SecTech

Introduction to SecTech

SecTech workshop at WISE11

Qiang Tang
qiang.tang@list.lu

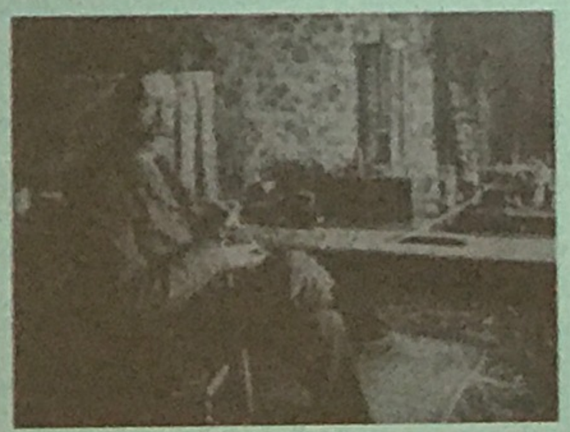
Cyber attack is not new

SecTech

Dot-dash-diss: The gentleman hacker's 1903 lulz

A century ago, one of the world's first hackers used Morse code insults to disrupt a public demo of Marconi's wireless telegraph

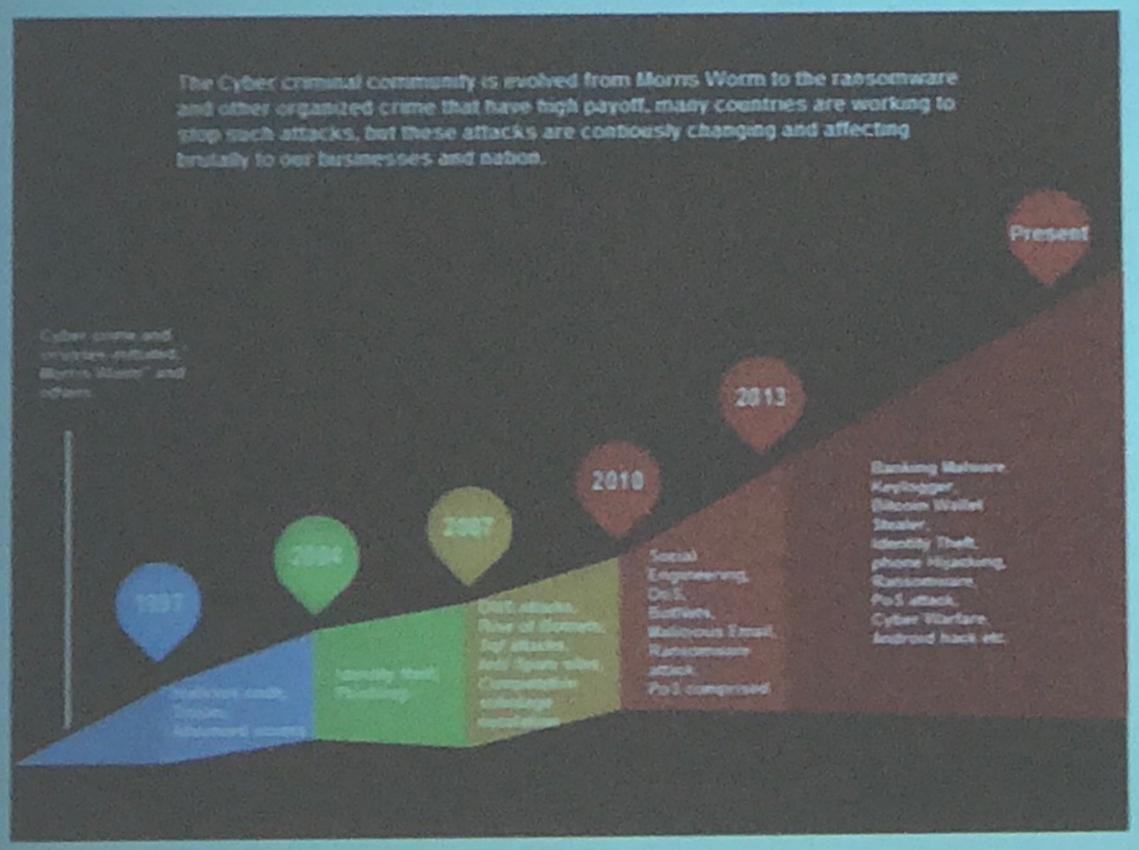
By **Paul Marks**



LATE one June afternoon in 1903 a hush fell across an expectant audience in the Royal Institution's celebrated lecture theatre in London. Before the crowd, the physicist John Ambrose Fleming was adjusting arcane apparatus as he prepared to demonstrate an emerging technological wonder: a long-range wireless communication system developed by his boss, the Italian radio pioneer Guglielmo Marconi. The aim was to showcase publicly for the first time that Morse code messages could be sent wirelessly over long distances. Around 300 miles away, Marconi was preparing to send a signal to London from a clifftop station in Poldhu, Cornwall, UK.

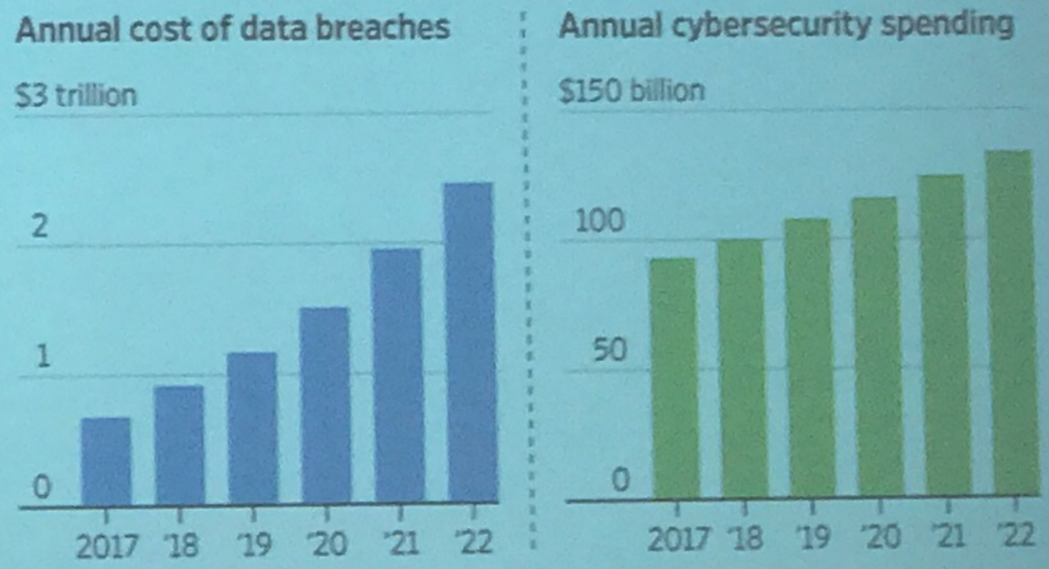
Cybersecurity is m&m important

SecTech



Growing Threat

Estimated increases in data-breach costs and global cybersecurity spending over the next five years



Source: Juniper Research

THE WALL STREET JOURNAL.

Source: https://resources.infosecinstitute.com/evolution-in-the-world-of-cyber-crime/#gref

Cybersecurity has a multi-faceted/disciplinary nature

SecTech

Cybersecurity is a multi-faceted and multidisciplinary computing-based discipline involving technology, people, information, and processes to enable assured and trustworthy operations. It involves the creation, operation, analysis, testing, monitoring, and improvements of secure computer systems.

Cybersecurity includes aspects of policy, law, ethics, risk management, and human factors. Legal, regulatory, and policy frameworks need to address security while protecting public safety, ensuring confidentiality and privacy of information, and enabling innovation.

Cybersecurity is an inherently Multi-disciplinary endeavor requiring policy leaders, computing professionals, researchers, mathematicians, engineers, social scientists, ethicists and psychologists to achieve its objectives.

Source: https://www.acm.org/binaries/content/assets/public-policy/2016_euacm_cybersecurity_white_paper.pdf

Ctd, particularly cybersecurity education

SecTech

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Core Modules

Security Management
Introduction to Cryptography and Security Mechanisms
Network Security
Computer Security (Operating Systems)
Security Technologies
Secure Business Architectures

Optional Modules

Legal and Regulatory Aspects of Information Security
Cyber Crime
Smart Cards, RFIDs and Embedded Systems Security
Software Security
Digital Forensics
Security Testing
Cyber Security
Human Aspects of Security and Privacy

uni.lu
UNIVERSITÉ DU LUXEMBOURG

Core Modules

Algorithms for Numbers and Public-Key Cryptography
Principles of Security Engineering
Symmetric Key Cryptography and Security of Communications
Cryptocurrencies and the Cryptographic Blockchain
Security Modelling
Security Protocols
Fault and Intrusion Tolerance
Management of Information Security
Open Network Security

Not too late to start

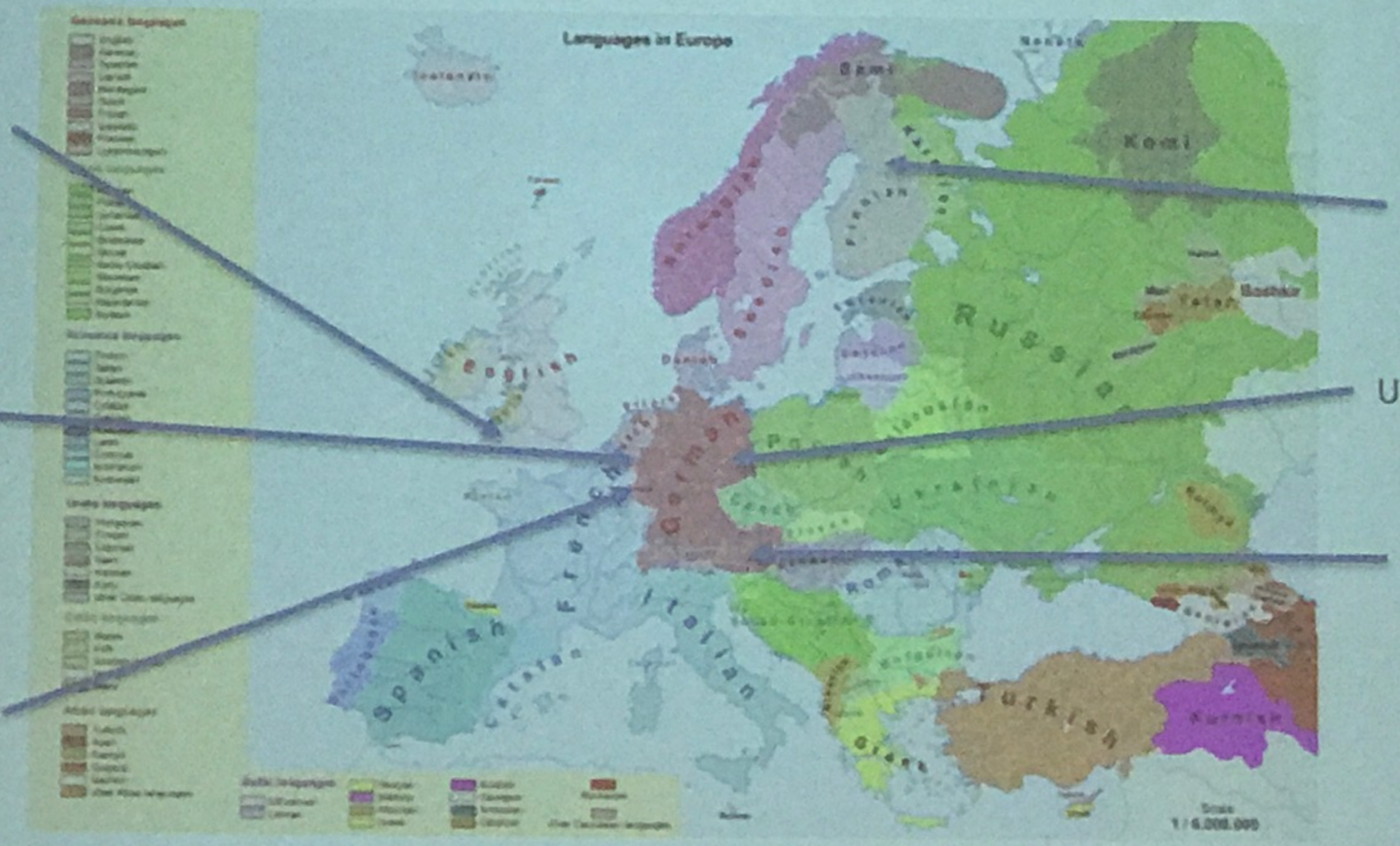
SecTech

- Digital Single Market Strategy (2015)
  - A single cybersecurity market strategy
- EU-wide cybersecurity legislation (2016)
- ……
- Increasing funding opportunities for cybersecurity (450M for 2017-2020)
- Do not forget the enormous national efforts from member states

Erasmus+ SecTech (2017-2018)

SecTech

Innovation and Excellence in Cyber-security teaching in Higher Education



University of Plymouth

University of Oulu

KU Leuven

University of Regensburg

University of Vienna

Luxembourg Institute of Science and Technology

CSEC2017:
Cybersecurity Curricular Guidelines

Presented by:

Matt Bishop
Dept. of Computer Science
University of California at Davis
1 Shields Ave.
Davis, CA 95616-8562 USA

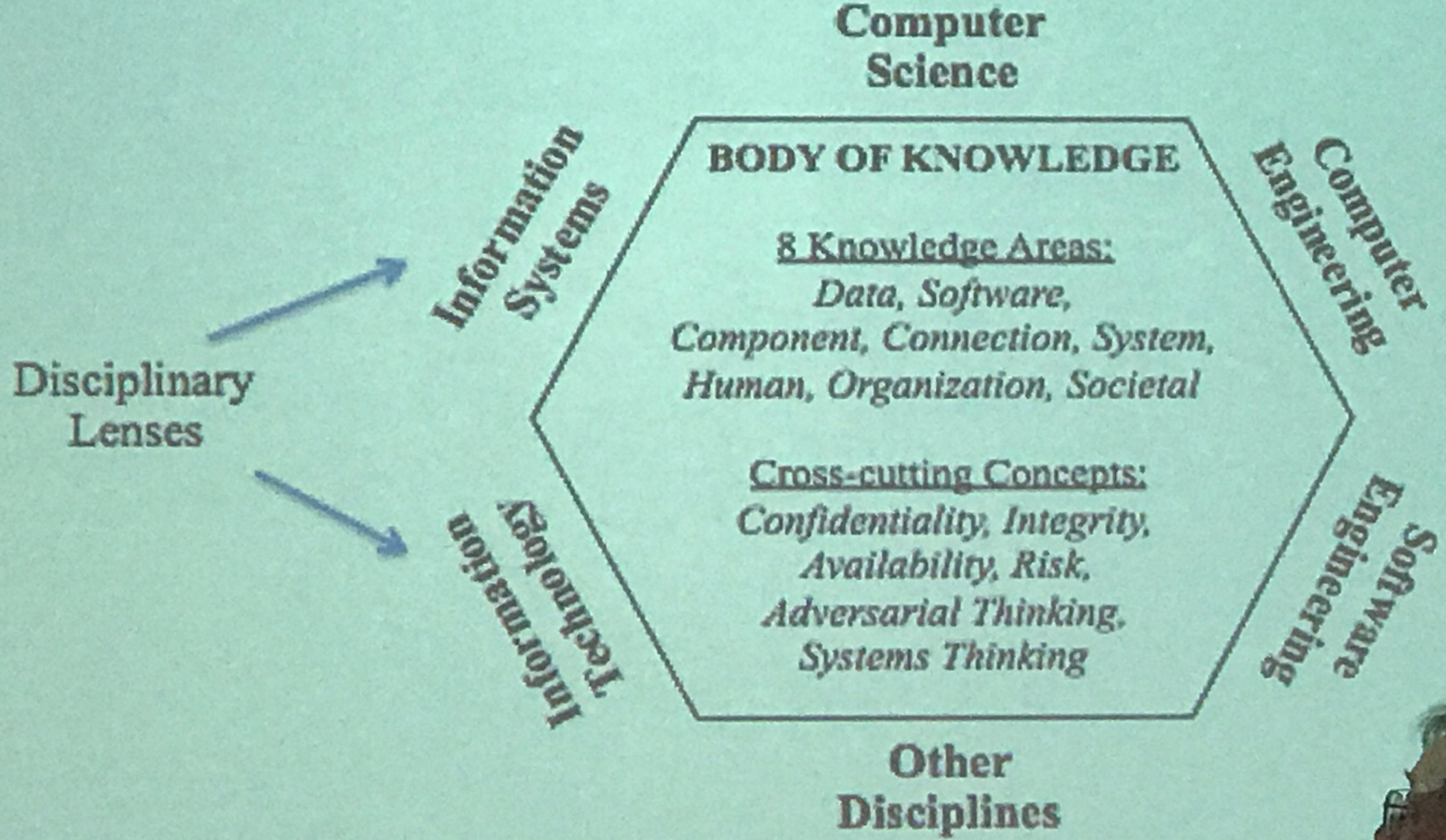
email: mabishop@ucdavis.edu
www: http://seclab.cs.ucdavis.edu/~bishop
phone: +1 (530) 752-8060

Bases for Guidelines

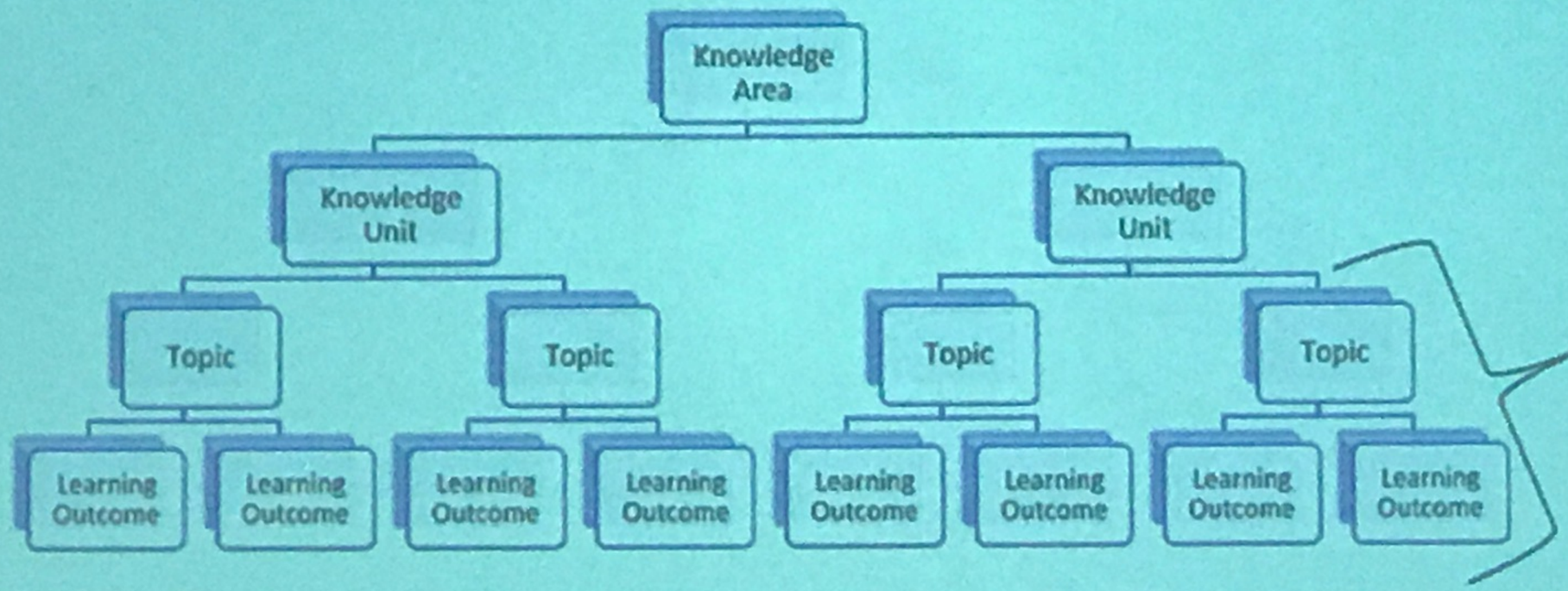
Cybersecurity education programs should:

- Be based on core knowledge and skills;
- Have a computing-based foundation
- Teach concepts applicable to a broad range of cybersecurity expertise;
- Emphasize ethical obligations and responsibilities; and
- Be flexible so programs can tailor their curriculum to any specialized needs

CSEC 2017 Thought Model



Knowledge Area Organization



Knowledge Area Descriptions

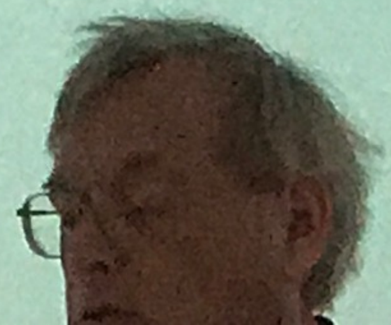
- **Component Security:** focuses on the design, procurement, testing, analysis and maintenance of components integrated into larger systems.

- **Connection Security:** focuses on the security of the connections between components including both physical and logical connections

Earth as they underlie everything

Knowledge Area Essentials

- The essential concepts of each knowledge area capture the cybersecurity proficiency that every student needs to achieve regardless of program focus.
- Essentials should be introduced early and reinforced throughout every cybersecurity program.
- These concepts may also appear as specific knowledge units, as topics within knowledge units, or as aggregates of topics across knowledge units. Taken together, the essential concepts in all of the knowledge areas should be covered in every cybersecurity program.
- In the curricular volume, the essential concepts are explicitly identified for each knowledge area along with learning outcomes.



SecTech Curriculum Example

ybersecurity Education: Initial Analysis

SecTec

- A fragmentation of cybersecurity education among institutions in a national and international context
- Resource shortage preventing the establishment of complete implementations of cybersecurity curricula
- Few clear practical concepts for cybersecurity (educational) resource development
  - Workforce development in both professional and research capacity
- Too few institutions providing a full cybersecurity degree program today
  - Often only an add-on to existing degree programs

uilding the Environment

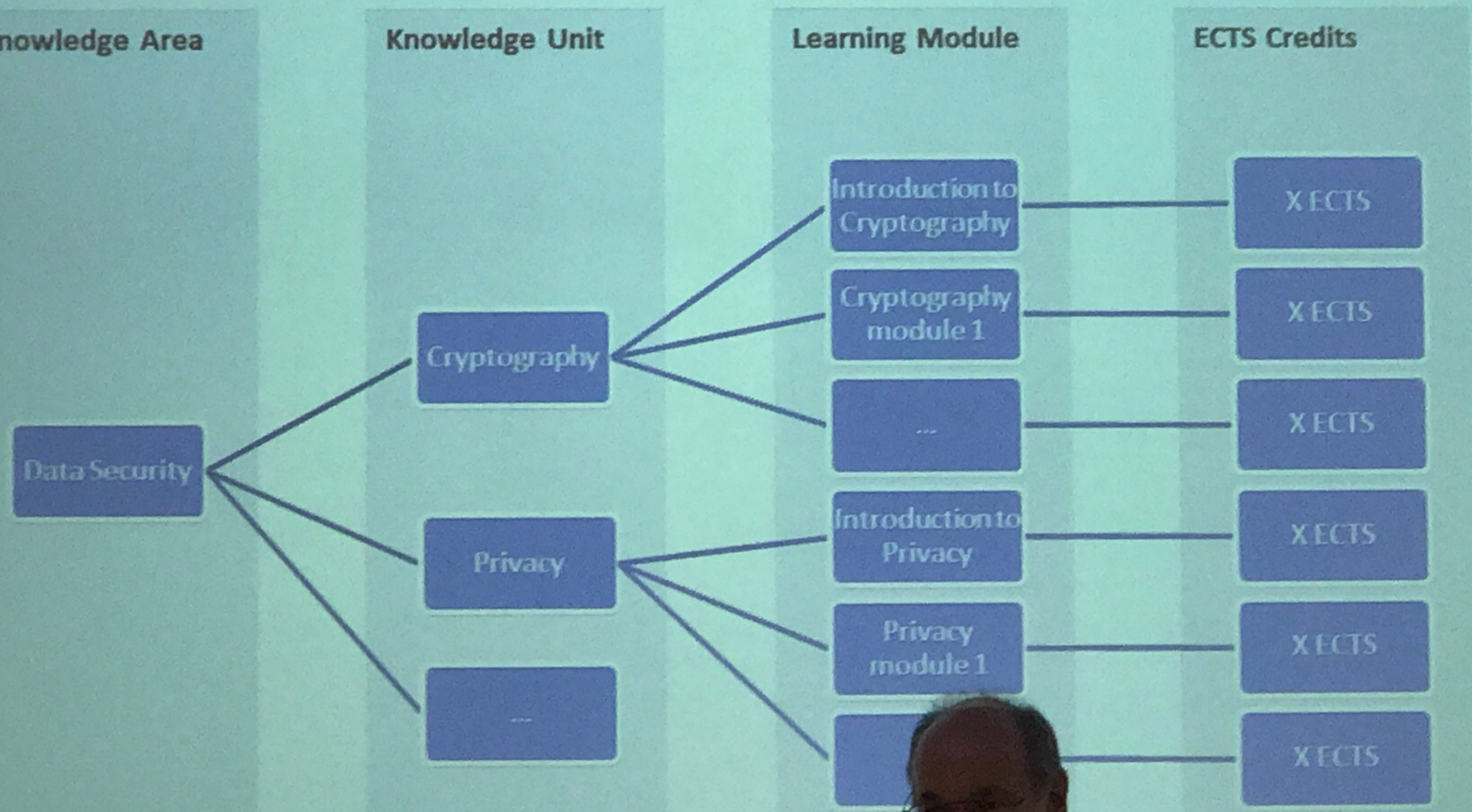
SecTe

- Building a community
  - Attracting contributors to develop, maintain and deliver content
- Implementation
  - Creating an environment that allows collaborative content development and delivery
- Sustainability
  - Keeping contributors interested in the mid- and lo term

The SecTech Curriculum Example

Basic Structure (~ where we can best relate to CSEC2017)

SecTec



SecTech

Mapping the Example to the CSEC2017 Model

SecTech workshop at WISE11

Teemu Tokola and Ludwig Englbrecht

Mapping the Example to CSEC2017

SecTech

- The CSEC2017 defines eight *knowledge areas*
  - Data Security
  - Software Security
  - Component Security
  - Connection Security
  - System Security
  - Human Security
  - Organizational Security
  - Societal Security

- These areas have been adopted for the SecTech curriculum

Mapping the Example to CSEC2017

SecTech

- Each *knowledge area* contains several *knowledge units*
- Depending on the institutional lens and disciplinary lens the topic and learning outcome of a *knowledge unit* are defined

- For the SecTech curriculum example we defined these as follows
  - Institutional lens: **(mixed) decentralized cybersecurity curriculum**
  - Disciplinary lens: **multi-disciplinary lens**

Mapping the Example to CSEC2017

SecTech

- The existing competencies of the project partners were used as a starting point for defining the *knowledge units* of the SecTech curriculum
  - These have been identified through intensive research

- In addition, new learning content was created to compensate any gaps as effectively as possible

SecTech

The SecTech Online Toolset

SecTech workshop at WISE11

Thomas Schaberreiter

The Current Education Environment

- Traditional classroom education
  - Students are physically present in a classroom
  - A teacher deliveres the content
  - Fixed and inflexible course schedules

- Advantages over pure online education
  - Proven Concept
  - Development of social skills
  - Communication and team building
  - Direct interaction between teacher and learner

Blended Approach

SecTech

- Combine advantages of traditional education and online education
  - Educational institutions can not ignore the developments
  - Do not replace, but supplement current degree program/ course frameworks and procedures

- Requirements for a distributed curriculum
  - Distributed development and management of teaching material
  - Course management and administration
  - Possibility of remote lecturing
  - Improved communication channels
    - Contributors and teachers, students

Virtual Learning Environments

SecTech

- Content characteristics
  - Static vs. interactive content
  - Embed interactive elements, e.g. quizzes, directly in content
  - Track learning progress (completeness, times, scores, …)

- Interoperability
  - Integrate content with management and administration tools
  - Allow collection and analysis of interactive elements
  - Allow content to work with different environments

- Relevant standards
  - SCORM (Sharable content object reference model)/ ExperienceAPI
    - Advanced Distributed Learning Initiative (ADL)
  - LTI (Learning Tool Interoperability)
    - IMS Global Learning Consortium

The SecTech Toolset

- A virtual learning environment
  - Content creation and management
    - Xerte online toolkit (https://xerte.org.uk/)
    - iSpring free PowerPoint plugin (https://www.ispringsolutions.com/ispring-free)
  - Learning management system (LMS)
    - Moodle (https://moodle.org/)
  - Virtual classroom
    - BigBlueButton (https://bigbluebutton.org/)
- Selection Criteria
  - Preferably free and open source
  - Integration between tools (e.g. shared account management)
  - Preferably server side deployment to avoid local installs

The SecTech Toolset

SecTech

- A virtual learning environment
  - Content creation and management
    - Xerte online toolkit (https://xerte.org.uk/)
    - iSpring free PowerPoint plugin (https://www.ispringsolutions.com/ispring-free)
  - Learning management system (LMS)
    - Moodle (https://moodle.org/)
  - Virtual classroom
    - BigBlueButton (https://bigbluebutton.org/)
- Selection Criteria
  - Preferably free and open source
  - Integration between tools (e.g. shared account management)
  - Preferably server side deployment to avoid local installs