Managing Enterprise Cybersecurity MIS 4596

Class 1

Agenda

- Instructor
- Introduction
- Course overview
- Need for Cybersecurity Professionals

Instructor

David Lanter

Director - Information Technology Auditing and Cyber Security Programs

Philadelphia, Pennsylvania · 500+ connections · Contact info

Experience

Director - Information Technology Auditing and Cyber Security (ITACS) programs
Temple University – Fox School – Management Information Systems
Aug 2016 – Present · 5 yrs 1 mo
Greater Philadelphia Area

Vice President - Information Management Systems
CDM Smith
Sep 2001 – Aug 2016 · 15 yrs

Research Director
Rand McNally
Oct 1998 – Jun 2001 · 2 yrs 9 mos

GeoModeling QA Lead / Software Design Engineer
Microsoft
Oct 1996 – Jun 1998 · 1 yr 9 mos

President
Geographic Designs Inc.
Jan 1989 – Jun 1996 · 7 yrs 6 mos

Assistant Professor
University of California, Santa Barbara
Jan 1990 – Jun 1995 · 5 yrs 6 mos

Systems Analyst
Grumman Data Systems
Mar 1986 – Aug 1987 · 1 yr 6 mos

Software Engineer
Navigation Sciences
Jun 1985 – Jan 1986 · 8 mos
Bethesda, Maryland

Education

University of South Carolina
Ph.D., Geographic Information Processing
1987 – 1989

Temple University - Fox School of Business and Management
Master's Degree, IT Auditing and Cyber Security
2013 – 2015

State University of New York at Buffalo
Master's degree, Geographic Information Systems
1983 – 1986

Clark University
Bachelor's degree (with Honors), Science, Technology, and Society: Risk-Hazards/Computer Science
1981 – 1983

Licenses & Certifications

Certified Information Systems Auditor® (CISA)
ISACA
Issued Apr 2015 · No Expiration Date
Credential ID 15122708
See credential

GISP - Certified Geographic Information Systems Professional
GISCI
Issued Apr 2015 · No Expiration Date
See credential

Outdoor Leader
National Outdoor Leadership School

Agenda

- ✓Instructor
- Introduction
- Course overview
- Need for Cybersecurity Professionals

Course objective

- This course is a broad introduction to the managerial issues of information security
- Because security is multifaceted, the topics of the class range widely, including technical, managerial, physical, and psychological issues
- A key objective of the class is to develop a security mindset, in which one learns to think like an attacker for ways to exploit a system

Course objectives’

- Explain cybersecurity as a key enterprise risk and how it can be managed
- Understand methods used to identify, protect against, detect, respond to, and recover from cybersecurity threats
- Use techniques of ethical hacking to perform penetration testing to assess vulnerabilities in information systems
- Communicate risk in assessment reports that support management decisions

The value of business' data is at a peak

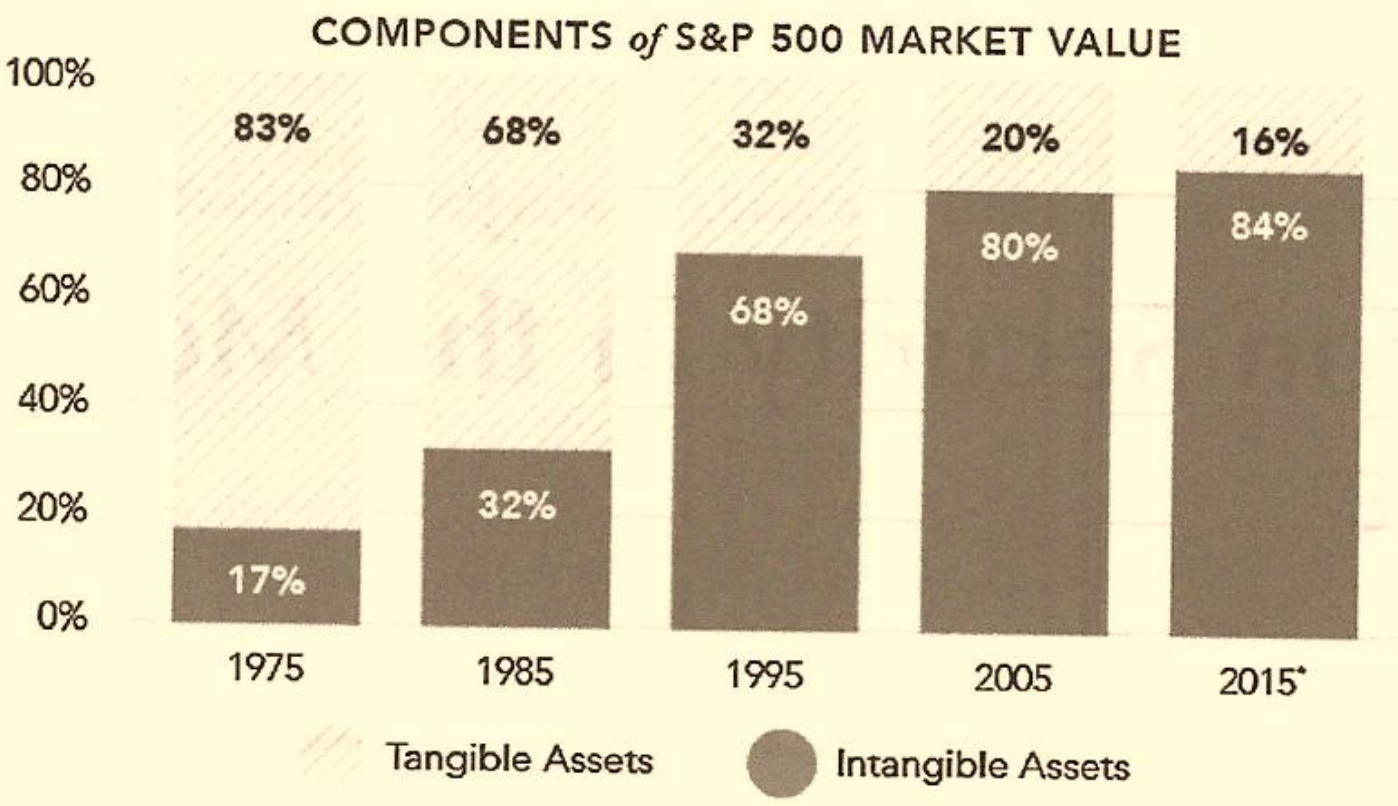


FIGURE 1.1 Change in public company assets from tangible to intangible.

"A generation ago the asset base of US public companies was more than 80% tangible property" (e.g. raw materials, real estate, railroad cars…)

"Today… intangibles… account for more than 80% of listed company value"

Computers and Information Security Handbook, J. Vacca, 2017, pp. 3-4

Transformation of Information Security

1970 data security examples

Guarding the photocopier

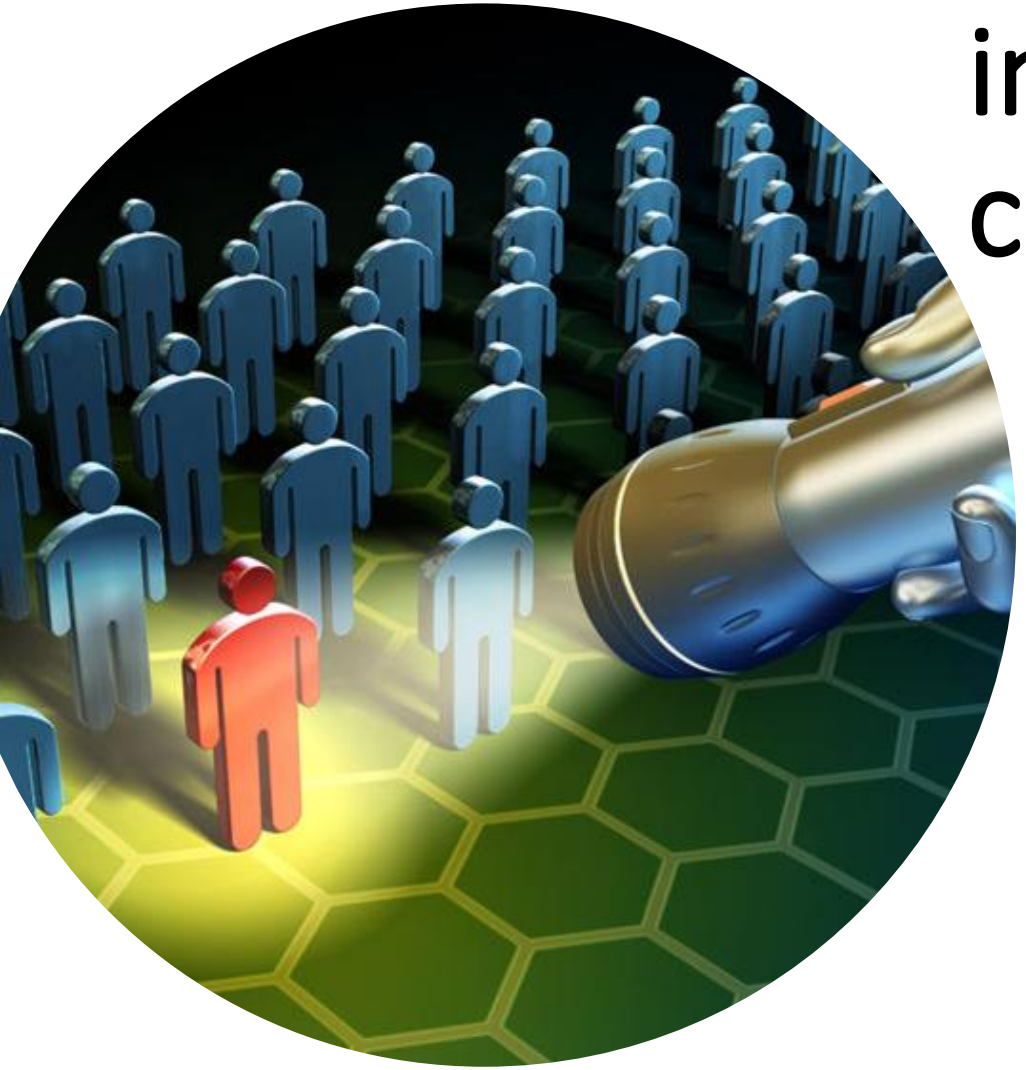
Watching who went in and out of the front door

Today's data security must consider

Devices able to grab gigabytes of data and move them anywhere in the world in an instant

Laptops, tablets and smartphones with direct connection to company data are endpoints in a global network, creating thousands to millions of "front doors" leaving industry at its most vulnerable

What one thing about information security has not changed over the years?



Human beings remain the primary vector for loss of corporate value

AND

Humans also control the processes and technologies central to information security function that preserves corporate value

Key concepts

Information and Information System security = Cybersecurity

…means protecting information and information systems from unathorized:

- *Access, use, disclosure of information* ***Confidentiality***
- *Unauthorize modification of information* ***Integrity***
- *Disruption and destruction of information* ***Availability***

Key concepts

Threat

Potential for the occurrence of a harmful event such as a cyber attack

Vulnerability

Weakness that makes targets susceptible to an attack

Risk

Potential of loss from an attack

Risk Mitigation

Strategy for dealing with risk

What is a threat?

Physical

Technical

Administrative

Anything that has the potential to lead to unauthorized:

- ***Access, use, disclosure***
- ***Modification***
- ***Disruption or Destruction***

of an enterprises' information or information systems

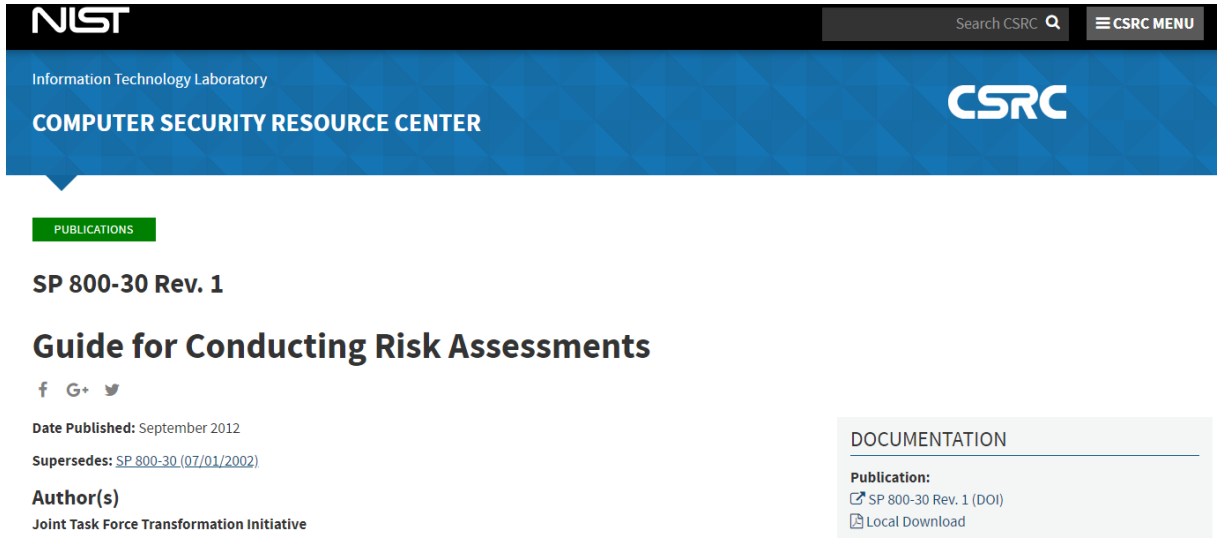
What is a threat…

Threats to information and information systems include:

- Purposeful attacks
- Human errors
- Structural Failures
- Environmental disruptions

Taxonomy of threat sources

1. Adversarial
2. Accidental
3. Structural
4. Environmental



https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

Type of Threat Source	Description	Characteristics

ADVERSARIAL
- Individual
  - Outsider
  - Insider
  - Trusted Insider
  - Privileged Insider
- Group
  - Ad hoc
  - Established
- Organization
  - Competitor
  - Supplier
  - Partner
  - Customer
- Nation-State
	Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources (i.e., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies).	Capability, Intent, Targeting

ACCIDENTAL - User - Privileged User/Administrator	Erroneous actions taken by individuals in the course of executing their everyday responsibilities.	Range of effects

STRUCTURAL
- Information Technology (IT) Equipment
  - Storage
  - Processing
  - Communications
  - Display
  - Sensor
  - Controller
- Environmental Controls
  - Temperature/Humidity Controls
  - Power Supply
- Software
  - Operating System
  - Networking
  - General-Purpose Application
  - Mission-Specific Application
	Failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances which exceed expected operating parameters.	Range of effects

ENVIRONMENTAL
- Natural or man-made disaster
  - Fire
  - Flood/Tsunami
  - Windstorm/Tornado
  - Hurricane
  - Earthquake
  - Bombing
  - Overrun
- Unusual Natural Event (e.g., sunspots)
- Infrastructure Failure/Outage
  - Telecommunications
  - Electrical Power
	Natural disasters and failures of critical infrastructures on which the organization depends, but which are outside the control of the organization.
	Note: Natural and man-made disasters can also be characterized in terms of their severity and/or duration. However, because the threat source and the threat event are strongly identified, severity and duration can be included in the description of the threat event (e.g., Category 5 hurricane causes extensive damage to the facilities housing mission-critical systems, making those systems unavailable for three weeks).
		Range of effects

Adversarial Threats

"Security involves making sure things work, not in the presence of random faults, but **in the face of an intelligent and malicious adversary** trying to ensure that things fail in the worst possible way at the worst possible time."

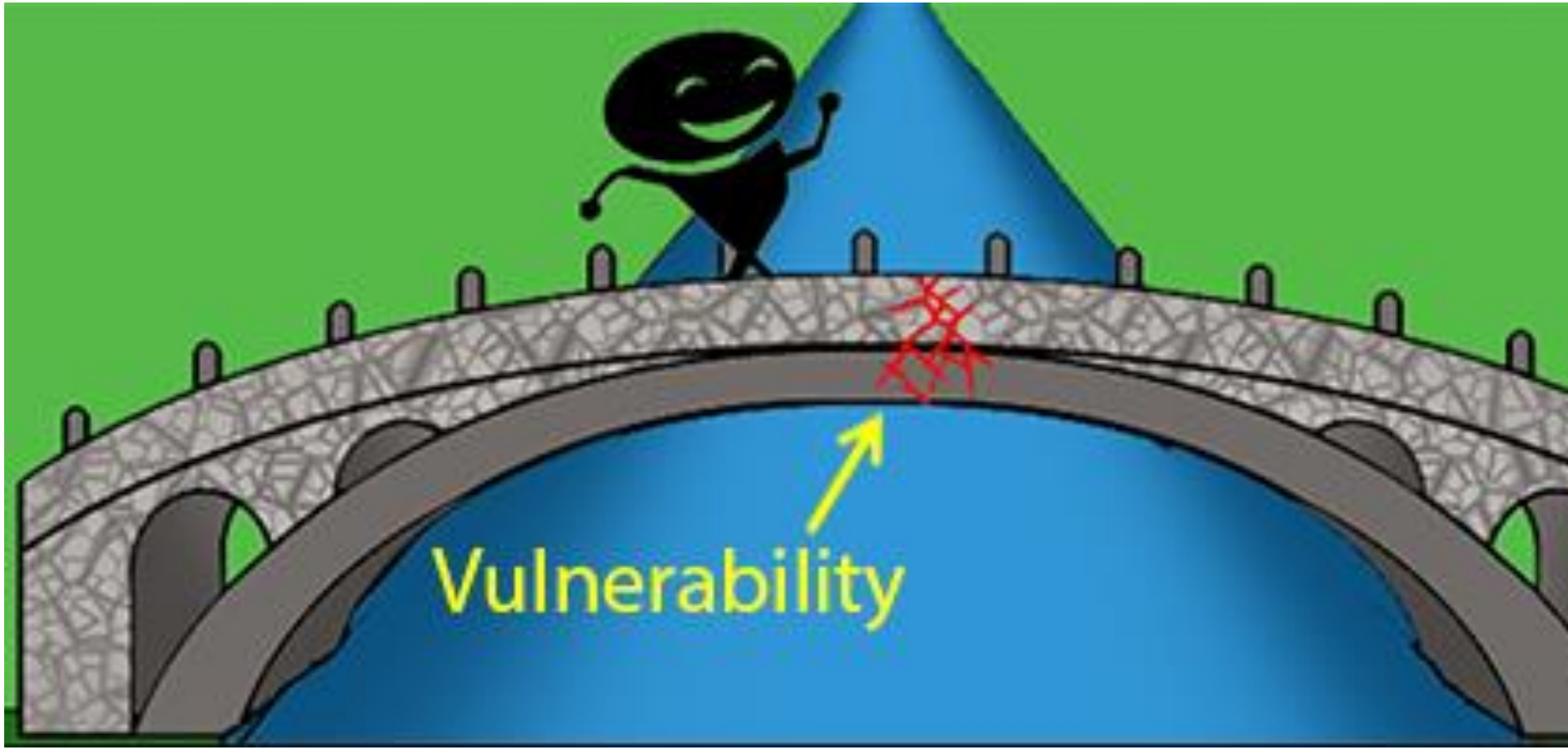
– Bruce Schneier

Type of Threat Source	Description	Characteristics

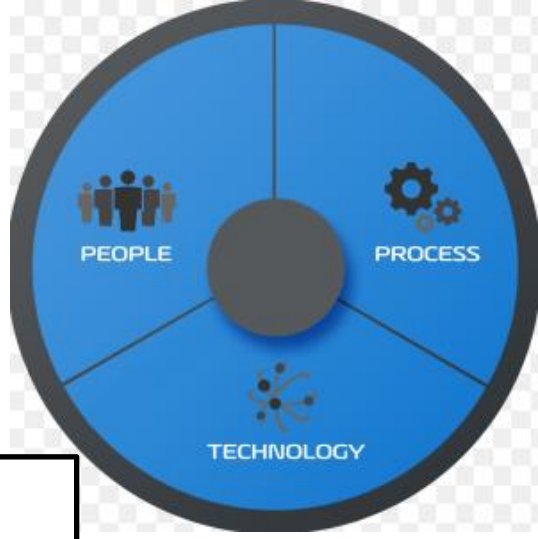
ADVERSARIAL
- Individual
  - Outsider
  - Insider
  - Trusted Insider
  - Privileged Insider
- Group
  - Ad hoc
  - Established
- Organization
  - Competitor
  - Supplier
  - Partner
  - Customer
- Nation-State
	Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources (i.e., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies).	Capability, Intent, Targeting

More information can be found in class notes

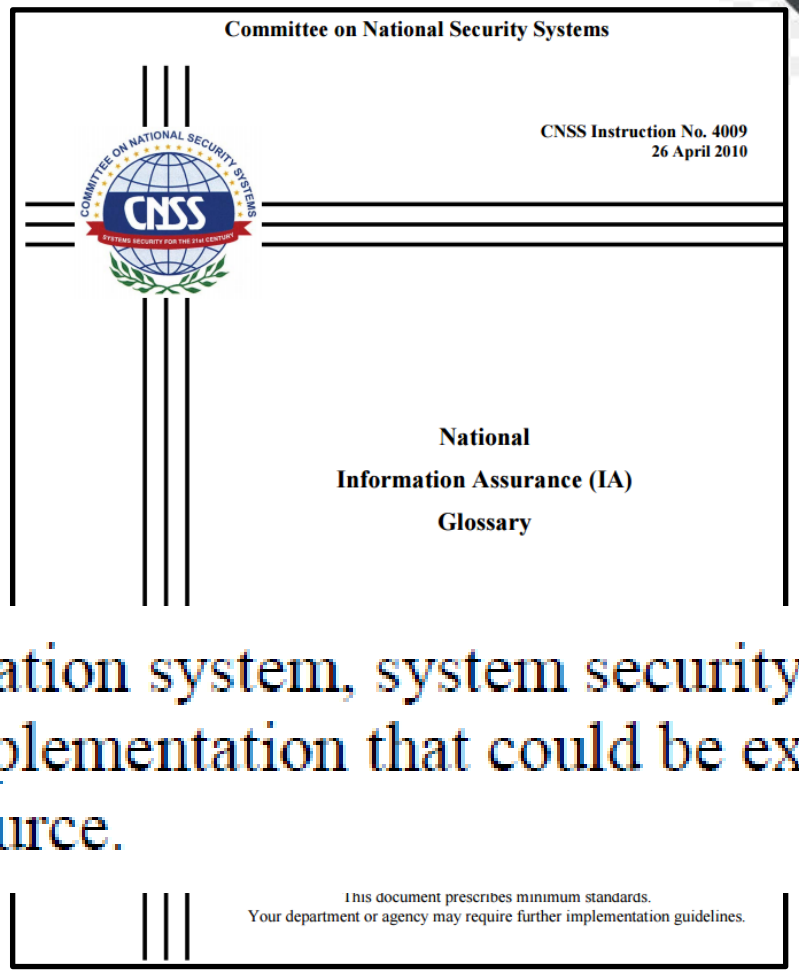
What is a Vulnerability?



What is a Vulnerability?



Any unaddressed susceptibility to a Adversarial, Accidental, Structural or Environmental threat is an information security vulnerability



Committee on National Security Systems

CNSS Instruction No. 4009
26 April 2010

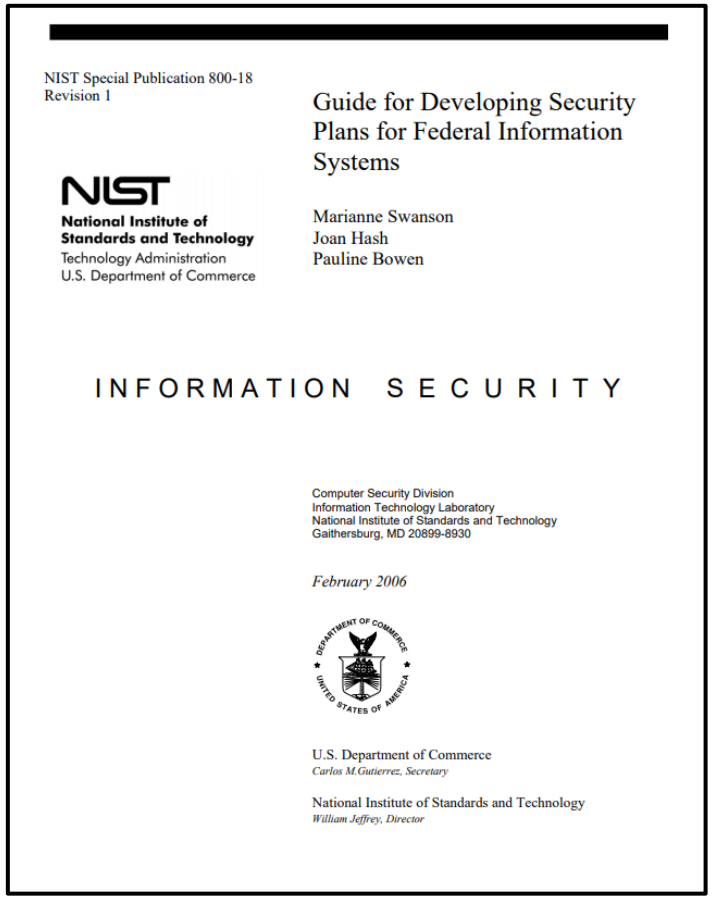
National
Information Assurance (IA)
Glossary

This document prescribes minimum standards.
Your department or agency may require further implementation guidelines.

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Vulnerabilities are…

Inadequacies in any of these 17 areas which lead to negative impacts:



NIST Special Publication 800-18
Revision 1

Guide for Developing Security Plans for Federal Information Systems

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Marianne Swanson
Joan Hash
Pauline Bowen

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

February 2006

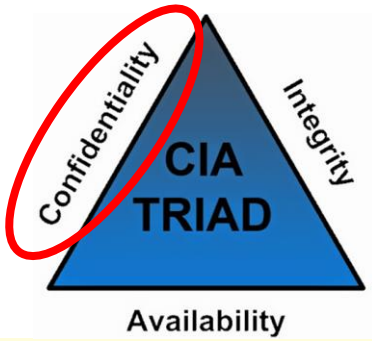
U.S. Department of Commerce
Carlos M.Gutierrez, Secretary

National Institute of Standards and Technology
William Jeffrey, Director

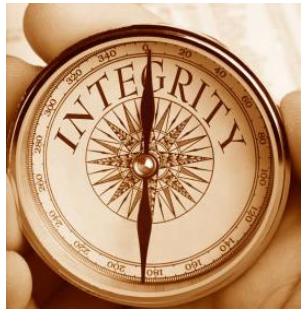
Cybersecurity Controls protect against impacts

CLASS	FAMILY
Management	Risk Assessment
Management	Planning
Management	System and Services Acquisition
Management	Certification, Accreditation, and Security Assessments
Operational	Personnel Security
Operational	Physical and Environmental Protection
Operational	Contingency Planning
Operational	Configuration Management
Operational	Maintenance
Operational	System and Information Integrity
Operational	Media Protection
Operational	Incident Response
Operational	Awareness and Training
Technical	Identification and Authentication
Technical	Access Control
Technical	Audit and Accountability
Technical	System and Communications Protection

Vulnerability to what ?



	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.



	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

FIPS 199 Standards: Security objectives relate to avoiding negative impacts

FIPS PUB 199

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Standards for Security Categorization of Federal Information and Information Systems

Impact ratings:

- ***High:*** *Severe or catastrophic adverse effect*
- ***Moderate:*** *Serious adverse effect*
- ***Low:*** *Limited adverse effect*

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Security Categorization Standard is used to determine the security categorization of an information system that contains, processes and/or transports information

The generalized format for expressing the security category, SC, of an information system is:

SC information system = {(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *impact*)},

where the acceptable values for potential impact are LOW, MODERATE, or HIGH.

…remember the impact ratings:

- **High impact:** Severe or catastrophic adverse effect
- **Moderate impact:** Serious adverse effect
- **Low impact:** Limited adverse effect

Example with multiple information types:

SC contract information = {(**confidentiality**, MODERATE), (**integrity**, MODERATE), (**availability**, LOW)},

and

SC administrative information = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}.

The resulting security category of the information system is expressed as:

SC acquisition system = {(**confidentiality**, MODERATE), (**integrity**, MODERATE), (**availability**, LOW)},

What is a Risk?

A measure of the potential impact of a threat resulting from an exploitation of a vulnerability

Potential loss resulting from unauthorized:

- *Access, use, disclosure*
- *Modification*
- *Disruption or destruction*

…of an enterprises' information

Can be expressed in quantitative and qualitative terms

Physical

Technical

Administrative (organizational, governance)

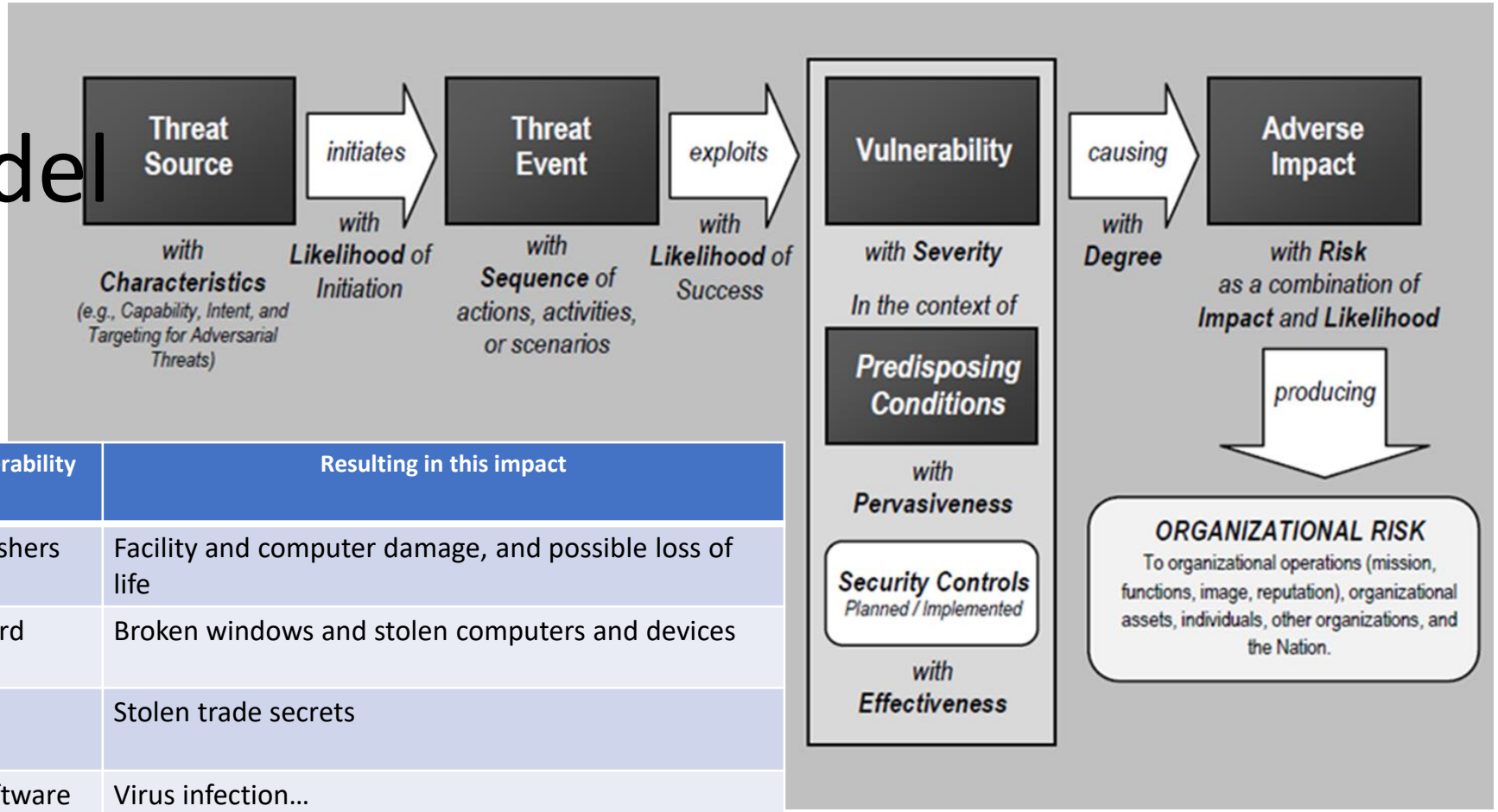
What are examples of Information security risks ?

- Economic impact and financial loss
  - Replacement costs (software, hardware, other)
  - Backup restoration and recovery costs
  - Reprocessing, reconstruction costs
  - Theft/crime (non-computer, computer)

- Loss of life
- Losses due to fraud, theft, larceny, bribery
- Impact of
  - lost competitive edge
  - lost data
  - lost time
  - lost productivity
  - lost business

- Bankruptcy
- Business interruption
- Frustration
- Ill will
- Injury
- Impacts of inaccurate data

An IT risk model



Type	Threat Source	Can exploit this vulnerability	Resulting in this impact
Physical	Fire	Lack of fire extinguishers	Facility and computer damage, and possible loss of life
Physical	Intruder	Lack of security guard	Broken windows and stolen computers and devices
Technical	Contractor	Lax access control mechanisms	Stolen trade secrets
Technical	Malware	Lack of antivirus software	Virus infection…
Technical	Hacker	Unprotected services running on a server	Unauthorized access to confidential information
Administrative	Employee	Lack of training	Unauthorized distribution of sensitive information

NIST SP 800-30r1 “Guide for Conducting Risk Assessments”, page 21

Cybersecurity Objectives

Quantitative Risk Assessment

$$\textit{Annual Loss Expectancy} =$$

Single Loss Expectancy

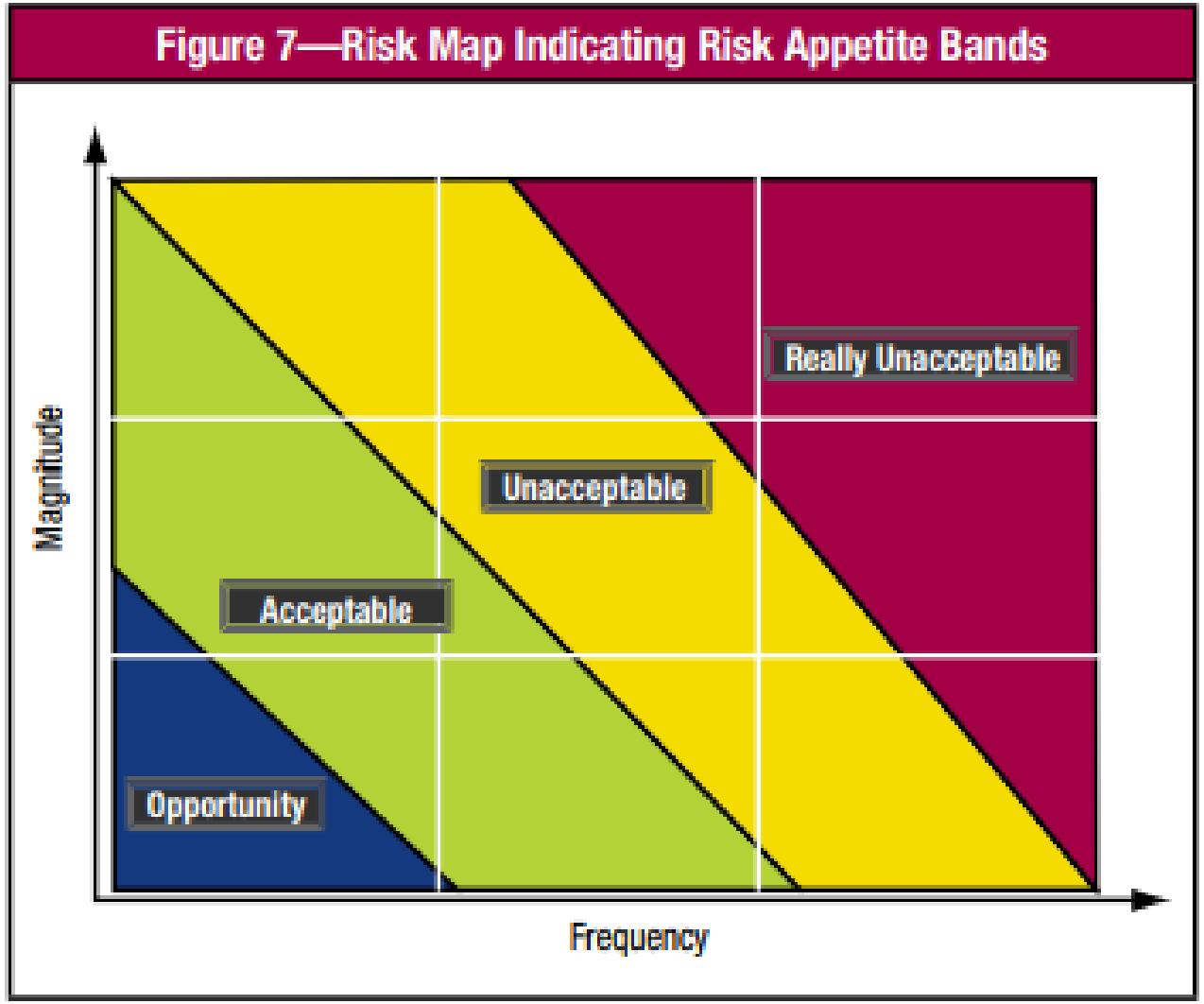
$\times$

Annualized Rate of Occurrence

Qualitative Risk Assessment

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

How do you determine if a risk is acceptable?



Course objectives

- ✓ Explain cybersecurity as a key enterprise risk and how it can be managed
- ➢ Understand methods used to identify, protect against, detect, respond to, and recover from cybersecurity threats
- Use techniques of ethical hacking to perform penetration testing to assess vulnerabilities in information systems
- Communicate risk in assessment reports that support management decisions

Risk Management Techniques

Once threats and risks are identified, each risk can be managed by:

1. Avoidance
2. Acceptance
3. Transfer
4. Mitigation (“Controls”)

Information identification, categorization and risk evaluation is the first step in information systems security…

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

This course will help you understand how information risk to an enterprise is evaluated and security of information systems is assessed

Course objectives

- ✓ Explain cybersecurity as a key enterprise risk and how it can be managed
- ✓ Understand methods used to identify, protect against, detect, respond to, and recover from cybersecurity threats
- ➢ Use techniques of ethical hacking to perform penetration testing to assess vulnerabilities in information systems
- Communicate risk in assessment reports that support management decisions

Ethical Hacking & Penetration Testing

This course will help you gain insight into cybersecurity risk controls and one specific type cybersecurity risk assessment…

"Penetration testing is a specialized type of assessment conducted on information systems or individual system components to identify vulnerabilities that could be exploited by adversaries.

Such testing can be used to either validate vulnerabilities or determine the degree of resistance organizational information systems have to adversaries within a set of specified constraints (e.g., time, resources, and/or skills).

Penetration testing attempts to duplicate the actions of adversaries in carrying out hostile cyber attacks against organizations and provides a more in-depth analysis of security-related weaknesses/deficiencies."

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

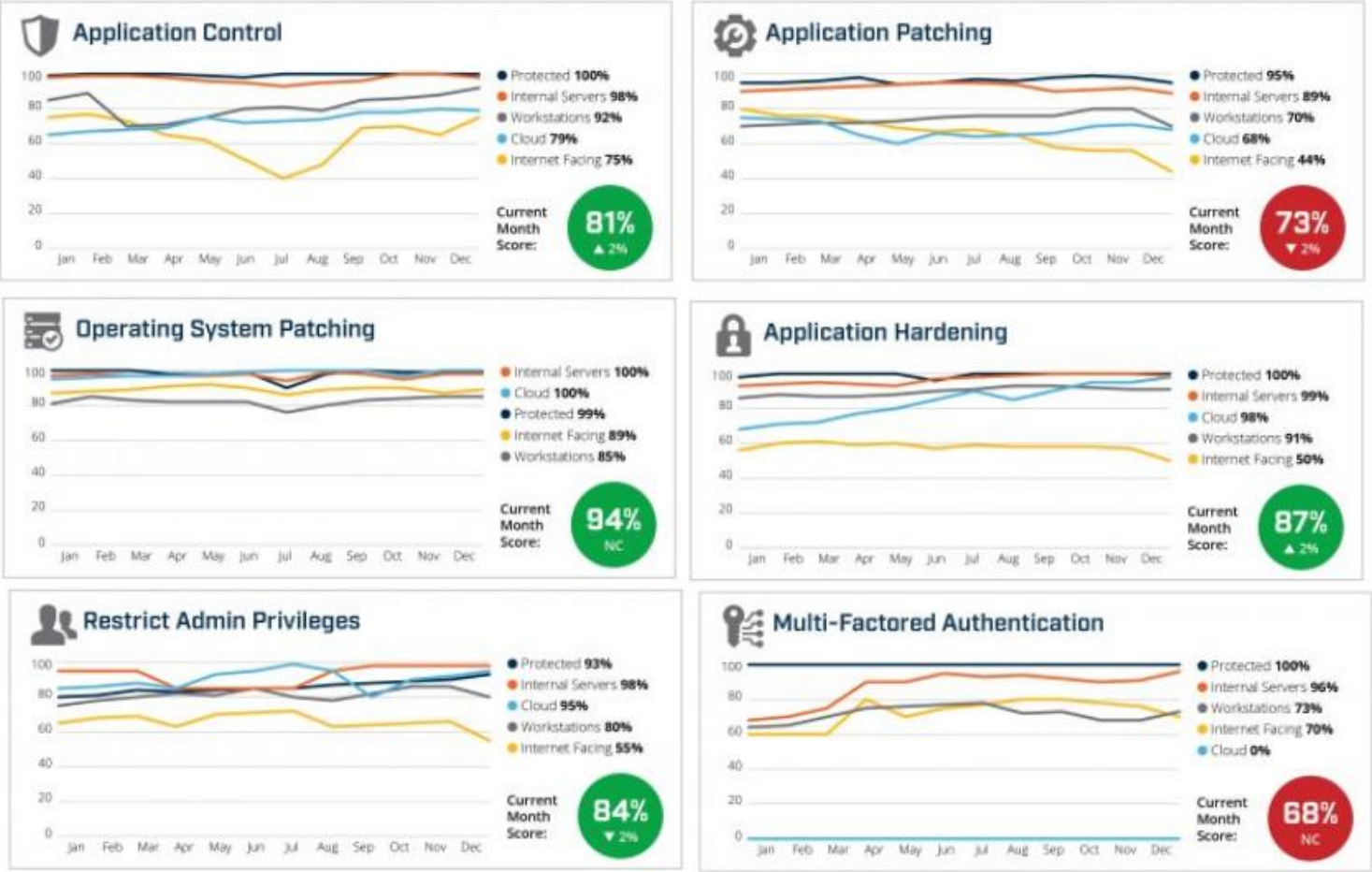
Course objectives

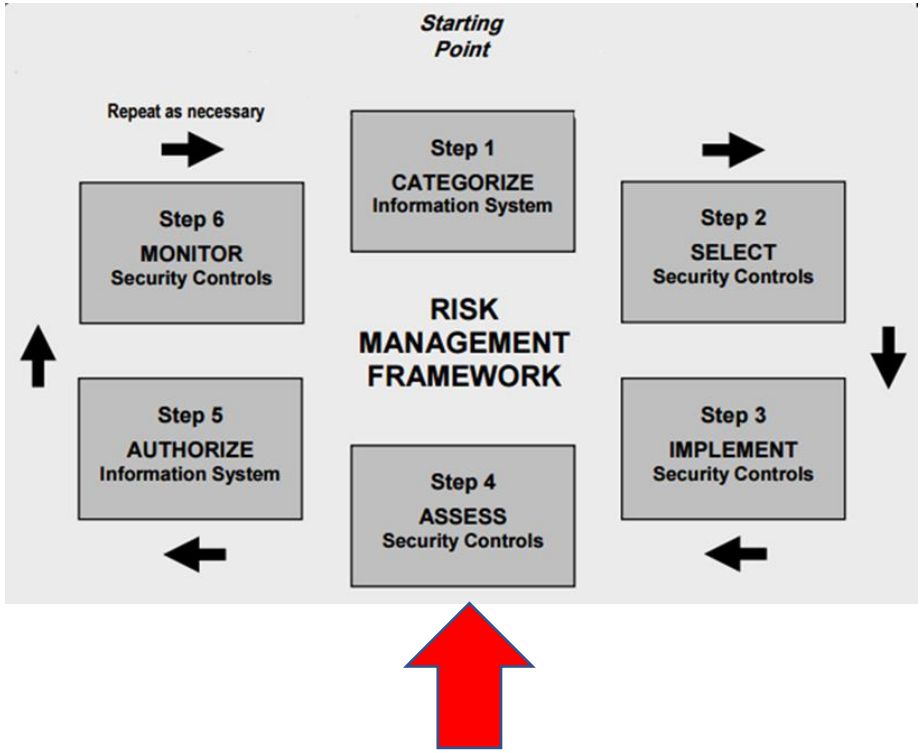
- ✓ Explain cybersecurity as a key enterprise risk and how it can be managed
- ✓ Understand methods used to identify, protect against, detect, respond to, and recover from cybersecurity threats
- ✓ Use techniques of ethical hacking to perform penetration testing to assess vulnerabilities in information systems
- ➢ Communicate risk in assessment reports that support management decisions

Course Learning Goals

- Develop a security mindset
  - Learn to think like a security professional—how to identify threats like an attacker, and how to model and mitigate those threats.
- Gain a working knowledge of methods to protect data
  - Gain a working knowledge of modern methods of protecting data: encryption, hashing, confidentiality, authentication, integrity, non-repudiation, certificates, and IP security.
- Learn methods of attack and defense
  - Learn methods of attacking systems and how to protect against those methods of attacks.
- Appreciate the broad disciplines required for IS security
  - Appreciate the broad disciplines required for information security to work. We'll cover subjects as comprehensive as cryptology, physical security, psychology, and management, based on based on the NIST Cybersecurity Framework Version 1.1 (https://www.nist.gov/cyberframework/framework) and the NIST Risk Management Framework (https://csrc.nist.gov/projects/risk-management/about-rmf).
- Communicate security risks and responses effectively
  - This course is a Temple-designated writing intensive course. As such, a substantial portion of the course will be devoted to practicing capable, proficient communication of cybersecurity risks, threats, mitigations, and responses to relevant stakeholders for their decision making.

Risk Assessment and Mitigation Recommendations





Agenda

- ✓ Instructor
- ✓ Introduction
- ➢ Course overview
- Need for Cybersecurity Professionals

Syllabus and Course website

Fox School of Business
TEMPLE UNIVERSITY

MIS 4596 – Managing Enterprise Cybersecurity – Fall 2021
Section 002 – CRN 23258
Tuesday/Thursday 3:30 – 4:50 PM, 1810 Liacouras Walk – Room 210

Instructor

David Lanter
Office: Speakman 209C and online via Zoom
Office Hours: Tuesday 2:00pm–3:00 pm (by prearrangement) and by appointment via Zoom
Email: *david.lanter@temple.edu*
e-profile: *http://community.mis.temple.edu/dlanter/*

Information Technology Assistant

- Vanessa Marin – vanessa.marin@temple.edu

Course Textbook and Materials

- Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd or 3rd Editions, by Ross Anderson. Free PDF of the book: http://www.cl.cam.ac.uk/~rja14/book.html
- Harvard Business Coursepack for MIS 4596 – two required cases are available for purchase at Harvard Business Publishing for $8.50 here: https://hbsp.harvard.edu/import/856818
- Security Assignments by Dave Eargle and Anthony Vance at http://security-assignments.com/. A number of this course's labs and milestone assignments beginning with Lab 3 require lab virtual machine access for Google Cloud Platform (GCP) available for purchase for $40 here: https://security-assignments.com/store/
- Other materials will be made available throughout the semester
- (Optional) "Secrets and Lies: Digital Security in a Networked World," by Bruce Schneier
  - Temple Library : https://onlinelibrary-wiley-com.libproxy.temple.edu/doi/book/10.1002/9781119183631
  - Amazon.com : https://www.amazon.com/dp/0471453803/

Class Sites

- **MIS Community** - https://community.mis.temple.edu/mis4596sec002fall2021/
- **Canvas** - https://templeu.instructure.com/courses/102405

- 1 -

MIS
MANAGEMENT INFORMATION SYSTEMS

Managing Enterprise Cybersecurity
MIS 4596.002 ■ Fall 2021 ■ David Lanter

SCHEDULE | ABOUT | LABS | LECTURE MATERIALS

Schedule

DATES	TOPIC & ASSIGNMENTS DUE	READINGS
Tuesday, 8/24/2021	Introduction to the Course	Anderson, Ch. 1
Thursday, 8/26/2021	Threat modeling	Read the beginning of each chapter, skim the rest of the chapter: "Threat Modeling," by Adam Shostack, Introduction, Chapter 1, Chapter 4 Optional: Schneier, Chapter 21
Tuesday, 8/31/2021	Risk Assessment	
Thursday, 9/2/2021	**Lab 1: Threat Modeling due** ***Start Milestone 1: Risk Assessment Report Draft*** Information Privacy	Tim Cook, "Technology can harm, can help"
Tuesday.9/7/2021	Introduction to Linux | Google Cloud Platform (GCP)	
Thursday, 9/9/2021	**Lab 2: Web Privacy and Anonymity Lab due** Introduction to Cryptography	Anderson, Chapter 5

RECENT ANNOUNCEMENTS

[More Announcements...]

Grading

Milestones	Group	40%
Labs	Individual	25%
Mid-Term Exam	Individual	15%
Final Exam	Individual	20%
Total		**100%**

Schedule (subject to change)

Week	Tuesday	Thursday	Topics
1	Aug 24	Aug 26	Introduction Threat Modeling
2	Aug 31	Sep 2	Risk Assessment Information Privacy
3	Sep 7	Sep 9	Introduction to Linux and Google Cloud Platform Introduction to Cryptography
4	Sep 14	Sep 16	Symmetric Cryptography No Class Meeting
5	Sep 21	Sep 23	Asymmetric Cryptography Digital Certificates and Public Key Infrastructures
6	Sep 28	Sep 30	Authentication and Passwords Password Cracking
7	Oct 5	Oct 7	Individual work on Midterm exam - No Class Meeting Introduction to Networking
8	Oct 12	Oct 14	Vulnerability Scanning
9	Oct 19	Oct 21	Vulnerability Exploitation
10	Oct 26	Oct 28	Human Element–Info. Security in Organizations Physical Security
11	Nov 2	Nov 4	Network Security Monitoring Incident Response – Equifax Case Study
12	Nov 9	Nov 11	Incident Recovery Maersk Case Study
13	Nov 16	Nov 18	Malware Analysis
	Nov 23	Nov 25	Fall Break – No Class Meeting Thanksgiving Break – No Class Meeting
14	Nov 30	Dec 2	Course Wrap-Up

Other Key Dates and Deadlines (subject to change)

Thurs, Sep 2	Start Milestone 1: Risk Assessment Report Draft
Sat, Sep 11	Deadline for Milestone 1: Risk Assessment Report Draft Due
Sat, Sep 18	Deadline for Milestone 2: Risk Assessment Final Report Due
Mon, Oct 4	Midterm Exam opens
Sat, Oct 9	Deadline for Midterm exam
Tue, Oct 19	Start Milestone 3: Penetration Test
Sat, Nov 6	Deadline for Milestone 3: Penetration Test Report Due
Thurs, Dec 8	Final Exam opens
Sat, Dec 11	Deadline for Milestone 4: Penetration Test Report with Mitigations Due
Wed, Dec 15	Deadline for final exam
Thurs, Dec 16	Deadline for completion of all lab assignments

All assignments and exams are due by 11:59 PM EST.

Course materials – readings…

Information Security Management | Assignments

By Drs. Dave Eargle and Anthony Vance

- Labs
- Book and Film Lists
- Reading Topics
- In-class Activities
- Projects
- Store

MIS
MANAGEMENT INFORMATION SYSTEMS

Managing Enterprise
MIS 4596.002 ■ Fall 2021

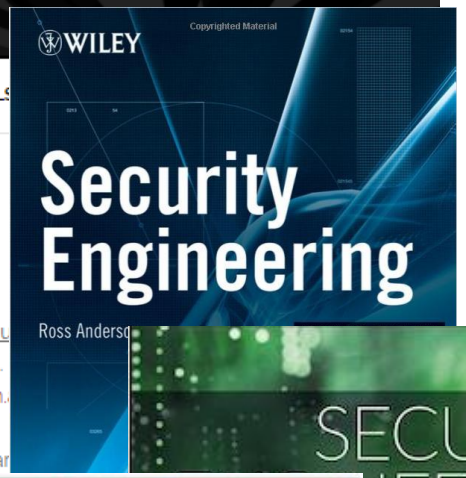
SCHEDULE | ABOUT | LABS | LECTURE MATERIALS

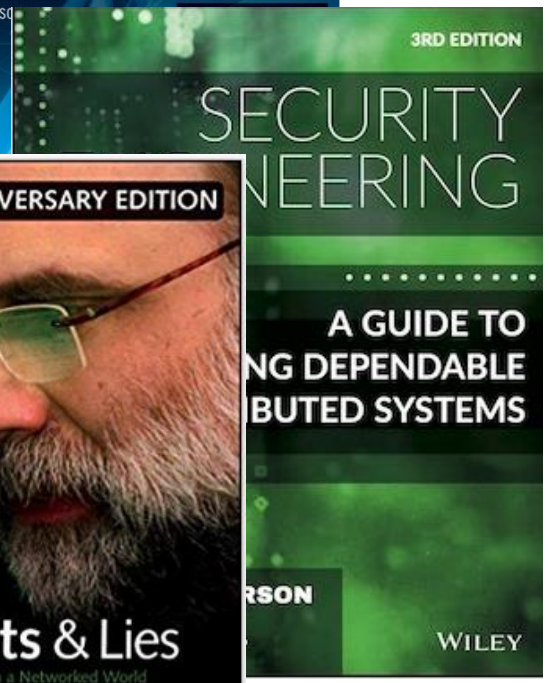
- Course overview
- Course materials
- Grading and Assignments
- Instructor

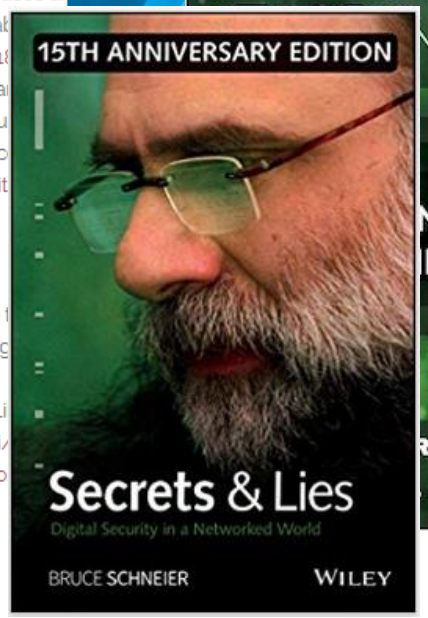
Cou…s

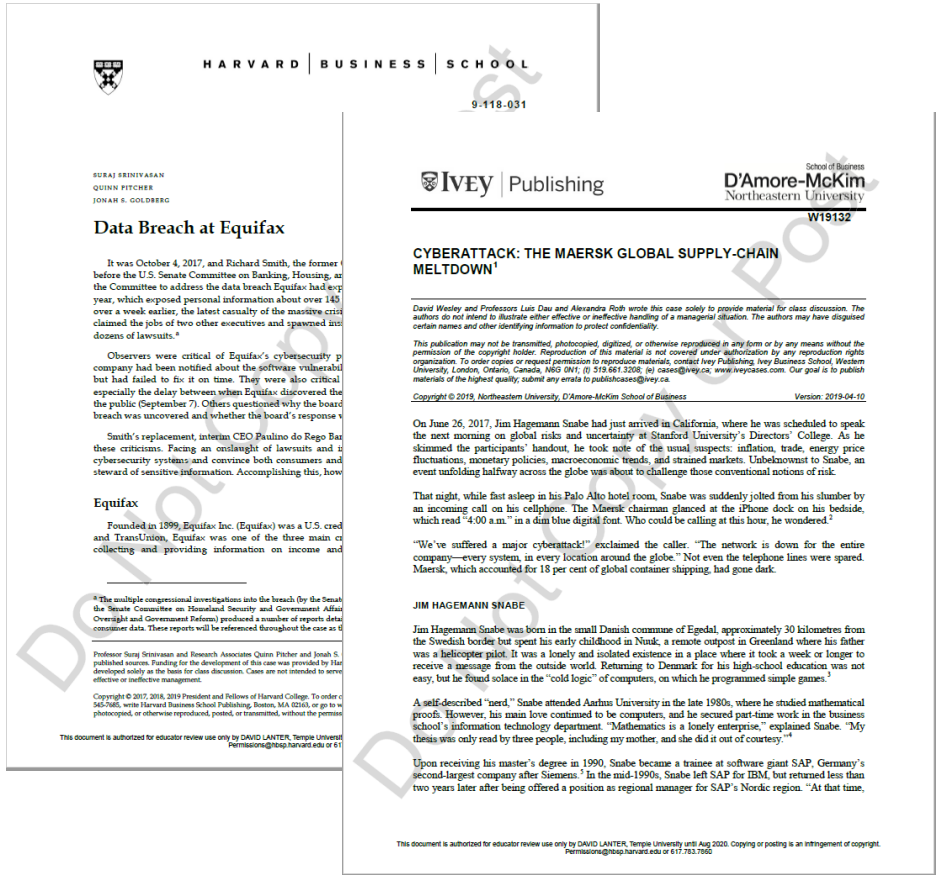
The follov…

- Req… …gineering: A Gu… Systems 2nd or 3rd Edition, by Ross Anderson.
  - Free PDF of the book: http://www.cl.cam…
  - Amazon: http://a.co/gbzf6zP
- **Required Case Studies:** Two business cases ar… from Harvard Business Publishing availab… https://hbsp.harvard.edu/import/856818…
- **Security Assignments:** by Dave Eargle a… assignments.com/. A number of this cou… with Lab 3 require lab virtual machine ac… for purchase for $40 here: https://securit…
- Other materials will be maded available t…
- **Optional Textbook:** "Secrets and Lies: Dig… Schneier.
  - Available online via Temple Li… com.libproxy.temple.edu/doi/…
  - Amazon: https://amzn.com/o…









HARVARD | BUSINESS | SCHOOL

9-118-031

SURAJ SRINIVASAN
QUINN PITCHER
JONAH S. GOLDBERG

Data Breach at Equifax

It was October 4, 2017, and Richard Smith, the former … before the U.S. Senate Committee on Banking, Housing, ar… the Committee to address the data breach Equifax had exp… year, which exposed personal information about over 143… over a week earlier, the latest casualty of the massive crisi… claimed the jobs of two other executives and spawned ini… dozens of lawsuits.[8]

Observers were critical of Equifax's cybersecurity p… company had been notified about the software vulnerabil… but had failed to fix it on time. They were also critical… especially the delay between when Equifax discovered the… the public (September 7). Others questioned why the board… breach was uncovered and whether the board's response w…

Smith's replacement, interim CEO Paulino do Rego Bar… these criticisms. Facing an onslaught of lawsuits and i… cybersecurity systems and convince both consumers and… steward of sensitive information. Accomplishing this, how…

Equifax

Founded in 1899, Equifax Inc. (Equifax) was a U.S. cred… and TransUnion, Equifax was one of the three main cr… collecting and providing information on income and…

[8] The multiple congressional investigations into the breach (by the Senat… the Senate Committee on Homeland Security and Government Affai… Oversight and Government Reform) produced a number of reports detai… consumer data. These reports will be referenced throughout the case as t…

Professor Suraj Srinivasan and Research Associates Quinn Pitcher and Jonah S. … published sources. Funding for the development of this case was provided by Har… developed solely as the basis for class discussion. Cases are not intended to serve… effective or ineffective management.

IVEY | Publishing

School of Business
D'Amore-McKim
Northeastern University

W19132

CYBERATTACK: THE MAERSK GLOBAL SUPPLY-CHAIN MELTDOWN[1]

David Wesley and Professors Luis Dau and Alexandra Roth wrote this case solely to provide material for class discussion. The authors do not intend to illustrate either effective or ineffective handling of a managerial situation. The authors may have disguised certain names and other identifying information to protect confidentiality.

On June 26, 2017, Jim Hagemann Snabe had just arrived in California, where he was scheduled to speak the next morning on global risks and uncertainty at Stanford University's Directors' College. As he skimmed the participants' handout, he took note of the usual suspects: inflation, trade, energy price fluctuations, monetary policies, macroeconomic trends, and strained markets. Unbeknownst to Snabe, an event unfolding halfway across the globe was about to challenge those conventional notions of risk.

That night, while fast asleep in his Palo Alto hotel room, Snabe was suddenly jolted from his slumber by an incoming call on his cellphone. The Maersk chairman glanced at the iPhone dock on his bedside, which read "4:00 a.m." in a dim blue digital font. Who could be calling at this hour, he wondered.[2]

"We've suffered a major cyberattack!" exclaimed the caller. "The network is down for the entire company—every system, in every location around the globe." Not even the telephone lines were spared. Maersk, which accounted for 18 per cent of global container shipping, had gone dark.

JIM HAGEMANN SNABE

Jim Hagemann Snabe was born in the small Danish commune of Egedal, approximately 30 kilometres from the Swedish border, but spent his early childhood in Nuuk, a remote outpost in Greenland where his father was a helicopter pilot. It was a lonely and isolated existence in a place where it took a week or longer to receive a message from the outside world. Returning to Denmark for his high-school education was not easy, but he found solace in the "cold logic" of computers, on which he programmed simple games.[3]

A self-described "nerd," Snabe attended Aarhus University in the late 1980s, where he studied mathematical proofs. However, his main love continued to be computers, and he secured part-time work in the business school's information technology department. "Mathematics is a lonely enterprise," explained Snabe. "My thesis was only read by three people, including my mother, and she did it out of courtesy."[4]

Upon receiving his master's degree in 1990, Snabe became a trainee at software giant SAP, Germany's second-largest company after Siemens.[5] In the mid-1990s, Snabe left SAP for IBM, but returned less than two years later after being offered a position as regional manager for SAP's Nordic region. "At that time,

Course materials – schedule…

MIS
MANAGEMENT INFORMATION SYSTEMS

Managing Enterprise Cybersecurity

MIS 4596.002 ■ Fall 2021 ■ David Lanter

SCHEDULE | ABOUT | LABS | LECTURE MATERIALS

Schedule

DATES	TOPIC & ASSIGNMENTS DUE	READINGS
Tuesday, 8/24/2021	Introduction to the Course	Anderson, Ch. 1
Thursday, 8/26/2021	Threat modeling	Read the beginning of each chapter, skim the rest of the chapter: "Threat Modeling," by Adam Shostack, Introduction, Chapter 1, Chapter 4 Optional: Schneier, Chapter 21
Tuesday, 8/31/2021	Risk Assessment	
Thursday, 9/2/2021	**Lab 1: Threat Modeling due** ***Start Milestone 1: Risk Assessment Report Draft*** Information Privacy	Tim Cook, "Technology can harm, can help"
Tuesday,9/7/2021	Introduction to Linux | Google Cloud Platform (GCP)	
Thursday, 9/9/2021	**Lab 2: Web Privacy and Anonymity Lab due** Introduction to Cryptography	Anderson, Chapter 5

RECENT ANNOU

[More Announcements...]

DATES	TOPIC & ASSIGNMENTS DUE	READINGS
Tuesday, 8/24/2021	Introduction to the Course	Anderson, Ch. 1
Thursday, 8/26/2021	Threat modeling	Read the beginning of each chapter, skim the rest of the chapter: "Threat Modeling," by Adam Shostack, Introduction, Chapter 1, Chapter 4 Optional: Schneier, Chapter 21
Tuesday, 8/31/2021	Risk Assessment	
Thursday, 9/2/2021	**Lab 1: Threat Modeling due** ***Start Milestone 1: Risk Assessment Report Draft*** Information Privacy	Tim Cook, "Technology can harm, can help"

DATES	TOPIC & ASSIGNMENTS DUE	READINGS
Tuesday, 8/24/2021	Introduction to the Course	Anderson, Ch. 1
	eat modeling	Read the beginning of each chapter, skim the rest of the chapter: "Threat Modeling," by Adam Shostack, Introduction, Chapter 1, Chapter 4 Optional: Schneier, Chapter 21
	k Assessment	
	1: Threat Modeling e ***rt Milestone 1: Risk essment Report ft*** rmation Privacy	Tim Cook, "Technology can harm, can help"
	oduction to Linux | ogle Cloud Platform P)	
	2: Web Privacy and onymity Lab due oduction to ptography	Anderson, Chapter 5
	estone 1: Risk essment Report ft due	
	nmetric ptography	Anderson, Chapter 5
	Class Meeting	
	3: Introduction to ogle Cloud Platform and Linux Tutorial due	

Grading…

Milestones (40%)

There are four group milestone projects that will help students develop professional cybersecurity and communication skills.

- Milestone 1: Risk Assessment Draft
- Milestone 2: Final Risk Assessment Report
- Milestone 3: Penetration Test Report
- Milestone 4: Penetration Test with Mitigation Report

You will write each Milestone report as a stand-alone document in which you introduce terms and concepts you use and present your analysis in a concise, focused, error-free format that is easy to read and understand

"Writing-Intensive" Course

A main goal of this class is to help you convey information to another person in the clearest most effective written manner possible

Good technical writing skills are essential to professionals working in fields involving:

- Technology
- Information requirements
- Data analysis
- Regulations and policies
- Procedures and business workflow processes
- Instructing others in how to accomplish tasks

https://studentsuccess.temple.edu/w-courses/guidelines.html

Milestones…

Milestone Assignments (group projects)

Milestone 1: Risk Assessment Report Draft Create a draft risk assessment report for a financial management system.

Milestone 2: Final Risk Assessment Report Incorporate feedback from the instructor on the draft and improve and submit your final version of the report.

Milestone 3: Penetration Test Report draft Create a vulnerability and penetration assessment report of a server. Teams of students will be given an IP address of a server to assess for security weaknesses.

Milestone 4: Final Penetration Test with Mitigations Report Incorporate the feedback you receive on your Penetration Test Report draft and add recommendations for mitigating each identified vulnerability to create a Final Penetration Test with Mitigations Report.

Labs…

Technology Requirements

Information Security Assignments

This course will use lab and milestone project assignments at http://security-assignments.com/, developed by Dave Eargle and Anthony Vance. Access to the resources in this site will require subscription with a fee. A number of this course's labs and milestone assignments beginning with Lab 3 require lab virtual machine access for Google Cloud Platform (GCP) available for purchase for $40 here: https://security-assignments.com/store/

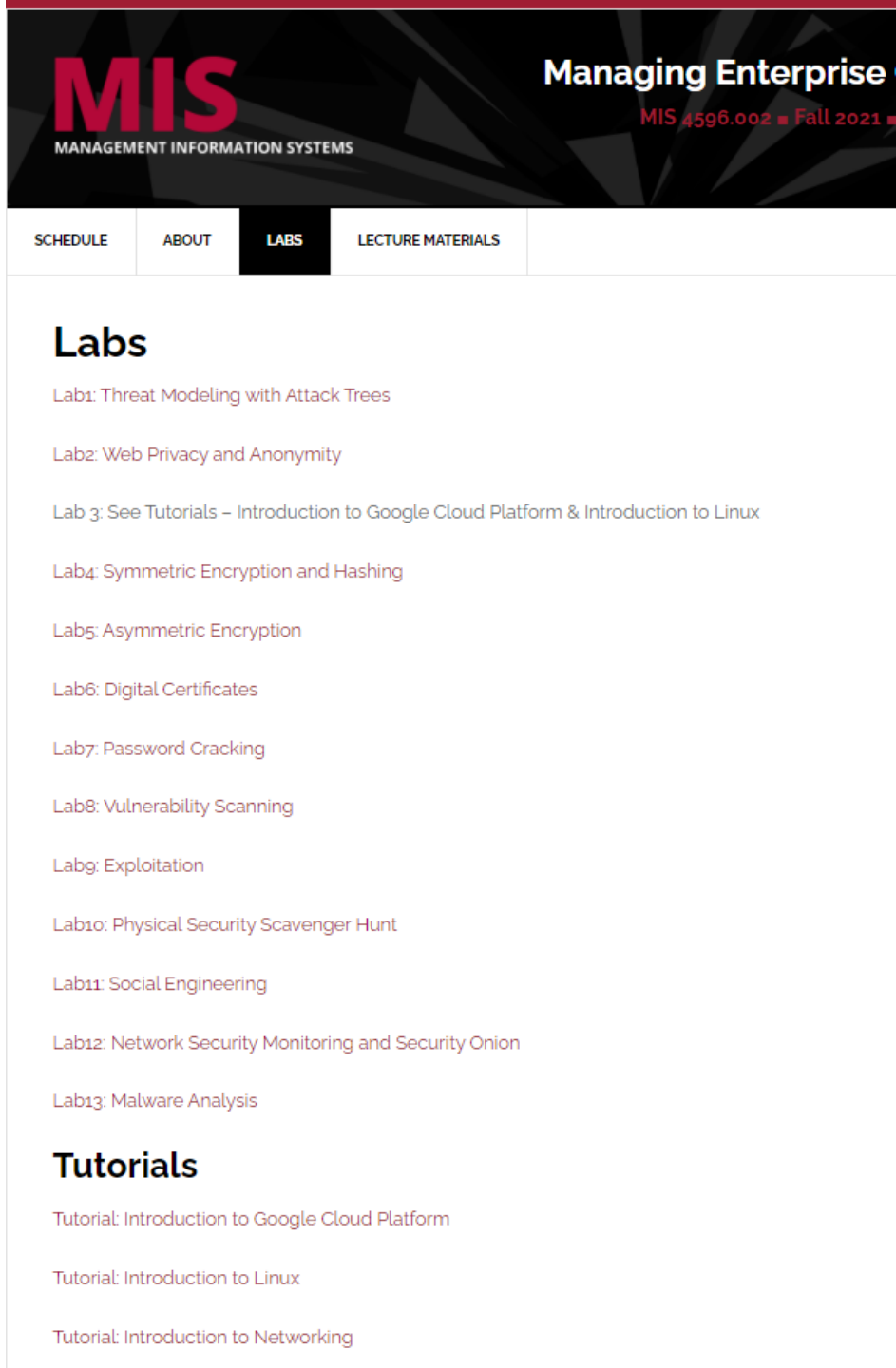
Google Cloud Platform (GCP)

This course uses GCP to run tools and virtual machines necessary to complete assignments. New accounts on GCP receive a $300 credit for no cost. Students should be able to complete this class without going over the credit and incurring cost. The instructor will have the students launch a virtual machine instance on GCP from which they can complete class assignments. The students will be able to remotely connect to the instance using Chrome Remote Desktop, which works just like a browser tab. To help reduce the risk of incurring costs above the free $300 students should manage their GCP accounts and shut down the machine between uses.

Lab Peer Support

Students are encouraged to help each other complete lab assignments. When a student offers help to another to complete one lab assignment, he/she will receive a 3% extra credit to the lab assignment.

- For example, if Michael reports that Molly helped him for Lab #2, Molly will receive a 3% extra credit to her Lab #2 grade. If Molly is reported to have helped two of her classmates, she will receive an 6% extra credit.
- The one who receives help must submit the helper's name in Canvas submission. (In other words, Michael should report that he has received help from Molly.)
- A student can report receiving help only from one student in one lab. (Michael cannot report help from both Molly and Stuart.)



Exams

Mid-Term (15%) and Final Exams (20%)

- The mid-term and final exams will be open-book and open-note exams over Canvas.
- The mid-term exam opens at Oct 4 and is due by Oct 9, 11:59 PM (subject to change).
- The final exam opens at Dec 9 and is due by Dec 15, 11:59 PM (subject to change). It is cumulative and covers the entire semester.
- There will be no extension to the deadlines for completing exams.

Certification Option for the Exams

- As an option, students seeking certification may replace both the mid-term and final exams by passing CompTIA Security+ certification (https://www.comptia.org/certifications/security) or other certification approved by the instructor.
- Students can substitute the score on the certification plus an adjustment (5% for the Security+) for the mid-term and final exams. For example, if a student receives an 85% on Security+, he/she receives 90% of the points for the two exams.
- To receive credit for the certification, the student must show evidence of having taken the certification exam by December 5.

Agenda

- ✓ Instructor
- ✓ Introduction
- ✓ Course overview
- ➢ Need for Cybersecurity Professionals

Information Security Analysts

Summary | What They Do | Work Environment | How to Become

Summary

Quick Facts: Information Security Analy	
2020 Median Pay	$103,59 $49.80 p
Typical Entry-Level Education	Bachelo
Work Experience in a Related Occupation	Less tha
On-the-job Training	None
Number of Jobs, 2019	131,000
Job Outlook, 2019-29	31% (Mu
Employment Change, 2019-29	40,900

What Information Security Analysts Do

Information security analysts plan and carry out security meas

Work Environment

Most information security analysts work for computer companies, consulting firms, or business and financial companies.

How to Become an Information Security Analyst

Most information security analyst positions require a bachelor's degree in a computer-related field. Employers usually prefer to hire analysts with experience in a related occupation.

Pay

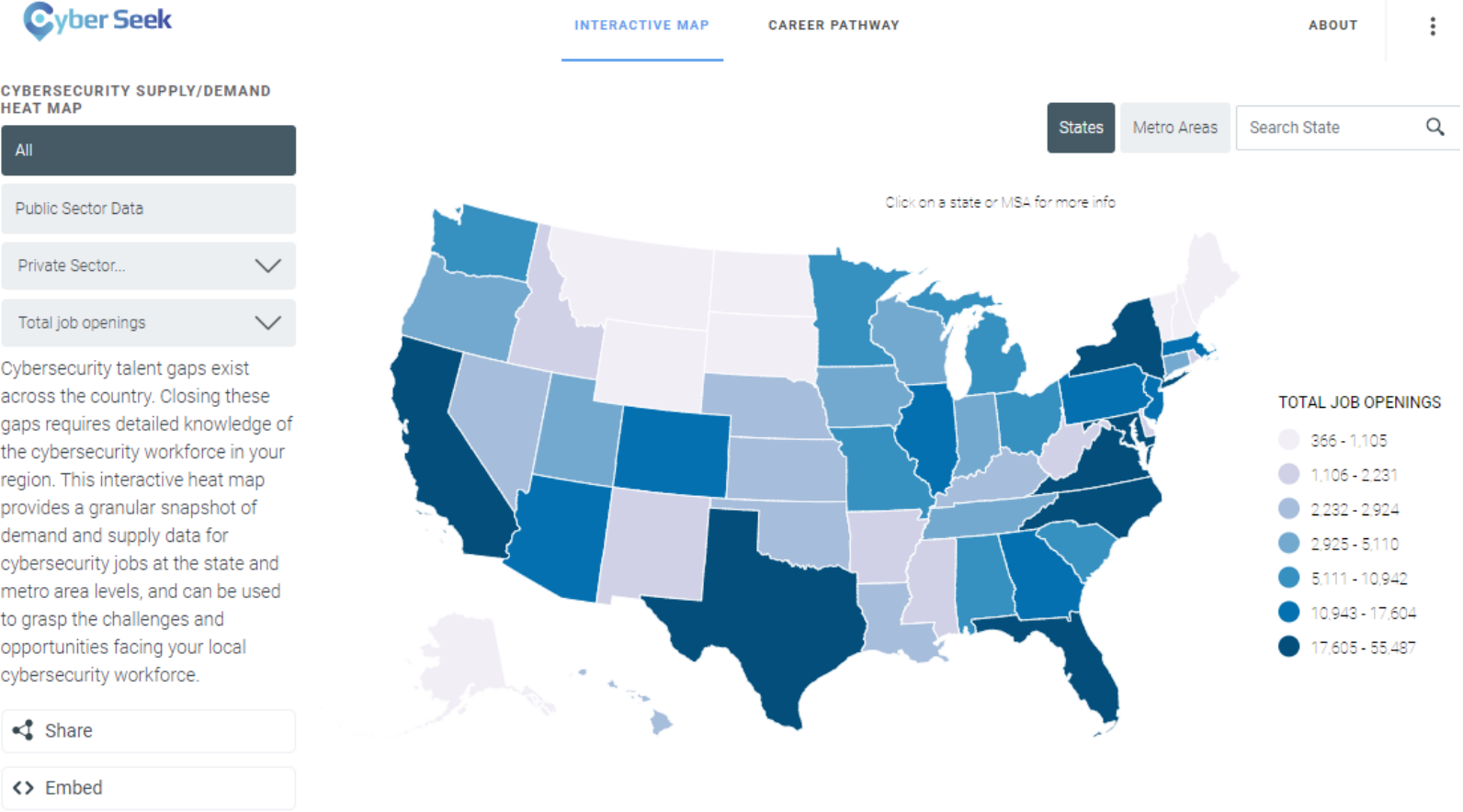
The median annual wage for information security analysts was $103,590 in May 2020.

Job Outlook

Employment of information security analysts is projected to grow 31 percent from 2019 to 2029, much faster than the average for all occupations. Demand for information security analysts is expected to be very high, as these analysts will be needed to create innovative solutions to prevent hackers from stealing critical information or causing problems for computer networks.

Summary

Quick Facts: Information Security Analysts	
2020 Median Pay	$103,590 per year $49.80 per hour
Typical Entry-Level Education	Bachelor's degree
Work Experience in a Related Occupation	Less than 5 years
On-the-job Training	None
Number of Jobs, 2019	131,000
Job Outlook, 2019-29	31% (Much faster than average)
Employment Change, 2019-29	40,900



National level

TOTAL CYBERSECURITY JOB OPENINGS

464,420

TOTAL EMPLOYED CYBERSECURITY WORKFORCE

956,341

SUPPLY OF CYBERSECURITY WORKERS

Very Low

CYBERSECURITY WORKFORCE SUPPLY/DEMAND RATIO

National average
2.1

GEOGRAPHIC CONCENTRATION

Average

LOCATION QUOTIENT

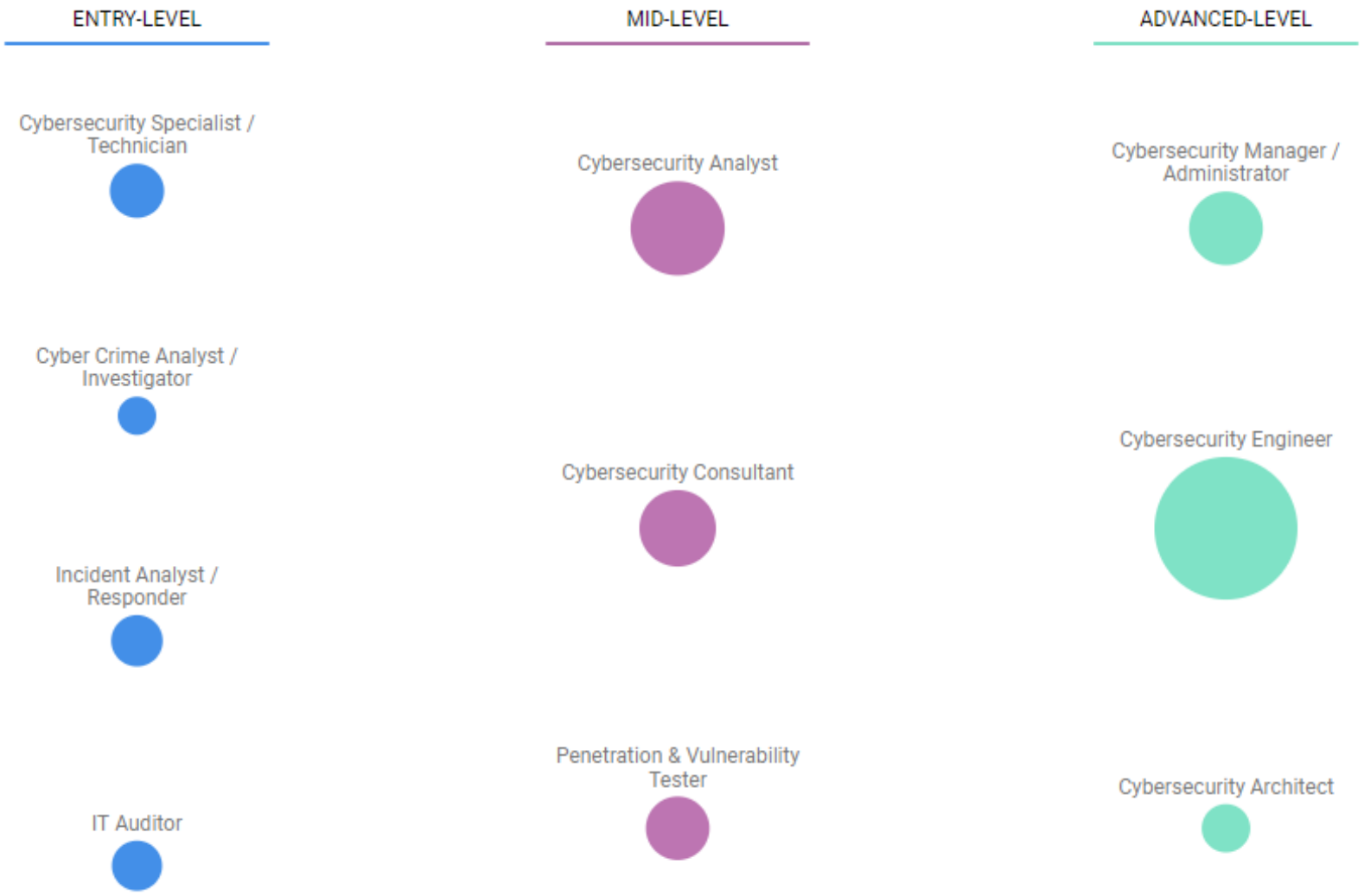
National average
1.0

TOP CYBERSECURITY JOB TITLES

- Cybersecurity Analyst
- Cybersecurity Consultant
- Cybersecurity Manager
- Software Developer
- Systems Engineer
- Network Engineer
- Penetration & Vulnerability Tester
- Cybersecurity Specialist
- Incident & Intrusion Analyst

https://www.cyberseek.org/heatmap.html

Example job types



http://www.cyberseek.org/pathway.html

Agenda

- ✓ Instructor
- ✓ Course overview
- ✓ Introduction
- ✓ Need for Cybersecurity Professionals