerabilities and threats that pose potential risks. There are three main goals or objectives for information and information systems: confidentiality, integrity, and availability. Each one of these objectives contributes to the overall security and protection of information needed within an organization. Along with these goals, FIPS 199 lists three levels of potential impact if a breach were to take place (jeopardizing the confidentiality, availability, or integrity). These levels are Low, Moderate, and High.

            When analyzing Ready.gov for their sensitivity level, it can be concluded that there would be a high level of potential impact if a breach were to occur. A loss of the available information can lead to a detrimental effect on those who rely on the information to keep their businesses or personal lives well-prepared for a disaster. This means that the availability will be compromised because the effectiveness will be greatly reduced. According to NIST, if the potential impact is high, a loss of one of the three main objectives can cause a serious loss of mission resulting in the organization being unable to perform its necessary functions (NIST, n.d.).

**Security Issues**

            Along with the benefits associated with digital government information, there are some issues that need to be addressed with Ready.gov. When opening up the webpage, one has the option to “receive e-mail updates” when they enter their e-mail address. If there were to be a breach in the agency and an unauthorized user obtained access to the webpage, a risk of malicious e-mails could be sent out to individuals who previously signed up. Not only could this type of issue arise, there could be potential disruption of information and data released to the public, causing the information to become unavailable. Networks, assets, and services may all be at stake when a threat poses a risk or vulnerability.

Although there are some issues involved, it is beneficial that Ready.gov does not take purchases or conduct in any form of sales which may ask for an individual’s credit card number or personal information. Instead, they offer free publications for those who would like to learn more about their information and resources. The only issue with these free publications is if the downloadable files become infected with malicious software. These files could then be downloaded onto government or personal computers and cause future attacks or breaches to occur.

**Architectures and Security Issues with Web Applications**

Ready.gov delivers services and information through the use of web applications such as Twitter and Facebook. Users of these social media networks can “follow” or “like” for the latest notifications or updates. According to DigitalGov, managers should be conscious of possible intrusions in these social media accounts (DigitalGov, n.d.). The unauthorized use of computer systems or resources can result in significant risk (GAO, 2015). These risks include:

* Theft of resources and funds
* Unauthorized access to national security information, sensitive information, business information, and PII
* Organizations being unable to accomplish missions and duties
* Attacks towards other systems
* Network damage and/or disruption to services
* Loss of integrity and trust from public with government agencies

(GAO, n.d.)

It is crucial to analyze and identify the security issues when using certain applications due to the negative effects that can follow an unsuspected breach.

**Best Practices & Recommendations**

            Although there are potential issues and risks, there are solutions and practices that can be followed in order to help prevent attacks and damage from occurring. According to DigitalGov, there should be proper communication amongst the entire chain of managers and their roles. Reviews of each application or platform should be conducted that assess the strengths and weaknesses. Creating a plan that offers a list of appropriate teams to contact in the event of a cyber-vandalism attack (DigitalGov, n.d.). Establishing and creating accounts through .mil or .gov can improve and secure web standards. Authentication methods should be put in place which offers confirmation for those who are accessing these types of accounts (DigitalGov, n.d.). Along with these practices, it is important to ensure policies cover the following criteria:

* Update passwords regularly
* Regular security checks should be conducted
* Information on who to contact in the event of a security threat or breach
* Updated accounts to ensure those who are not with company do not have access
* Ensure all networks are protected, under a work VPN, have strong firewalls, and display websites with digital certificates
* Regular training on the social media use
* Conduct and assess business continuity plans
* Test all plans to ensure all weaknesses and potential weak spots are addressed

(DigitalGov, n.d.)

      These types of recommendations and practices can offer better security of the digital government when using web applications. Keeping updated policies and regulations is very important to provide a well-constructed service to the public and federal agencies.

**References**

DigitalGov. (n.d.). *Readiness, Recovery, Response: Social Media Cyber-Vandalism Toolkit*. Retrieved April 4, 2016, from DigitalGov: https://www.digitalgov.gov/resources/readiness-recovery-response-social-media-cyber-vandalism-toolkit/

GAO. (2015, April 22). *Actions Needed to Address Challenges Facing Federal Systems*. Retrieved April 4, 2016, from United States Government Accountability Office: http://www.gao.gov/assets/670/669810.pdf

Merriam-Webster. (n.d.). *Full Definition of Information*. Retrieved April 4, 2016, from Merriam-Webster Dictionary: http://www.merriam-webster.com/dictionary/information

Merriam-Webster. (n.d.). *Service*. Retrieved April 4, 2016, from Merriam-Webster Dictionary: http://www.merriam-webster.com/dictionary/service

National Initiative for Cybersecurity Careers and Studies. (n.d.). *Explore Terms: A Glossary of Common Cybersecurity Terminology*. Retrieved March 17, 2016, from NICCS: https://niccs.us-cert.gov/glossary#letter\_p

Obama, B. (n.d.). *Digital Government*. Retrieved April 4, 2016, from White House: https://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government.html

Security, D. o. (n.d.). *Ready*. Retrieved April 4, 2016, from Ready: https://www.ready.gov/

U.S. Department of Commerce. (2004, February). *Standards for Security Categorization of Federal Information and Information Systems*. Retrieved April 4, 2016, from Federal Information Processing Standards Publication FIPS PUB 199: http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf