hacc.hawaii.gov

Happy Aloha Friday!

Workshop #2

Cyber Strategies for Securing Data

May 22, 2020

Agenda

1:00 PM Welcome

REMINDERS: 1) Workshop is being recorded

2) Presentation will be available and sent to the email you used to register for the workshop

Presentation: Vincent Hoang, State Chief Information Security Officer, State of Hawaii Office of Enterprise Technology Service

Topic: State Cyber Strategies Overview

Q&A

Cort Chambers, Ph.D., Security Analyst Hawaii State Fusion Center, Information Technology Instructor at PCATT

Topic: Techniques on Identifying Security Threats & how to help you to protect both yours and your client's data

Q&A

2:30 PM Mahalo & Stay Connected: hacc.Hawaii.gov

Cyber Security Team

Protects all branches of government that today share a common access point to the Internet — where most cyber threats originate!

Enables the State to shift a majority of security work previously done by contractors to skilled State personnel.

Allows ETS to pursue cost-effective solutions for cybersecurity by providing additional training to State employees.

“Hacker” defined

1. A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary.
2. One who programs enthusiastically (even obsessively) or who enjoys programming rather than just theorizing about programming.

http://www.catb.org/jargon/html/H/hacker.html

NIST Cyber Security Framework
Risk Management Framework

Tier / Function	1	2	3	4
Identify				
Protect				
Detect				
Respond				
Recover				

Current Profile					
Target Profile					

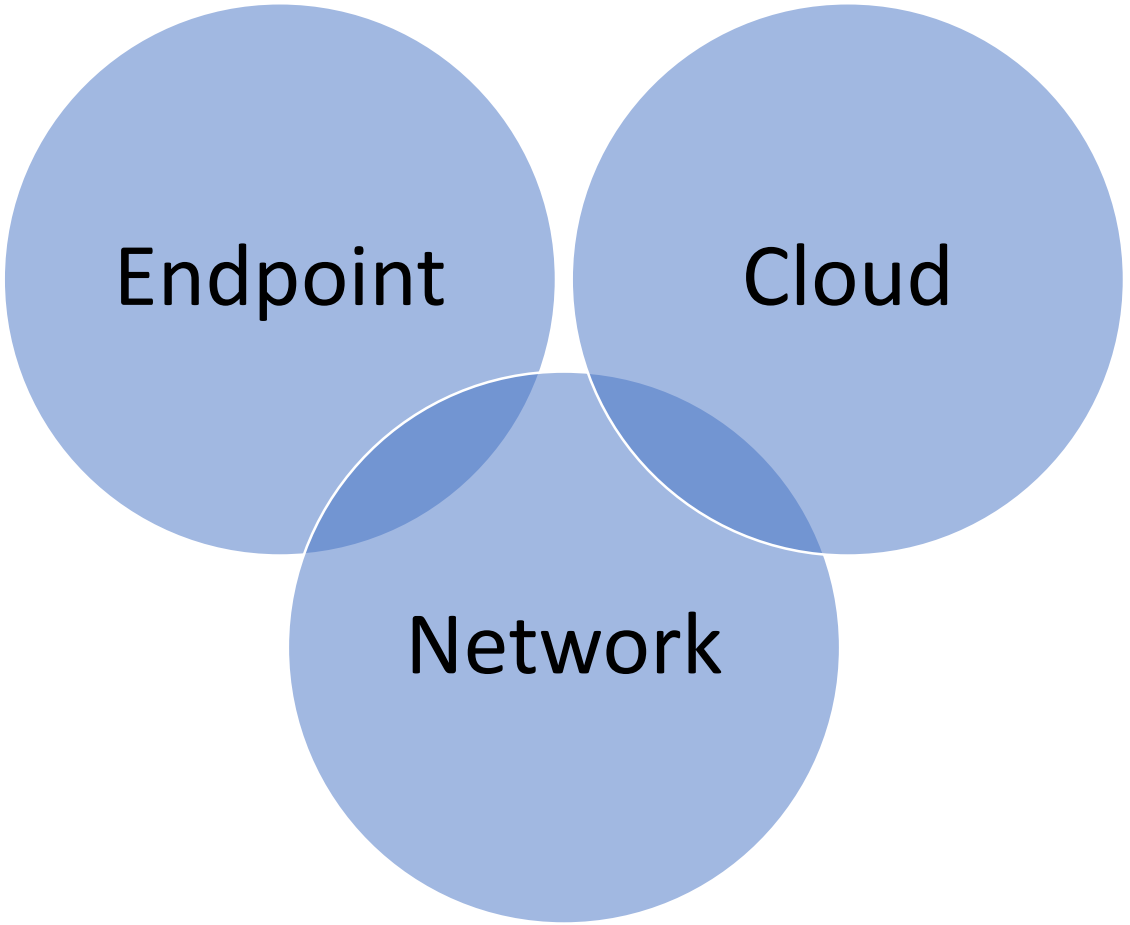
https://www.nist.gov/cyberframework

CIS Controls
Technical Controls Framework

CIS Center for Internet Security®

https://www.cisecurity.org/controls/

Budget Priorities



NSA | CSS

David Hogue, Technical Director
NSA Cybersecurity Threat Operations Center
RSA Conference 2018

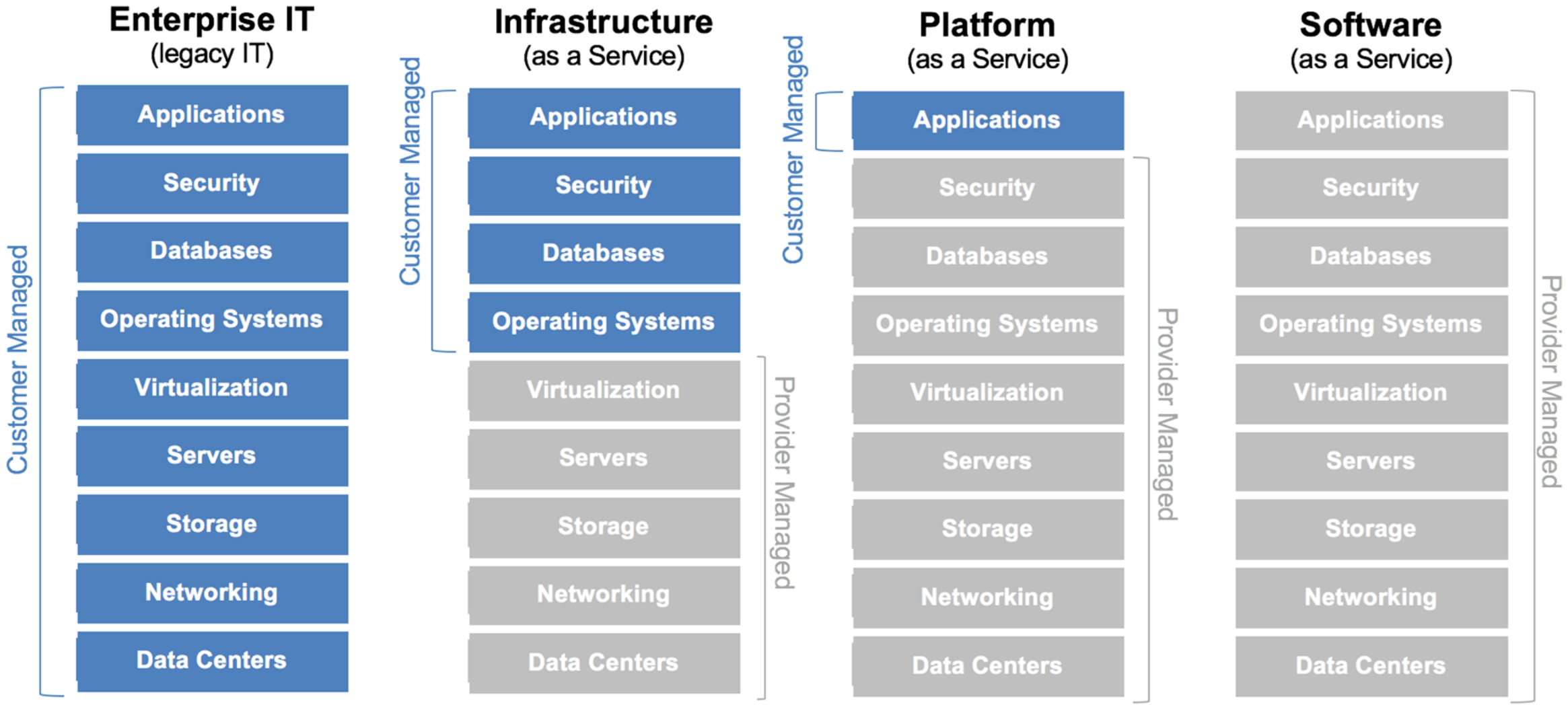
“The vulnerability that took down Equifax last year when it was released in March, we had a nation-state actor within 24 hours scanning looking for unpatched servers within the DoD,”

“At NSA we have not responded to an intrusion response that’s used a zero day vulnerability in over 24 months,” Hogue said.

“The majority of incidents we see are a result of hardware and software updates that are not applying.”

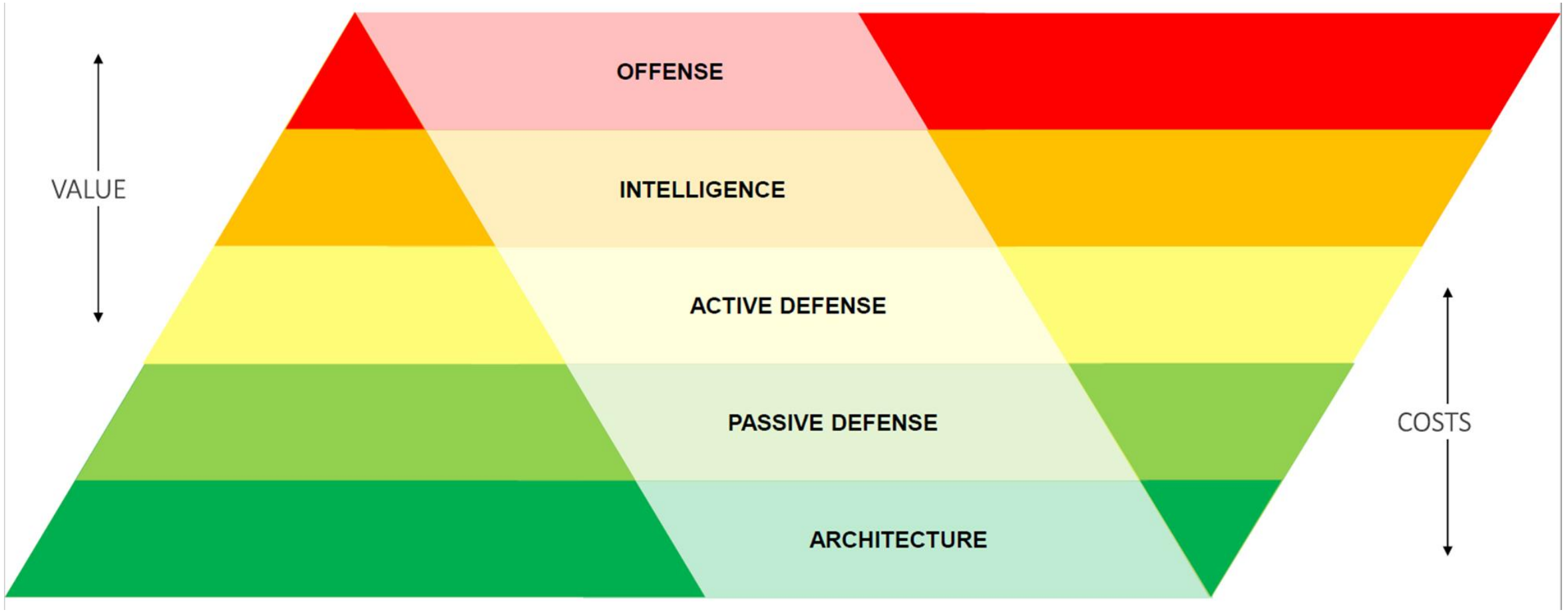
https://www.databreachtoday.com/blogs/nsa-silence-zero-days-p-2623

Cloud Services
Tying it together



https://mycloudblog7.wordpress.com/2013/06/19/who-manages-cloud-iaas-paas-and-saas-services/

Sliding Scale of Cyber Security
Improve ROI by Building Solid Foundations



Build a Solid Base to Support Higher Order Programs

OWASP Top 10

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

https://owasp.org/www-project-top-ten/

Questions?

Next..