Meeting summary for CISA/CyberHawaii Security Leadership Webinar (03/05/2024)

Quick Summary

Jenn stressed the importance of interpersonal and communication skills, risk management, governance, honesty, and integrity in security leadership. Charissa then highlighted the significance of cybersecurity in small businesses, emphasizing that it's not solely an IT issue and the risks associated with third-party providers. The team also discussed the importance of security awareness training and incident response planning.

Summary

Cybersecurity Leadership Webinar Series

Al from Cyber Hawaii introduced the second webinar in the 2024 Fortify Cybersecurity Educational Series, a collaboration with the Cybersecurity and Infrastructure Security Agency and supported by a grant from the Hawaii Department of Business, Economic Development and Tourism. The webinar focused on cybersecurity leadership, emphasizing that leadership is not limited to a specific title but involves factoring security into the strategy and operations of a business. Jennilyn LaBrunda, a cybersecurity professional, presented the webinar, underscoring the importance of interpersonal and communication skills, risk management, governance, honesty, and integrity in security leadership. Jenn also discussed the main responsibilities of a security leader, which include developing and implementing a cybersecurity strategy, building a cybersecurity culture, managing threats and incidents, aligning cybersecurity with business goals, finding the balance between security and productivity, risk management, assessing vendor and third-party risks, staying informed about emerging threats, and prioritizing risks and threats.

Cybersecurity Culture and Regulatory Compliance

Jenn stressed the importance of understanding industry-specific risks and staying compliant with regulations. She suggested subscribing to regulatory updates, conducting regular internal audits, and building a security-aware culture to resists cyber-attacks. Jenn introduced the cybersecurity performance goals published by Cis, emphasizing their role in identifying prioritization areas and potential future investment. She also highlighted the use of tools such as the Cybersecurity Evaluation Tool and the Known Exploited Vulnerabilities Catalog to prioritize organization risk. Jenn emphasized the significance of cybersecurity culture in organizations and recommended training on basic cybersecurity, conducting training regularly, and aligning cybersecurity practices with the organization's values and goals. She stressed the importance of phishing awareness training and recommended appointing a Chief Information Security Officer or a cybersecurity leader to champion a strong cybersecurity culture. Charissa then took over the presentation.

Cybersecurity Essential for Small Businesses

Charissa addressed the importance of cybersecurity in small businesses, dispelling common myths. She emphasized that cybersecurity is not solely an IT issue, as it affects the entire business. Charissa highlighted that small businesses are often targeted due to lax security measures, and a strong firewall and antivirus program are not enough to ensure security. She also clarified that moving to the cloud does not exempt businesses from cybersecurity risks. Charissa shared alarming statistics about the vulnerability of small businesses to cyber-attacks and the potential for significant financial loss. She concluded by highlighting the need for businesses to take cybersecurity seriously, particularly those that have moved their services to the cloud.

Data Responsibility and Access Control in Businesses

Charissa emphasized the importance of data responsibility and access control in businesses. She highlighted the risks associated with third-party providers, using a recent incident involving HMSA and Navvice as an example. She further stressed the need for careful assessment of service providers and their compliance with logging requirements for compliance purposes. Charissa called for business owners to take initiative, get approval from top leaders, and establish clear policies that all employees understand and comply with. She also noted the importance of training for compliance and emphasized the need for full user participation.

Cybersecurity Training and Incident Response Planning

During the Q&A period, Charissa, Al, and Jenn discussed the importance of security awareness training and incident response planning. They emphasized the potential competitive disadvantages businesses could face if they neglected security and suggested planning for quick recovery and resilience. They also discussed the risks associated with an air-gapped computer and the need to assume eventual attack. Jenn explained the process of reporting suspected cybersecurity incidents and emphasized the importance of planning for incidents. Al highlighted the importance of leadership in risk management within the context of cybersecurity and recommended resources for further learning. It was agreed that the slides and recording from the meeting would be sent to all attendees and the next webinar would focus on mentorships in cybersecurity.

Next steps

• Al will post the recording of the presentation and the slides on the CyberHawaii website. He will send an email when the material has been posted along with a survey that attendees are requested to fill out.