Teaching CyberSecurity Across The Disciplines
(with a focus on women and minorities)

UNIVERSITY of HAWAI'I®
MAUI COLLEGE

Debasis Bhattacharya, Lorraine Lopez-Osako
University of Hawaii Maui College, HI
Karina Bhattacharya - University of Houston, TX
debasisb@hawaii.edu maui.hawaii.edu/cybersecurity
HI-TEC Miami, FL, 2018

Agenda

- Background
- Cybersecurity Education - Traditional
- Cybersecurity Education - Across Disciplines
  - Overall Approach
- Case Study
  - Malware in Small Doctor Offices
  - Design of Secure Wearables
- 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
  - Median age 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, NSA GenCyber
- Supported by NSF Grants
  - ATE Program Award# 1204904 (2012-15)
  - SFS Program Award# 1437514 (2015-17)
- Applied for NSA/DHS CAE CDE

Cybersecurity Education - Across Disciplines/Segments

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

Cybersecurity Education - Across Disciplines

- Focus on 6 disciplines at Associate Degree level
  - Accounting
  - Healthcare
  - Electronics
  - Hospitality
  - Business
  - Administration of Justice
- Open to disciplines at other universities - U of Houston
- Supported by NSF
  - SFS Capacity Building Grant - Award# 1437514
  - ATE Grant - Award# 1700562

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
  - **Highlight high tech industry examples that involves cybersecurity**
- Engage employers who will hire students with cyber skills
  - Hotels, banks, tourism, hospitals, 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!

Overall 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 and projects 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!

- Hands-on projects engage diverse students with fun work!
- 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.

Case Study

- Awareness of Malware in Small Medical Practices
- Location of Study - Maui
- Duration of Study - Spring 2018
- Student Researcher - **Lorraine Lopez-Osako**
    - Student in the Applied Business and IT program
    - UH Maui College BAS graduate May 2018
  - Visited 15 small medical offices
  - Sent out survey to all doctors
  - Received 10 complete, valid responses
  - Created a CyberSecurity poster for doctor’s office

Cybersecurity in Small Practices

This is a CONFIDENTIAL survey for a Research Project with UHMC. There will be no links to any information obtained to you, the type of practice or your practice. Please answer as honestly as poss Results will only be reviewed as a compilation of results.

* Required

1. **How much time did you think about cybersecurity before this survey?** *
   Mark only one oval.

	1	2	3	4	5	
Never	◯	◯	◯	◯	◯	Always

2. **In Hawaii, how safe do you feel from cybersecurity attacks?** *
   Mark only one oval.

	1	2	3	4	5	
Safe	◯	◯	◯	◯	◯	Not Safe at all

3. **In your opinion, what could be the most damaging to a practice?** *
   Mark only one oval.

- ◯ Exposure of financial information and loss of money
- ◯ Exposure of practice information
- ◯ Exposure of patient information
- ◯ Other: _____

4. **What are the roadblocks of the professional that prohibit from being more engaged in cybersecurity?** *
   Mark only one oval.

- ◯ Awareness
- ◯ Education
- ◯ Time
- ◯ Cost of cybersecurity
- ◯ Other: _____

5. **How informed do you feel about Cybersecurity?**
   Mark only one oval.

	1	2	3	4	5	
Uniformed	◯	◯	◯	◯	◯	Informed

6. **What steps do you take, if any, to guard against cybersecurity attacks.** *
Check all that apply.

- [ ] User Passords
- [ ] Administrative Passwords
- [ ] Protocol for responding to phone calls
- [ ] Protocol for responding to emails
- [ ] Using a USB to keep information
- [ ] Computers in a locked room
- [ ] Back Up information
- [ ] Other: _____

7. **In your opinion, what will it take to increase patient information hygiene?**

_____

_____

_____

_____

_____

8. **Do you have anything else to add or suggest?** *

_____

_____

_____

Problem with Small Medical Offices

- Healthcare offices are a perfect target for ransomware cyberattacks because there is a growing demand for systems interactions, critical infrastructures and the use of cellular internet connections.
- Also, because small practices are low profile and are less likely to spend much time or practice on protection against attacks.
- This allows attackers to identify vulnerabilities and launch attacks (Abouzakhar, 2017). Attackers have been successful at attacking small practices because of low profile and low protection (healthit, 2010).
- Most offices are not aware they have been infected with ransomware until they see their computer screen demanding cyber currency.
- All information such as patients' records, financial information and anything else stored on the computer are held hostage unless the terms for release have been met.

Proposal - CyberSecurity Hygiene for Small Biz

- Use secured internet
- Use strong passwords that change often
- Multi-Factor authentication
- Maintain Anti-Virus Software
- Use an electronic health record system (EHR) and firewall
- Limit access for each individual to minimize data breaches
- Physical access of devices should be controlled

Key Findings

Small healthcare practices are a target for attacks due to their limited security protocols and small office staff.

Relying on human error, attackers can permeate a system before anyone detects the attack, resulting in exposure of data, data held for ransom and loss of data.

By taking steps to safeguard the practice, data and personnel, the healthcare professionals can minimize the attacks.


Use Strong Passwords:
•Different Passwords for Different Sites
•Change Regularly
•Never Share via Email or Documents
Cyber Security
is in Your Hands
*Install Blocking
Software
*Install Updates
*No Clicking Unknown
Emails
*Turn on Firewalls
*Split Network into
Workstations
Backup Regularly:
3-2-1
-3 Copies
-2 Different Types
-1 Stored Offsite
Adobe Spark

The Design of Secure Wearables

Karina Bhattacharya
Industrial Design Student, The University of Houston

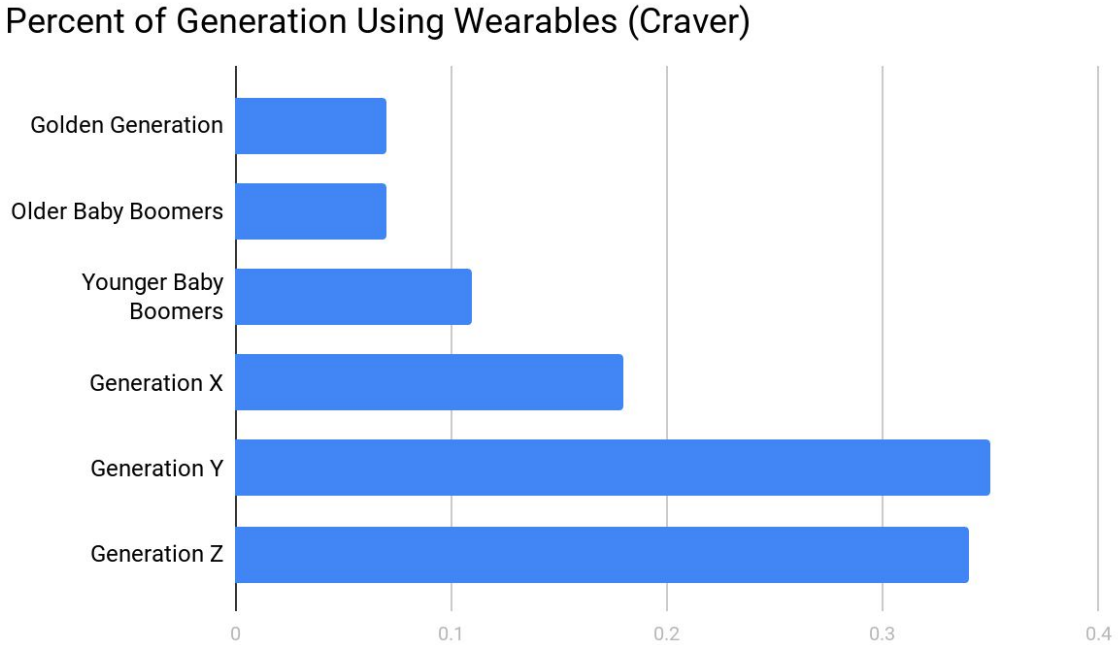
Medical Wearables

Rising Market

- Wearable medical devices:
  - Health and fitness
  - Remote patient monitoring
  - Home healthcare
- Market Value
  - 2017: 6.22 billion USD
  - 2022: 14.41 billion USD
- Shipments
  - 13,460 in 2018
  - 97,620 in 2022

L. Rosenbaum. (2016, March 1). Should You Really Take 10,000 Steps a Day? Retrieved from https://blog.fitbit.com/should-you-really-take-10000-steps-a-day/

Usage Patterns



Usage Solutions

- Cryptographically secure
- Authenticating updates
- Programmed microcontroller
- Eliminate extra interfaces

Craver, J. (2015, October 7). Young people way ahead of use in wearables. Benefits Selling. Breaking News. Retrieved from https://search-proquest-com.ezproxy.lib.uh.edu/docview/1719467329?accountid=7107&rfr_id=info%3Axri%2Fsid%3Aprimo

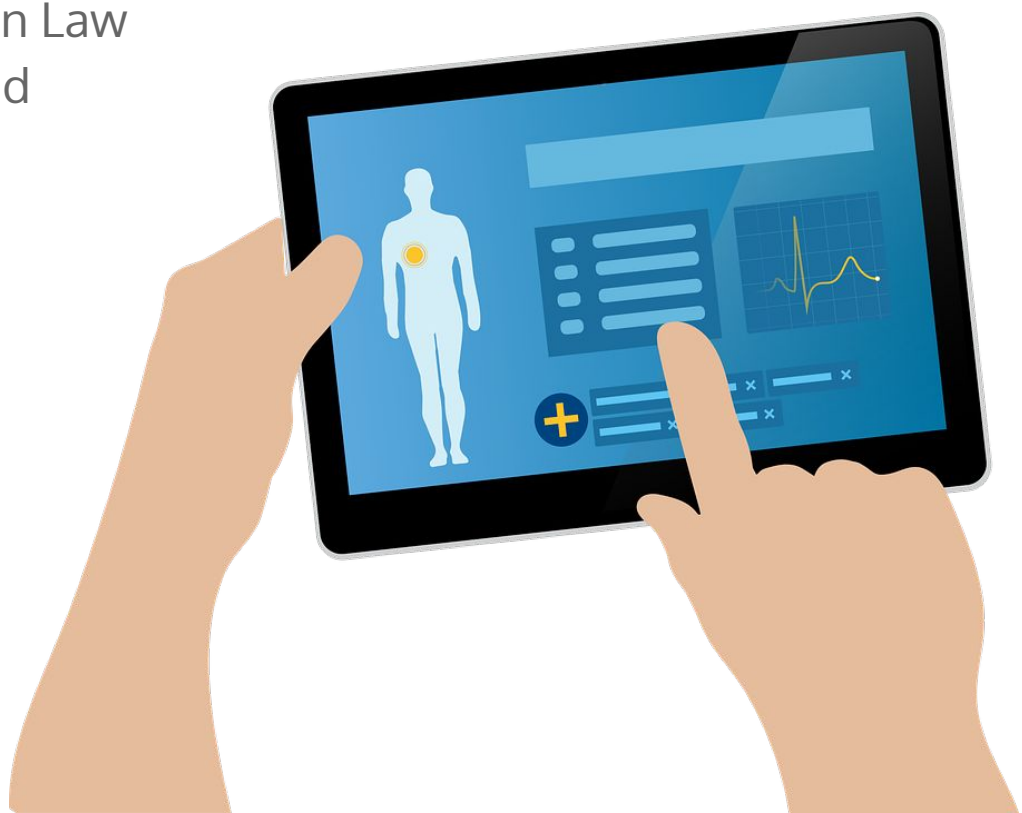
Wireless Sensor Networks

- “Biocitizen” (Swan 2012)
- Confidentiality, Integrity, Authenticity
- Privacy
- Denial of Service attacks
- False Data Injection

Fitbit Charge HR. Retrieved from https://www.fitbit.com/chargehr?

Policy

- Texas Data Breach Notification Law
- Health Information Privacy and Portability Act
- GDP Privacy Legislation



From the Consumer

- Losing the wearable
- Consumers' Valued Features
  - 24-hour battery
  - Physical Comfort
- Fitness wearables: Low Risk purchase
- Medical devices: High Risk purchase

References

Rohan. (2018, January 23). Wearable Medical Devices Market Worth 14.41 Billion USD by 2022. MarketsandMarkets. Retrieved from https://www.prnewswire.com/news-releases/wearable-medical-devices-market-worth-1441-billion-usd-by-2022-670703613.html

Projected healthcare wearable device shipments worldwide from 2015 to 2021 (in 1,000 units). (2018). [Graph illustration on health wearable shipments worldwide as of September 2016]. *Statista*. Retrieved from https://www.statista.com/statistics/607932/projection-of-the-healthcare-wearable-device-shipments-worldwide/

Jones, J. & Gouge, C. (2017). Design Principles for Health Wearables. *Communication Design Quarterly, 5*. Retrieved from http://delivery.acm.org.ezproxy.lib.uh.edu/10.1145/3140000/3131205/p40-jones.pdf?ip=129.7.158.43&id=3131205&acc=ACTIVE%20SERVICE&key=B63ACEF81C6334F5%2E4E5EDBE671A33DAE%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&__acm__=1530842875_f8ab5cc1801cbf36b583b5f13f7232d0

Ho, K. & Yao, C. (2017, December). Health apps, wearables, and sensors: The advancing frontier of digital health. *British Columbia Medical Journal, 59*(10). Retrieved from http://web.a.ebscohost.com.ezproxy.lib.uh.edu/ehost/pdfviewer/pdfviewer?vid=1&sid=aaad58df-d9dd-419a-a83b-5fa92535a736%40sessionmgr4010 Arias, O. & Wurm, J. (2015, April-June). Privacy and Security in Internet of Things and Wearable Devices. *IEEE Transactions on Multi-Scale Computing Systems, 1*(2). Retrieved from https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7321811&tag=1

Rantakari, J. & Ignet, V. (2016, February). Charting Design Preferences on Wellness Wearables. *Proceedings of the 7th Augmented Human International Conference 2016, Article 28*. Retreived from https://dl-acm-org.ezproxy.lib.uh.edu/citation.cfm?doid=2875194.2875231

Tuma, S. (2013, January 11). Texas' Amended Data Breach Notification Law is Expansive. BrittonTuma. Retrieved from https://www.jdsupra.com/legalnews/texas-amended-data-breach-notification-33265/

Craver, J. (2015, October 7). Young people way ahead of use in wearables. Benefits Selling. Breaking News. Retrieved from https://search-proquest-com.ezproxy.lib.uh.edu/docview/1719467329?accountid=7107&rfr_id=info%3Axri%2Fsid%3Aprimo

Sabbah, E. & Kang, K. (2008). An application-driven approach to designing secure wireless sensor networks. Wireless Communications and Mobile Computing. 8. Retrieved from https://onlinelibrary.wiley.com/doi/epdf/10.1002/wcm.583

UNIVERSITY of HAWAI'I®
MAUI COLLEGE

Questions? Comments? Feedback?!

Debasis Bhattacharya
debasisb@hawaii.edu
Lorraine Lopez-Osako
cl41@hawaii.edu
Karina Bhattacharya
klbhattacharya@uh.edu
maui.hawaii.edu/cybersecurity