Cybersecurity4All - Teaching cybersecurity across the disciplines

UNIVERSITY of HAWAI'I®
MAUI COLLEGE

Debasis Bhattacharya
debasisb@hawaii.edu
maui.hawaii.edu/cybersecurity
PCATT IT Symposium, 2017

Agenda

- Background
- Cybersecurity Education - Traditional
- Cybersecurity Education - Across Disciplines
  - Approach
- Case Study
  - Faculty Workshop
  - NSA GenCyber
  - AFA CyberPatriot
- Target Modules
- Challenges/Benefits
- Q&A

Background - College

- University of Hawaii Maui College
  - Serves Maui County - islands of Maui, Molokai and Lanai
  - 150,000 or so resident population
  - 2 Million or so tourists per year!
  - 3000+ full-time commuter students
  - 20 or so Associate Degrees
  - 3 Baccalaureate Degrees
  - 66% or so women students
  - Average of students ~25 years
  - Non-traditional students
  - Commuter island college

Cybersecurity Education - Traditional

- Certificates in Cybersecurity
  - Low Level - Intro, Network+, Security+
  - Higher Level - Ethical Hacking, Forensics
- Internships
  - Government, banks, utilities
- Baccalaureate Degree
  - Applied Business and Info Tech
  - Cybersecurity courses are embedded
- Cyber competitions and Workshops
  - NSA GenCyber, US AFA CyberPatriot
- Supported by NSF Grants
  - ATE Program Award# 1204904
  - SFS Program Award# 143751

Cybersecurity Education - Across Disciplines & Segments

- Cybersecurity educations cuts across various segments
  - Community College program disciplines
  - Gender
  - Minorities
  - Background - high schools, professionals, returning veterans etc
  - Various Industries
    - Accounting, Hospitality, Law Enforcement, Utility, Tourism etc.
- One size education does not fit all types of students!

Cybersecurity Education - Across Disciplines

- Focus on 5 disciplines at Associate Degree level
  - Accounting
  - Administration of Justice
  - Electronics
  - Hospitality, Travel and Culinary
  - Business
- Supported by NSF SFS Capacity Building Grant
  - Award# 1437514

Cybersecurity Education - Across Student Population

- Focus on students from a variety of backgrounds
  - Women
  - Minorities
  - Veterans
  - Working Professionals
  - High School Students
  - Remote students who rely totally on distance education
  - Economically disadvantaged
  - Low math/science proficiency
  - Non-technical
  - Non-traditional
  - Not interested in Cybersecurity as a career!

Diverse Cybersecurity Education - Overall Approach

- Obtain administration and other institutional support
- Identify key faculty leaders in key disciplines
- Engage faculty and students
  - Guest Lectures in classes
- Engage employers who will hire students with cyber skills
  - Hotels, banks, tourism industry, law enforcement
- Identify one or two existing courses in each discipline
  - Explore cybersecurity modules that can be embedded
- Hold workshop with faculty from various disciplines
  - Stipend helps!
- Create modules and help faculty member teach it!

Case Study - Faculty Workshop

- Target Audience and Disciplines
  - Faculty from Accounting, Business, Electronics, Hospitality,Culinary
- Date - May 19, 2017
  - All Day Faculty Workshop (summer overload)
  - $350 stipend, supported by NSF SFS Award# 1437514
  - Finalize target courses for Fall 2017, discuss security modules/labs
- Topics
  - Ransomware, Bitcoins, Blockchains, Security Culture, Hacking Labs
- Goals for Academic Year 2017-2018
  - Target two courses - introductory, intermediate/advanced
  - Create cybersecurity modules and embed in existing courses
  - Modules are based on KUs from NSA/DHS CAE CDE program

Case Study - Summer Cyber Workshops

- Target Audience
  - Middle and High School Students
- Dates - June 2017
  - Details at www.gencyber-hi.org and www.maui.hawaii.edu/cybersecurity
- NSA GenCyber - www.gen-cyber.com
  - Free Five Day camp for Beginner and Intermediate Students
  - Covers wide range of cybersecurity topics and career interests
  - 10 Principles, ethics, secure coding, networking hacking, crypto, CTF
- Air Force Association CyberPatriot - www.uscyberpatriot.org
  - Free Cyberpatriot camp - preparation for competitions - www.cyberhui.org
  - CyberPatriot X - Training in September, competition November
  - Students learn about careers and field through a competition

Intro Module - Fundamentals of Info Sec

Fundamental Security Design Principles

Definition: The intent of this Knowledge Unit is to provide students with basic security design fundamentals that help create systems that are worthy of being trusted.

Topics: Separation (of domains) Isolation Encapsulation Least Privilege Simplicity (of design) Minimization (of implementation) Fail Safe Defaults / Fail Secure Modularity Layering Least Astonishment Open Design Usability

Intro Module - Policies, Ethics and Compliance

Policy, Legal, Ethics and Compliance

Definition: The intent of this Knowledge Unit is to provide students with and understanding of information assurance in context and the rules and guidelines that control them.

Topics: HIPAA / FERPA Computer Security Act Sarbanes – Oxley Gramm – Leach – Bliley Privacy (COPPA) Payment Card Industry Data Security Standard (PCI DSS) State, US and international standards / jurisdictions Laws and Authorities US Patriot Act BYOD issues Americans with Disabilities Act, Section 508

Intro Module - Business, Management

Cybersecurity Planning and Management

Definition: The intent of this Knowledge Unit is to provide students with the ability to develop plans and processes for a holistic approach to cybersecurity for an organization.

Topics: CBK Operational, Tactical, Strategic Plan and Management Business Continuity / Disaster Recovery C-Level Functions Making Cybersecurity a strategy (part of core organizational strategy) Change control

Intro Module - Hospitality

Security Program Management

Definition: The intent of this Knowledge Unit is to provide students with the knowledge necessary to define and implement a security program for the protection of an organizations systems and data.

Topics: Project management, Resource management, Project budgeting (cost benefit, net present value, internal rate of return) Risk management and Analysis Quality Assurance / Quality Control Monitoring and Control Deliverables Timelines Security Awareness, Training and Education Security Baselines Change Management, Patch Management Roles and Responsibilities of the Security Organization Compliance with Applicable Laws and Regulations

Intermediate Module - Hospitality, accounting etc.

Fraud Prevention and Management

Definition: The intent of this Knowledge Unit is to provide students with the necessary knowledge to develop plans and processes for a holistic approach to preventing and mitigating fraud throughout the system lifecycle.

Topics: Symptom Recognition Data Driven Detection Investigation of Theft Concealment Conversion Methods Inquiry and Reporting Financial, Revenue and Inventory Liability and inadequate disclosure Consumer fraud

Intermediate Module - Administration of Justice

Device Forensics

Device Forensics Definition: The intent of this Knowledge Unit is to provide students with the ability to apply forensics techniques to investigate and analyze a device.

Topics: Mobile Device Analysis Tablets SmartPhones GPS (must include hands-on activities) Outcomes: Students will be able to describe methods for the acquisition/analysis of mobile devices (e.g., device storage, system data, cell tower logs). Students will be able to explain the legal issues related to mobile device forensic activities.

Advanced Module - Accounting

Forensic Accounting

Definition: The intent of this Knowledge Unit is to provide students with the ability to apply forensics techniques to respond to and investigate financial incidents.

Topics: Investigative Accounting Fraudulent Financial Reporting Misappropriation of Assets Indirect Methods of Reconstructing Income Money Laundering Transnational financial flows Litigation services Evidence Management Economic Damages and Business Valuations

Advanced Module - Electronics, Sustainability Studies

Industrial Control Systems

Definition: The intent of this Knowledge Unit is to provide students with an understanding of the basics of industrial control systems, where they are likely to be found, and vulnerabilities they are likely to have.

Topics: SCADA Firewalls Hardware Components Programmable Logic Controllers (PLCs) Protocols (MODBUS, PROFINET, DNP3, OPC, ICCP, SERIAL) Networking (RS232/485, ZIGBEE, 900MHz, BlueTooth, X.25) Types of ICSs (e.g., power distribution systems, manufacturing) Models of ICS systems (time driven vs. event driven) Common Vulnerabilities in Critical Infrastructure Systems Ladder Logic

Challenges

- Faculty members need to be open and interested!
  - Cybersecurity does not appeal to all
- Faculty members need to see value
  - Inserting course modules within an existing syllabus and timeframe
- Students need need to see value!
  - See cybersecurity as a means to enhance job/career opportunities
- Embedding new courses takes time and work
  - Faculty member needs time off existing work to create new modules
- Ongoing training to ensure new faculty can learn InfoSec
  - Making this sustainable requires one-two years of effort
- Administration needs to be behind all this effort!

Benefits!

- Cyber savvy workforce can come from various disciplines!
- Increase interest in cybersecurity from a diverse group
- Grow the overall awareness of cybersecurity defense
- Enhance ability of non IT faculty to teach cyber topics
- Requirement for NSA/DHS CAE application

6. Cyber Defense is a Multidisciplinary practice at the Institution
The institution must demonstrate that CD is not treated as a separate discipline, but integrated into additional degree programs within the institution.

UNIVERSITY of HAWAI'I®

MAUI COLLEGE

Questions? Comments? Feedback?!

Debasis Bhattacharya

debasisb@hawaii.edu

maui.hawaii.edu/cybersecurity