Security Risk Assessment

Prepared For:

ABC Demo

Prepared By:

PII PROTECT

April, 2015

Section 1

Executive Summary

An extensive security risk assessment was performed that evaluated how personally identifiable information (PII) is currently being protected. The security risk assessment looked at administrative, physical and technical safeguards.

The methodology that was used to perform the security risk assessment was based on risk assessment concepts and processes described in NIST SP 800-30 Revision 1. An overview of the Risk Assessment process is defined below:

Step	Process
1	Identify and document all PII repositories
2	Identify and document potential threats and vulnerabilities to each repository
3	Assess current security measures
4	Determine the likeliness of threat occurrence
5	Determine the potential impact of threat occurrence
6	Determine the level of risk
7	Determine additional security measures needed to lower level of risk
8	Document the findings of the Risk Assessment

The assessment included the offices located at:

ABC Demo, 123 Fake Street.

Section 2

General Areas to Focus on

1) **Portable Media** – a significant majority of all breaches involved portable media. Portable media includes; laptops, smartphones, USB Hard Drives, USB Flash drives, Portable Backup Media, CDs, DVDs, etc. Portable media is very easily lost, stolen or misplaced. It is critical that special attention be focused on protecting PII on portable media.

    a. **Minimize the amount of PII** – if portable media must be used for transporting PII then it is important to restrict the amount of PII on portable media to the minimal needed to perform a function or task.
    b. **Limit access** – it is important to limit who can copy PII to portable media. It is also important to ensure that prior approval has been granted before PII is allowed to be copied onto portable media.
    c. **Track portable media** – ensure that a procedure is in place that tracks all portable media containing PII that enters or leaves the organization.
    d. **Encrypt portable media** – ensure that proper encryption is utilized to protect PII on portable media. Ensure that portable media is not removed from an organization unless the PII is encrypted.

2) **Malware –** according to the 2010 Verizon RISK report in cooperation with the United States Secret Service, 38% of all security breaches (across all industries including healthcare, financial, retail, etc.) were due to data being stolen after a malware (computer virus and/or spyware) infection. It is critical that anti-malware protection be put in place and properly maintained to prevent and eliminate malware infections. It may be necessary to implement multiple malware protections that protect desktops, servers, email, websites, etc.

3) **Workforce Training –** it is important to ensure that the workforce is properly trained to protect PII. Organizations that properly train their workforce on securing PII lower their risk of data breaches. Training includes the following:
    a. **Formal Training** – ensure that each member of the workforce receives formal training on how to secure and protect PII.
    b. **Security Reminders** – ensure that workforce members receive reminders on best practices for protecting PII. Security reminders may include notifications of rapidly spreading or malicious malware, critical software updates that should be applied, best practices for securing PII, changes to policies and procedures, etc.

4) **Physical Security –** ensuring that systems containing PII are properly secured will lower the risk of data breaches. Systems include servers, desktops, laptops, portable media, etc. Where possible, servers and other systems containing PII should be located in a secure location. Access to the secure location should be restricted to workforce members that require access to perform their job function.

5) **Cyber Insurance –** some threats and risks to organizations cannot be mitigated to zero (i.e. Tornado destroying an office). Even organizations that implement strong security policies could run the risk of a data breach. Some data breaches occur due to employee misconduct (intentional or unintentional), computer viruses, phishing scams, etc. Breaches of PII can be costly due to breach reporting requirements, remediation services including information technology, forensics, legal, credit monitoring and possible regulatory fines. Cyber insurance can offset the expenses of PII related data breaches.

Section 3.1	**Administrative Safeguards**	
	Finding	**Recommendation**
➢	Procedures are not in place that require services providers (business associates and/or 3rd party vendors) to protect sensitive data	Agreements should be developed and implemented to ensure that all service providers appropriately safeguard PII and sensitive data to prevent breaches and unauthorized access to the data. It is critical that each of the organization's service providers have signed agreements that clearly states that they will protect sensitive data. In addition each service provider should show proof that they are properly safeguarding any sensitive data that they store, maintain or access. Proof of data safeguards may include employee security training, performing a security risk assessment, having policies and procedures, having a security incident response plan, PCI / GLBA / HIPAA compliance, etc.
➢	Disaster Recovery procedures need to be implemented and validated	Ensure that a disaster recovery (DR) procedure has been defined and documented. The DR procedure should ensure that an up to date copy of critical business data (including any sensitive data) is accessible in the event of a disaster. Implement the required DR infrastructure and procedures. The DR process should be periodically tested and validated. A data criticality analysis should be performed to determine how critical the data is to the organization. Data criticality might be rated as High, Medium or Low. A DR plan might restore access to data that has a High or Medium criticality level first and then restore access to data that has a lower criticality level.
➢	A security response plan needs to be developed and implemented	A detailed procedure must be developed to address security incidents such as: unauthorized access to the network, hardware containing PII or sensitive data is lost or stolen, email containing sensitive data is sent insecurely, passwords shared amongst workforce members or potential access of PII or sensitive data due to a computer virus or malicious code.A security incident response team should be formed and a security incident response plan (SIRP) should be developed. The SIRP should include steps to capture critical incident details, stop the incident, notify affected individuals and prevent future incidents. All employees should know who to contact and what to do in the event of a security incident.

➢	Emergency operations procedures need to be implemented and validated	Ensure that emergency operations procedures have been defined and documented. Emergency operations procedures will help guide an organization in case of floods, tornados, power failures, weather related emergencies, terrorist activities, etc. Emergency operations should include employee contact information, vendor contact information, insurance information and financial account information. Procedures should also be defined and documented that describe business continuity in the event of an emergency.
➢	All workforce members should receive security training	Implement a training program that educates all workforce members on how to protect and safeguard PII and sensitive data. Workforce members should receive periodic security reminders on how to protect and safeguard PII and sensitive data.
➢	The lack of formal Information Security Policies could lead to data breaches	Formal and documented Information Security Policies should be implemented on the procedures used to protect sensitive information. Workforce members should be trained on the policies to ensure that they are properly protecting sensitive information.
➢	Procedures are not in place to classify the sensitivity of data	A formal process should be implemented that classifies all data that the organization collects, stores or accesses by the sensitivity of the data. Data could be classified as low sensitivity, moderate sensitivity or high sensitivity (Personally Identifiable Information[PII], Protected Health Information [PHI], Social Security Numbers, Credit Card Numbers, etc.). Workforce members should be made aware of the sensitivity of an organization's data and trained on the proper handling procedures for the various levels of sensitivity. Understand the sensitivity of data and how to properly handle the data will minimize the likelihood of a data breach.

Section 3.2	**Physical Safeguards**	
	Finding	**Recommendation**
➢	Physical security to protect PII and sensitive data must be implemented	Ensure that servers and systems that store PII and sensitive data are located in a secure location. Access should be limited to personnel that require access to perform their job function. All access to the secure location should be recorded and logged. The secure location should be safe from environmental issues such as flooding, overheating and electrical problems.
➢	The movements of portable devices and media should be tracked and proper disposal procedures should be implemented	Portable devices that store PII and sensitive data should be tracked and records should be maintained of their movement in and out of an organization. Disposal of portable devices and media with PII and sensitive data should follow a standard process to guarantee the proper destruction of device and /or the removal of any PII and sensitive data. The amount of PII and sensitive data stored on portable devices and media should be limited.
➢	Implement a security patch update procedure to ensure systems that contain PII and/or sensitive company data are properly secured	To protect PII and sensitive data from vulnerabilities, all systems, especially those that store or access PII and sensitive data, should be properly patched with the latest software security patches. Security patches for servers and desktop operating systems as well as applications should be kept current.
➢	Ensure that PII and sensitive data is protected on monitors and is protected from unauthorized access	Privacy screens can protect PII and sensitive data from unauthorized access by workforce members, vendors and visitors.Privacy screens should be utilized on all systems in common areas that might allow visitors to gain access to sensitive data. In addition, privacy screens on computers that are not in common areas will prevent unauthorized access to sensitive data by someone looking over a workforce member's shoulder.In addition, systems should have automatic timeouts or locking screen savers to protect PII and sensitive data on screens of workforce members that leave their desk. Applications that contain PII and sensitive data should timeout after a period of inactivity.

➢	Intrusion Detection and Prevention System (IDPS) along with Security Information Event Management (SIEM) should be implemented	An intrusion detection and prevention system (IDPS) is a device or software application that monitors network or system activities for malicious activities or policy violations. Any malicious activities or policy violations are logged or sent to a person or system that is in charge of monitoring. IDPS may also respond to detected threats by attempting to prevent the threat from succeeding. It is recommended that an IDPS be implemented to further protect the PII and sensitive data. A procedure should be created that addresses steps required to respond to threats and/or attacks. These procedures should be incorporated into the Security Incident Response Plan. It is recommended that a Security Information and Event Management (SIEM) tool and process be implemented. SIEM technology provides real-time analysis of security alerts generated by network hardware and applications. SIEM technology also provides data log collection to allow detailed insight into data access. SIEM technology is one of the best ways to know if a network is under attack or if an attacker has successfully accessed the network. SIEM technology will provide detailed insight into what data was and was not accessed by an attacker.
➢	Vulnerability /Penetration Testing	Penetration testing is a simulated external attack on key components of the infrastructure. Penetration testing can reveal weakness, technical flaws and opportunities for malicious code or hackers to gain access to sensitive data.Vulnerability testing is a process of identifying weaknesses in both internal and external facing hardware and software. These weaknesses can be exploited to gain access to sensitive data. It is recommended that extensive Penetration and Vulnerability scans be performed on all aspects of infrastructure. Vulnerability and penetration testing should be performed on internal networks and systems as well as external systems (i.e. web servers) and firewalls, wireless access points and remote access implementations. Any technical flaws or weakness should be mitigated.
➢	Employee monitoring or restricting of access has not been implemented	The organization should evaluate the use of employee monitoring and restricting employee to access certain websites. Employee monitoring of access to internal and external resources (websites, etc.) will enable an organization to collect and evaluate any suspected unauthorized access to sensitive data. In addition, restricting access to certain websites may reduce the likelihood of malicious code from entering the organization's network.

Section 3.3	Technical Safeguards	
	Finding	**Recommendation**
➢	Implement strong password policies	Ensure that appropriate password policies are implemented and enforced. Polices include: password aging, requiring complex passwords, disabling of user accounts after a number of failed password attempts, and ensuring that userids and passwords are not shared amongst workforce members.
➢	System auditing and log review procedure not in place	Ensure that all systems that contain PII and sensitive data have auditing enabled and that all access to sensitive data is properly recorded. Auditing should record, at a minimum, who accessed sensitive data, what data was accessed, and when the data was accessed. A process must be implemented to periodically review the audit logs to ensure that only appropriate access to sensitive data is occurring. Any improper or unauthorized access, or access attempts, should be reported immediately.
➢	Utilize data encryption to protect PII and sensitive data	One of the best ways to protect PII and sensitive data is by utilizing data encryption. Many federal and state regulations provide a "Safe Harbor" (not requiring notification to individuals that might be affected) for data that is encrypted in the event the data is lost or stolen. All portable devices and media including laptops, tablets, USB Drives, CDs, DVDs and backup tapes should utilize encryption to protect the sensitive data. Workstations and servers that have PII and sensitive data should be considered candidates for encryption as well. In addition, all emails and communications that contain PII and sensitive data should utilize encryption to protect the contents of the communication. Wireless and Remote access to networks and systems that contain sensitive data should utilize encryption to prevent unauthorized access to sensitive data.
➢	Implement smartphone startup and time out password mechanisms	Smartphones could contain or access PII and sensitive data and should be protected in the event they are lost or stolen. Implementing startup and timeout passwords can help prevent unauthorized access to PII and sensitive data.

Section 4

Threats and Risk with Existing Controls

The report shows all threats to personally identifiable information (PII) and sensitive company data with existing controls (safeguards and existing security measures). The probability of the threat, the impact to PII and sensitive company data and the overall risk level has been determined based on the responses to the risk assessment questions that were completed on the Security Portal.

Threats with Existing Controls

Threat	Probability w/Existing Controls	Impact w/Existing Controls	Risk w/Existing Controls	Risk
Unauthorized access to data / theft	Medium	High	High	
Stolen or lost smartphone may contain PII and/or sensitive company data	Medium	High	High	
Hackers could gain unauthorized access to network	Medium	High	High	
Stolen or lost laptop / portable media containing PII and/or sensitive company data	Medium	High	High	
Virus/Worm/Malicious code could negatively impact the network	High	High	High	
Not adequately destroying electronic media may leave information available to unauthorized persons	High	High	High	
Hardware failures could impact the availability of PII and/or sensitive company data	Medium	High	High	
A Service Provider could cause a data breach	Medium	High	High	
Flood Internal	Low	High	Medium	
Explosion could damage main computing infrastructure	Low	High	Medium	

Terminated employee accesses system - corrupts, steals or destroys data	Low	High	Medium	
Physical intrusion by unauthorized persons	Low	High	Medium	
Unauthorized persons may use an unattended workstation	Medium	Medium	Medium	
Insecure email could contain confidential information	Medium	Medium	Medium	
Employee passwords could be shared	Medium	Medium	Medium	
Temporary or new employees may be insufficiently trained	Medium	Medium	Medium	
Acts of God: flood, tornado, tsunami, hurricane	Low	High	Medium	
A power failure could interrupt employee access	Low	High	Medium	
An employee accesses PII and/or sensitive company data that should not have access to the data	Medium	Medium	Medium	
An employee may post PII and/or sensitive company data on a social network or public forum	Medium	Medium	Medium	