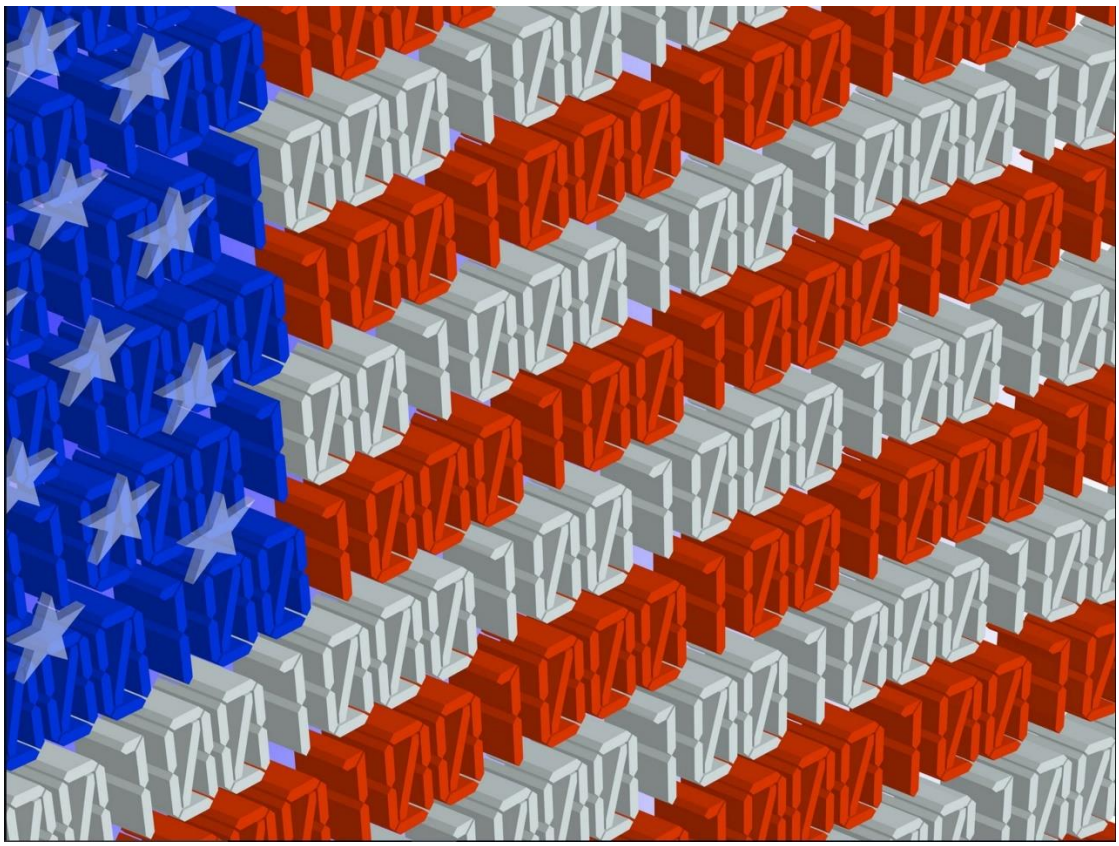
CASE STUDY #2:

Can We Ensure that Digital Government Services are Secure?



DeBora King
CSIA 360 7980
Cybersecurity in Government Organizations (2172)
April 1, 2017

University of Maryland University College – Spring Semester, 2017

INTRODUCTION

The growing list of government agencies that have fallen victim to hackers include the White House unclassified network, the State Department's unclassified email system, the USPS employee personal data (800,000 affected), and NOAA's unscheduled maintenance (Storm, 2014). One of the largest hacks to date may be the Office of Personnel Management's hidden malware which allowed access into the agency's server which may have resulted in stolen personal data of as many as 21.5 million victims (Eng, 2015). Although the government may not have predicted the magnitude of data breaches, the E-Government Act of 2002 was a blessing and a liability. It was put in place to elevate the management and promotion of electronic government. However, making information available to the public brings about risk to sensible and personal identifiable information (PII). So, Section 208 of the E-Government Act requires Privacy Impact Assessments (PIAs) to aid in protecting the collection, maintenance or dissemination of PII (Department of Justice, 2014). A portion of the Federal Information Security Management Act of 2002 (which was updated to the Federal Information Security Modernization Act of 2014) [FISMA] was designed to require minimum controls standards and guidelines to manage Federal information and information systems (NIST, 2017). The Obama Administration answered the call to action on improving digital services in May, 2012 when they launched a comprehensive Digital Government Strategy (Howard, 2012). Executive Order 13571 addresses streaming service delivery and improving customer service (Office of the Press Secretary, 2011), and Executive Order 13576 addresses delivering an efficient, effective, and accountable government (Office of the Press Secretary, 2011). The call for action to government agencies is to "build a 21st century digital Government that delivers better digital services to the American people" (U.S. Department of State, n.d.). A part of that digital strategy is Open Data Policy which includes the following goals: increased operational efficiencies at reduced costs; improve services and support mission needs; safeguard personal information and to increase public access to

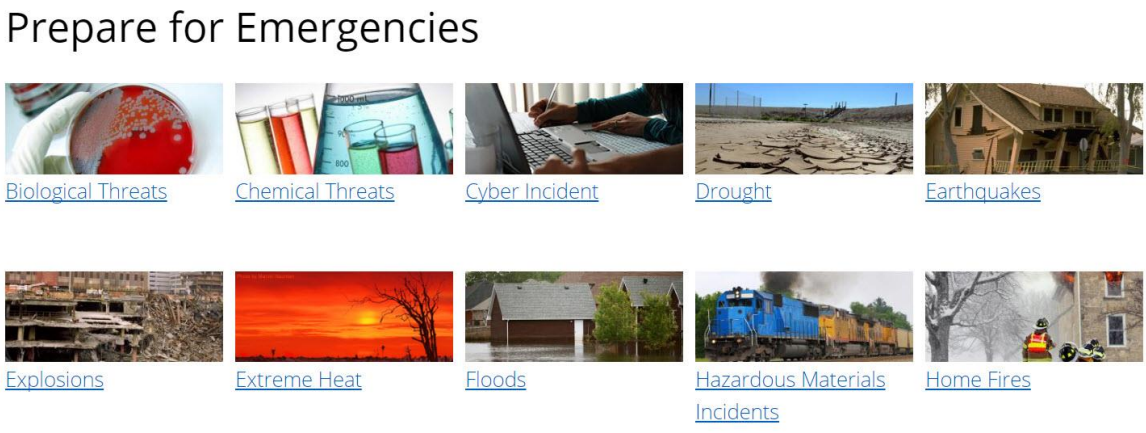
valuable government information; and publicly reports progress in meeting requirements. In this discussion panel we will research the information and services of *Ready.gov*., examine its security issues and offer recommendations for best practices.

OVERVIEW OF *READY.GOV* INFORMATION & SERVICES

Ready.gov is a PSA campaign that was launched in 2003. The purpose of this website is to offer information to the public about emergency preparedness. People who access this site can expect heightened education about how to prepare, plan and keep abreast of emergency situations which include natural and man-made disasters (Ready.gov, n.d.).

Types of Information

The image below is a page directly from the Ready.gov website. Those who browse the website can expect to gain more information about how to prepare for the following hazards (biological threats, chemical threats, cyber incidents, drought, earthquakes, extreme heat, explosions, floods, hazardous materials incidents, home fires, household chemical emergencies, hurricanes, landslides and debris' flow, nuclear power plants, power outages, pandemic, radiological dispersion device, severe weather, snowstorms and extreme cloud, space weather, thunderstorms and lightening, tornadoes, tsunamis, volcanoes, and wildfires (Ready.gov, n.d.):




Household Chemical Emergencies

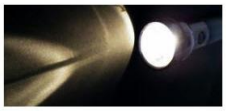

Hurricanes


Landslides & Debris Flow


Nuclear Blast


Nuclear Power Plants


Pandemic


Power Outages

Radiological Dispersion Device


Severe Weather


Snowstorms & Extreme Cold


Space Weather


Thunderstorms & Lightning


Tornadoes


Tsunamis


Volcanoes


Wildfires

Population Served by Website

The following population includes members of the public that are served as an intended audience of *Ready.gov*.

- State and Local Emergency Managers, Promoters of Preparedness
- Individuals and Families
- Business/Private Sector
- Youth Advocates
- First Responders
- Faith Based Groups
- Non-Profit/Community Groups
- Computer Emergency Readiness Teams (CERT)

- Colleges/Universities
- State and Local Governments
- Tribal and Territorial Governments
- Medical Facilities/Healthcare
- Seniors
- Pet Owners
- Seekers of Access and Functional Needs

Sensitivity Level for Website

In the event of a data breach, whether it be a loss of confidentiality, integrity or availability, the Federal Information Processing Standards Publication (FIPS Publication) 199 specifies three levels of potential impact on organizations or individuals. These levels are defined as low (with a limited adverse effect), medium (with a serious adverse effect), or high (with a severe or catastrophic adverse effect) [FIPS PUB 199, 2004].

In researching the types of data that is collected, displayed, processed and stored by Ready.gov, sensitive information is not likely to be present. It appears that the public information managed on their web server has no potential impact from a loss of confidentiality (i.e., personal privacy does not appear to be an issue or risk of being compromised). However, since the website relies on accurate information from a wide range of resources, impact from a loss of integrity is moderate (i.e., ensuring information non-repudiation and authenticity is necessary) . And since this information has a vast amount of an audience from government and the community, timely and reliable access to information would imply a moderate impact. Hence, in following the generalized format for expressing the security category, SC for information types are outlined below:

SC public information = {**confidentiality**, NA}, **integrity**, MODERATE), {**availability**, MODERATE}.

SC investigative information = {**confidentiality**, NA}, **integrity**, MODERATE), {**availability**, MODERATE}.

SC administrative information = {**confidentiality**, LOW}, **integrity**, LOW), {**availability**, LOW}.

READY.GOV SECURITY ISSUES

Fortunately, for *Ready.gov*, the impact on sensitive data or identifiable information is not as big an issue as some other government agencies. *Ready.gov* has links to many resources. For example, when clicking on the link to access Youth Preparedness Council application from *Ready.gov*, the site informs the user that they will be redirected to another site, but linked site collects the user's personal information, such as the user's address and date of birth. It is when accessing these other resources that exposure to threats become more likely. To name a few issues that can impact government servers, here are a few examples: Imperva, a security firm, reports that vulnerabilities from the JBoss Application server, which is an open-source Java EE-based application server, is responsible for the hacking of government agencies and universities (Constantin, 2013). A security flaw in Adobe's ColdFusion web application development platform was is the culprit of government agencies that were hacked, such as the U.S. Army, Department of Energy, Department of Health and Human Services and possibly more agencies (InfoSecurity, 2013). An FBI alert identifies a nation-state sponsored group APT6 that orchestrating a network where phishing attacks were launched (under the radar) since 2011 (Franceschi-Bicchierai, 2016). A series of websites had been used as command and control servers to infiltrate government computer systems.

In the last section categorization of the information system was assessed based on FIPS Publication 199, which is **Step 1** according to NIST SP 800-53 (NIST, 2013). There are five additional steps to implanting information security standards and guidelines. These additional steps include:

Step 2 - selecting the applicable security controls baseline from the above categorization;

Step 3 - implementing the security controls and documenting the design, development and implementation details for the controls;

Step 4 - assessing the security controls to determine the extent to which the controls are implanted correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system;

Step 5 - authorizing information system operation based on a determination of risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation and use of the information system and the decision that this risk is acceptable; and

Step 6 - monitoring the security controls in the information system and environment of operation on an ongoing basis to determine control effectiveness, changes to the system/environment, and compliance to legislation, Executive Orders, directives, policies, regulations, and standards.

RECOMMENDATIONS FOR BEST PRACTICES

The following best practices are recommended for *Ready.gov* for ensuring Web application security during the design, implementation, and operation.

Comply with Third-party Website and Application Requirements:

Since Ready.gov has a social media platform and provides links to many additional resources, complying with M-17-06 (Policies for Federal Agency Public Websites and Digital Services) will be a fitting best practice for the kind of services it provides. Items must be used for "intended purpose directly related to an agency function" and this practice confirms the validity of the website's platform (Office of Financial Chief Information Officer, n.d.).

Keep Software up to Date:

Updated software is usually updated, patched or released after the development and testing to enhance features or mitigate against vulnerabilities to government systems. Updating system software removes yet another increased risk for providing digital government services.

Strengthen Data Encryption:

Some government agencies may be easily accessible due to weak data encryption (Pepitone, 2015). In this digital era, school-children with little or no formal network training are delving into accessing network systems. Their success may be the result of an agency which does not take measures to encrypt sensitive data.

Implement Two-Factor Authentication (2FA):

This practice will provide an additional level of security beyond just a username and password (if both are weak there is a heightened exposure of systems being vulnerable to security breaches). But adding a fingerprint to the authentication process could make it harder for hackers to get into government systems (Thakkar, 2016).

Obtain Strong Intrusion Detection and Prevention Systems (IDPS):

NIST Special Publication 800-94 has recommendations for systems designing, implementing, configuring, securing, monitoring and maintaining network systems to monitor suspicious network activity and identify potential threats (Scarfone and Mell, 2007).

Cybersecurity Awareness Training for Government Workers:

The Department of Health and Human Services developed a training manual that informs users about information security, policy and governance, physical access controls, email and internet security, security outside the office, privacy, insider threat, and incident reporting. Continual practice of user awareness will be beneficial to protection of digital government services (HHS.gov, 2016)

References:

Storm, D. (2014, November 17). *List of hacked government agencies grows: State Department, White House, NOAA & USPS. ComputerWorld*. Retrieved from http://www.computerworld.com/article/2848779/list-of-hacked-government-agencies-grows-state-department-white-house-noaa-and-usps.html

Eng, James. (2015, October 1). *OPM hack: Government finally starts notifying 21.5 million victims*. NBC News. Retrieved from http://www.nbcnews.com/tech/security/opm-hack-government-finally-starts-notifying-21-5-million-victims-n437126

The United States Department of Justice. (2014, June 18). *E-Government Act of 2002*. Retrieved from https://www.justice.gov/opcl/e-government-act-2002

NIST. (2017, January 30). *Federal Information Security Modernization Act (FISMA) implementation*. Retrieved from http://csrc.nist.gov/groups/SMA/fisma/

U.S. Department of State. *Digital government strategy*. Retrieved from https://www.state.gov/digitalstrategy/

Howard, A. (2012, May 23). *White House launches new digital government strategy*. Radar. Retrieved from http://radar.oreilly.com/2012/05/white-house-launches-new-digit.html

The White House Office of the Press Secretary (2011, April 27). *Executive Order 13571 – streamlining service delivery and improving customer service*. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2011/04/27/executive-order-13571-streamlining-service-delivery-and-improving-custom

The White House Office of the Press Secretary (2011, June 13). *Executive Order 13576 – Delivering an efficient, effective, and accountable government*. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2011/06/13/executive-order-13576-delivering-efficient-effective-and-accountable-gov

Ready.gov. *About the ready campaign*. Retrieved from https://www.ready.gov/about-us

FIPS PUB 199. (February, 2004). *Standards for security categorization of Federal information and information systems*. NIST. Retrieved from http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

NIST Special Publication 800-53. (2013, April). *Security and privacy controls for Federal information systems and organizations*. NIST. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Constantin, L. (2013, November 19). *Hackers exploit JBoss vulnerability to compromise servers*. Computerworld. Retrieved from http://www.computerworld.com/article/2486065/cybercrime-hacking/hackers-exploit-jboss-vulnerability-to-compromise-servers.html

InfoSecurity. (2013, November 21). *Anonymous said to be exploiting ColdFusion in government hacks*. Retrieved from https://www.infosecurity-magazine.com/news/anonymous-said-to-be-exploiting-coldfusion-in/

Franceschi-Bicchierai, L. (2016, April 4). *FBI says a mysterious hacking group has had access to US Govt files for years*. Motherboard. Retrieved from https://motherboard.vice.com/en_us/article/fbi-flash-alert-hacking-group-has-had-access-to-us-govt-files-for-years

Office of the Federal Chief Information Officer. (n.d.). *Comply with third-party website and application request*. Retrieved from https://policy.cio.gov/web-policy/3rd/

Pepitone, J. (2015, June 5). *Federal data breach: can the government protect itself from hackers?* NBC News. Retrieved from http://www.nbcnews.com/tech/security/federal-data-breach-can-government-protect-itself-hackers-n370556

Thakkar, D. (2016, August 25). *Two-factor authentication mandatory for Federal Government websites and contractors*. Bayometric. Retrieved from https://www.bayometric.com/two-factor-authentication-mandatory/

Scarfone, K. and Mell, P. (2007, February). *Guide to intrusion detection and prevention systems (IDPS)*. Retrieved from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf

Office of the Chief Information Officer. (2016). *The Department of Health and Human Services cybersecurity awareness training*. Retrieved from https://www.hhs.gov/ocio/securityprivacy/awarenesstraining/cybersecurity-awareness.pdf