It was impressive to read Mitnick's ideas on securing passwords and vulnerabilities associated with different password techniques. However, I have five questions I would pose to Mitnick about our company's privacy issues and to foster a compliance posture for our organization.

1. How do you assess the security risks to our company's systems, people, and assets in terms of data privacy? Can you identify current risks and attacks to the privacy of our customers and company data? The rationale for this question is that NIST emphasizes the importance of developing procedures to identify security risks, as this is crucial for establishing an effective foundation that enables organizations to prioritize risk management strategies and business needs (NIST 2018).

2. What strategies should be employed to protect our company's assets, and what procedures should be implemented to ensure asset management? NIST emphasizes the need for organizations to develop techniques to implement appropriate safeguards to ensure the delivery of critical services and contain the impact of potential security incidents (NIST 2018).

3. What techniques would you employ to detect vulnerabilities and continuously monitor for potential risks and attacks within our systems? NIST requires organizations to implement strategies that would help them with the timely discovery of vulnerabilities within their systems (NIST 2018).

4. How would you develop incident response strategies and techniques that can be used to formulate response strategies for detected security incidents? NIST expects organizations to implement appropriate actions to contain the impact of potential incidents (NIST 2018).

5. How do you plan to develop recovery procedures that can be incorporated into our systems to ensure a holistic recovery plan for our company's assets? NIST encourages organizations to utilize appropriate activities that will promote resilience and restore impaired services in a timely manner (NIST 2018).

The crucial aspect of establishing a NIST framework to promote privacy and secure infrastructure is to ensure that organizations establish actionable steps that can be employed before, during, and after attacks to mitigate their impact. Additionally, establishing security compliance must adhere to different laws by federal and state privacy policies and other regulations related to the company enterprise like HIPPA and HITECH Act.

References

Mitnick, K. D., & Vamosi, R. (2017). *The art of invisibility: The world's most famous hacker teaches you how to be safe in the age of big brother and big data*. Little, Brown and Company.

National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.04162018