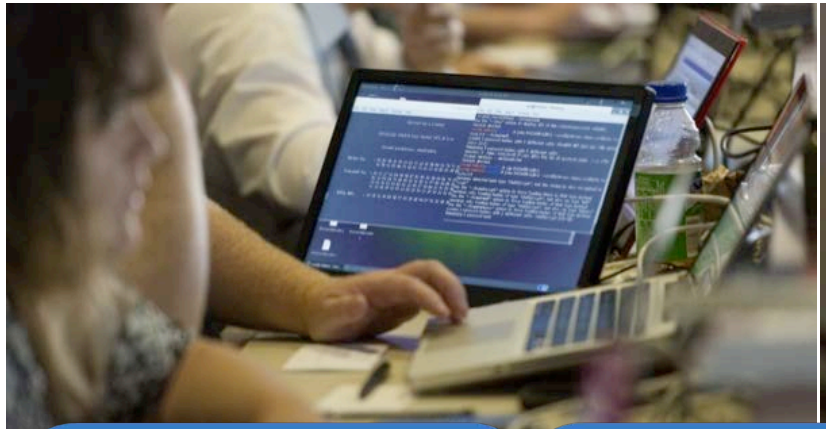
University of Delaware Cybersecurity Initiative

Dr. Starnes Walker
Founding Director

October 24, 2017

UNIVERSITY OF DELAWARE

Cybersecurity Initiative



Educational Programs

- Certificate Program
- Minor Degree
- Masters Degree
- 4+1 Program
- 2+2 Program

Partnerships

- Industry Corporate
- Government
- Academia

Research

- Fundamental Research
  - Network, Computer & Systems Security
  - Information Assurance
  - Cyber Defense and Offense
  - Behavioral Analysis
- Classified Research

Outreach

- Student Internships
- Summer K-12 Camps
- Bridge Programs
- Workshops & Seminars
- Business Cooperative Extension

Digital Innovation

Regulatory Compliance

Increased Security Risk

Legacy Systems

Operations
Profit

Latest
Technology

Business Vs. Cybersecurity

MULTIPLE CYBER THREAT ACTORS

Impact to Assets:
Hardware,
Software,
Data

Nation States I

Nation States II

Nation States III

Cyber Espionage

Cyberterrorists

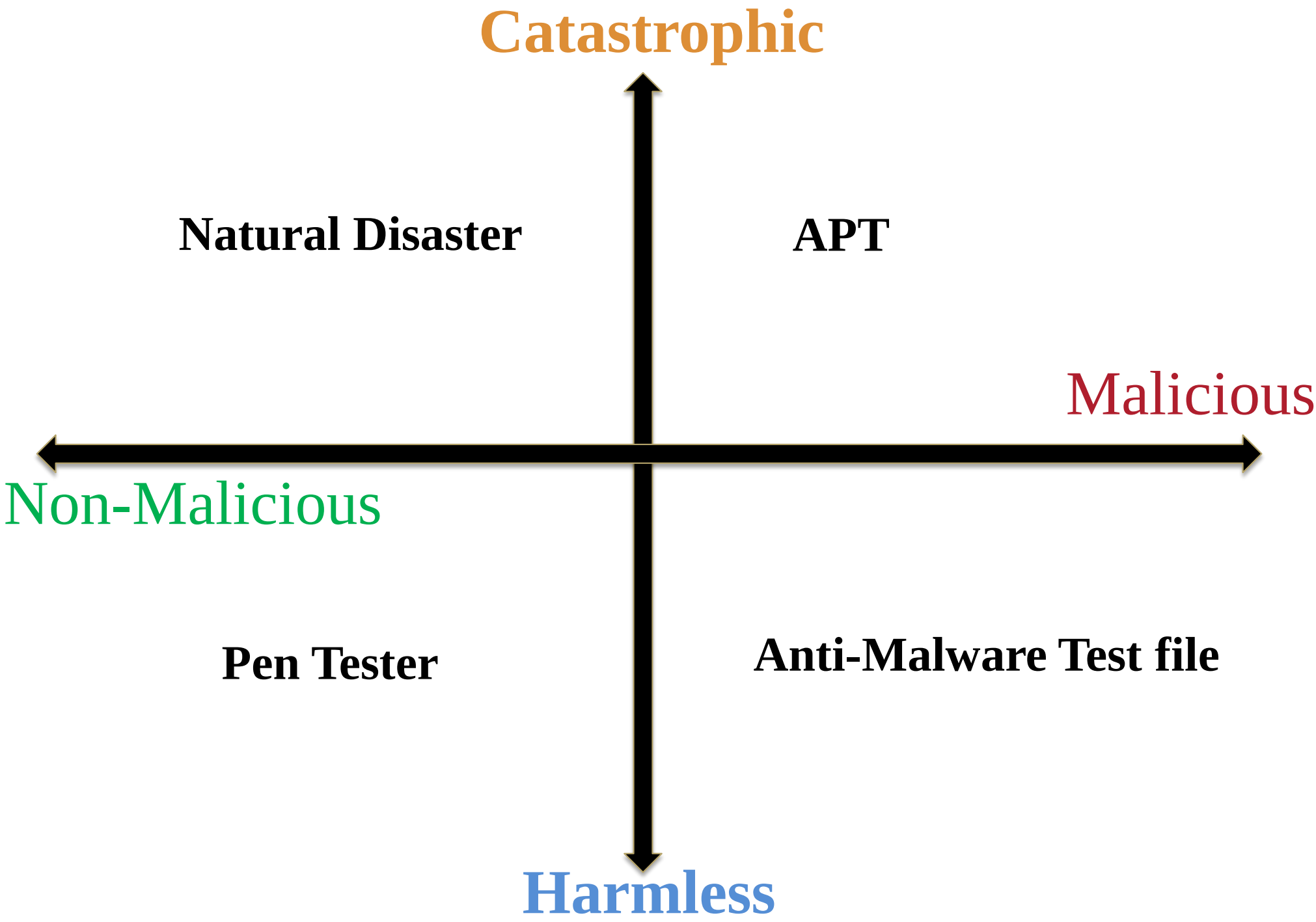
Hacktivists

Cyber Criminals

Lone Hackers

Terrorists

Resources

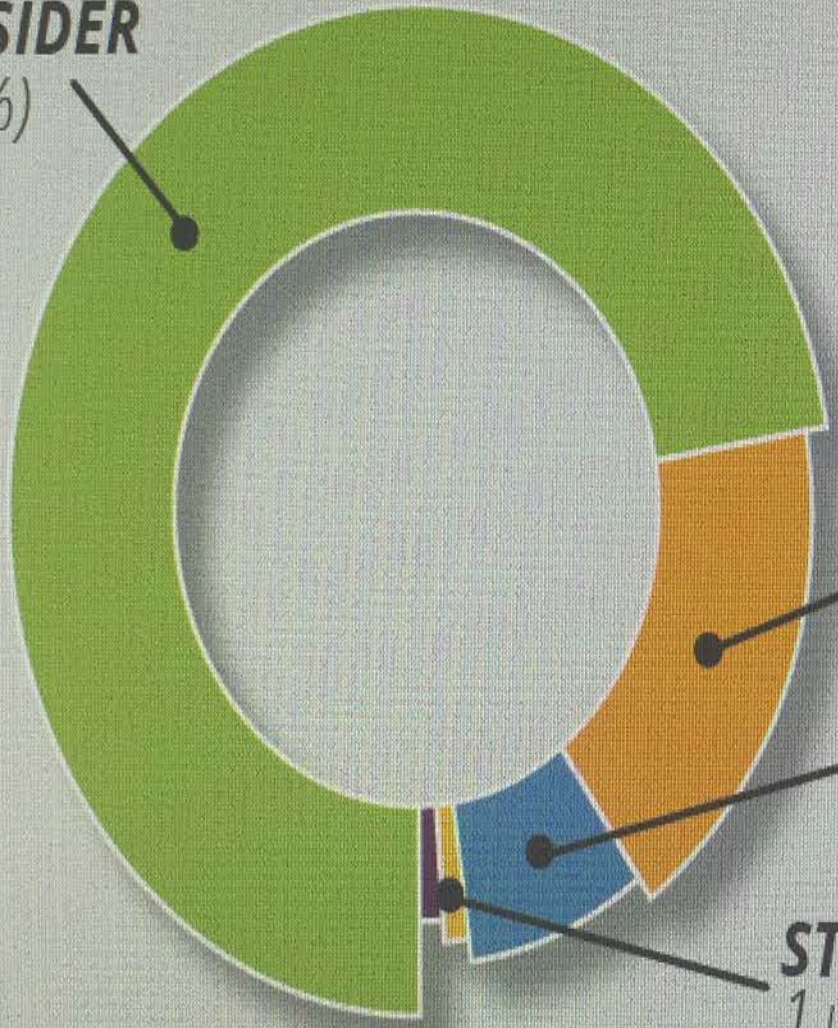

Catastrophic
Natural Disaster
APT
Malicious
Non-Malicious
Pen Tester
Anti-Malware Test file
Harmless

9B Records lost since 2013

Less than 1% was encrypted

Source: Gemalto

NUMBER OF BREACH INCIDENTS BY SOURCE FIRST HALF OF 2017



MALICIOUS OUTSIDER
679 INCIDENTS (74%)

ACCIDENTAL LOSS
166 INCIDENTS (18%)

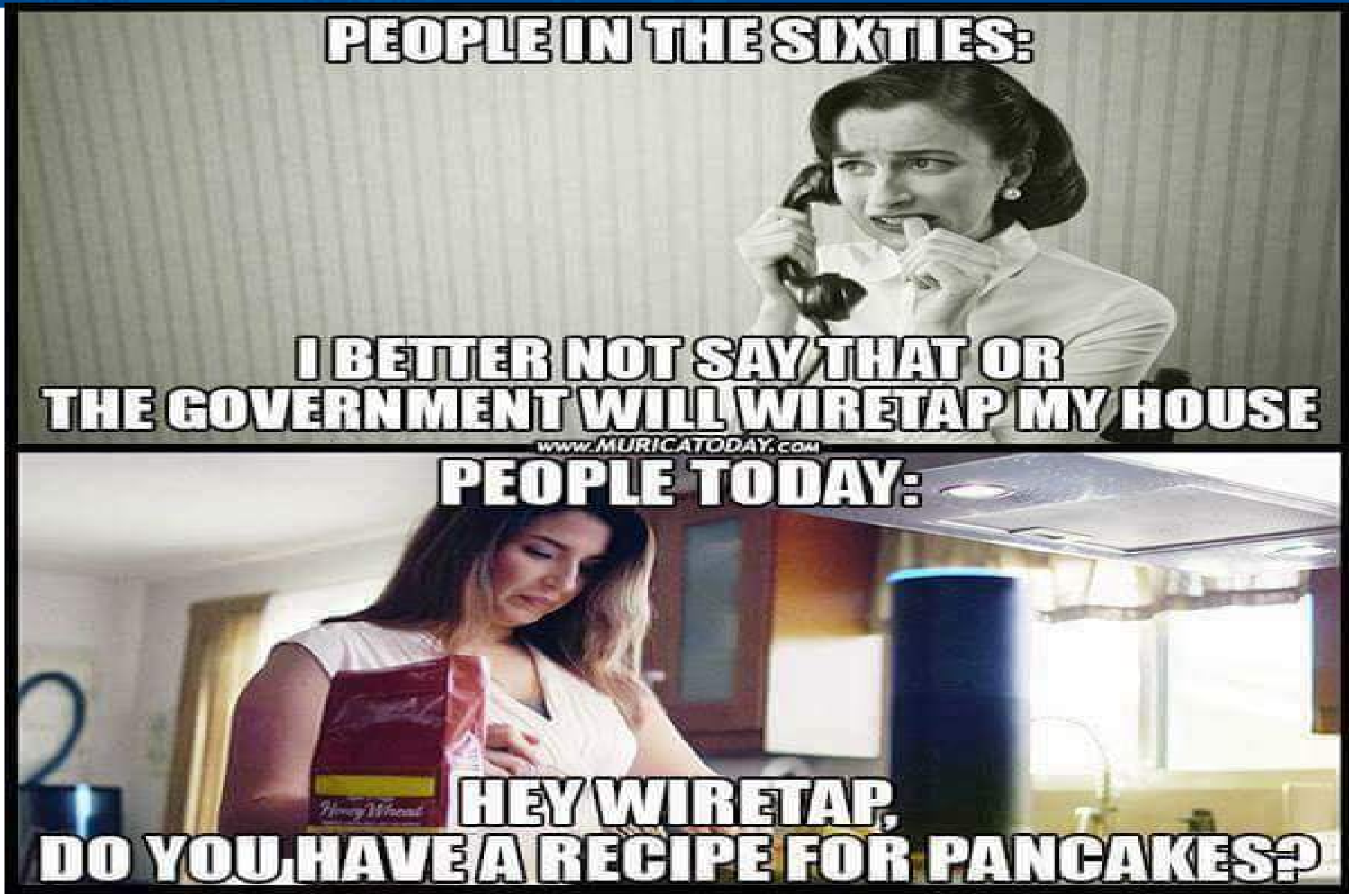
MALICIOUS INSIDER
71 INCIDENTS (8%)

STATE SPONSORED
1 INCIDENT (<1%)

918
TOTAL BREACHES
1 UNKNOWN INCIDENT

Source: BREACHLEVELINDEX.COM
January 2017 to June 2017

While many organizations are focused on detecting and stopping outside threats, the internal threats — malicious insiders, accidental loss, and other negligence — can be a forgotten risk


PEOPLE IN THE SIXTIES:
I BETTER NOT SAY THAT OR THE GOVERNMENT WILL WIRETAP MY HOUSE
www.MURICATODAY.com
PEOPLE TODAY:
HEY WIRETAP, DO YOU HAVE A RECIPE FOR PANCAKES?

Some reasons cybersecurity will remain a concern

- Widespread use of new platforms (IOT)
- Cyber threats are increasing
- Increasingly available/simple use of exploit kits
- Increasing more sophisticated attacks with specific targets
- Increased use of bring your own device and work from home
- Mobile devices used for point of attacks
- Non-attribution towards threat actors
- The Economic Impact

ERM, Cyber Governance and Litigation/Regulatory Risk

- **Overlapping Regulation Concerns: Never before have we had some much cybersecurity guidance out there for areas of critical infrastructure; and so little security**

Why the emphasis on regulation?
Most laws are national – Internet is borderless

Regulation == rules == made to be broken or ignored intentionally or unintentionally == fines and penalties == litigation against company, directors and officers == loss of reputation == loss of trust

= company death and destruction of shareholder value!

$115 million settlement; 10X the largest previous settlement

ebay EQUIFAX THE HOME DEPOT

Center for Strategic & International Studies
World wide cost of cyber crime $445B

TARGET

SONY

ارامكو السعودية
Saudi Aramco

BUSINESS DAY

Equifax Says Cyberattack May Have Affected 143 Million in the U.S.

By TARA SIEGEL BERNARD, TIFFANY HSU, NICOLE PERLROTH and RON LIEBER SEPT. 7, 2017

Equifax, one of the three major consumer credit reporting agencies, said on Thursday that hackers had gained access to company data that potentially compromised sensitive information for 143 million American consumers, including Social Security numbers and driver's license numbers.

The attack on the company represents one of the largest risks to personally

Chinese compiling 'Facebook' of U.S. government employees

Microsoft finds new computers in China preinstalled with malware-- Malware embedded inside counterfeit versions of Windows on brand-new laptop and desktop computers is engineered to conduct DoS attacks via the Nitol botnet

THE WALL STREET JOURNAL.

Russia Has Turned Kaspersky Software Into Tool for Spying

Searches exploited popular Russian-made antivirus software to seek classified material, officials say

Why the Focus on Cybersecurity Governance and the Board of Directors?

What should banks learn from the cyberINsecurity we face today?

1. Boards are busy; but are you talking about your cyber posture?
2. Board meetings are not perfect; too much on the agenda always; but are you talking about your cyber risk assessment
3. **Cybersecurity is not an IT issue; its everyone's issue** – especially the board and the CEO of a public company (Target, Equifax, Anthem, etc.).
4. Even the biggest companies have had issues you wouldn't have suspected, but are you ignoring IT and Data security?
5. Cyber is like an iceberg; we only know what we can see (and that is not a lot)

How often are you talking about cybersecurity?

Know yourself as a company = audits, ethical hackers

Financial Risk
Market Risk
Liquidity Risk
Credit Risk
Technology =
Cybersecurity Risk

Enterprise Risk For CEOs and Boards

Cyberspace = Public & Private Networks
= Internet =

NIST Cybersecurity Framework provides a common lexicon

- **The NIST Cybersecurity Framework:**
- **Applies on a "guidance" basis to all 18 areas of critical infrastructure**; *applies to federal government and contractors doing business with the government on a mandatory basis:*
- Provides for **common language** that all stakeholders can understand, from the board room to the server room, to the Security Operations Center;
- **Provides a step by step approach to allow a company to understand, and improve, its cybersecurity posture**; already adopted by over 30% of US businesses.

What can your company do to be more cyber safe?

Take Holistic View

IT Assessment of the Network / Determine your vulnerabilities

- Pen testing / Supply Chain ?
- Risk Assessment / third party assessments
- Information Assessment – Encrypt certain Personal Information

Take Action to fix the weakness in your system

Human Factors: How do we train & protect our workforce

- Move certain data into archived databases with strict control

Business Continuity Plan – communication / crisis mgt plan

Continually Evaluate systems / Get Informed

Ensure Legal and Regulatory Compliance, REPEAT

What can companies do? You may need outside help:

CIS Controls and CIS Benchmarks are global industry best practices endorsed by leading IT security vendors and governing bodies

CSC 1: Inventory of Authorized and Unauthorized Devices 6
CSC 2: Inventory of Authorized and Unauthorized Software 10
CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers 13
CSC 4: Continuous Vulnerability Assessment and Remediation 17
CSC 5: Controlled Use of Administrative Privileges 21
CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs 24
CSC 7: Email and Web Browser Protections 27
CSC 8: Malware Defenses 31
CSC 9: Limitation and Control of Network Ports, Protocols, and Services 34
CSC 10: Data Recovery Capability 36
CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches 38
CSC 12: Boundary Defense 41
CSC 13: Data Protection 46
CSC 14: Controlled Access Based on the Need to Know 50
CSC 15: Wireless Access Control 53
CSC 16: Account Monitoring and Control 56
CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps 59
CSC 18: Application Software Security 63
CSC 19: Incident Response and Management 66
CSC 20: Penetration Tests and Red Team Exercises 69

https://cybersecurityventures.com/cybersecurity-500-list

What can companies do? What can you do?

Gartner Identifies the Top Security Technologies 2017

- Cloud Workload Protection Platforms
- Remote Browser
- Deception
- Endpoint Detection and Response
- Network Traffic Analysis
- Managed Detection and Response
- Microsegmenation
- Software-Defined Perimeters
- Cloud Access Security Brokers
- OSS Security Scanning /Software Composition Analysis for DefSec Ops
- Container Security

- https://www.gartner.com/newsroom/id/3744917?utm_content=bufferb67a2&utm_medium=social&utm_source=linkedin.com&utm_campaign=buffer

Three steps that every company should take to mitigate the overall cost and adverse consequences that result from a security breach:

1. Control access and authentication of users.
2. Encrypt all sensitive data at rest and in motion,
3. Securely manage and store all of your encryption keys.

Top Down Approach = Strong Leadership
Security Policies in Place = Effective Management
Data Classification & Security Scheme = Understand your business

* By implementing each of these three steps into your IT infrastructure, companies can effectively prepare for a breach, avoid falling victim to one while ensuring shareholders their data was encrypted

Remember: No “one size fits all” prescription

How safe is your home network?

Friends, Family, Colleagues can break our security even when we do the right thing?

How much information are you giving away?

Most digital pictures posted to Facebook obtain GPS coordinates
Convenience vs Privacy & Security

Do you connecting your work computer through home network (if so are you using a VPN?)

Are you connecting you work computer to public WiFi

All WiFi has security flaws but are you using a secure password?

What can companies do? What can you do?

- **Train Employees in Security Principles**
  90% of users fail to do the basics
- **Search/find best practices & apply; especially for online banking**
- **Update & patch computers / protect information**
- **Use a secure password / multi-factor authentication** Use a different one for each account, site /service
- **Develop a Business continuity management plan that includes cyber & network security – access points, transmission protection**
- **Create a mobile device action plan**
- **Back-up important data**
- **Control physical access to your computers**
- **Limit employee access to data and information / limit software**
- **Test "Secure coding / software development"** – what does the code do, what shouldn't it be doing – need to make sure what your installing
- **Encrypt all sensitive data**
- **If you need help – hire or employ free resources: DTI, Small Business Development Center: https://delawaresbdc.org/**

UNIVERSITY of DELAWARE
CYBERSECURITY INITIATIVE

What are we doing at UD?

UDCSI Distinguished Board

OUR PARTNERS

University of Delaware | Cybersecurity Initiative

Bank of America

Battelle
The Business of Innovation

Carnegie Mellon University

THE CHERTOFF GROUP

INL
Idaho National Laboratory

DSU
Delaware State University

DELAWARE TECHNICAL COMMUNITY COLLEGE

DUPONT

FireEye

GE

IBM

HARFORD COMMUNITY COLLEGE

Honeywell

KANSAS CITY NSC
National Security Campus

JPMORGAN CHASE & CO.

Morgan Stanley

NIST

Pacific Northwest
NATIONAL LABORATORY

HOSTING
TAKING YOU FURTHER

IDA

leidos

AKZ Partners

PURDUE UNIVERSITY

Raytheon

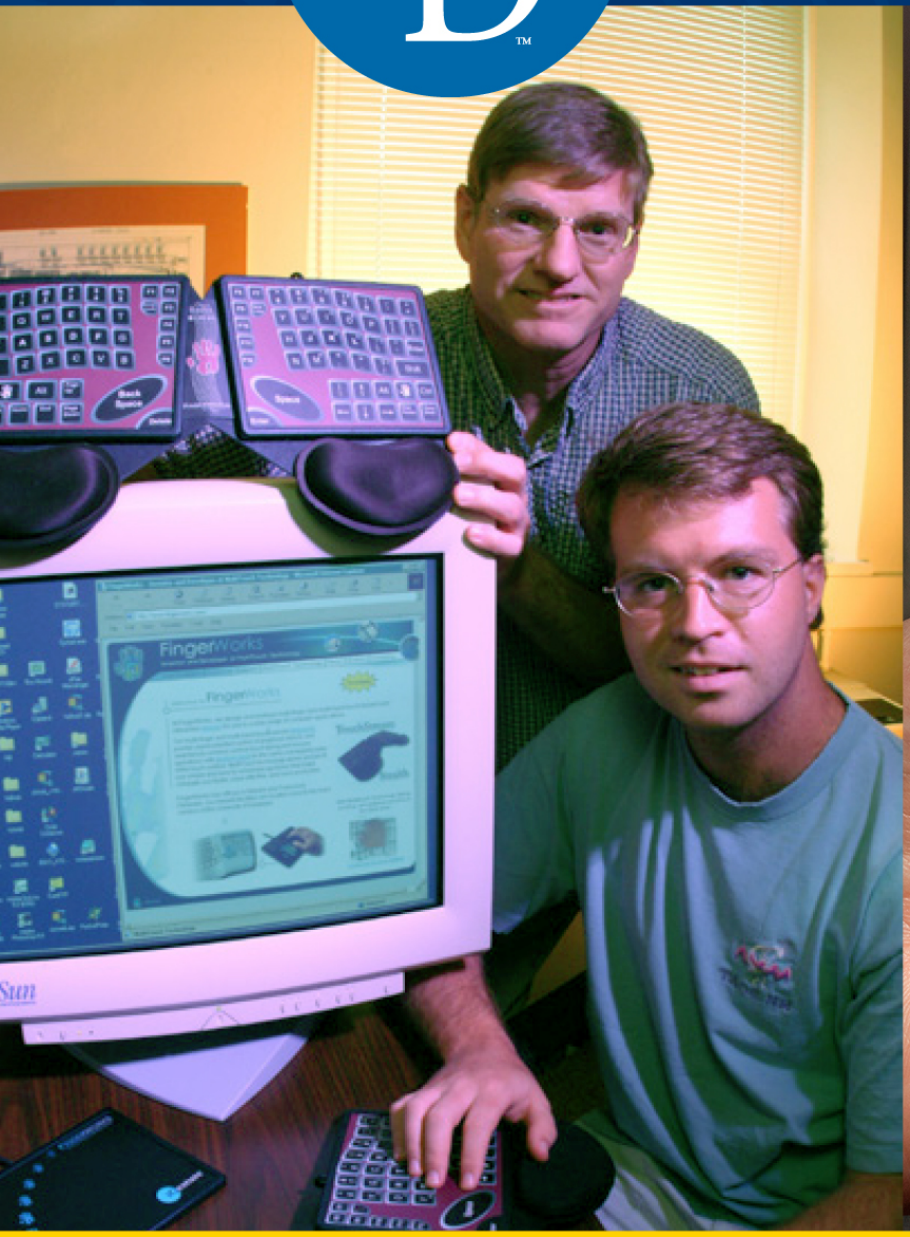
SWIFT

THE UNIVERSITY of TEXAS SYSTEM
FOURTEEN INSTITUTIONS. UNLIMITED POSSIBILITIES.

CERDEC
US ARMY – RDECOM

U.S.ARMY

RESEARCH

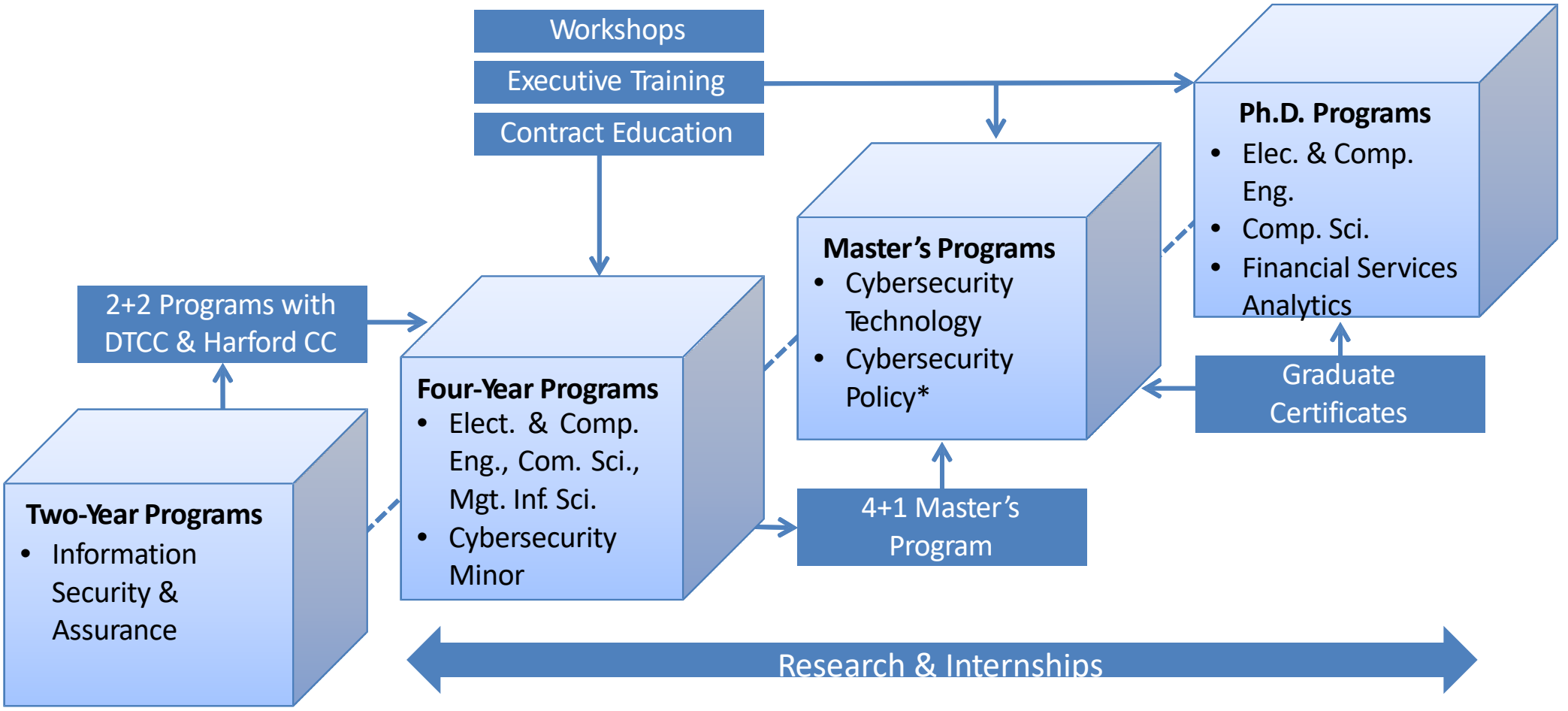

FingerWorks


Search
Mentors' Circle
University of Delaware

- **Stephan Bohacek**, ECE/CIS: networking, cloud aps performance, ad-hoc networks
- **John Cavazos**, CIS/ECE, JP Morgan Chase Faculty Fellow machine learning, software analysis and validation, malware characterization and detection
- **Haining Wang**, ECE, cloud and network security, online fraud defense / system security
- **Chase Cotton**, ECE, exfiltration, malware detection, virtualization and orchestration, forensics, high-availability
- **Robert Coulter**, Math, cryptography, trust
- **John D'Arcy**. Business, counter-measures, deterrence, compliance, insider threat
- **Fouad Kiamilev**, ECE, high speed digital systems, hardware trust, vehicle systems
- **Chien-Chung Shen**, CIS, networking, multi-level cyber simulations
- **Guang Gao**, ECE, High-performance computing (HPC) and big data systems: Security and resilience; Security and protection model/management for open systems/environments.

EDUCATION

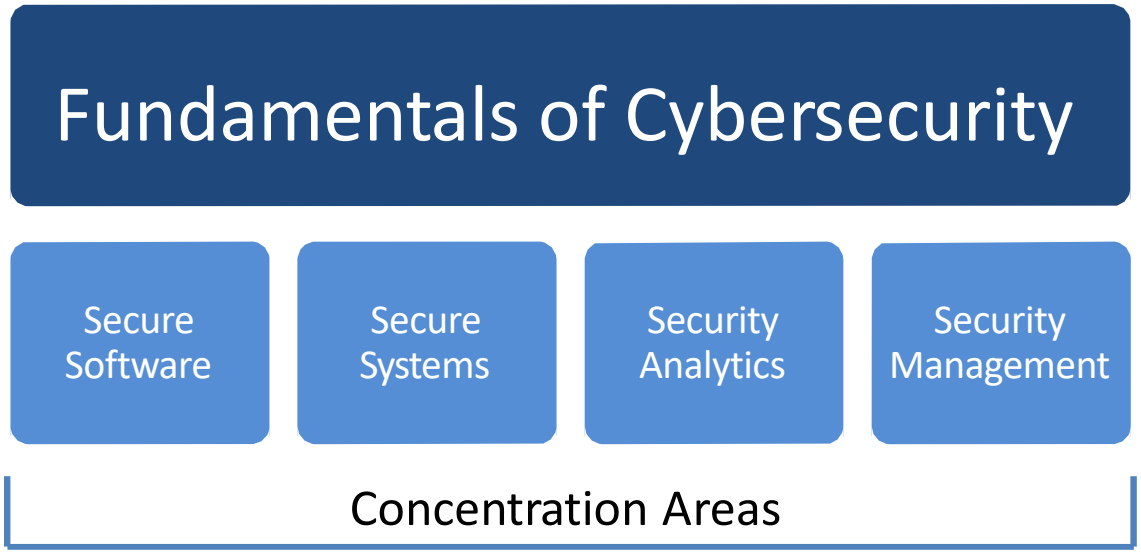
Cybersecurity Education Portfolio



Cybersecurity MS and Certificates

MS Degree Requirements: 10 courses (30 cr)

- 5 Fundamentals of Cybersecurity† courses
- 5 courses in an area of Concentration

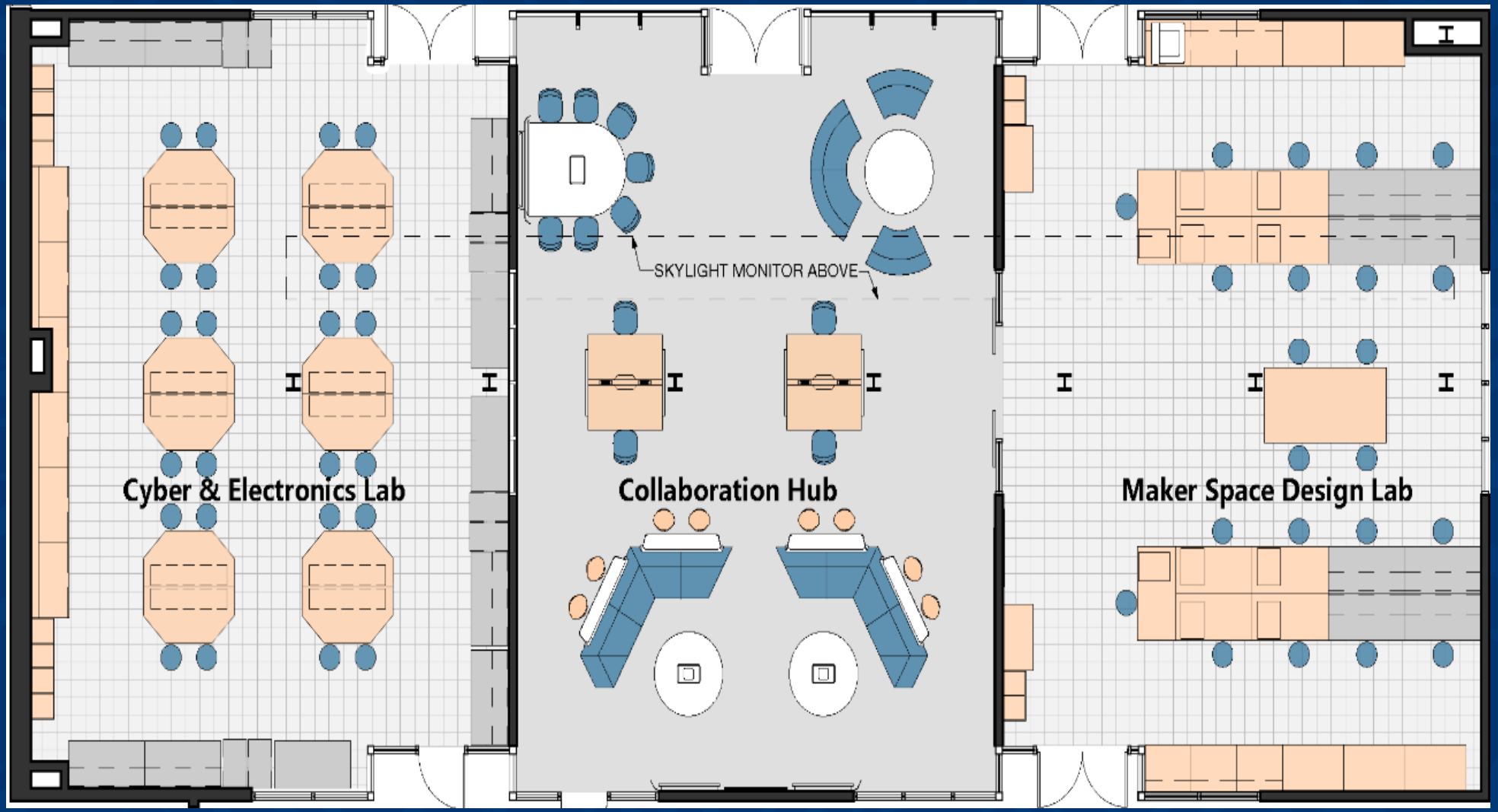


- Graduate Certificates can be earned in:
  - Fundamentals of Cybersecurity
  - Secure Software
  - Secure Systems
  - Security Analytics
  - Secure Business Systems

- Certificate Requirements: 3 courses (9 cr) in Certificate Area. Fundamentals of Cybersecurity Certificate must be earned before Concentration Area Certificates.

†Courses available online

Cyber Innovation Suite

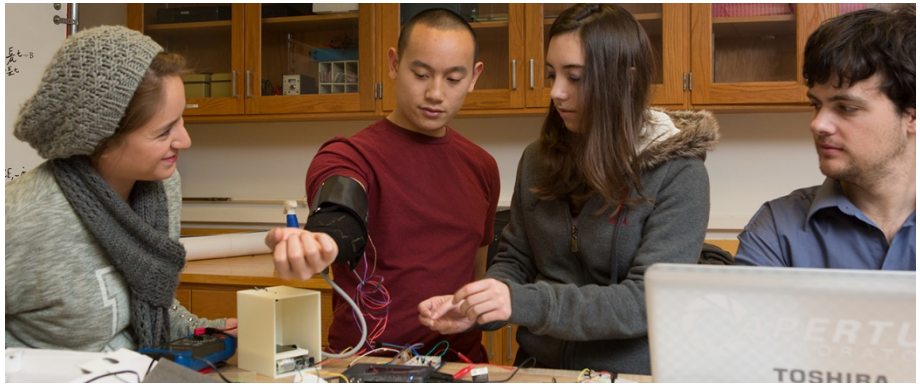


Cybersecurity Scholars Program

Just launched, the program will integrate with any major and train you to become a thought leader in cybersecurity. You will collaboratively assess the most pressing cyber-defense questions and develop both cultural and technical solutions.

Vertically Integrated Projects

- **Artgineering**
- **Cloud Crypto**
- **Drone Team**
- **E-Textiles**
- **Grid-Integrated Vehicles**
- **High Performance Computing**
- **Self-Driving Scooter**



A NEW MINDSET for data security / cybersecurity is needed if organizations are to stay ahead of the attackers and more effectively protect their data against data breaches in the future.

My briefing was intended to alert you, and all those involved in cyber threat monitoring so we can increase our vigilance towards the growing cyber threat

There is no single, easy and effective solution to cybersecurity, however, acts of aggression can be discouraged through public policies, defensive measures, hopefully a resurgence in US based computer manufacturing and cooperation from all


UNIVERSITY of
DELAWARE
CYBERSECURITY
INITIATIVE
Questions