RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **LAB2-R08**

Motivating Human Compliance: Mitigating Passive Insider Threat

Tonie Flores

Technical Communications
Data-Doctor.Info
@datadoctorinfo

MK Palmore

VP, Field CSO (Americas)
Palo Alto Networks
@mk_palmore

Keyaan J Williams

CEO, Cyber Leadership and Strategy Solutions, LLC (CLASS-LLC)
@_CLASSllc

Topics

- Educate
  - Generic case study
  - Specific case study
- Learn
  - How to tell there is a problem
  - Who is responsible
- Apply
  - Use the C2M2 to Develop your Cybersecurity Workforce

RSAConference2020

Acme Technologies
Case Study

Multiple (Potential) Threat Vectors - Generic

Threat Landscape

- Increasing digital threats targeting both business and consumers
- Adversaries (Criminal, APT, Hacktivists, Insiders)
  - Global Criminal Enterprises
- Emerging Technologies = Increased Threat Attack Surface
  - Cloud
  - AI
  - IOT
- Global Nature of Business Requiring Access to Digital Information

Acme Technologies

- 4-5 Years (Ops)
- 500 Employees, $10M Revenue (prior year)
- Operating (Americas, Europe & Asia)
- 5-person security staff (No CISO Equivalent)
  - Prior event, depth not fully understood
  - Tools geared towards outside attacker activity
- No GRC, Standardization lacking

Discussion

- Do startups need a security professional?
- How does GRC benefit the information security program?
- Who are Acme's intellectual property adversaries?
  - External
  - Internal
- What is the value proposition of infosec tools?
- Who are the cybersecurity stakeholders?

RSAConference2020

Singapore Health

Highlighting the importance of developing your cybersecurity workforce

Singapore Health Case Study

Background

- In July 2018, a data breach of SingHealth exposed the protected health information and prescription data of 1.5 million citizens of Singapore, including Prime Minister Lee Hsien Loong.
- The breach was caused by ineffective system management, a lack of employee training, and other preventable flaws that the organization allowed to persist in the environment.

Singapore Health Case Study

Outcomes

- Fired!
  - Infrastructure Systems Team Lead
  - Senior Cyber Security Manager
- Demoted/Reassigned!
  - Information Security Officer
- Fines!
  - IHiS was fined S$750,000
  - SingHealth was fined S$250,000

RSAConference2020

Develop Cybersecurity Workforce

What Leadership Must Do

Leadership Responsibilities

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

Apply

- Next week you should:
- In the first three months following this presentation you should:
- Within six months you should:

References

1. Cybersecurity Capability Maturity Model Version 1.1
2. Public Report of the Committee of Inquiry (COI) into the cyber attack on Singapore Health Services Private Limited Patient Database