Teaching cybersecurity across the disciplines

Debasis Bhattacharya
debasishb@hawaii.edu
maui.hawaii.edu/cybersecurity
Hi-TEC Conference, Salt Lake City, UT, 2017
Agenda

Background
Cybersecurity Education - Traditional
Cybersecurity Education - Across Disciplines
  Approach
Case Study
Target Modules
Challenges/Benefits
Q&A
Background - College

University of Hawaii Maui College
Serves Maui County - 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 Camps, Competitions: GenCyber, CyberPatriot

NSF Grants - ATE Program Award# 1204904 - SFS Program Award# 1437514
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 a few disciplines at Associate Degree level

  Accounting
  Administration of Justice
  Allied Health (Nursing)
  Electronics
  Hospitality and Tourism
  General 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

Target Disciplines

Accounting, Business, Electronics, Hospitality

Fall 2016

Guest Lectures

Spring 2017

Target two courses - introductory, intermediate

Summer 2017

All Day Faculty Workshop (summer overload)
$350 stipend, supported by NSF SFS Award# 1437514
Finalize target courses for Fall 2017, create labs

Fall 2017

Create cybersecurity modules and embed in courses
Modules are based on KUs from NSA/DHS CAE CDE program
Why Bother?

Incentives for Students across disciplines
• Learn some details about an emerging field, that is hot on the media!
• Study cybersecurity within the context of their own chosen field of study

Incentives for IT Faculty
• (Possible) Release Time during Fall Semester – Guest Lectures, Prepare Labs/Courses
• (Possible) Release Time during Spring Semester – Mentor non-IT Faculty to teach
• Apply for NSF SFS Capacity Grant, and others funding sources = Summer Overload $

Incentives for non-IT Faculty
• Embed Cybersecurity modules within their own courses
• Learn about cybersecurity through free workshop + stipend!
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 an understanding of information assurance in context and the rules and guidelines that control them.

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
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 organization's systems and data.

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.
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.

Advanced Module - Electronics

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.
Questions? Comments? Feedback?! 

Debasis Bhattacharya  
debasisb@hawaii.edu  
maui.hawaii.edu/cybersecurity