Douglas Roberts

010396218

C700: Secure Network Design Performance Assessment

A. The primary physical vulnerabilities that puts the security posture of Psinuvia at risk are both in regards to the physical facilities of the company. While some of the data (PII, patient health information, etc.) in under control of the customer, much of the data is under the stewardship Psinuvia. As such, it is required that Psinuvia safeguards the facilities in which the data are stored. Worldwide facilities (USA, Canada, and Singapore) are required to be properly secured and have security on premise 24 hours a day. On boarding and off boarding employees will appropriately grant and revoke employee access to facilities and systems by means of access cards, passwords, and multi-factor authentication (including fingerprint biometrics).

The second physical vulnerability that must be addressed is the lack of business continuity plan (BCP) for all facilities, worldwide. Should any threat via disaster (natural, human, or otherwise) be realized at any Psinuvia facility, without a BCP, the company will not be able to operate. Lacking plans for the continuous operations of business, employees will not know what needs to be prioritized, or even how to do so, for recovery.

The first physical threat facing Psinuvia is from its former chief scientist who is in Saint Petersburg, Russia, after having left the company. Insider threats are amongst the greatest threats any company may face. Without strong administrative controls in place (i.e., NDA’s, on boarding and off boarding policies, acceptable use policies, background checks), proprietary properties and trade secrets may be compromised when losing key employees, like the company’s former chief scientist. Additionally, it is of paramount importance the Psinuvia has revoked all access to company property and facilities by the former scientist.

The second physical threat is from nature. Psinuvia maintains offices globally, in Texas, Canada, and Singapore. Specifically, the operation Hub in Dallas is subjected to the annual environmental occurrences, namely flooding and tornadoes. Psinuvia currently only has a rudimentary business continuity plan in place. If a flood or tornado were to affect the facilities in Dallas, the company would be ill equipped or prepared to mitigate any damage done and would likely not be able to maintain operations.

B. Two logical vulnerabilities that put the security posture at risk of Psinuvia and must be addressed, are in regard to its data. First, because the company deals with medical devices collects payment via credit cards, it maintains highly sensitive information like credit cards numbers, addresses, and health records and conditions. This PII (personally identifiable information) and PHI (protected health information) should be stored on separate servers and accessible on separate VLAN’s from other business operations. The data should be encrypted using symmetric encryption, with the keys on a separate server from the PII and PHI.

The second logical vulnerability is in the scale and size of the company. The company physically operates out of three different countries who have their own differing laws. Beyond that, Psinuvia has customers all around the world, whose citizens and their respective data are subject to a wide variety of laws. Psinuvia must adhere to rules and regulations like Health Insurance Portability and Accountability Act (HIPAA) and General Data Protection Regulation (GDPR). By not being in compliance with regulations and standards of HIPAA, GDPR, and others, Psinuvia could face civil, regulatory, and even criminal lawsuits.

Psinuvia also faces logical threats that put its security posture at risk. With annual sales of $700 million representing unchallenged market share and profits in its segment of the medical diagnostic and treatment system (MDTS), hackers and cyber criminals are a constant threat. Valuable company assets like patient data, technology and trade secrets, and money make Psinuvia a target from script kiddies to organized crime to potentially persistent threat actors.

Another threat Psinuvia faces is regarding the infrastructure on which it operates. Wi-Fi and wireless systems interface with propriety company equipment and carry patient PII and PHI. Out of sate equipment, insecure access points, unpatched systems, and weak encryption at any point of the network can result in data leakage, loss, or theft. If customers cannot trust their information will be transported and maintained safely, Psinuvia may be sued or regulated out of business.

C. Psinuvia will adhere to industry standards and policies for acceptable use policies (AUP’s), mobile device management (MDM), password use policies (PUP’s), personally identifiable information (PII). The industry standards are outlined below:

**Industry standards for AUP**

NIST SP 800-18 (<https://csrc.nist.gov/publications/sp800>) explains that within AUP’s, users have certain responsibilities and expected behaviors. Not adhering to the AUP can open individuals up to certain consequences. Additionally, users must be informed of, and agree that they understand and will follow the rules outlined in an AUP. Asset owners who enact AUP’s are responsible for developing a security plan, maintaining the system being used, update the plan and system as necessary, and ensure users are trained on the AUP.

**Industry standards for MDM**

NIST SP 800-124 Revision 1 contains industry guidelines for the security of mobile devices. Data should be managed and maintained centrally, with devices not allowed to store data locally. Additionally, the enterprise devices must partition the phone so that other data and systems of the operating device are separate from the capacity to access company data. Device location, remote lockout, and remote wiping capabilities and policies must also be in place.

**Industry standards for PUP**

NIST SP 800-63B contains recommendations and standards for password use. Passwords must be hashed using secure hashing algorithms (SHA2, SHA3) and be anywhere from eight to 64 characters in length. Previous versions on NIST SP 800-63B also recommended passwords expire after 30 days and use at least one special character and number. While the latest 800-63B advises against those standard practices, Psinuvia should use MFA and specifically biometric fingerprints to bolster password protection.

**Industry standards for policies for PII**

NIST SP 800-122 is a NIST Special Publication that outlines protecting the confidentiality of PII. Policies and procedures should outline who has access to PII, incident response to the loss or leakage or breach of PII data, and limit the use, collection, and disclosure of PII maintained by the company.

D. As per the Independent Security Report, Psinuvia will maintain separate departments of (1) Compliance and Risk and (2) Security. At a minimum, each department will be maintained by one Directors, respectively. Where able and necessary, each Director may hire any Managers and Specialists of Compliance and Risk or Security. The duties will be assigned as follows:

|  |  |
| --- | --- |
| **Compliance and Risk Department** | **IT Department Duties** |
| Director of Compliance and Risk | **Develop** policies regarding data:  collection,  maintenance,  limitation, and  disposal  **Determine** and develop policy for the storing and maintenance of sensitive data  **Conduct** BIA  **Develop** audit policies and procedures  **Develop** employee education and training  **Assist** the legal and regulatory compliance officers  **Support** the Data Protection Officer |
| Compliance and Risk Manager | **Assist** the Director of Compliance and Risk, as necessary |
| Compliance and Risk Specialist | **Assist** the Compliance and Risk Manager, as necessary |
| **Security Department** | **IT Department Duties** |
| Director of Security | **Physical** security  **Ensure** proper marking of sensitive data and assets  **Data** loss prevention (DLP)  **Enforce** policies regarding data:  collection,  maintenance,  limitation, and  disposal  **Enforce** policy for the storing and maintenance of sensitive data  **Support** the Data Protection Officer |
| Security Manager | **Assist** the Director of Security, as necessary |
| Security Specialist | Assist the Security Manager, as necessary |

E. Psinuvia does not have any policy or procedures documents to bring it in compliance with the Payment Card Industry Data Security Standards (PCI DSS). According to the PCI Security Standards Council (https://www.pcisecuritystandards.org/merchants), to meet minimum requirement of the PCI DSS, the company must adhere to operational and technical standards around building and maintaining a secure network and systems, protecting account data, maintaining a vulnerability management program, implementing strong access control measures, regularly monitoring and testing networks, and maintaining an information security policy.

To bring Psinuvia in line with the above PCI DSS standards for security policy, the company will appoint an officer of the company as the PCI DSS Compliance Officer. That person will be responsible for assigning PCI DSS compliance managers for each physical location and business unit of the company. All PCI DSS related reports and audits conducted by the Compliance Officer will be reported directly to the CEO and board of directors.

The PCI DSS Compliance Officer will implement strong access control measures by ensuring the company follows best practices and procedures regarding customer PII (personally identifiable information), uses best available end-to -end encryption for all credit card transaction and transmission of sensitive data, and uses multi factor authentication (MFA) on all company mobile devices and computer systems.

Additionally, the company will follow the latest and accepted industry standards per the Secure Software Lifecycle and Secure Software Standards. Psinuvia will utilize up to date and patched Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). All network devices and interfaces will likewise be up to date, patched, monitored, and have remediation controls in place should any secure network violations occur*.*

F. To ensure Psinuvia follows the General Data Protection Regulation (GDPR), the following best practices and principles are recommended (https://gdpr.eu/checklist): lawful basis and transparency, data security, accountability and governance, and privacy rights. For lawful basis and transparency, Psinuvia will conduct annual internal information audits. As a company with more than 250 employees, it is mandated that Psinuvia can show auditors a complete detailed list of updated processing activities. To be in compliance with regulatory requirements, the internal audits will ensure that the processing activity lists include the type of data, the method by which the company acquired the data, the purpose of the data, and access to the data.

For data security, This PII (personally identifiable information) and PHI (protected health information) will be stored and maintained on separate servers from other company data. PHI and PII will also be anonymized, encrypted, and hashed. The principle of least privilege will be followed regarding access to the information, and regular audits will be performed to ensure these rules are enforced.

For accountability and governance, should there be any data leakage or breach, appropriate legal framework will be followed, and requisite law enforcement and governments will be notified. An officer of the company will be assigned as the GDPR Compliance Officer. That person will be responsible for assigning GDPR compliance managers for each physical location and business unit of the company. All GDPR related reports and audits conducted by the Compliance Officer will be reported directly to the CEO and board of directors.

Finally, for privacy rights, the GDPR Compliance Officer will maintain a staff of, at a minimum, one customer experience and support (CES) manager and one customer experience and support specialist. The responsibilities of the CES department will include, but are not limited to, developing efficient systems for customers to request and receive updates on data stored by Psinuvia on each customer, enabling customers to update or change their information, and request deletion of their data (if possible or necessary).

G. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 requires Psinuvia to follow standards and rules for their customers privacy and security. For compliance with privacy and security, Psinuvia will develop policies and procedures around four pillars: annual audits, remediation and response, employee awareness and training, third party policies. First, for annual audits, Psinuvia will conduct internal audits and assessments on an annual basis (or more often if required by law or necessity). These audits include, but are not limited to, physical security and access, device security, patient privacy, handling of PII and PHI, and data access.

For remediation and response, any deficiencies must be noted and shared with the appropriate stakeholders and plans for remediation drawn up as soon as possible. Appropriate management and stakeholders are required to immediately implement solutions. In the event of data breach, the company will follow best practices and adhere to appropriate legal framework (i.e. notify public of breach within 72 hours as per GDRP) to announce said breach, fix issues that lead to the breach, and comply with law enforcement and government.

Regarding employee awareness and training, Human Resources (HR) will conduct on boarding, quarterly, and annual training for all company personnel concerning HIPAA requirements for the company at large, and for each employee individually. Additionally, an officer of Psinuvia will be assigned the role of HIPAA Compliance Officer. That person will be responsible for assigning HIPAA compliance managers for each physical location and business unit of the company. All HIPAA related reports and audits conducted by the Compliance Officer will be reported directly to the CEO and board of directors.

Finally, strict policies and procedures regarding the collection and sharing of data with third parties (vendors, business partnerships) will follow least privilege rules. There will be annual reviews of each third party that will include, but are not limited to, identification of associations, scope of associations, legal requirements and reviews of partnerships, and review of NDA’s and confidentiality agreements.

Failure to maintain the standards set forth in HIPAA may result in various penalties. HIPAA violations are categorized in a tier structure. That structure, per violation, is as follows (<https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096>):

|  |  |  |  |
| --- | --- | --- | --- |
| **Tier 1** | **Tier 2** | **Tier 3** | **Tier 4** |
| Result of Lack of Knowledge  $100 - $50,000 | Result of Reasonable Cause  $1,000 - $50,000 | Result of Willful Neglect  $10,000 - $50,000 | Result of Willful Neglect (over 30 days uncorrected)  $50,000 and up |

In addition to financial penalties, it is also possible to incur criminal charges and potential penalties under HIPAA. While not as common, if someone profits by way of stealing, gaining access to, or disclosing PHI, they may face the following criminal penalties:

|  |  |  |
| --- | --- | --- |
| **Tier 1** | **Tier 2** | **Tier 3** |
| Via reasonable cause or ignorance  Up to 1 year in jail | Obtaining PHI under false pretenses  Up to 5 years in jail | Obtaining PHI for personal gain or malicious intent  Up to 10 years in jail |

H. According to the independent security report, Psinuvia only just has a Business Continuity Plan (BCP). This is unacceptable, and the below additions to the existing BCP are recommended:

**Goals and strategy for execution**

The goals of the BCP, in order, are (1) Safety and security of people (2) Safety and security of property (3) Continue normal business operations. Should a disaster strike any Psinuvia facilities, recovery will immediately a predesignated local Incident Response Leader (IRL) will take charge. For each geography, there will be one IRL and three lieutenants, to provide redundancy. Data from each site will have backups stored at off site facilities (hot sites if possible), with additional redundancies stored at geographically dissimilar sister locations. For example, should a flood affect the offices in Dallas, backup data can be recovered from Canada or Singapore. Raid 5 with striping, or Raid 10 is the standard.

In a similar fashion to data backups, every Psinuvia location will maintain year-round personnel from each separate business unit that can take over duties and responsibilities of their coworkers should any one location becomes inoperable (i.e. HR is headquartered in Dallas, but maintains HR employees and assets in both Canada and Singapore capable of continuing operations if a tornado affects the Dalla HQ).

**Provisions and Processes**

First, foremost, and throughout, the top priority is the health and safety of people. Managers will keep emergency call rosters of their employees and must report head counts and issues with their personnel within one hour of an announced emergency. Site managers will also hold regular safety drills (fire, tornado, or other) and ensure each building and each individual floor maintains adequate emergency and medical equipment.

Quarterly and annual inventories and asset valuations will be conducted on buildings, facilities, infrastructure, and equipment. Psinuvia will have up to date and legally compliant insurance for all property and personnel. Managers will ensure all requirements are met, as outlined by the insurance companies, to always stay in compliance with respective policies.

**Training and Education**

Human Resources (HR) will conduct on boarding, quarterly, and annual training for all company personnel concerning BCP and disaster planning as a whole. Training will include company plans, policies, and procedures, as well as what is expected of each employee individually. Each physical location and business unit of the company will have BCP awareness training for their respective role, as well as pre-identified BCP leaders, should an emergency surface. Annual First Aid, CPR, and AED training will be offered to all employees, and required for people managers.

**Citations**

Chapple, M., Stewart, J. M., & Gibson, D. (2021). Chapter 1 Security Governance Through Principles and Policies *CISSP (ISC)2 Certified information systems security professional official study guide* (9th ed.).John Wiley & Sons, Inc.

Chapple, M., Stewart, J. M., & Gibson, D. (2021). Chapter 3 Business Continuity Planning *CISSP (ISC)2 Certified information systems security professional official study guide* (9th ed.).John Wiley & Sons, Inc.

Chapple, M., Stewart, J. M., & Gibson, D. (2021). Chapter 18 Disaster Recovery Planning *CISSP (ISC)2 Certified information systems security professional official study guide* (9th ed.).John Wiley & Sons, Inc.

Antonucci, D. (2017). Chapter 7 Identifying, Analyzing, and Evaluating Cyber Risks. In *The Cyber Risk Handbook: Creating and measuring effective cybersecurity capabilities*. essay, John Wiley & Sons.

Antonucci, D. (2017). Chapter 17 Legal and Compliance. In The Cyber Risk Handbook: Creating and measuring effective cybersecurity capabilities. essay, John Wiley & Sons.

Moschovitis, C. (2018). Chapter 7 Threats. In *Cybersecurity program development for Business: The Essential Planning Guide*. essay, Gildan Media.

Moschovitis, C. (2018). Chapter 8 Vulnerabilities. In *Cybersecurity program development for Business: The Essential Planning Guide*. essay, Gildan Media.

Moschovitis, C. (2018). Chapter 11 Incident-Response Planning. In Cybersecurity program development for Business: The Essential Planning Guide. essay, Gildan Media.

PCI DSS for Large Organizations Special Interest Group. (2020, February). *Information Supplement: PCI DSS for Large Organizations*.

PCI Security Standards Council. (2022, June 23). *Merchant resources*. PCI Security Standards Council. Retrieved from https://www.pcisecuritystandards.org/merchants/

Horizon 2020 Framework Programme of the European Union. (n.d.). *GDPR Compliance Checklist*. GDPR.eu. Retrieved from https://gdpr.eu/checklist/

(OCR), O. for C. R. (2021, August 16). *HIPAA for professionals*. HHS.gov. Retrieved from https://www.hhs.gov/hipaa/for-professionals/index.html

HIPAA Journal. (2022, September 5). *What are the penalties for HIPAA violations? 2022 update*. HIPAA Journal. Retrieved from https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/

Center for Internet Security. (2021, October 28). *The 18 CIS controls*. CIS. Retrieved from <https://www.cisecurity.org/controls/cis-controls-list>

Search. CSRC. (n.d.). Retrieved from https://csrc.nist.gov/publications/sp800