FBI Data Information Protection Procedure Policy

Anonemis Research
Simenona Martinez
AnonemisResearch.com

FBI Data Information Protection Procedure Policy

Overview

This report identifies what a cyber threat in the on context of data in various categories within industries. What to look for, how each category differs and how every threat is unique. This aspects are only the partial battle as these attacks change and vary from industry to industry but in common they all have bad actors.

Malware, Phishing, Social Engineered Attacks, Whale Attacks, Malicious links, Ransomware and worms, just to name a few which are all different in ways that can compromise users with every day risk.

These threats have been categorized with reaction and repair procedures, as it is crucial to minizine monetary damage and loss of data.

Assessment Example

- **Week 1:** *Ciphering Cybersecurity:* Breaking the code within the code. Securing your networks from threats seen and unseen. Assuring that your system in update with anti-virus software and configuration.
- **Week 2:** *What is a threat?* Categories. *Malware, Phishing, Social Engineered Attacks, Whale Attacks, Malicious links, Ransomware and worms*, just to name a few which are all different ways users are at every day risk.
- **Week 3:** *How can I protect myself, company and family?* Different zones require different precautions within industry. Having update to date and successfully configured software is the foundation to any efficient operation.
- **Week 4:** *First AID Cybersecurity*. Learning how to responded to a cyber emergency with confidence even when the operation requires trial and error. Everything is a learning opportunity in this industry but it will cost you.

  Insurance is available if your budget permits and actively researching similar attacks within your industries will allot an opportunity of acquiring enough insurance to cover the breach, which is essential. The option of having a secure system with a rapid response to security breaches are encouraged and highly effective. A post attack plan, reports, review and repair is critical in a cybersecurity setting.

  Time is money and money is reputation in terms of damages. Having a comprehensive understanding of cybersecurity and how to use methods and software to your advantage is the key foundation of the methodology of running an efficient enterprise.

- **In conclusion,** the framework within cybersecurity is forever-changing because innovations and methods are created and/or changed daily. You can be an expert or novice but regardless, you can empower yourself by being aware of threats and how to respond. Response will inevitability

change and update regarding the framework, however, knowing the fundamentals is critical in any situation.

- **Laws:**
- Federal Trade Commission (FTC)
- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Privacy Protection Act of 1980 (PPA)

Researching cybersecurity-related guidelines, initiatives, and resources that your country has for its citizens.

For the United States, Cybersecurity Act of 2015 changed the landscape and framework of cybersecurity. Congress passed legislation that allowed companies in the U.S to share personal information related to cybersecurity with the government. The government could use this information as evidence to prosecute crimes. This protocol was enforced to protect citizens rights and privacy, not violate it. The Homeland Security Act (2002) has proven to be effective with the introduction of NIST. Both GLBA and HIPPA are also in place to protect both citizen and government.

Applied to the principles of privacy, regulatory compliance, and civil and criminal laws discussed in this report.

Spam and Phishing is a concern to unassuming consumers who click on links which appear familiar or safe. Online shopping increases the chances of breaches because of the exchange of customer information while using third-party applications. It puts consumers at a higher risk of having their data stolen. Both patients and physicians require added protection in their position of vulnerability. Bots and Malware seem to be prominent on popular social networking sites, again, phishing is about being aware of the links you click and knowing what spam often looks like. Backing information and Data is essential to operating any enterprise, both personal and business related, especially with regarding ransomware threats. Establishing privacy and protection for the financial market and public communication as a whole.

Key Laws and Policy Principles

- Federal Trade Commission (FTC)
- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Privacy Protection Act of 1980 (PPA

Applied Within Context

Scenario 1

You join your small local bank as a junior compliance analyst. The bank has recently gone through a difficult financial period due to the pandemic and low interest rates. To

compensate, the bank has let many senior analysts go and has hired junior analysts and interns instead.

During your first week, you learn that the bank is preparing to start its semiannual compliance process that involves mailing various documents to clients. This process is both lengthy and resource intensive. As a new hire, you want to create a good impression and decide to optimize the process.

As you review some notes left by a senior analyst, you notice a task about mailing privacy notices explaining the nonpublic personal information that the bank collects from its clients. It also includes sending clients special instructions how to opt out of this data collection. You decide to skip this assignment because you believe it's less important than your other tasks.

The Gramm-Leach-Bliley Act (GLBA) is in full force regarding this task. The GLBA requires under federal law that financial institution notify costumers how the use their data and information. It is also explains how the protect that data and information, so skipping this task would be ill-advised as it is an critical element of policy within financial institution. In order to optimize this process excel spreadsheets would be instrumental in modernizing this process by using methods that have proven to work, for example filtering customers to avoid following up with those who have already opt out. Sending a secure notice via email would be effective but would advise against text since that seems less secure.

Scenario 2

You go to your primary care physician for a routine annual physical examination. When you arrive at the clinic, you notice that it appears busier than usual. Several patients are standing in line to check in. The reception staff is attending to multiple patients simultaneously. While waiting, you realize that you can overhear the interactions between the receptionists and the patients, including personal healthcare information.

Health Insurance Portability and Accountability Act (HIPAA) would be enforced on behalf of the patient, healthcare worker and listener. Any information repeated would be a violation of that act and could result in jail time. HIPAA incorporates that element into its terms and policy extending to all patients, including those in the waiting room that could possibly overhear confidential information.

Scenario 3

A tech startup looking to disrupt the current social media landscape is gaining significant momentum. Until recently, most people were completely unaware of this company and its technology. However, this changed when a high-profile entrepreneur tweeted about the new platform and invited millions of followers to join it. Since then, the platform has been attracting thousands of new users every day.

The company hires you as an independent privacy consultant to review the platform and identify any issues. After reviewing detailed product documentation and conducting numerous interviews with different internal business leaders, you conclude that the

company is engaged in deceptive actions. For instance, the company claims that it doesn't sell user data and that it provides its users with complete data configuration control. However, these claims appear to be unfounded. You believe that the company is misleading the trust of its users, investors, and employees.

The start up is currently violating the Privacy Protection Act of 1980 (PPA, specially under the "Work product materials" Materials (textual, written), other than contraband or the fruits of a crime or things otherwise criminally possessed, or the means of committing a criminal offense, that – o are prepared, produced, authored, or created in anticipation that the materials will be communicated to the public; are possessed for the purpose of communicating the materials to the public; and o include mental impressions, conclusions, opinions, or theories of the person who prepared, produced, authored, or created such material." They are also in violation of the Federal Trade Commission (FTC) with use of not meeting standards and bad practices.

Scenario 4

An emergency room employee is about to finish a long Friday shift. They are looking forward to visiting their friends and starting the weekend. However, more patients enter the emergency room, which makes the employee wonder whether they will manage to leave on time. The employee decides to share their concern with friends by taking a photo of the patients waiting in the emergency room and posting it on social media.

Health Insurance Portability and Accountability Act (HIPAA). This is a violation of HIPAA in the highest order. It violates the workers privacy by providing a location where individuals are compromised. It violates the privacy of the patient, surrounding staff and other patients seeking care that might have been captured in the image. It also put the social media platform at risk for third-party violation with the user providing sensitive data and information to a boarder audience that can not always be specially accounted for on some social platforms.

Scenario 5

An editor at a small newspaper is working on a controversial story about a high-profile criminal activity taking place in the local city government. A couple of days before the story is set to publish, local law enforcement visits the newspaper's headquarters and demands all unpublished materials from the editor.

Privacy Protection Act of 1980 (PPA) evokes the protection of both journalist and government officials. Law enforcement may operate in this matter to avoid public outcry which could result in unrest and safety risk. Perhaps, law enforcements has protocol for rolling out information regarding their officials, for protection and best interest of both the government and journalist.

Conclusion

The 2015 San Bernardino mass shooting is one of the most recent high-profile cases where the United States government demanded access to confidential data from an organization.

One of the perpetrators in the attack had a locked iPhone that the FBI wanted to investigate, but could not unlock. In February 2016, the FBI asked Apple to create software that could disable the iPhone security function that erases data after a certain number of failed attempts to unlock the device.

Apple declined to assist and said that doing so would undermine its policy and weaken the security of its products. Consequently, a few US court orders were issued mandating Apple to comply, all of which were opposed by Apple.

In March 2016, the US Department of Justice withdrew its suits against Apple and announced that it had unlocked the iPhone without Apple's assistance. At the time, it was unclear how. However, in April 2021, it emerged that an Australian cybersecurity organization had secretly created a solution that allowed the FBI to unlock the device.

Apple had a moral obligation to help the FBI unlock the iPhone in this particular case. However, law enforcement agencies need to establish a third party authentication system and regulations for all mobile companies operating in the united states or otherwise within jurisdiction to comply, accessing information regarding cases or threats.

Law enforcement agencies should be protected to intervene under law and regulations with an active warrant. Apple has no judication in this matter and therefore a secure third party application would not compromise their policies regarding the privacy of their customers because it would be out of their judication and they would not need to be an active participate, as this software would be readily available to all government agencies.

Regardless of your personal feelings about the government or existing administration, the government should have access to all data and technology regarding consumers as it is a crucial aspect of homeland security.

In conclusion, the FBI should not share details on how they unlocked the iPhone with Apple as that classified information, a classification that Apple should have no jurisdiction in. The information should remain isolated within the department, as it is a public declaration of a vulnerability within our own establishment and policy with our venders, outside providing information to law enforcement when permitted, it is to remain confidential.

Resources:

- "How an iPhone became the FBI's public enemy No. 1 (FAQ) (Links to an external site.)" by Sean Hollister and Connie Guglielmo
- "The FBI wanted to unlock the San Bernardino shooter's iPhone. It turned to a little-known Australian firm. (Links to an external site.)" by Ellen Nakashima and Reed Albergotti

Anonemis Research
Simenona Martinez
AnonemisResearch.com