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 · 3 yrs 6 mos

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 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

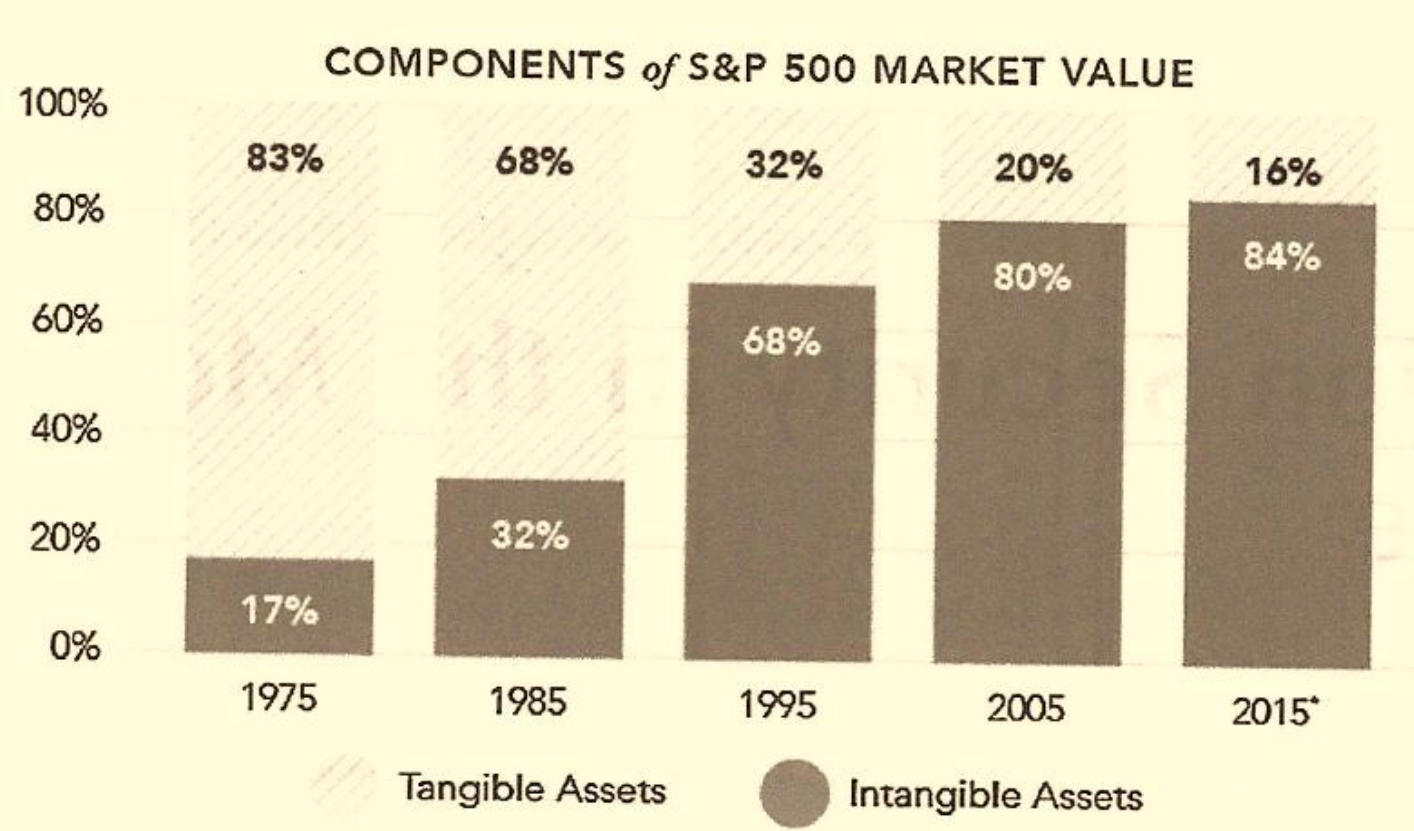


FIGURE 1.1 Change in public company assets from tangible to intangible.

"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

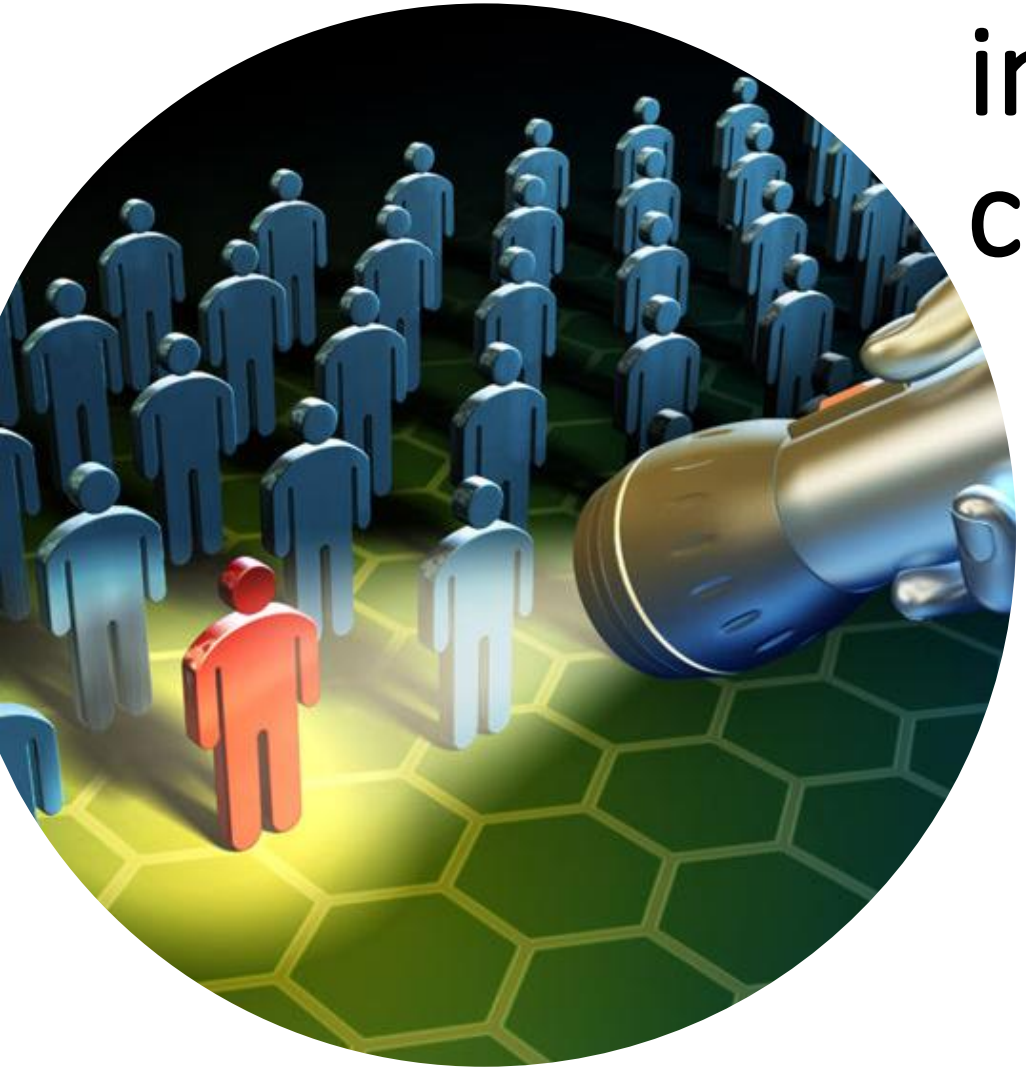
Guarding the photocopier

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:

- *Unauthorized 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?

Any thing that has the potential to lead to:

- ***Unauthorized access, use, disclosure***
- ***Modification***
- ***Disruption or Destruction***

of an enterprises' information

Physical

Technical

Administrative

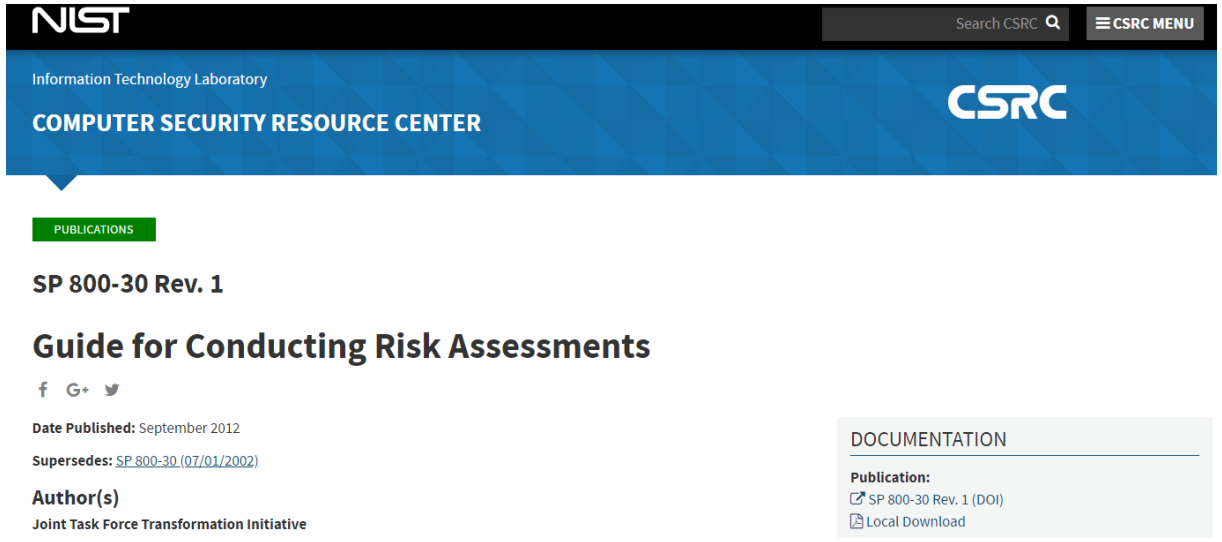
What is a threat…

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."

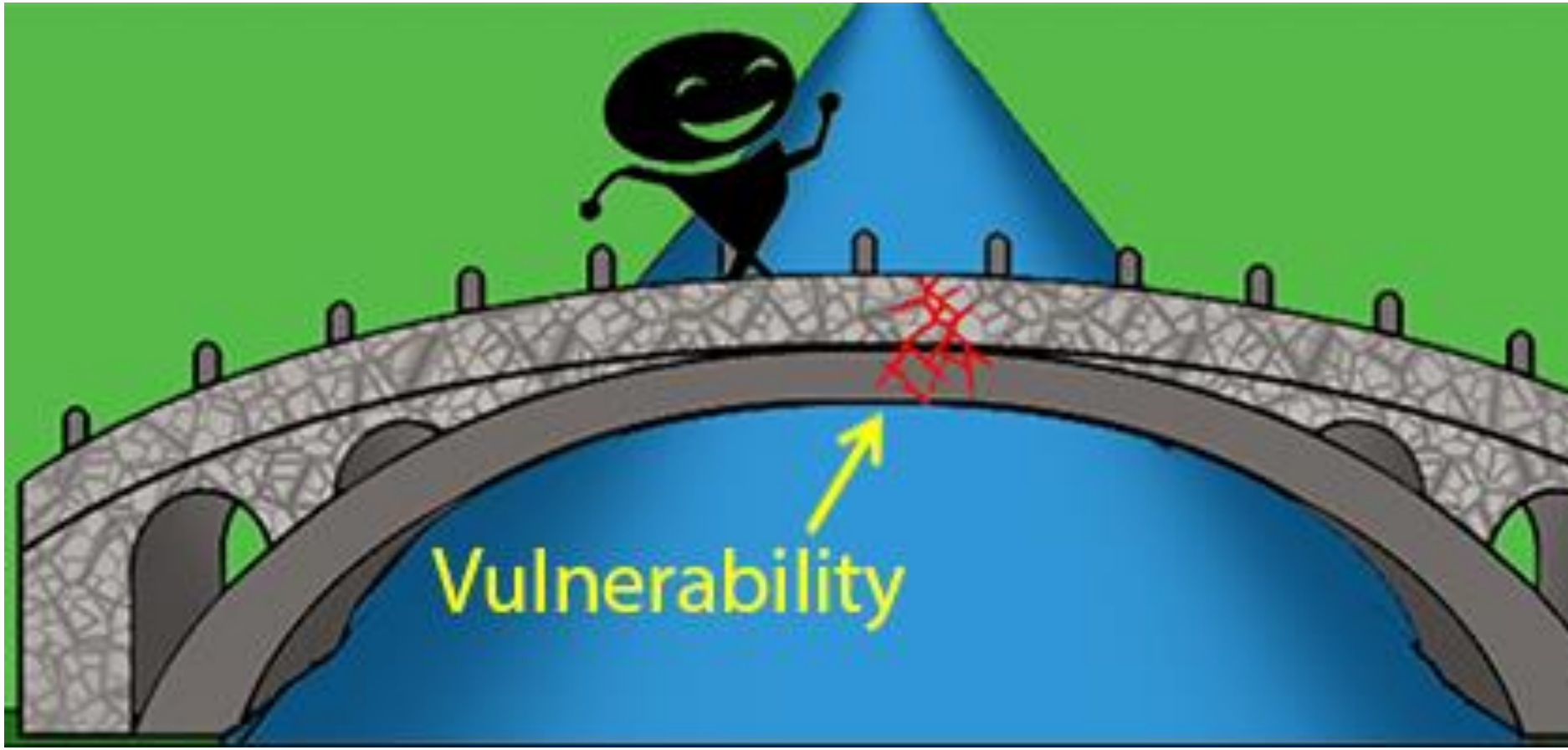
– Bruce Schneier

Type of Threat Source	Description	Characteristics

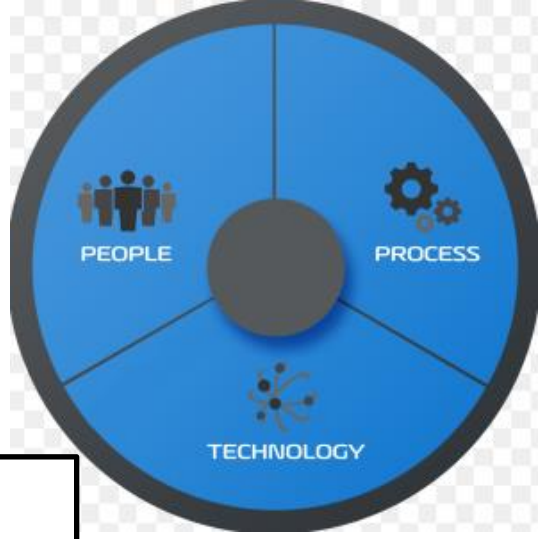
ADVERSARIAL
- Individual
  - Outsider
  - Insider
  - Trusted Insider
  - Privileged Insider
- Group
  - Ad hoc
  - Established
- Organization
  - Competitor
  - Supplier
  - Partner
  - Customer
- Nation-State
	Individuals, groups, organizations, or states that seek to exploit the organization's dependence 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

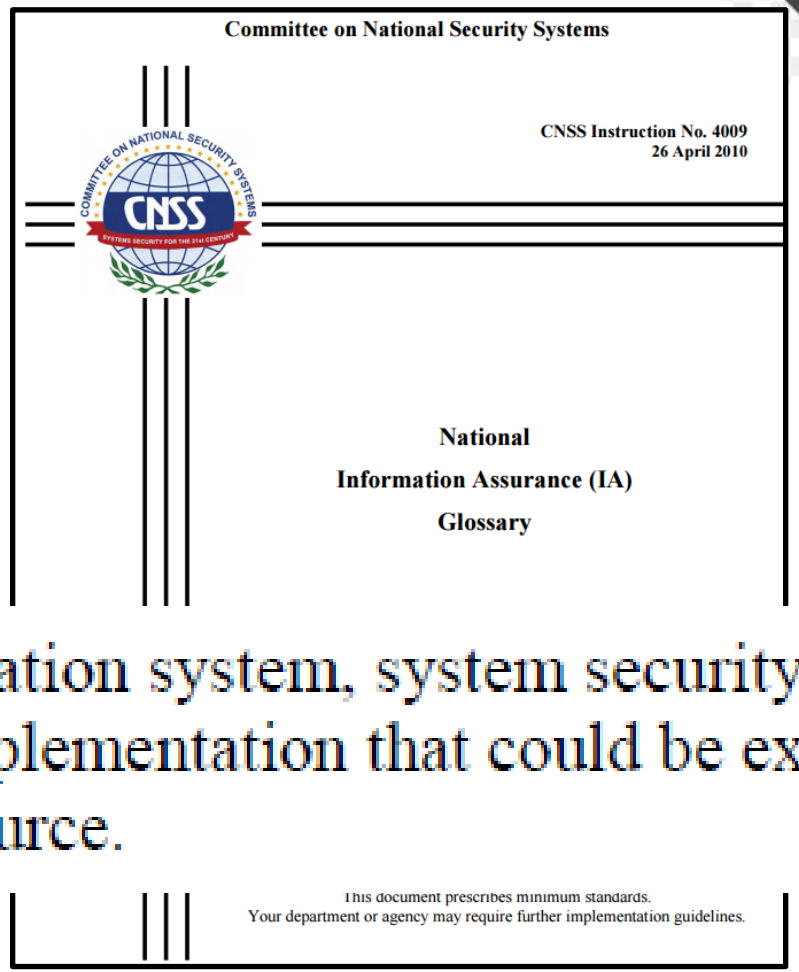
What is a Vulnerability?



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

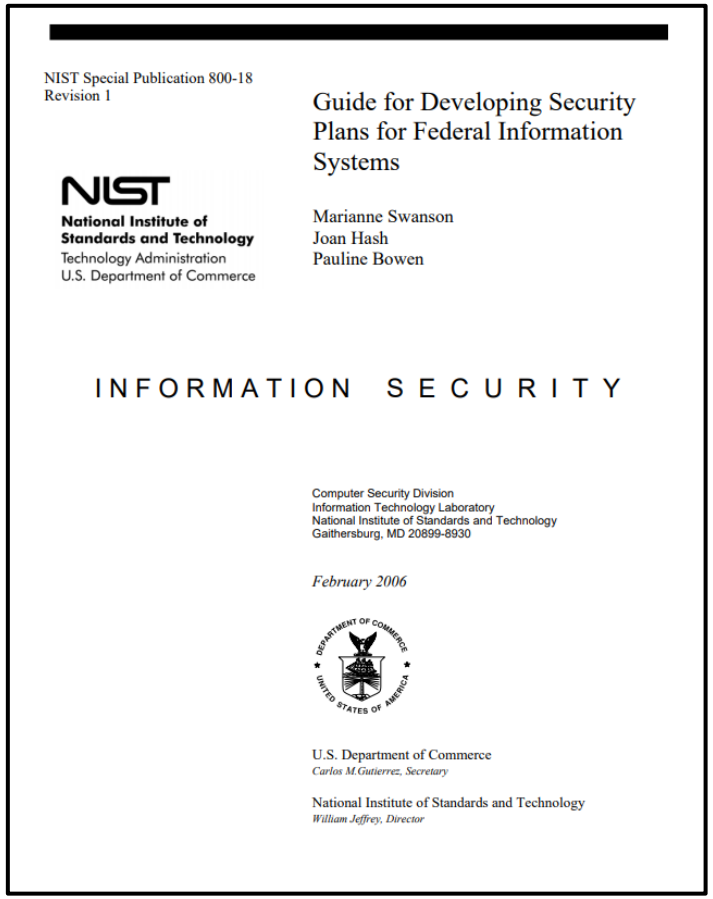
National
Information Assurance (IA)
Glossary

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

Marianne Swanson
Joan Hash
Pauline Bowen

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

INFORMATION SECURITY

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

February 2006

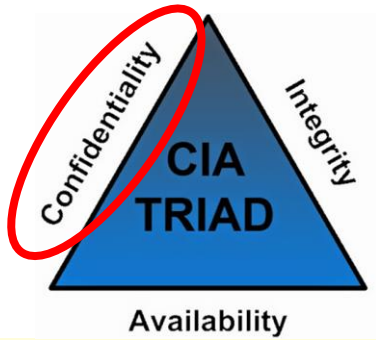
U.S. Department of Commerce
Carlos M.Gutierrez, Secretary

National Institute of Standards and Technology
William Jeffrey, Director

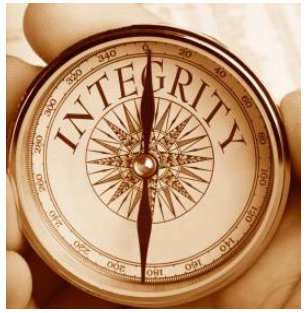
Cybersecurity Controls protect against impacts

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?

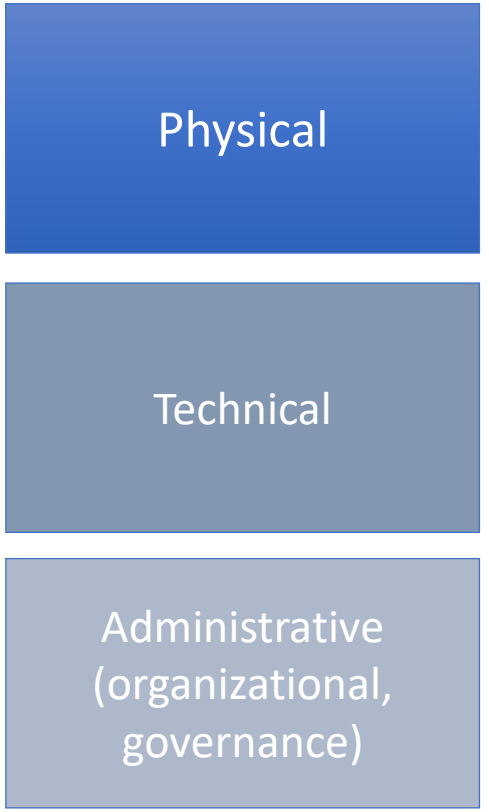
A measure of the potential impact of a threat resulting from an exploitation of a vulnerability

Potential loss resulting from unauthorized:

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

…of an enterprises' information

Can be expressed in quantitative and qualitative terms



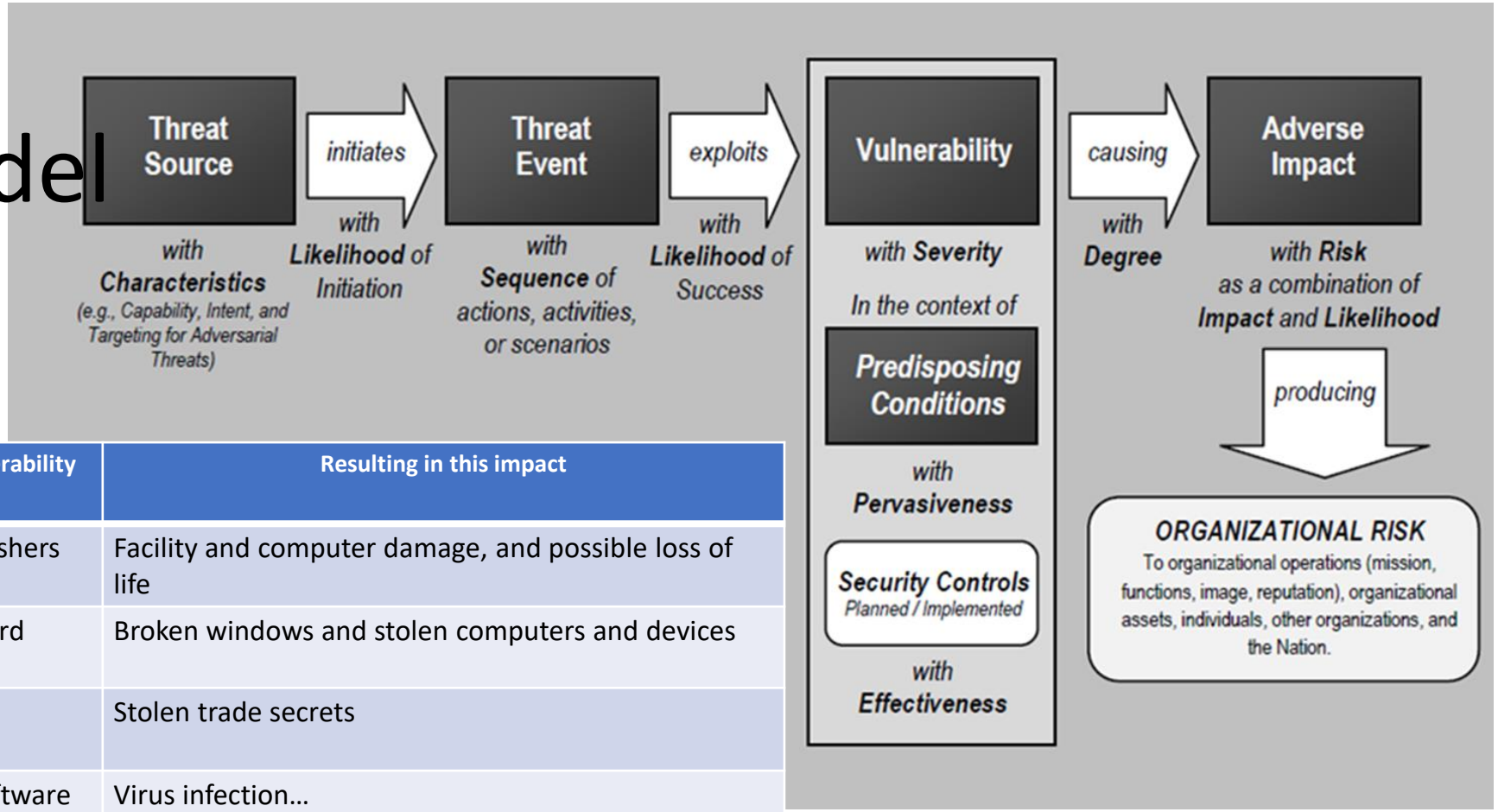
What are examples of Information security risks ?

- 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

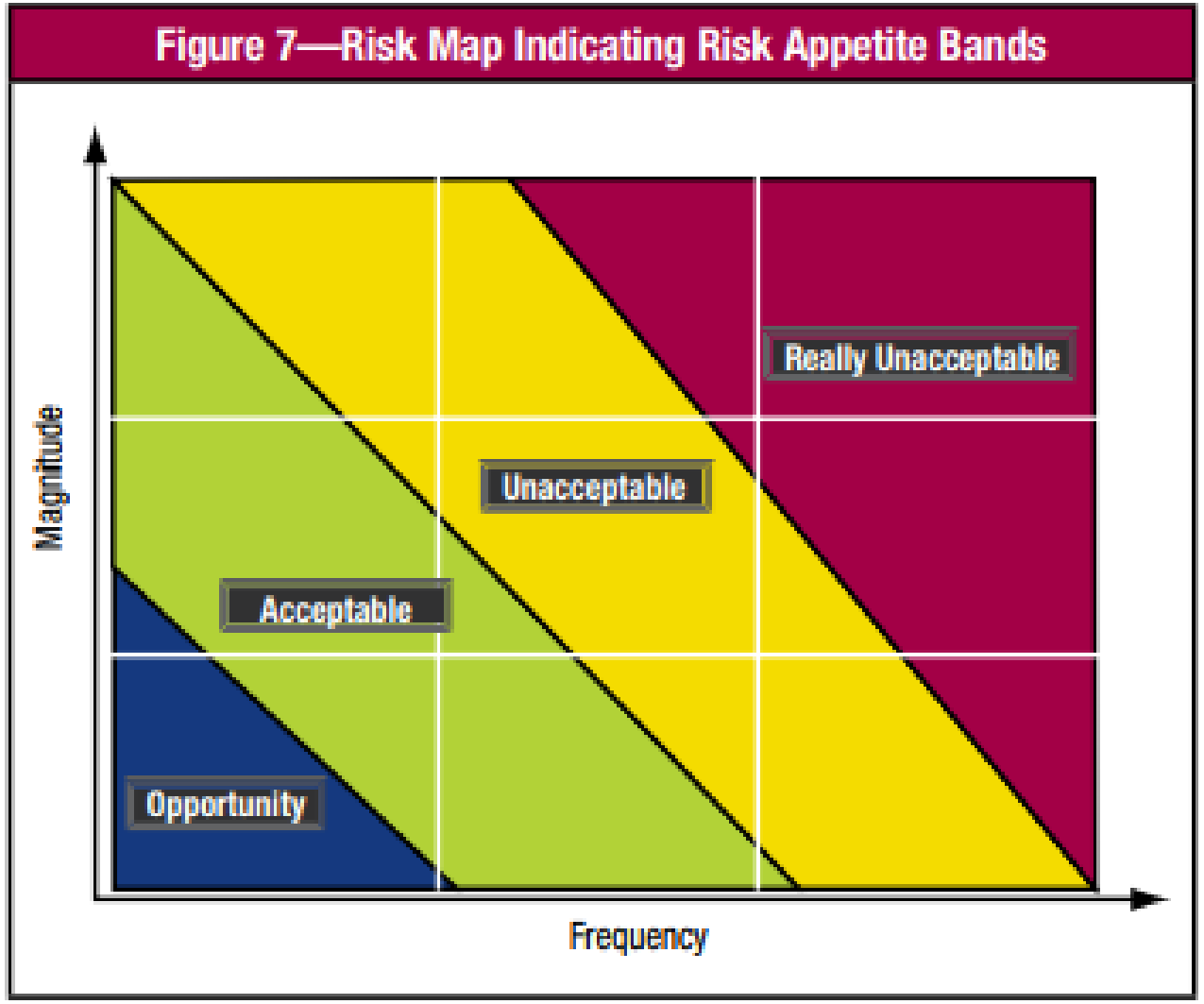
×

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…

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).

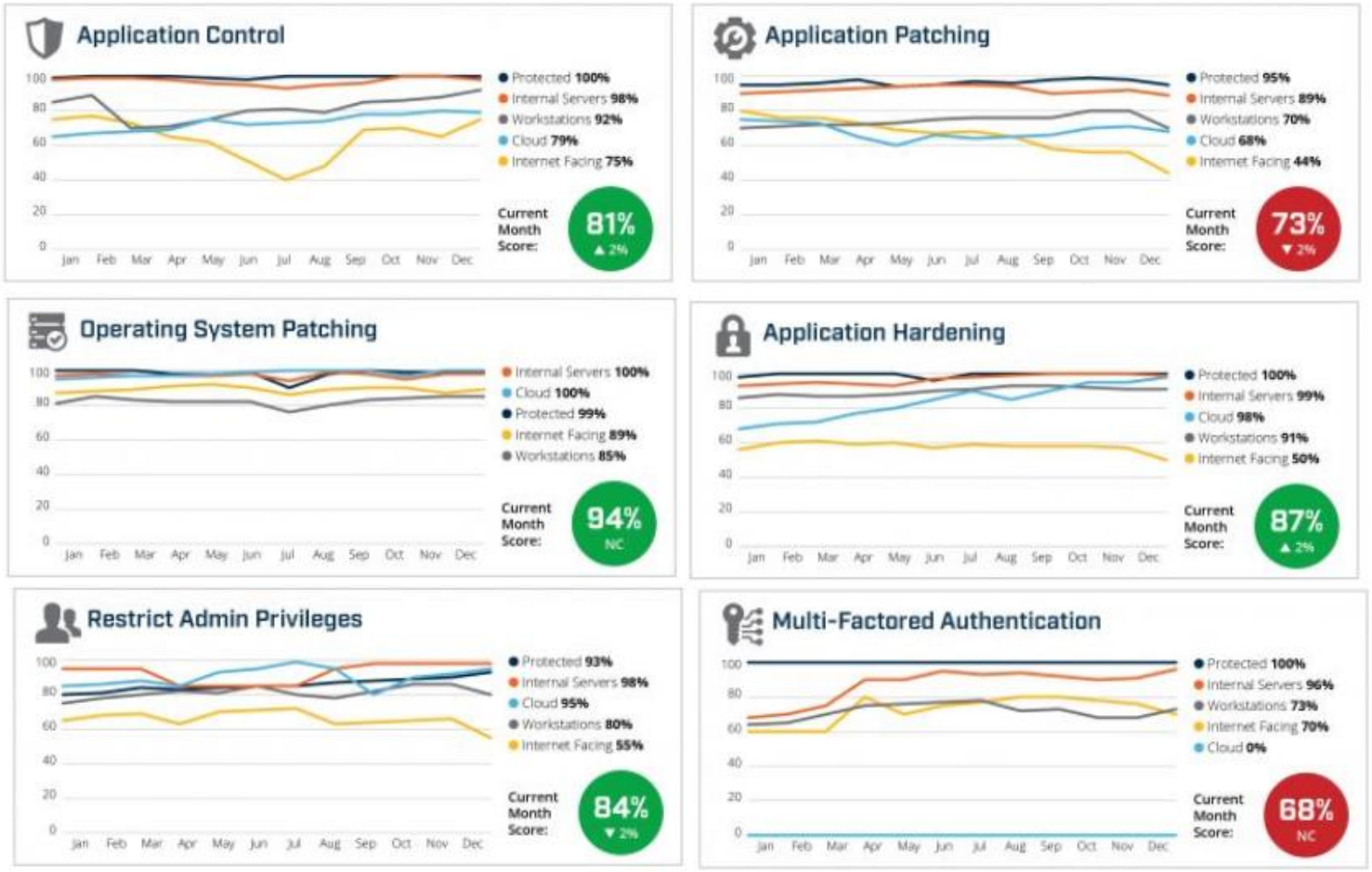
Penetration testing attempts to duplicate the actions of adversaries in carrying out hostile cyber attacks against organizations and provides a more in-depth analysis of security-related weaknesses/deficiencies.”

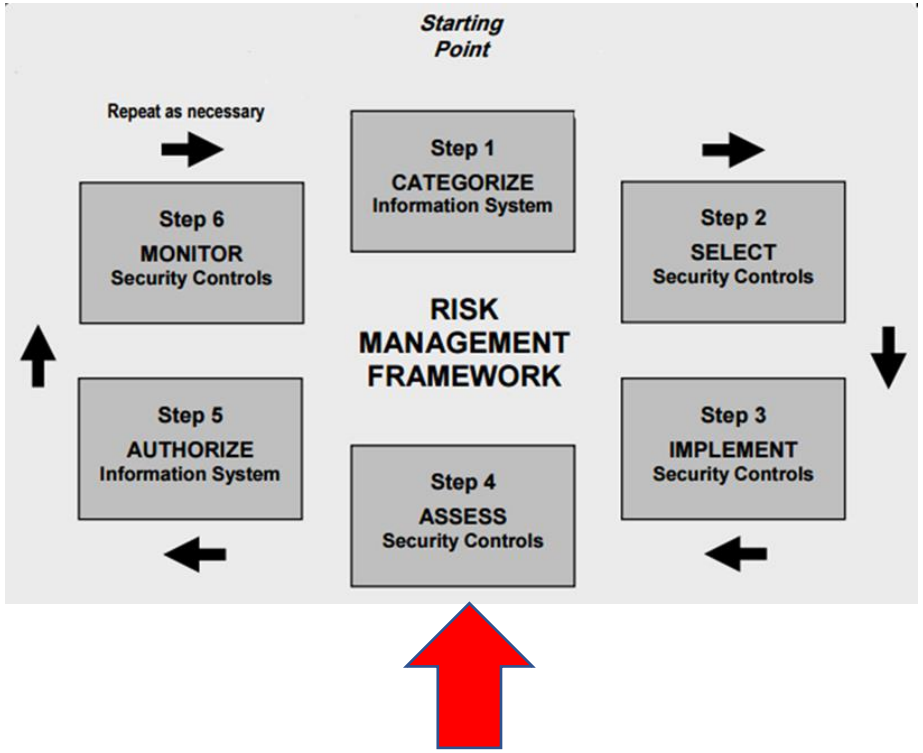
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

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

Risk Assessment and Mitigation Recommendations

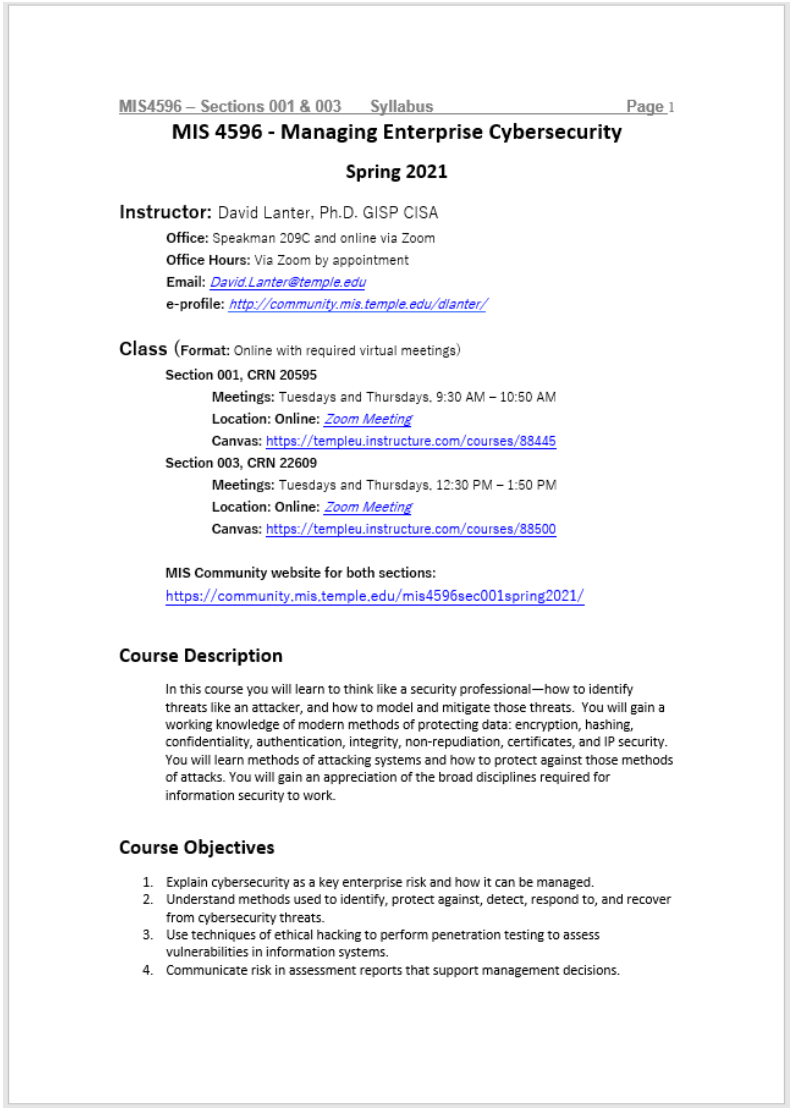




Agenda

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

Syllabus and Course website (001 & 003)



MIS4596 – Sections 001 & 003 Syllabus Page 1

MIS 4596 - Managing Enterprise Cybersecurity

Spring 2021

Instructor: David Lanter, Ph.D. GISP CISA

Office: Speakman 209C and online via Zoom
Office Hours: Via Zoom by appointment
Email: David.Lanter@temple.edu
e-profile: http://community.mis.temple.edu/dlanter/

Class (**Format:** Online with required virtual meetings)

Section 001, CRN 20595
Meetings: Tuesdays and Thursdays, 9:30 AM – 10:50 AM
Location: Online: Zoom Meeting
Canvas: https://templeu.instructure.com/courses/88445

Section 003, CRN 22609
Meetings: Tuesdays and Thursdays, 12:30 PM – 1:50 PM
Location: Online: Zoom Meeting
Canvas: https://templeu.instructure.com/courses/88500

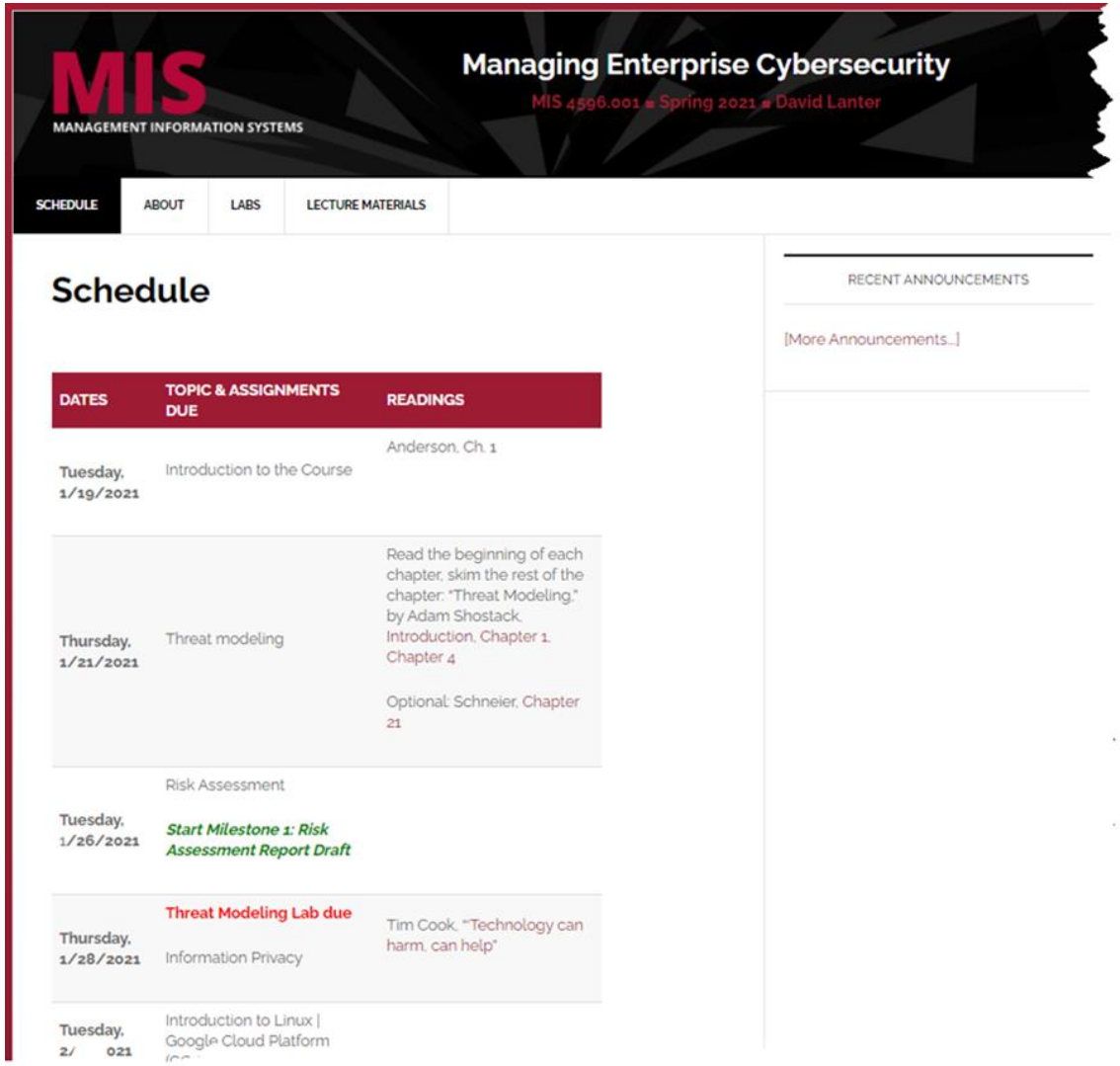
MIS Community website for both sections:
https://community.mis.temple.edu/mis4596sec001spring2021/

Course Description

In this course you will learn to think like a security professional—how to identify threats like an attacker, and how to model and mitigate those threats. You will gain a working knowledge of modern methods of protecting data: encryption, hashing, confidentiality, authentication, integrity, non-repudiation, certificates, and IP security. You will learn methods of attacking systems and how to protect against those methods of attacks. You will gain an appreciation of the broad disciplines required for information security to work.

Course Objectives

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



MIS
MANAGEMENT INFORMATION SYSTEMS

Managing Enterprise Cybersecurity
MIS 4596.001 ■ Spring 2021 ■ David Lanter

SCHEDULE | ABOUT | LABS | LECTURE MATERIALS

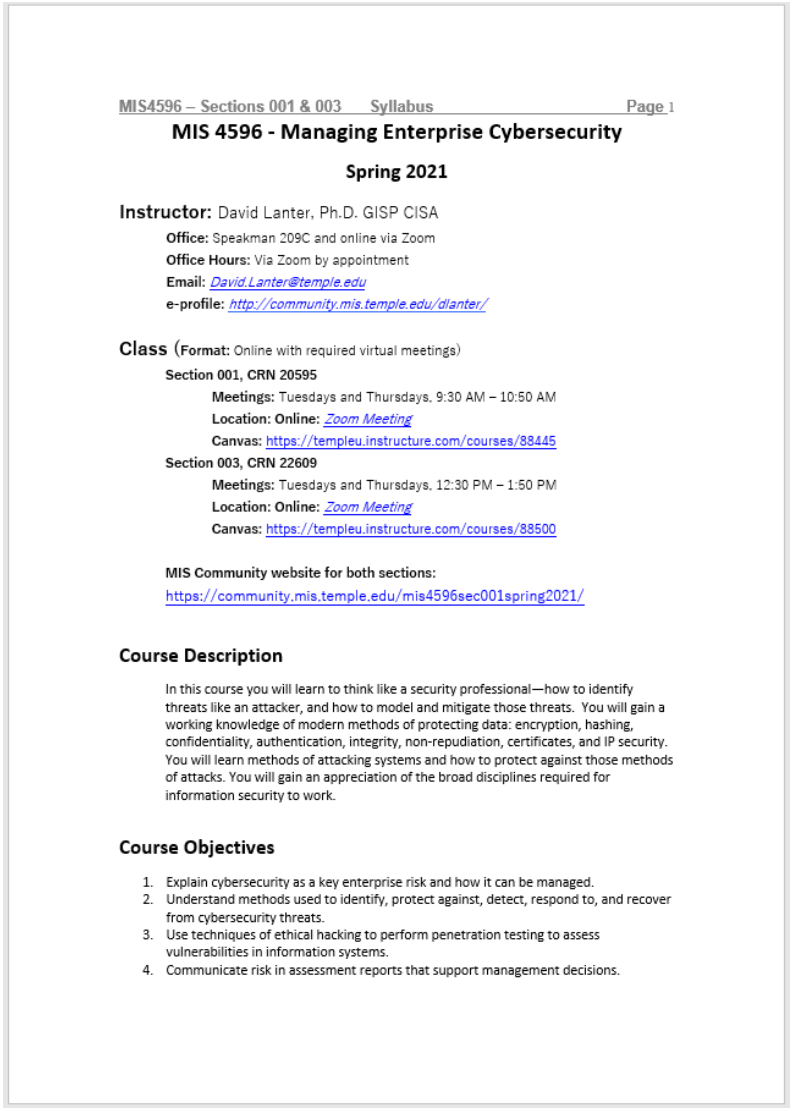
Schedule

DATES	TOPIC & ASSIGNMENTS DUE	READINGS
Tuesday, 1/19/2021	Introduction to the Course	Anderson, Ch. 1
Thursday, 1/21/2021	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, 1/26/2021	Risk Assessment ***Start Milestone 1: Risk Assessment Report Draft***	
Thursday, 1/28/2021	**Threat Modeling Lab due** Information Privacy	Tim Cook, "Technology can harm, can help"
Tuesday, 2/ 021	Introduction to Linux | Google Cloud Platform	

RECENT ANNOUNCEMENTS

[More Announcements...]

Syllabus and Course website (001 & 003)



MIS4596 – Sections 001 & 003 Syllabus Page 1

MIS 4596 - Managing Enterprise Cybersecurity

Spring 2021

Instructor: David Lanter, Ph.D. GISP CISA

Office: Speakman 209C and online via Zoom
Office Hours: Via Zoom by appointment
Email: David.Lanter@temple.edu
e-profile: http://community.mis.temple.edu/dlanter/

Class (**Format:** Online with required virtual meetings)

Section 001, CRN 20595
Meetings: Tuesdays and Thursdays, 9:30 AM – 10:50 AM
Location: Online: Zoom Meeting
Canvas: https://templeu.instructure.com/courses/88445

Section 003, CRN 22609
Meetings: Tuesdays and Thursdays, 12:30 PM – 1:50 PM
Location: Online: Zoom Meeting
Canvas: https://templeu.instructure.com/courses/88500

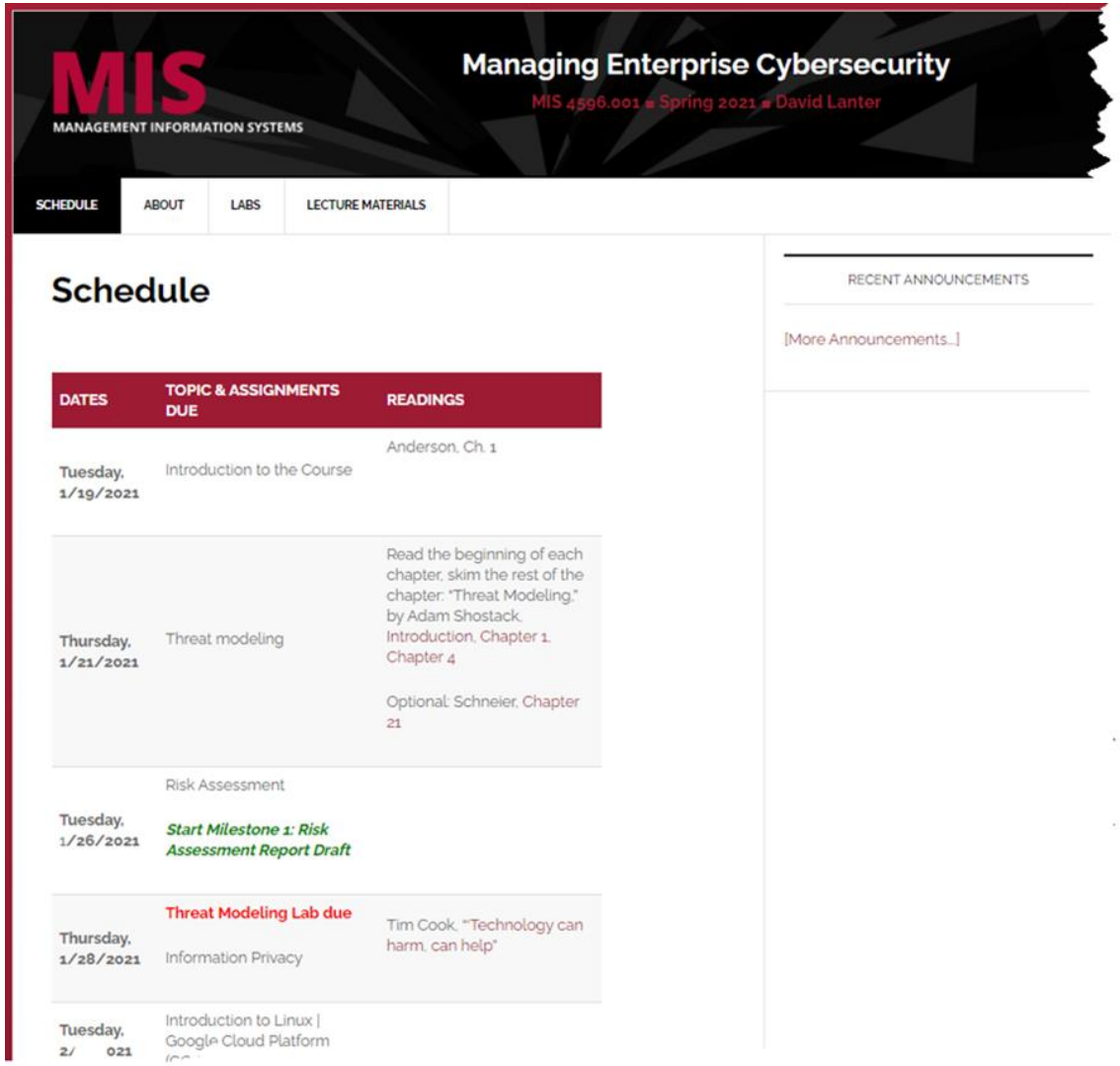
MIS Community website for both sections:
https://community.mis.temple.edu/mis4596sec001spring2021/

Course Description

In this course you will learn to think like a security professional—how to identify threats like an attacker, and how to model and mitigate those threats. You will gain a working knowledge of modern methods of protecting data: encryption, hashing, confidentiality, authentication, integrity, non-repudiation, certificates, and IP security. You will learn methods of attacking systems and how to protect against those methods of attacks. You will gain an appreciation of the broad disciplines required for information security to work.

Course Objectives

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



MIS
MANAGEMENT INFORMATION SYSTEMS

Managing Enterprise Cybersecurity
MIS 4596.001 ■ Spring 2021 ■ David Lanter

SCHEDULE | ABOUT | LABS | LECTURE MATERIALS

Schedule

DATES	TOPIC & ASSIGNMENTS DUE	READINGS
Tuesday, 1/19/2021	Introduction to the Course	Anderson, Ch. 1
Thursday, 1/21/2021	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, 1/26/2021	Risk Assessment ***Start Milestone 1: Risk Assessment Report Draft***	
Thursday, 1/28/2021	**Threat Modeling Lab due** Information Privacy	Tim Cook, "Technology can harm, can help"
Tuesday, 2/ 021	Introduction to Linux | Google Cloud Platform	

RECENT ANNOUNCEMENTS

[More Announcements...]

Schedule (see MIS Community website for Lab due dates)

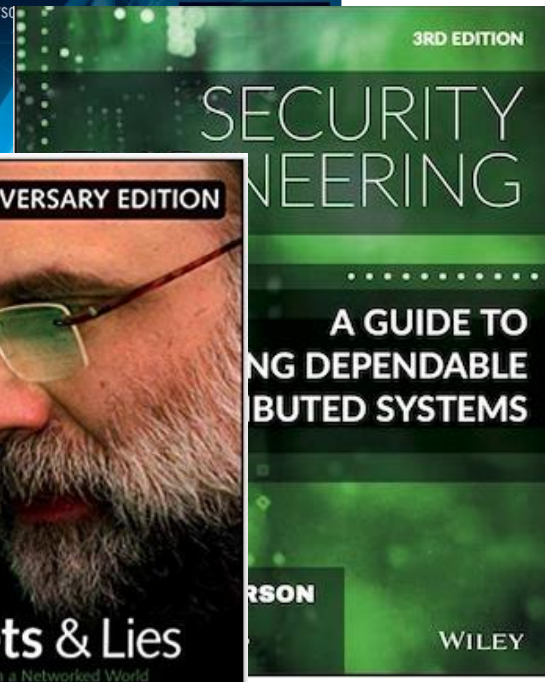
Week	Topics
1	Introduction to the Course Threat Modeling
2	Risk Assessment Information Privacy
3	Introduction to Linux and Google Cloud Platform Information Security in Organizations
4	Introduction to Cryptography Symmetric Cryptography
5	Asymmetric Cryptography Digital Certificates and Public Key Infrastructures
6	Wellness Day – No class Authentication and Passwords
7	Password Cracking Introduction to Networking
8	Vulnerability Scanning Vulnerability Exploitation
9	Vulnerability Exploitation continued Milestone group workday
10	Physical Security Human Elements of Security
11	Network Security Monitoring Incident Response
12	Respond Case Study - Equifax Milestone group workday
13	Malware Analysis Recovery Case Study – Maersk
14	Group workday Course Wrap up

Other Key Dates and Deadlines (subject to change)

Tue, Jan 26	Milestone 1 starts
Sat, Feb 13	Deadline for Milestone 1
Sat, Feb 27	Deadline for Milestone 2
Tue, Mar 9	Mid-term exam opens
Wed, Mar 17	Deadline for mid-term exam
Thu, Mar 18	Milestone 3 starts
Sat, Apr 10	Deadline for Milestone 3
Mon, Apr 26	Deadline for Milestone 4
Tue, Apr 29	Final exam opens
Wed, May 4	Deadline for the final exam

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

Course materials – readings…



Readings

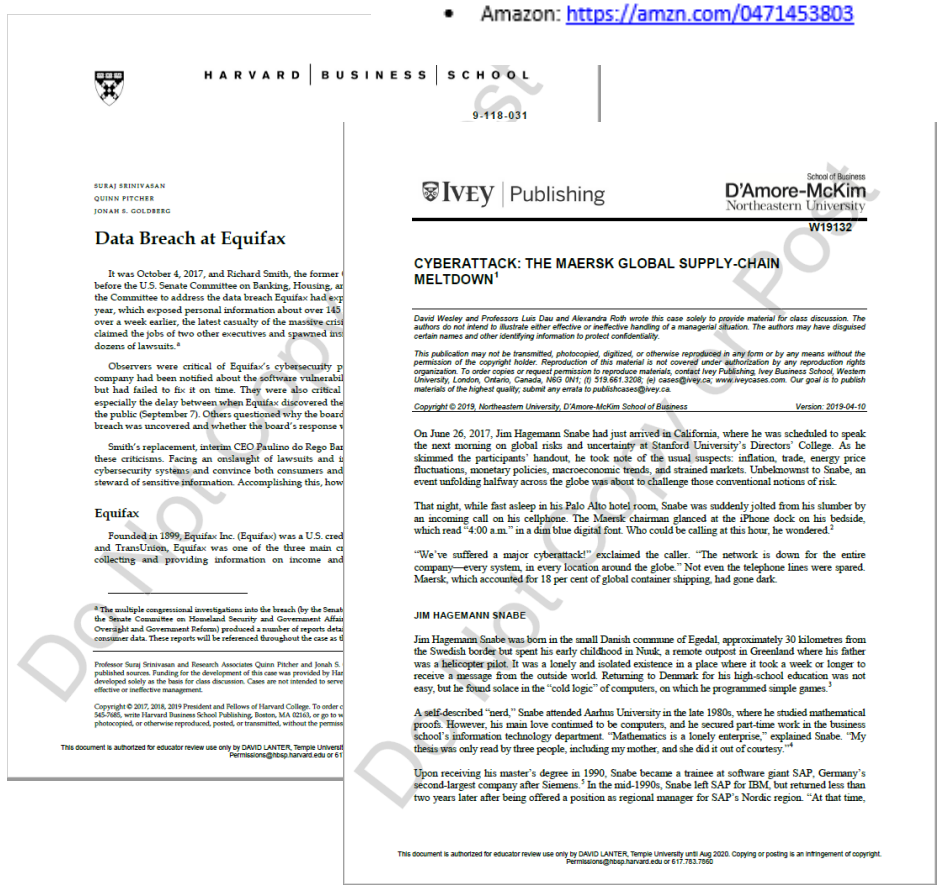
Required Textbook: Security Engineering: A Guide to Building Dependable Distributed Systems 2nd Edition, by Ross Anderson.

- Free PDF of the book: http://www.cl.cam.ac.uk/~rja14/book.html
- Amazon: http://a.co/9bzf6zP

Required Case Studies: Two business cases are available as a course pack for purchase from Harvard Business Publishing available for $8.50 here: https://hbsp.harvard.edu/import/787157

Optional Textbook: "Secrets and Lies: Digital Security in a Networked World," by Bruce Schneier.

- Available online via Temple Library: https://goo.gl/ty5y2Z
- Amazon: https://amzn.com/0471453803


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, a
the Committee to address the data breach Equifax had ex
year, which exposed personal information about over 145
over a week earlier, the latest casualty of the massive cris
claimed the jobs of two other executives and spawned ins
dozens of lawsuits.[4]

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

[4] The multiple congressional investigations into the breach (by the Senat
the Senate Committee on Homeland Security and Government Affair
Oversight and Government Reform) produced a number of reports deta
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.

Copyright © 2017, 2018, 2019 President and Fellows of Harvard College. To order c
545-7685, write Harvard Business School Publishing, Boston, MA 02163, or go to w
photocopied, or otherwise reproduced, posted, or transmitted, without the permiss

This document is authorized for educator review use only by DAVID LANTER, Temple Universit
Permissions@hbsp.harvard.edu or 61

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.

This publication may not be transmitted, photocopied, digitized, or otherwise reproduced in any form or by any means without the permission of the copyright holder. Reproduction of this material is not covered under authorization by any reproduction rights organization. To order copies or request permission to reproduce materials, contact Ivey Publishing, Ivey Business School, Western University, London, Ontario, Canada, N6G 0N1; (t) 519.661.3208; (e) cases@ivey.ca; www.iveycases.com. Our goal is to publish materials of the highest quality; submit any errata to publishcases@ivey.ca.

Copyright © 2019, Northeastern University, D'Amore-McKim School of Business *Version: 2019-04-10*

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

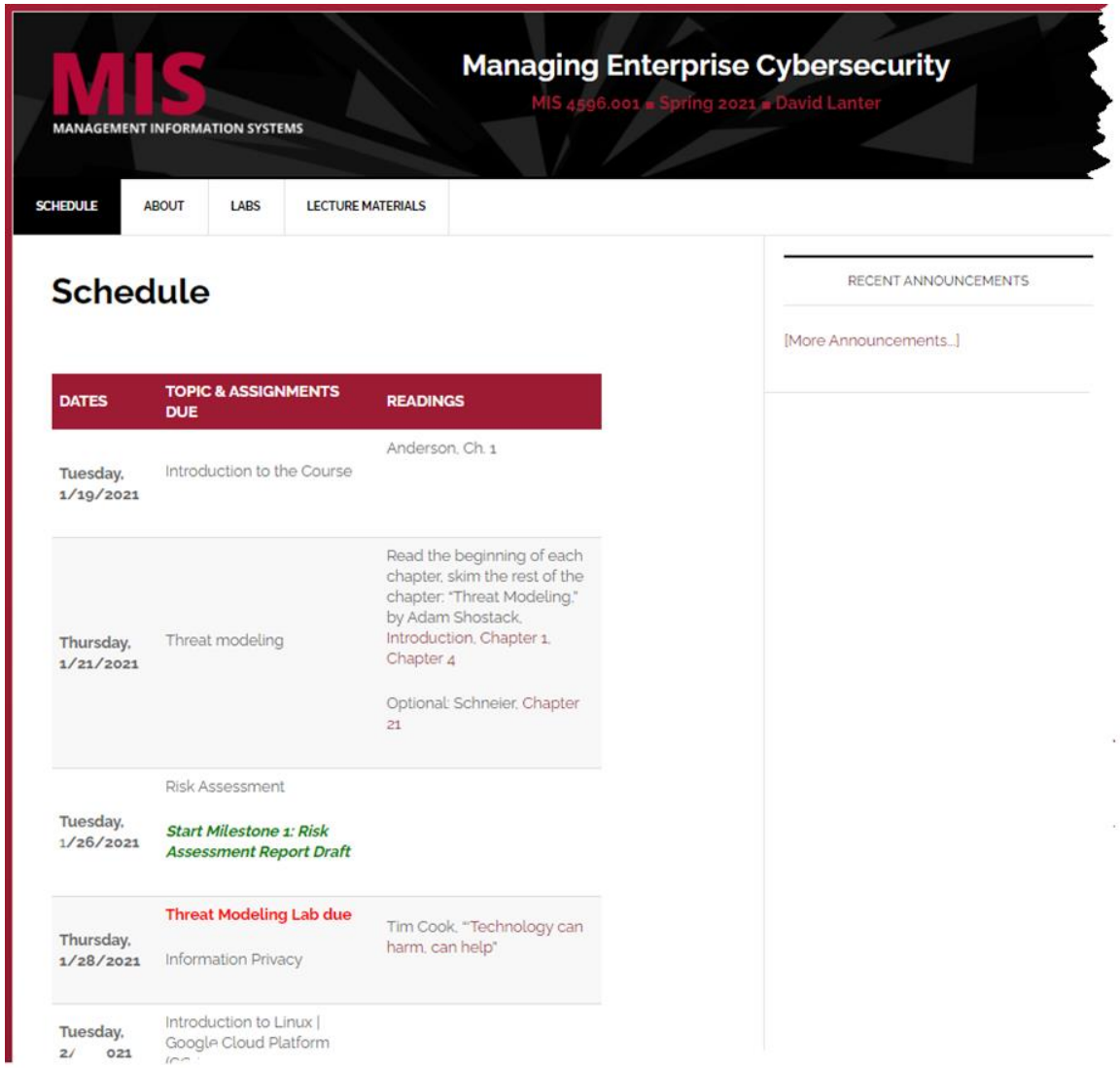
Jim Hagemann Snabe was born in the small Danish commune of Egedal, approximately 30 kilometres from the Swedish border but spent his early childhood in Nuuk, a remote outpost in Greenland where his father was a helicopter pilot. It was a lonely and isolated existence in a place where it took a week or 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]

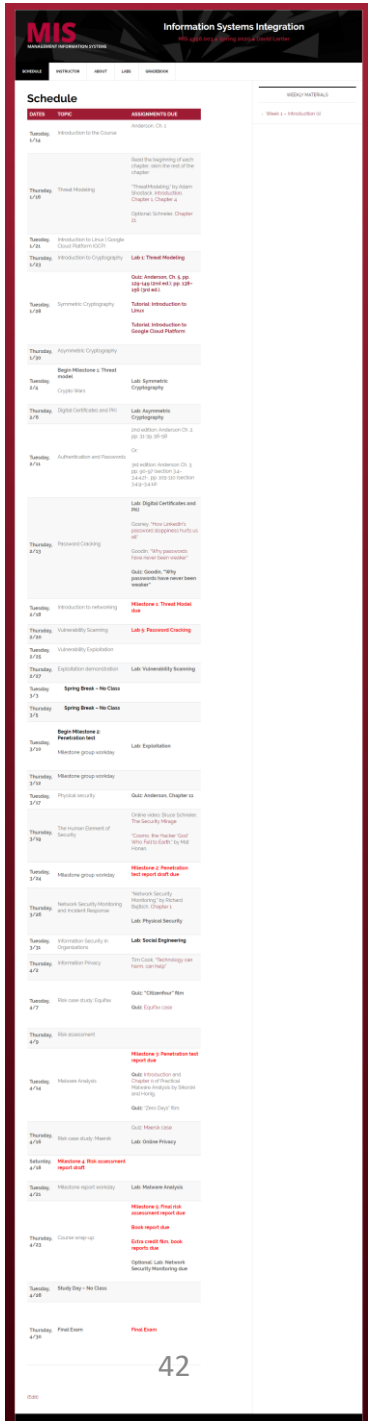
Upon receiving his master's degree in 1990, Snabe became a trainee at software giant SAP, Germany's second-largest company after Siemens.[5] In the mid-1990s, Snabe left SAP for IBM, but returned less than two years later after being offered a position as regional manager for SAP's Nordic region. "At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

This document is authorized for educator review use only by DAVID LANTER, Temple University until Aug 2020. Copying or posting is an infringement of copyright. Permissions@hbsp.harvard.edu or 617.783.7860

Course materials – schedule…



DATES	TOPIC & ASSIGNMENTS DUE	READINGS
Tuesday, 1/19/2021	Introduction to the Course	Anderson, Ch. 1
Thursday, 1/21/2021	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, 1/26/2021	Risk Assessment ***Start Milestone 1: Risk Assessment Report Draft***	
Thursday, 1/28/2021	**Threat Modeling Lab due** Information Privacy	Tim Cook, "'Technology can harm, can help"
Tuesday, 2/2/2021	Introduction to Linux | Google Cloud Platform (GCP)	
Thursday, 2/4/2021	**Web Privacy and Anonymity Lab due** Information Security in Organizations	
Tuesday, 2/9/2021	**Introduction to Google Cloud Platform and Linux Tutorial Lab due** Introduction to Cryptography	



Grading

Item	Weight
Milestones	40%
Labs	20%
Midterm Exam	15%
Final Exam	20%
Participation	5%
	100%

Grading Scale			
93 – 100	A	73 – 76	C
90 – 92	A-	70 – 72	C-
87 – 89	B+	67 – 69	D+
83 – 86	B	63 – 66	D
80 – 82	B-	60 – 62	D-
77 – 79	C+	Below 60	F

Grading…

Category	Points	Weight
Milestone 1: Risk Assessment Draft	50	5%
Milestone 2: Final Risk Assessment Report	50	5%
Milestone 3: Penetration test report draft	100	10%
Milestone 4: Penetration test draft with mitigations	200	20%
Labs	200	20%
Midterm Exam	150	15%
Final Exam	200	20%
Participation	50	5%

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 (5%) Create a draft risk assessment report for a financial management system.

Milestone 2: Final Risk Assessment Report (5%) Incorporate feedback from the instructor on the draft and improve and submit your final version of the report.

Milestone 3: Penetration Test Report draft (10%) 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 (20%) 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…

Category	Points	Weight
Labs	200	20%

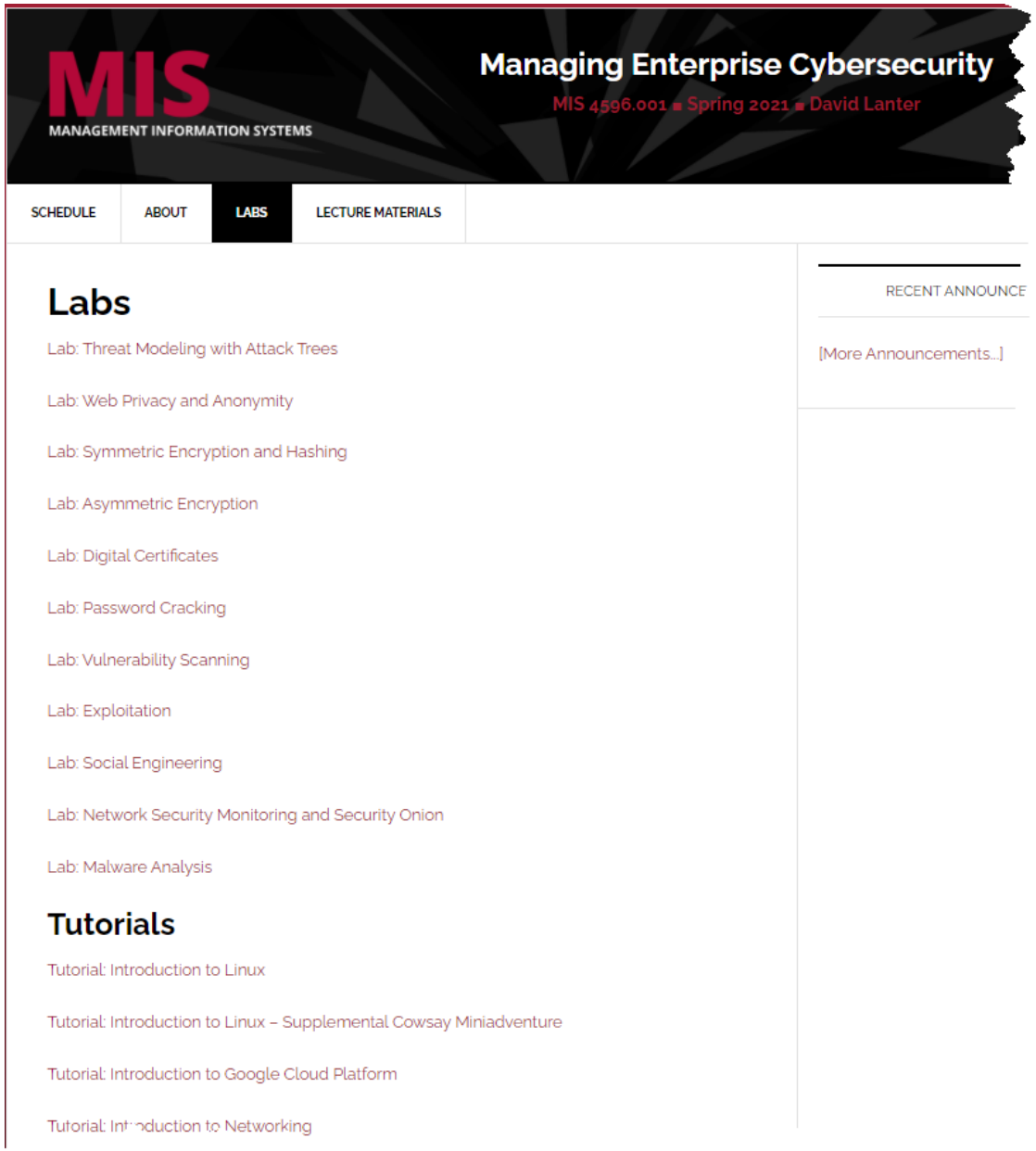
Labs

Labs are hands-on learning activities introduced in class and completed outside of class. Labs are typically due one and a half weeks after they are introduced.

There are 12 labs. However, only your top 9 highest lab scores will be counted toward your lab grade.

Technology Requirements

Google Cloud Platform (GCP): This course uses Google Cloud Platform (GCP) to run tools and virtual machines necessary to complete assignments. New accounts on GCP receive a $300 credit. You should be able to complete this class without going over that cost. I will have you launch a virtual machine instance on GCP from which you can complete class assignments. You will be able to remotely connect to your instance using Chrome Remote Desktop, which works just like a browser tab.



Exams

Take home open book midterm and final exams

- Midterm exam opens 3/9 and is due 3/17
- Cumulative final exam open 4/29 and is due 5/4

Category	Points	Weight
Midterm Exam	150	15%
Final Exam	200	20%

Certification Option: 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 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 April 22.

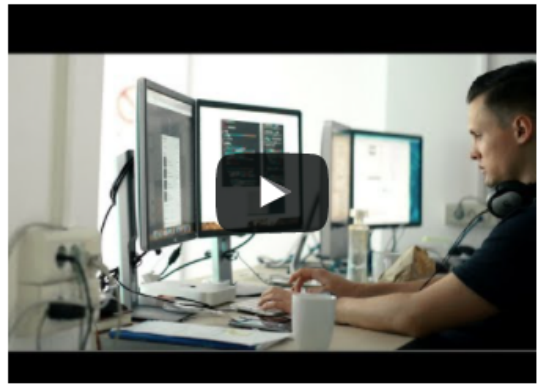
Agenda

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

Information Security Analysts

Summary

Quick Facts: Information Security Analysts	
2019 Median Pay	$99,730 per year $47.95 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



What Information Security Analysts Do

Information security analysts plan and carry out security measures to protect an organization's computer networks and systems.

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 [illegible] May [illegible]

CYBERSECURITY SUPPLY/DEMAND HEAT MAP

All

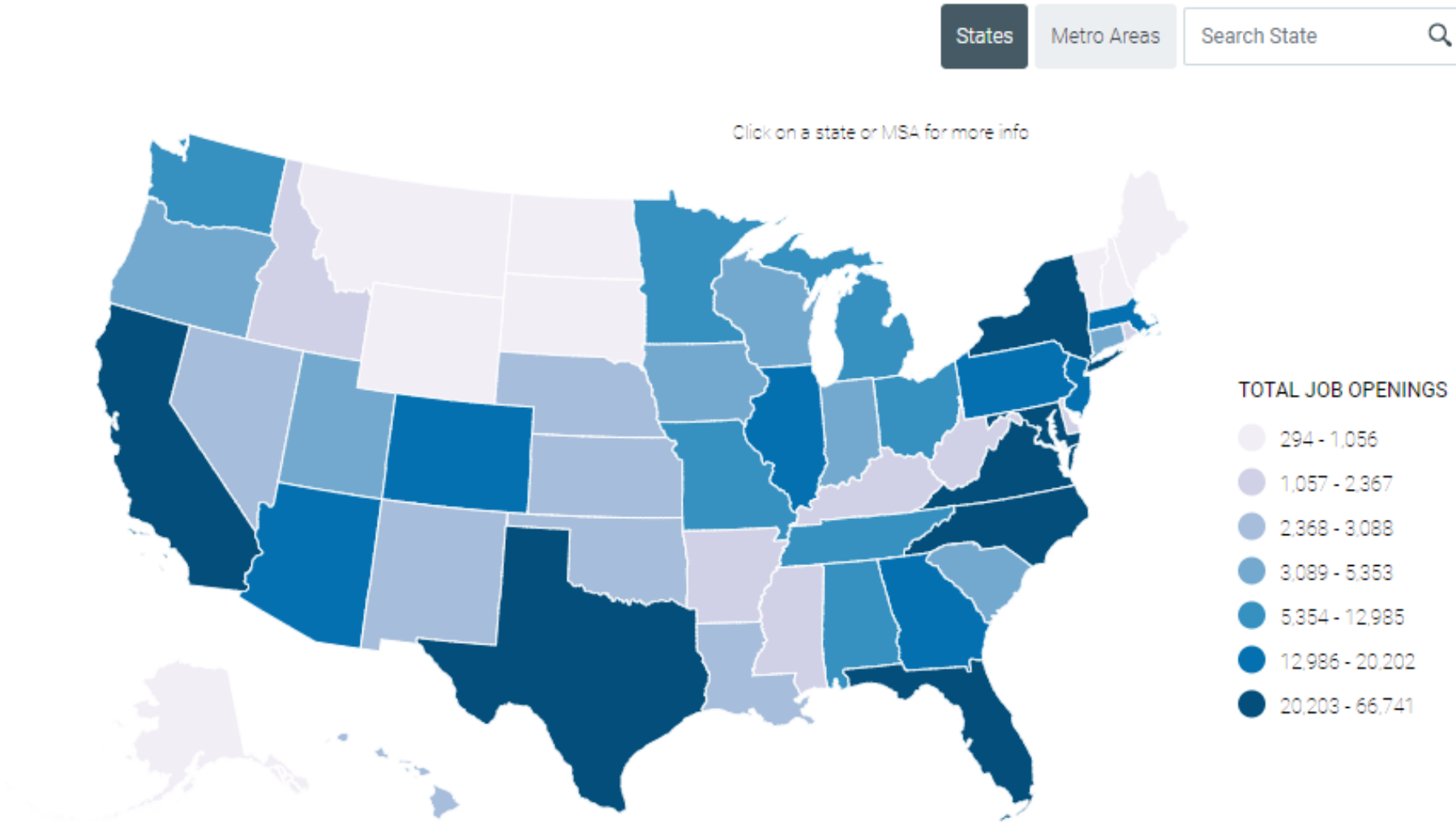
Public Sector Data

Private Sector...

Total job openings

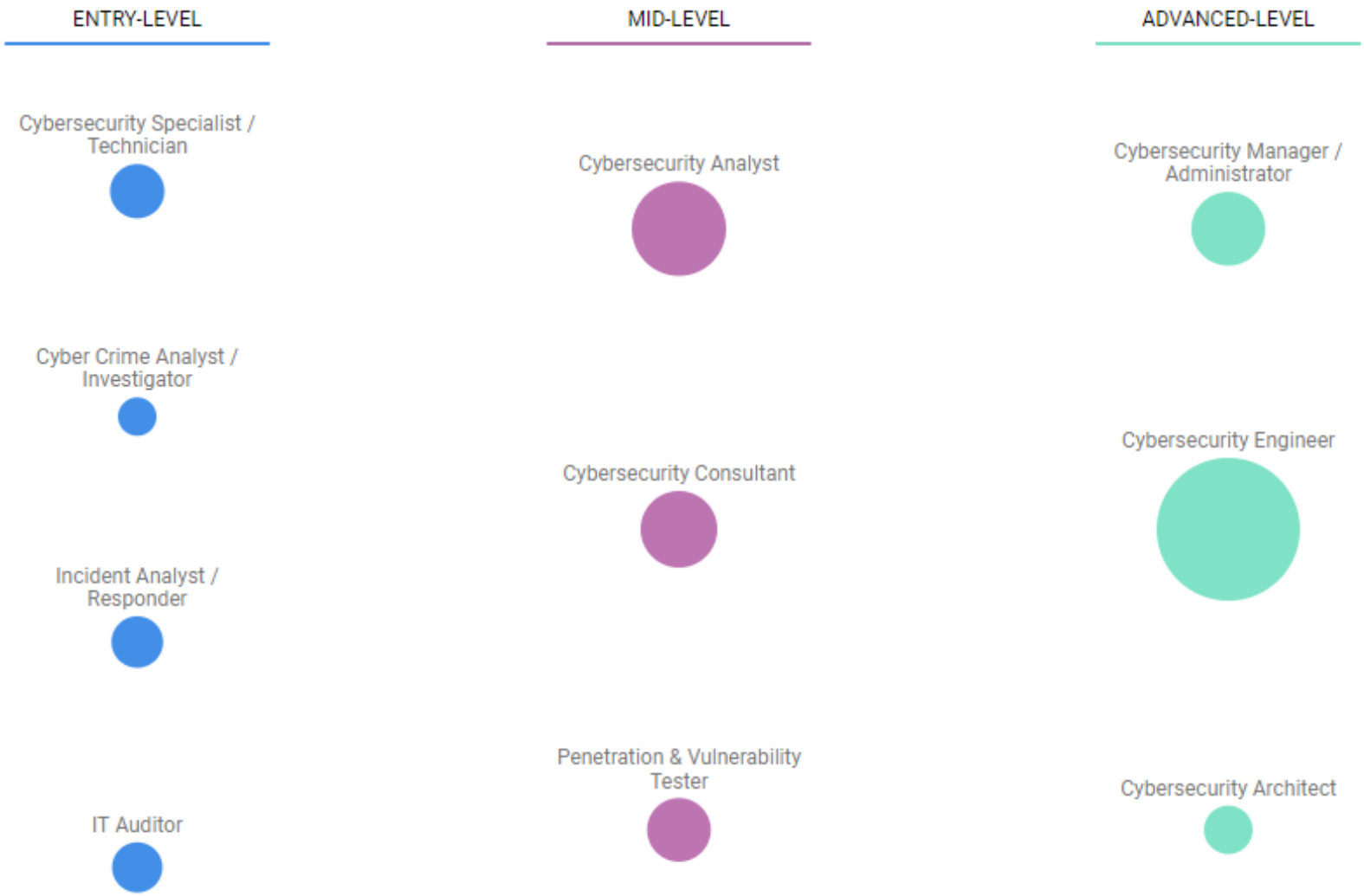
Cybersecurity talent gaps exist across the country. Closing these gaps requires detailed knowledge of the cybersecurity workforce in your region. This interactive heat map provides a granular snapshot of demand and supply data for cybersecurity jobs at the state and metro area levels, and can be used to grasp the challenges and opportunities facing your local cybersecurity workforce.

Share



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

Example job types



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

Agenda

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