RSAConference2020

Learning Labs

Motivating Human Compliance:

Mitigating Passive Insider Threat

Session ID: LAB2-R08

Tonie Flores, tftwsl@gmail.com

MK Palmore, mpalmore@paloaltonetworks.com

Keyaan J Williams, keyaan.williams@class-llc.com

Table of Contents

Session Summary

Security professionals work to protect internet users from cybercrime while users find creative ways to circumvent rules and put themselves in harm's way. Why would they do that! How can management detect and mitigate the danger? This learning lab presented interactive scenarios to give participants an experience to take home and put into practice.

Agenda

- Overview - Current State of Play in Cybersecurity
- Introduction of Case Study 1 - Acme Technologies
    - Team Discussion and Review
    - Group Discussion and Review
- Introduction of Case Study 2 - Singapore Health
    - Team Discussion and Review
    - Group Discussion and Review
- Takeaways

Key Insights and Considerations

Current Cyber Threat Landscape

- Increasing Digital Threats targeting businesses and consumers
- Increasing complexity of protecting the digital assets of global organizations
- Emerging Technologies
    - Cloud, AI, IoT
- InfoSec should scale and grow with the organization

Case Study 1 - Acme Technologies

- Don't treat security as an afterthought, especially in the start-up environment
- InfoSec best practices and frameworks should form the basis of your approach
- As you enter the global landscape your risk naturally increases
- InfoSec touches all aspects of the business. No one is immune

Case Study 2 - Singapore Health

- Ensure cybersecurity training is made available to cybersecurity personnel
- Ensure cybersecurity knowledge, skill, and ability gaps are identified for all roles with significant security responsibilities
- Address identified gaps through recruiting and/or training
- Ensure cybersecurity training is provided before granting access to critical corporate assets and information

Takeaways

- Adherence to best practices decreases the chances of experiencing a significant infosec incident
- Frameworks and maturity models provide a great roadmap for leveling up your organization's security apparatus
    - Compliance is the floor, not the ceiling to evaluating your security practices
- Employee awareness and training remains a core component of full approach to InfoSec
    - Drive the right behavior

Instructor Contact Details

Tonie Flores

tftwsl@gmail.com

https://www.linkedin.com/in/tonieflores/

MK Palmore, Palo Alto Networks

mpalmore@paloaltonetworks.com

https://www.linkedin.com/in/mkpalmore/

Keyaan J Williams

keyaan.williams@class-llc.com

https://www.linkedin.com/in/keyaan/