ISO/IEC Standard 27000 Section 3 provides a framework for understanding cybersecurity concepts and definitions. One of the key takeaways is that people can be the biggest cybersecurity risk, either unknowingly e.g. due to human error, or intentionally e.g. due to malicious intent. Effective management of people is crucial to overcoming these challenges. The importance of managing people for cybersecurity purposes has been the subject of a lot of research.

According to a study by Krombholz et al. (2015), employees can be the weakest link in cybersecurity because they often lack knowledge of cybersecurity threats and how to prevent them. To address this challenge, organizations need to provide regular cybersecurity training that is tailored to employees' roles and responsibilities. Similarly, a study by Egelman et al. (2013) found that employees are often not motivated to follow security policies due to usability issues, time constraints or unwillingness to do so. Therefore, organizations should consider the usability and practicality of security policies when designing them.

Personnel management is another important aspect of cybersecurity. A study by Jung et al. (2017) found that insider threats, such as employees intentionally or unintentionally leaking sensitive information, are a significant risk to cybersecurity. The study recommends that organizations implement employee monitoring and access controls to prevent insider threats. Furthermore, a study by Khan and Khan (2019) emphasizes the importance of vetting personnel and conducting background checks before granting access to sensitive systems and data.

In addition to training and personnel management, cybersecurity awareness is essential for managing people. A study by Levy et al. (2016) found that cybersecurity awareness programs can be effective in improving employees' knowledge of cybersecurity threats and best practices. The study recommends that awareness programs should be interactive and tailored to employees' job functions. Similarly, a study by Lai et al. (2019) found that a security culture that emphasizes the importance of cybersecurity can improve employees' awareness and behaviour.

Finally, the competence of employees can be considered to be crucial to cybersecurity. Employees that are properly trained and skilled in their roles are more likely to perform their job functions securely and less likely to comprise the security of the system.

In conclusion, managing people is crucial for mitigating the risk of cybersecurity incidents. Academic research has emphasized the importance of regular cybersecurity training, personnel management, cybersecurity awareness programs and employee competence in managing people for cybersecurity. Organizations can improve their cybersecurity posture by implementing these best practices and tailoring them to their unique needs and challenges.

References:

Egelman, S., Sotirakopoulos, A., Muslukhov, I., Beznosov, K., & Herley, C. (2013). Does my password go up to eleven? The impact of password meters on password selection. Proceedings of the 2013 Conference on Computer Supported Cooperative Work and Social Computing, 109-120.

Jung, J., Zhu, S., & Tambe, M. (2017). When and how to manage insider threats: A framework based on optimal timing and budgets. Management Science, 63(9), 2936-2955.

Khan, M. A., & Khan, M. U. (2019). Cybersecurity threats and vulnerabilities in organizations: A systematic literature review. Journal of Information Privacy and Security, 15(1), 27-48.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. Proceedings of the 9th International Conference on Availability, Reliability and Security, 328-337.

Lai, C. H., Chen, C. W., & Chang, C. L. (2019). The impact of information security culture on information security awareness and behavior. Journal of Information Privacy and Security, 15(1), 1-25.

Levy, N., Ramim, M. M., & Schurr, A. (2016). The effect of awareness and training programs on employees' knowledge of information security policy and compliance intentions. Journal of Information Privacy and Security, 12(3-4), 161-176.