Financial Cyber Skills Development

Sri Dhanush Reddy Kondapalli

CWID: 10476150

FIN 545-WS

Financial Cyber Skills Development

1. Explain why the development of knowledge and skills is so essential in this subject area.

The development of knowledge and skills is essential in the field of cybersecurity in financial systems for a number of reasons. First, the financial sector is one of the most important and heavily regulated industries in the world. As such, it is critical that financial institutions have strong cybersecurity practices in place to protect themselves and their customers from cyber threats.

Second, the financial sector is increasingly reliant on technology, which can create new vulnerabilities. Financial institutions must be able to identify and mitigate these vulnerabilities to protect their systems [1]. Again, this requires a strong investment in knowledge and skills development. Finally, it is essential that financial institutions have strong communication and collaboration practices in place in order to effectively defend against cyber threats. This includes both internal communication and collaboration between different financial institutions. By sharing information and best practices, financial institutions can more effectively defend against cyber threats.

2. Identify three (3) industry credentials that could provide foundational knowledge. Explain the value of each.

There are many different industry credentials that could provide foundational knowledge for securing financial systems. Here are three examples: The Certified Information Systems Security Professional (CISSP) is a widely recognized credential in the cybersecurity field [2]. It is designed for professionals with at least five years of experience in the field. The CISSP covers a broad range of topics, including risk management, asset security, security engineering, communication and network security, and more.

The Certified in the Governance of Enterprise IT (CGEIT) is another widely recognized credential, designed for professionals with experience in IT governance. The CGEIT covers topics such as risk management, compliance, and strategic planning. The Certified Information Security Manager (CISM) is another credential that is designed for professionals with experience in information security management. The CISM covers topics such as risk management, incident response, and security program management. Each of these credentials provides valuable knowledge and skills for professionals in the field of cybersecurity in financial systems. By obtaining one or more of these credentials, financial professionals can demonstrate their commitment to staying up-to-date on the latest cybersecurity threats and best practices.

3. Identify three (3) individual, self-paced learning activities that each team member can individually pursue to develop relevant knowledge.

There are many different self-paced learning activities that team members can pursue to develop relevant knowledge in the field of cybersecurity in financial systems. Here are three examples:

- Read articles and blog posts on the latest cybersecurity threats and best practices. Some good sources of information include the CISSP website, the CGEIT website, and the CISM website.
- Attend webinars and conferences on cybersecurity. Some good sources of information include the SANS Institute and the ISACA.
- Get hands-on experience with cybersecurity tools and technologies. Many financial institutions offer internship or fellowship programs that give students and professionals the opportunity to gain hands-on experience with cybersecurity.

Each of the three self-paced learning activities listed above can help team members develop relevant knowledge in the field of cybersecurity in financial systems [3]. Reading articles and blog posts on the latest cybersecurity threats and best practices is a great way to stay up-to-date on the latest information. This can help team members identify new threats and learn about best practices for defending against them.

Attending webinars and conferences on cybersecurity is another great way to stay informed about the latest developments in the field. These events provide an opportunity to network with other professionals and learn about new tools and technologies. Finally, getting hands-on experience with cybersecurity tools and technologies is a great way to develop practical skills. Many financial institutions offer internship or fellowship programs that give students and professionals the opportunity to gain hands-on experience with cybersecurity. These programs can be extremely valuable in developing the skills necessary to defend against cyber threats.

4. Identify potential approaches leadership can take to promote a learning environment.

There are many different approaches leadership can take to promote a learning environment within a financial institution [4]. Here are three examples: First, encourage team members to pursue industry credentials. Financial institutions can provide incentives for team members to obtain industry credentials, such as the CISSP, CGEIT, or CISM. This shows a commitment to developing a strong knowledge base within the organization. Second, provide opportunities for hands-on experience. Many financial institutions offer internship or fellowship programs that give students and professionals the opportunity to gain hands-on experience with cybersecurity. This provides team members with the opportunity to develop practical skills.

Third encourage communication and collaboration. Financial institutions should encourage team members to share information and best practices. This can be done through internal communication channels, such as an intranet, or through external channels, such as industry associations. Each of these approaches can help leadership promote a learning environment within a financial institution. By taking these steps, leadership can show a commitment to developing the knowledge and skills necessary to defend against cyber threats.

References

[1] Parn, Erika A., and David Edwards. "Cyber threats confronting the digital built environment: Common data environment vulnerabilities and block chain deterrence." Engineering, Construction and Architectural Management (2019).

[2] Callen, Jennifer, and Jason E. James. "CYBERSECURITY ENGINEERING: THE GROWING NEED." Issues in Information Systems 21, no. 4 (2020).

[3] Mungo, Jamaine. "Examining the Aspects of Self Paced Cybersecurity Awareness Training: A Generic Qualitative Inquiry." (2022).

[4] Barrett, Peter, Alberto Treves, Tigran Shmis, and Diego Ambasz. "The impact of school infrastructure on learning: A synthesis of the evidence." (2019).