Security Risk Assessment

Prepared For:

Matrixforce

Prepared By:

June 27, 2019

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:

Matrixforce, 9810 East 42nd St. Ste. 209 Tulsa, OK 74146.

Section 2

General Areas to Focus on

In this section we have compiled 6 areas all organizations should focus on for lowering overall risks. These are not specific to your organization.

1) **E-mail phishing attacks -** Phishing emails are a leading cause of security breaches since they exploit a human-related vulnerability. According to the IBM Security Services 2014 Cyber Security Intelligence Index [1], 95% of all data breaches are a result of an employee or human-related error (e.g. phishing). In addition, according to the Verizon Data Breach Investigation Report (DBIR) [2], 92.4% of all malware is delivered via email. To remediate the ever-growing threat of phishing scams, we recommend that proper employee training procedures are implemented, and simulated phishing attacks are evaluated.

2) **Ransomware attacks -** One of the most dangerous and common types of malware is known as ransomware. According to the Verizon DBIR, ransomware is found in 39% of all malware related breaches and is the most prevalent type of malware across all business sectors. Ransomware is most commonly delivered in the form of a phishing email. Ransomware will encrypt all files on a computer or possibly the entire network and demand a ransom payment for the decryption code to unlock the files. A paid subscription to a reputable anti-virus software must be implemented across all network-connected devices within the organization, and virus/malware definitions are kept up to date. A data backup/recovery plan must be implemented and tested. Proper employee training procedures are also crucial to stopping ransomware attacks delivered through phishing emails and other channels.

3) **Accidental or intentional data loss -** Data loss is another way that PII confidentiality, integrity or availability may be compromised. Some common threats that result in data loss include: improper media disposal, insider threats, improper access to PII, loss or theft of devices containing PII, system vulnerabilities and a lack of employee security awareness, just to name a few. Auditing workforce access to systems containing health records or sensitive data is crucial to detecting malicious activities. In addition, role-based access and proper termination procedures should be implemented to ensure that there is no unauthorized access to PII.

[1] https://media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf
[2] https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf

4) **Loss or theft of equipment or data -** A leading cause of breaches results from the loss or theft of equipment or data. A significant number of reported breaches involved portable media. Devices such as USB drives, laptops, and backup drives are particularly vulnerable due to their portability and their high likelihood of traveling outside the organization. To help minimize the risk of a breach in this area, we recommend the following steps be taken:
    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 minimum 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 can 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.

5) **Attacks IoT devices -** Poor cybersecurity for the Internet of Things (IoT) devices can also pose a major risk to organizations. In many situations, these devices can be difficult or impossible to patch or update and could be running outdated operating systems. Some ways this risk can be mitigated is through proper communication and support agreements with equipment vendors, by disconnecting or segregating the equipment from the network and by tracking portable connected devices.

6) **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**
➢	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.

Section 3.2 - Physical Safeguards		
	Finding	**Recommendation**
➢	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.

Section 3.3 - Technical Safeguards		
	Finding	**Recommendation**
➢	No Finding	There are no recommendations for this section.

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**
Hardware failures could impact the availability of PII and/or sensitive company data	Medium	High	High	
Physical intrusion by unauthorized persons	Low	High	Medium	
Acts of God: flood, tornado, tsunami, hurricane	Low	High	Medium	
A power failure could interrupt employee access	Low	High	Medium	
Stolen or lost smartphone may contain PII and/or sensitive company data	Low	Medium	Low	
Not adequately destroying electronic media may leave information available to unauthorized persons	Low	Low	Low	
A Service Provider could cause a data breach	Low	Low	Low	
Stolen or lost laptop / portable media containing PII and/or sensitive company data	Low	Medium	Low	
Terminated employee accesses system - corrupts, steals or destroys data	Low	Medium	Low	

Lost or stolen backup media could have PII and/or sensitive company data	Low	Low	Low	
Unauthorized persons may use an unattended workstation	Low	Medium	Low	
Flood Internal	Low	Medium	Low	
Unauthorized access to data / theft	Low	Low	Low	
Explosion could damage main computing infrastructure	Low	Medium	Low	
Hackers could gain unauthorized access to network	Low	Low	Low	
Virus/Worm/Malicious code could negatively impact the network	Low	Medium	Low	
Unsecure email could contain confidential information	Low	Low	Low	
Employee passwords could be shared	Low	Medium	Low	
Temporary or new employees may be insufficiently trained	Low	Medium	Low	
An employee accesses PII and/or sensitive company data that should not have access to the data	Low	Medium	Low	
An employee may post PII and/or sensitive company data on a social network or public forum	Low	Medium	Low	