PPIT FINAL FALL 2022

Q1: Secure Cyber Approach for Data.ai Company

Given the scenario where Cyber secure identified unnecessary employee access to confidential data in Data.ai company, implementing a secure cyber approach is crucial. Referencing "A comprehensive approach to cyber resilience" article, the following steps can be taken:

- Access Control Review: Restrict employee access based on the principle of least privilege. Regularly review and update access permissions to limit data exposure internally.
- Employee Training: Conduct regular cybersecurity awareness training for all employees. Educate them about data handling practices, the importance of data protection, and recognizing potential threats like phishing or social engineering attacks.
- Data Encryption: Implement robust encryption methods for sensitive data stored within the company's databases and networks. Encrypting data at rest and in transit helps safeguard it even if unauthorized access occurs.
- Multi-Factor Authentication (MFA): Enforce MFA across all systems and applications. This additional layer of security reduces the risk of unauthorized access, even if login credentials are compromised.
- Regular Security Audits: Conduct periodic security audits and risk assessments to identify vulnerabilities and address them promptly. Regular penetration testing can simulate attacks to identify weak points in the system.
- Incident Response Plan: Develop a comprehensive incident response plan outlining steps to be taken in case of a cyber-breach. This plan should include protocols for containment, investigation, and recovery.
- Implement Secure Technologies: Employ advanced cybersecurity tools like intrusion detection systems, firewalls, antivirus software, and endpoint protection to actively monitor and defend against external and internal threats.

Q2: Measures to Reduce Cyber-Attacks (University of Calgary Case Study Context)

In the context of the University of Calgary case study, the following measures can be taken to mitigate the risk of cyber-attacks:

- Regular Updates and Patch Management: Ensure that all systems, applications, and software are regularly updated with the latest security patches to address vulnerabilities.
- Data Encryption and Backup: Encrypt sensitive data and maintain regular backups to prevent data loss in case of a cyber-incident. Secure and reliable backup systems are crucial.
- Employee Training and Awareness: Conduct specialized cybersecurity training programs for staff and faculty. Raise awareness about phishing attacks, social engineering, and best practices for data protection.
- Access Control and Segmentation: Implement strict access controls and network segmentation to limit unauthorized access to sensitive information. Restrict access on a need-to-know basis.
- Incident Response Plan: Develop and regularly update an incident response plan. Define roles, responsibilities, and protocols to respond swiftly and effectively to cyber incidents.
- Third-Party Risk Management: Vet and monitor third-party vendors' security practices and ensure they meet cybersecurity standards to mitigate potential risks arising from external partnerships.
- Continuous Monitoring and Threat Intelligence: Deploy tools for continuous monitoring of networks and systems. Use threat intelligence to identify and respond proactively to emerging cyber threats.

Q3: Defending Against Allegations on Blog Site (Steve's Case)

Steve can take several steps to defend himself and prove his innocence regarding wrong allegations on his blog site defaming a Fortune 50 company:

- Preservation of Evidence: Immediately preserve all evidence related to the blog posts, including server logs, timestamps, and any communications with the accusers. This can support Steve's innocence.
- Legal Counsel Engagement: Seek legal advice from a lawyer experienced in defamation and online content laws. They can guide Steve on the legal aspects and the best course of action.
- Issuing a Public Statement: Post a public statement on the blog site denying the allegations and indicating Steve's intent to resolve the issue lawfully. Avoid deleting or altering any content.
- Request Retraction or Correction: Contact the accusers or the company directly, requesting a retraction or correction of the false statements made against Steve.
- Gathering Witness Testimonies: Gather testimonials or evidence from any individuals who can vouch for Steve's character or the accuracy of the blog posts.
- File a Counterclaim: If legally viable, consider filing a counterclaim against the accusers for defamation or making false statements, depending on the specific circumstances and laws.
- Cooperate with Authorities: If legal proceedings ensue, cooperate fully with law enforcement or legal authorities by providing evidence and information to support Steve's innocence..

Q4: (a) What sort of breach was made by her employee, Mr. Ahmed?

Mr. Ahmed committed several breaches:

- Intellectual Property Theft: He unlawfully acquired and used Zainab's recipe/formula without authorization.
- Unauthorized Access & Data Theft: He gained access to Zainab's computer system and stole confidential business plans and documents.
- Misuse of Confidential Information: Ahmed shared Zainab's proprietary information and business plans without consent.
- Trademark and Patent Infringement: He registered the formula under his name, violating Zainab's intellectual property rights.

(b) Do you think the re-production of someone's idea is professionally and ethically allowed or not?

For Professional and Ethical Allowance:

- Encourages Innovation: Can foster competition and encourage innovation in the market.
- Improves Products: Allows for improvement upon existing ideas for better products or services.
- Market Diversity: Provides consumers with diverse choices and variations.

Against Professional and Ethical Allowance:

- Intellectual Property Rights: Violates the originator's intellectual property rights and undermines their efforts.
- Unfair Competition: Unethical to use someone else's hard work for personal gain without consent.
- Legal Implications: Can lead to legal repercussions including copyright infringement and patent violation.
- Trust and Integrity: Undermines trust and integrity in business relationships.

Q5: a) What approach should Ms. Zainab adopt to secure her recipe of Energy Drink.

- Non-Disclosure Agreements (NDAs): Require employees and partners to sign NDAs to safeguard sensitive information.
- Access Control: Limit access to critical data and systems only to authorized personnel.
- Data Encryption: Implement encryption measures for sensitive data storage.
- Regular Audits: Conduct routine audits to detect and prevent unauthorized access or data theft.

(b): Suppose, you are the owner of this Energy Drink brand. Now, you need to draft an Employer Contract, what clauses you would add in the contract to avoid the breach of idea or formula of the drink.

- Confidentiality Clause: Prohibit employees from disclosing or using confidential information without authorization.
- Non-Compete Agreement: Prevent employees from engaging in similar businesses or using acquired knowledge for a competing venture.
- Intellectual Property Ownership: Clearly state that all intellectual property developed during employment belongs to the company.
- Consequences of Breach: Outline penalties or legal consequences for breaching confidentiality or misusing company information.

Q6: (a) Considering yourself in place of Ms. Zainab, list the core points that she should have included in the MoU while signing the deal with her investor.

- Intellectual Property Rights: Clearly define ownership of the formula and any related intellectual property rights.
- Non-Disclosure Clause: Ensure confidentiality of sensitive business information.
- Restriction on Ownership Transfer: Restrict transfer or registration of the formula without explicit consent.
- Dispute Resolution Mechanism: Define a dispute resolution mechanism to resolve potential conflicts.

(b) Ms. Zainab plans to move her business to USA, if she had patented the formula in Pakistan, will it be protected over there as well?

Patenting the formula in Pakistan does not automatically protect it in the USA. Zainab would need to file for a patent in the USA to secure protection there.

Q7: (a) What rules of the data protection act were violated by Mr. Ahmed and How can Ms. Zainab pursue Mr. Ahmed in the court of law?

Data Protection Act Violations by Mr. Ahmed:

- Unauthorized Access: Ahmed accessed Zainab's computer system without permission.
- Data Theft: He stole confidential business plans and documents from the system.
- Misuse of Data: Ahmed used the stolen data for personal gain without consent.

Pursuing Mr. Ahmed:

Zainab can pursue Ahmed in court for unauthorized access, data theft, and misuse of confidential information under data protection and intellectual property laws.

(b) Why did Ms. Zainab's lawyer advised her to refrain from filing a lawsuit against Mr. Ahmed and the investor?

Zainab's lawyer likely advised against filing a lawsuit due to the potential risk of facing a defamation accusation. Ahmed and the investor may counter-claim defamation, which could harm Zainab's reputation and business further. The lawyer might have advised seeking alternative legal strategies or negotiations to mitigate risks while protecting Zainab's interests.

Q8: (a) We know that a penalty or fine should be introduced in any contract to safeguard the loss of either party in the contract whether it's time, effort or money. However, in clause 20, they introduced the non-solicitation clause. Provide any 2 points for both parties (Ensigten and GMI) that support or hurt their interests.

Two Points Supporting Ensighten's Interests:

- Protection of Intellectual Property: Ensighten may benefit from preventing GMI from soliciting its employees, safeguarding its intellectual property and proprietary information.

- Maintaining Employee Stability: It helps Ensighten maintain a stable workforce by preventing GMI from poaching its key employees, ensuring continuity in operations and expertise.

Two Points Hurting GMI's Interests:

- Restriction in Talent Acquisition: GMI may find it challenging to recruit skilled individuals from Ensighten's workforce, limiting its ability to hire the best talent.
- Potential Impact on Innovation: Restrictions on hiring from Ensighten may limit GMI's access to innovative ideas or diverse skill sets, potentially impacting its growth and development.

(b) First Read [clause 15.2 (Termination by Ensighten)] and then [clause 15.3 (Suspension)]. Now briefly explain in bullets, the meaning of this statement (mentioned in 15.3 suspension) "Ensighten determines in good faith that the customer has repeatedly failed to substantially perform any of its material obligations".

The statement "Ensighten determines in good faith that the customer has repeatedly failed to substantially perform any of its material obligations" means:

- Determining Failure to Perform: Ensighten, acting in good faith, concludes that the customer (GMI) has consistently and significantly failed to fulfill or carry out essential responsibilities or obligations as stipulated in the contract.
- Repetitive Non-Performance: GMI's repeated and substantial breaches or failures in meeting crucial contractual obligations lead to this determination.
- Trigger for Suspension: This determination empowers Ensighten to suspend or temporarily halt its services or obligations to GMI due to GMI's recurrent and substantial failures in meeting its contractual commitments.