As it has been discussed in the text and the lecture, risk is a constant in all projects.

As the newly appointed project manager for the deployment of a new biometric system across four locations (four major metropolitan areas and 12,000+ employees), the board has several questions for you as you begin.

- Coming into this deployment, what is one of the top foreseeable risks to this new system, and how likely is it to occur?
- What preparations should be made to respond to extreme events?
- What sort of risk should the company be willing to accept? Define risk tolerances for use in managing this particular deployment.
- What role does management have in leveraging the skill sets required to deploy the system?
- Are there any organizational blind spots that need immediate attention?

Given your understanding of risk and risk management, utilize your knowledge and skill to answer these questions. Use research and citations to back up your assertions.

Hi,

One of the top risks for this system is a data breach. The nature of the data itself is immutable. Exposure of biometric data can not only put employees at constant risk but also can create considerable legal risk for the company.

To mitigate against this risk, the company should encrypt data in transit and at rest. Multiple forms of authentication such as two-factor authentication can give employees additional layers of security and should co-exist with the biometric system. Employees should also be required to provide informed consent of their collection of biometric data prior to collection similar to the Illinois Biometric Information Privacy Act to lessen legal risk.

The company should accept a moderate amount of risk; if the deployment is unsuccessful, the company should be prepared to revert to another system. Again, multiple forms of authentication reduces the risk incurred by employees.

For deployment the project manager needs to consider the distribution of resources as well as the current ability of resources and their knowledge of biometric tools.

Lastly, a possible blindspot for deployment may be the locations themselves. In the U.S., states have their own laws surrounding biometric protection and they should be taken into account.

References

Johansen, A. G. (2019, February 8). *Biometrics and Biometric Data: What it is and is it Secure?* Norton. https://us.norton.com/internetsecurity-iot-biometrics-how-do-they-work-are-they-safe.html

Morais, L. (2020, May 6). *Biometric Data: Increased Security and Risks*. Security. https://www.securitymagazine.com/articles/92319-biometric-data-increased-security-and-risks

Odin. (n.d.) *What is Biometric Data and How is it Legally Protected?* Odin Law. https://odinlaw.com/what-is-biometric-data-and-how-is-it-legally-protected/

Project Management Institute. (2017). *A Guide to the Project Management Body of Knowledge*. Project Management Institute.

Hi Jeremy,

State with the most restrictive law: Illinois' Biometric Information Privacy Act (BIPA) imposes steep penalties for violations ($1000 for a negligent violation and $5000 for a reckless violation). The regulation provides injunctive relief as well if actual damages exceed the existing penalties. BIPA also grants recovery of attorney fees and litigation costs.

As recently as 2020, Facebook settled a BIPA class action lawsuit. The suit alleged that Facebook's facial recognition technology violates BIPA. The company shelled out $550 million to settle.

States with the least restrictive laws: California and Arkansas have laws that include biometric data in the definition of protected personal information.

References

Pester, R. (2020, February 14). *Patel v. Facebook: Facebook Settles Illinois Biometric Information Privacy Act ("BIPA") Violation Suit*. Jolt Digest. https://jolt.law.harvard.edu/digest/patel-v-facebook-facebook-settles-illinois-biometric-information-privacy-act-bipa-violation-suit

Prescott, N. A. (2020, January 15). *The Anatomy of Biometric Laws: What U.S. Companies Need To Know in 2020.* The National Law Review.

https://www.natlawreview.com/article/anatomy-biometric-laws-what-us-companies-need-to-know-2020

Hi David,

I think it's crucial to provide training on data breaches, especially given their increasing prevalence. Training on cybersecurity threats, in particular social engineering schemes, should occur for everyone who has access to a company’s network. Investing in a robust security education can’t be overlooked; human defenses are just as vital as technological defenses.