Analyzing Security at the FBI

Blue Team
Marcus Guevara
Sammy Wong
Shanaun Clayton
Dave Shields

Submitted to Dr. Michael Hanners

In Partial Fulfillment of CSEC620

University of Maryland University College

Table of Contents

Analyzing Security at the FBI

Since its inception in 1908, the Federal Bureau of Investigation – better known by its shortened name, the FBI – has been one of the most powerful and complex government law enforcement agencies in the USA and the world (Federal Bureau of Investigation, 2012). This powerful organization has changed and evolved throughout its time with especially radical changes after 9/11. Although the incredible amount of data the FBI has collected over its years gives the agency a large number of resources to use in solving some of the world's toughest crimes, it has also made them a very desirable target for cyber attackers. The data infrastructure that the FBI owns could house data about virtually anyone in the world and if penetrated, could result in the loss of unprecedented amounts of national and international security information.

Organization and Mission

Originally conceived as the Bureau of Investigation (BOI), the FBI was established on July 26, 1908 as a small force of special investigative agents consisting of ten former secret service agents and investigators from the department of justice. This small force was commissioned by the then Attorney General Charles Bonaparte under the presidency of Theodore Roosevelt. The two were considered "progressives" and at the time Americans usually looked to cities and states to fulfill most governmental responsibilities (Federal Bureau of Investigation, 2012). The need for a *federal* investigative agency grew from a need for an agency which had jurisdiction over crimes which stretched interstate boundaries. Crimes committed in one state were difficult to pursue in another state by the police of the city/state where the crime was committed. This coupled with the easier and more advanced transportation and communication of the twentieth century 'created a climate of opinion favorable to the federal government establishing a strong investigative tradition' (Federal Bureau of Investigation, 2012).

The Bureau of Investigation was renamed the United States Bureau of Investigation in 1932 and then again renamed the Federal Bureau of Investigation in 1935 (Federal Bureau of Investigation, 2012).

The FBI has grown to having over thirty five thousand employees including nearly fourteen thousand special agents with offices in major cities all over the United States (Federal Bureau of Investigation, 2012).Taken from the FBI's own website - the mission of the FBI is listed as follows:

> As an intelligence-driven and a threat-focused national security and law enforcement organization, the mission of the FBI is to protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States, and to provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners (Federal Bureau of Investigation, 2012).

Because the FBI is an "intelligence-driven" law enforcement society with a federal scope the FBI must maintain large sets of intelligence information in order to efficiently solve cases that span long periods of time or distance or have a particularly complex nature. The FBI is charged with protecting the nation from terrorist attacks which can include physical harm to large amounts of people or harm to the economic or technological infrastructure of the United States in order to create confusion, disarray, and panic to lead to the serious harm or destruction of the country. This can make for extremely complex cases involving a great deal of variables including cutting edge technology and very intelligent criminals. Often time's terrorists or criminals dedicate months or years to planning very sophisticated attacks and often times have a great deal of intelligent minds involved. Part of the FBI's infrastructure, or organization, is that they maintain large databases of information on crimes and criminals in order to be able to cross reference and possibly match prior crimes and behaviors to current cases. Having intelligence on any situation

can often help the FBI not only solve a current crime but possibly prevent criminals from committing future crimes.

To accomplish this, the FBI contains a few different databases and intelligence systems such as The Integrated Automated Fingerprint Identification System, or IAFIS. The IAFIS system is a "national fingerprint and criminal history system" that can be used by the FBI to cross reference fingerprints found on the scene of a crime or during an investigation with crimes committed in the past (Federal Bureau of Investigation, 2012). The IAFIS system does not only contain fingerprints but also contains corresponding criminal histories; mug shots; scars and tattoo photos; physical characteristics like height, weight, and hair and eye color; and aliases. The system also includes civil fingerprints, mostly of individuals who have served or are serving in the U.S. military or have been or are employed by the federal government (Federal Bureau of Investigation, 2012). Some of the other FBI databases include the sex offender registry and kidnapped or missing persons. The amount of information in all of the FBI's different databases is astounding and stands as a threat to the nation and the individuals who are contained in the databases if it were successfully taken advantage of by hackers.

Potential Threats

Cyber-warfare is an Internet-based conflict involving politically inspired attacks on information systems. Cyber warfare attacks can disable or disrupt websites, steal and alter top-secret data. Any country can wage a cyber-warfare on any country (TechTarget, 2010). According to a 2010 report from the Office of Management and Budget (OMB), cyber-attacks targeting the U.S. government from other countries have increased 40% since 2009.

China and Russia are the United States' biggest threats. These two countries have been responsible for "extensive illicit intrusions" into the U.S. networks. China and Russia have been high on the FBI cyber-watchers' list of concerns. Both countries are responsible for the largest number of attacks designed to steal foreign nations' security information (Goldman, 2011). In 2007, Chinese hackers accumulated as much as10 to 20 terabytes of confidential data stolen from government agencies. According to the National Security Agency, the FBI, U.S. Military Networks, and the Pentagon were attacked six million times in 2006. By 2010 there were approximately 6 million attacks per day (Goldman, 2011).

Cyber-attacks against government agencies are becoming more potent. Recent cyber-attacks such as computer breaches at the U.S. Senate and International Monetary Fund, and hacks at Google have shown attacks are not geared toward personal gain, but social change. This new kind of motivation could prove to be stronger than the drive to hack, steal, and cheat for financial gain (Kitten, 2011).

These so-called "Hacktivists" typically hack for political reasons, attacking governments and organizations. These groups deface websites, redirect traffic, launch denial-of-service attacks, and steal confidential information to make their point. For example, the Hacktivist group LulzSec dominated headlines last year with attacks on FBI, CIA, U.S. Senate, Sony, and PBS. Anonymous, a loosely affiliated international hacking group is known for providing information for WikiLeaks, claims its tactics intricate civil disobedience (Sophos AG, 2012, p. 3). The

beginning of 2012 showed a spike in Denial of Service attacks designed to disport websites using an army of computers.

Driven by the hacktivist goals, the group Anonymous temporally disrupted the FBI and Department of Justice websites after a controversial decision to take down a popular file uploading website, Megaupload (Stanich, 2012). In the past groups like Anonymous did not have the numbers to take on large websites, but after the uproar caused by SOPA and PIPA legislation, the Denial of Service software was downloaded 225,352 times. This new capacity gives hacktivist groups like Anonymous, Crazies, and LulzSec the ability to confront targets they could not previously attack (Stanich, 2012).

The FBI faces a range of threats from many different sources with the biggest threat coming from insiders with valid access to government systems. The economic downturn in the recent years has fueled many insider threat concerns. An insider threat usually involves a disgruntled employee who hacks, steals, or sells sensitive information for personal gain. Insiders are employees, contractors, or anyone who has access to a system. Insiders have some type of physical or administrative access to information systems and the greater the knowledge of the system, the greater risk of damage from that person. October 2010, WikiLeaks released more than 400,000 confidential documents given to them by inside employees in various government agencies that compromised key intelligence operations and could have potentially weakened national security.

This breach proved that outside hackers are not the only dangers to network security as an insider with a USB drive poses a larger threat to an organization's sensitive and confidential information (McLaughlin, 2011). The prevalence of WikiLeaks-styled insider threats gives a clear picture of the information security risks posed to organization by their own users.

The government, along with society, is becoming increasingly more integrated and reliant on technology as well as motivated to decrease costs and make productivity more efficient. One of the methods used to achieve these goals are to use less paper and more digital technology wherever possible. This means there is an increasing amount of personal and sensitive information floating in cyber space. The FBI uses the internet as a means to allow remote offices to access the network of information and systems containing data that may be used to correlate similar crimes or match fingerprints on a captured criminal. When connected to the internet the FBI systems are exposed to all of the dangers that plague the public internet. The cyber threats include such exploits and attacks as SQL Injection. The FBI's website may have a digital job application or some part of the site contains input fields. If the code takes the input and directly updates a database – a hacker may utilize SQL Injection to "inject" malicious code that would later be 'passed to an instance of SQL Server for parsing and execution', which could compromise the database and the information in it (Microsoft Developer Network, 2012). Other notable dangers posed by the internet include malware such as viruses and worms. Worms and viruses are programs which self-replicate. The difference in the two is that worms, unlike a virus,

‘are standalone software and do not require a host program or human help to propagate’ (“What is the difference: Viruses, Worms, Trojans, and Bots?”). Worms seek to exploit software and systems through known vulnerabilities and attacks. They may check for open ports or scan systems in order to determine vulnerabilities. The FBI, then, must be vigilant in staying up to date with current exploits and vulnerabilities as well as making sure the software is always up to date with the latest protection from known exploits so their systems do not fall prey to such attacks.

Regulatory Requirements

Being that the FBI is a government agency, it has a considerable number of governmental regulations that it must adhere to simply because it is a government agency. One of the original regulations that impact the information technology infrastructure of the FBI is the Paperwork Reduction Act. This particular act has been in progress since 1942 but reached the form that is in use today in 1995 when it was revised to discuss how electronic systems could be used to store government information and how that data was to be used by the agencies within the government (Relayea, 2000, pp. 368-377). The FBI must be cognizant of the regulations they agree to uphold under the PRA including data use and reduction of redundant forms.

Another government regulation that the FBI must abide by is the E-Government Act of 2002. The EGA is almost built atop the framework put in place by the Paperwork Reduction Act but it creates a more standardized set of guidelines for how the government must protect the data they collect and use in their electronic systems (Barker, 2011, pp. 96-97).

In the event of a breach of an FBI system, if the provisions of this act were violated, it would cause a tremendous security and public relations nightmare and likely deepen the already extreme distrust of the government by a large number of its citizens. Furthermore, all data that is processed on E-government systems interconnects with other e-government systems so there is almost an unspoken need for constant availability of that data to systems and to the citizens to which that data belongs as any downtime with that could cause private or even critical information to be unavailable.

Among all of the various regulations discussed previously, none of them are quite as impactful or vital to the FBI and its operations than the regulations imposed by the Federal Information Systems Management Act (FISMA) of 2002. This particular act is governed by the Federal Risk Management Framework (RMF) which was created by the National Institute of Standards and Technology (NIST) (Hulitt & Vaughn, 2010, pp. 139-140). By the provisions of FISMA, each government agency – including the FBI – has a baseline of security controls that must be implemented upon their information systems to ensure the data they contain is secured. The FISMA provisions are responsible for creating an entire framework of data security, redundancy, risk mitigation, and incident remediation of daily operations of government agencies (Glass, et al., 2009, pp. 54.17-18).

In the event of a breach at the FBI, there is no doubt that whatever system(s) impacted by the attack would be evaluated against the FISMA standard to determine if they were out of compliance. If the attack analysis determined that the machine was out of compliance on any number of audit checks, it could be easily explained that the system was not properly configured. On the other hand, if the machine was in compliance and still was compromised, the FBI would have to completely reevaluate the standard in response to new vulnerabilities.

The aforementioned regulations are some of the most well-known standards that the FBI must adhere to but there are many other – perhaps less notable – regulations that must also be discussed. One of those is the Freedom of Information Act (FOIA) of 1966 which is a combined piece with the Federal Records Act (FRA) of 1950. At its essence, the FRA is a document governing the types of things that each government agency must be willing to share with the other and FOIA is what allows for the public to request access to those records (Hill, 2011, p. 35). Despite the fact that there are specific guidelines governing the speed of return, the government reported in 2011 that there are still backlogs from as far back as 1991, most of which should have been easy to fill (National Security Archive, 2011).This regulation requires a certain amount of government transparency but is not likely to be very transparent for an organization such as the FBI.

Lastly, the Privacy Act of 1975 has a considerable impact on the way that FBI performs its duties as this particular legislation sets limitations on the amount of data the government maintains about its people. The guidelines are designed to allow citizens to have a choice in what types of data is collected about them (allowing for such things as the famous opt-out option among online privacy) and, within reason, provide that information to the individual at their request (Judy, David, Hayes, Ritter, & Rotenberg, 2009, p. 69.7). It is quite apparent that this rule works hand in hand with the FOIA and its statutes making it such that any person in the USA has permission to request any data from the government that they so choose to request and they also have the right to request data not be collected about them around certain restrictions. If the FBI were to witness a breach, the regulations such as FOIA and the Privacy Act would not really be impacted too much unless it was found that information had been collected that was not permitted to be collected under those regulations.

Liability Issues

For FBI, being the country's primary agency to handle cybercrime, there are liability issues in regards to protecting the country against cyber-attacks. According to USCYBERCOM, the US classified network is constantly being probed in a daily basis. Due to the nature of internet and its communication protocol, it is highly susceptible to interception and unauthorized access (Brenner, 2010). Our country's Internet infrastructure was not designed in favor of tracking cybercrimes and dealing with the burden of proof (Schackelford, S. & Andres, R., 2011).

For the FBI to be effective on protecting our nation's infrastructure, private businesses need to work with federal government on improving our security posture.
However, only 17% of companies report electronic crime loss to law enforcement. Part of the reason is the unclear definition of cybercrime and the borderless nature of the Internet make jurisdiction and prosecution difficult (Schackelford, S. & Andres, R., 2011).

In order to protect the confidentiality of the intelligence data gathered via different investigation channels, the FBI has the obligation to protect any data pertaining to national security and our citizens' privacy. However, most data breaches are not disclosed. One of the recent data breaches were performed by the hacking group Anonymous intercepted a conference call between FBI and UK Scotland Yard. In this event, it is believed that the email system had been compromised (BBC News, 2012).

Another liability issue related to the FBI is the uncertainty regarding what is considered an electronic crime. The government and public do not have the understanding and knowledge about vulnerabilities. Furthermore, there is lack of technology and expertise in dealing with emerging threats like advanced persistent threat in our infrastructure. When a cyber-attack

targets the US from other nations, international laws dictate if the state is responsible for the "attack" and then cyberspace becomes another domain of combat.

The FBI has some of the most advanced computer technologies in the world and is constantly on the frontlines detecting and investigating any incidents. The question remains, "How do we determine if this is an incident to be classified as cybercrime, cyber-war, or just an outrage?

In the area of cyber war, international laws continue to increase the state's responsibility. Most countries are dealing with the burden of proof when it comes to determining another state's involvement in a cyber-war scenario (Shackelford & Andres, 2011).In the age of the cyber warfare, the attacker might reside in the US and the US law enforcement (FBI) has the obligation to investigate those responsible for the attack. The International Law Commission's draft article VIII gives legal guidance regarding a state's responsibility for wrongful acts. Also, the US will be liable if it is proved that a US citizen acted on behalf of the country (Shackelford & Andres, 2011).

In addition, the law also can help determine if the actions of private citizens can be qualified as acting "agents" of those states (Proulx, 2005). In this scenario, it is clear to see the local law enforcement has a liability and obligation to not only investigate, but also prevent cyber incidents that occur on US soil. As the US could be held responsible for a cyber-attack against another country if US officials failed to take reasonable measures to prevent the crime such as investigate claims, or bring justice to the offenders. This indirect responsibility places emphasis on the country failure to fulfill its international obligations to prevent attacks against other nations (Proulx, 2005).

The FBI is working with other federal organizations and private companies to improve the existing security standards in the public arena.

The government can leverage its buying power to require better security measures from its business partners, law enforcement and standards organizations can amend current policies to clarify regulations on incident response and disclosure. Furthermore, the InfraGard, an information sharing and analysis organization, works with public and private entities to support research used in protecting our nation's data and its infrastructure (Infragard, 2012).With all the liability and responsibility of the FBI, security of its data and infrastructure is vital to our country's survival.

Conclusion

As the FBI has evolved over time, so have the technologies as well as the methods and techniques used to complete its mission. The FBI has built and maintained impressive technological resources that contain a great deal of intelligence concerning the United States and other nations. The information contained within the FBI does, however, make them a desirable target for cyber-attacks from citizens and foreign criminals alike. As a result, the FBI must take a very serious and complete approach to protect their data infrastructure from attacks including the potential threats of the internet, such as malware and vulnerability exploits because of the sensitivity of the data they hold. A successful attack could create a disaster for not only the FBI but for also the nation who relies heavily on the FBI every day for its protection. Thankfully, the Federal Bureau of Investigation does everything it can to protect the data it holds including adhering to several standardized systems and depending on the wonderful men and women who have made the organization what it is today.

Bibliography

Barker, W. C. (2011). E-Government Security Issues and Measures. In H. Bidgoli, *Custom Textbook for CSEC620* (pp. 96-107). Hoboken: John Wiley & Sons Publishing.

BBC News. (2012, February 3). *Anonymous Gain Access to FBI and Scotland Yard hacking call.* Retrieved February 18, 2012, from BBC News: http://www.bbc.co.uk/news/world-us-canada-16875921

Brenner, J. F. (2010). Privacy and Security: Why Isn't Cyberspace More Secure? *Communications of the ACM, 53*(11), 33-35. doi:Doi:10.1145/1839676.1839688

Federal Bureau of Investigation. (2012, February 19). *A Brief History of the FBI*. Retrieved from FBI: The Federal Bureau of Investigation: http://www.fbi.gov/about-us/history/brief-history/brief-history

Federal Bureau of Investigation. (2012, February 19). *Integrated Automated Fingerprint Identification System*. Retrieved from FBI: Federal Bureau of Investigation: http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis

Federal Bureau of Investigation. (2012, February 13). *Quick Facts*. Retrieved from The FBI: Federal Bureau of Investigation: http://www.fbi.gov/about-us/quick-facts

Glass, D., Davis, C., Mason, J., Gursky, D., Thomas, J., Carr, W., & Levine, D. (2009). Security Audits, Standards, and Inspections. In S. Bosworth, M. E. Kabay, & E. Whyne, *Computer Security Handbook Volume 2* (pp. 54.1-24). Hoboken: Wiley & Sons Publishers Inc.

Goldman, D. (2011, July 28). *China vs. U.S.: the cyber Cold War is raging*. Retrieved February 18, 2012, from CNN Money: http://money.cnn.com/2011/07/28/technology/government_hackers/index.htm

Hill, C. A. (2011, June 1). The Freedom of information Act - a Primer. *Journal of Tax Practice and Procedure, 13*(3), 35-47.

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

Infragard. (2012, February 18). *About InfraGard*. Retrieved from InfraGard: a collaboration for infrastructure protection: http://www.infragard.net/about.php?mn=1&sm=1-0

Judy, H. L., David, S. L., Hayes, B. S., Ritter, J. B., & Rotenberg, M. (2009). Privacy in Cyberspace: U.S. and European Perspectives. In S. Bosworth, M. E. Kabay, & E. Whyne, *Computer Security Handbook Vol. 2* (pp. 69.1-69.26). Hoboken: Wiley & Sons Publishing Inc.

Kitten, T. (2011, June 24). *Insider threats and cyber vigilantes*. Retrieved February 18, 2012, from The Fraud Blog with Tracy Kitten: http://www.bankinfosecurity.com/blogs.php?postID=987

McLaughlin, P. (2011, June 15). *WikiLeaks Breach Forces Government Agencies to Address Challenges of Insider Threat Detection, Blue River IT Creates "Cloud Threat Detection Service"*. Retrieved Feburary 19, 2012, from Enhanced Online News: http://eon.businesswire.com/news/eon/20110615006942/en/Blue-River-Information-Technology/Cloud-Threat-Detection-Services/Insider-Threats

Microsoft Developer Network. (2012, February 19). *SQL Injection*. Retrieved from MSDN: http://msdn.microsoft.com/en-us/library/ms161953.aspx

National Security Archive. (2011, September 1). FOIA Celebrates 45 Years; Backlogs Persist. *Information Management Journal, 45*(5), 18.

Proulx, V. (2005). Babysitting Terrorists: Should States Be Strictly Liable for Failing to Prevent Trans-border Attacks? *Berkeley Journal of International Law, 23*(3), 615-668.

Relayea, H. C. (2000). Paperwork Reduction Act Reauthorization and Government Information Management Issues. *Government Information Quarterly, 17*(4), 367-393.

Shackelford, S., & Andres, R. (2011). *State Responspibility for Cyber Attacks: Competing Standaards for a Growing Problem.* Retrieved from University of Cambridge Deopartment of Politics and International Studies: http://irps.ucsd.edu/assets/001/501281.pdf

Sophos AG. (2012, January 1). *Security Threat Report 2012: Seeing the threats through the hype*. Retrieved February 18, 2012, from Sophos: http://www.sophos.com/en-us/security-news-trends/reports/security-threat-report/html-03.aspx

Stanich, M. (2012, January 30). *Cyber attacks from hacktivist groups becoming more potent*. Retrieved Feburary 18, 2012, from PRWeb: http://www.prweb.com/releases/2012/1/prweb9133676.htm

TechTarget. (2010, March). *definition: cyberwarfare*. Retrieved February 18, 2012, from SearchSecurity: http://searchsecurity.techtarget.com/definition/cyberwarfare