

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

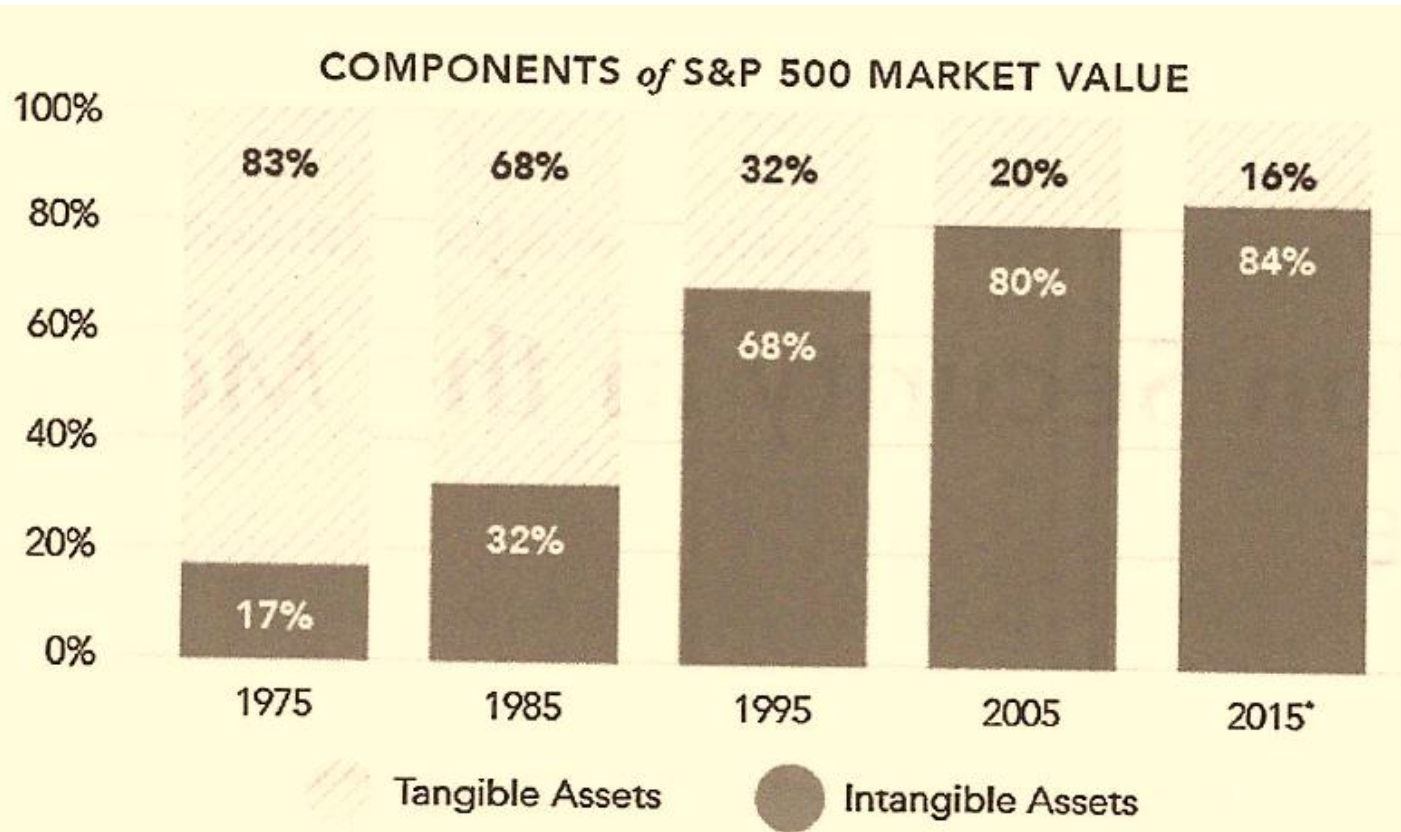


FIGURE 1.1 Change in public company assets from tangible to intangible.

“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”

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*
- Unauthorized modification of information*
- Disruption and destruction of information*

Confidentiality
Integrity
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?

Anything that has the potential to lead to unauthorized:

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

of an enterprises' information or information systems

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

Type of Threat Source	Description	Characteristics
ADVERSARIAL <ul style="list-style-type: none"> - Individual <ul style="list-style-type: none"> - Outsider - Insider - Trusted Insider - Privileged Insider - Group <ul style="list-style-type: none"> - Ad hoc - Established - Organization <ul style="list-style-type: none"> - 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 <ul style="list-style-type: none"> - User - Privileged User/Administrator 	Erroneous actions taken by individuals in the course of executing their everyday responsibilities.	Range of effects
STRUCTURAL <ul style="list-style-type: none"> - Information Technology (IT) Equipment <ul style="list-style-type: none"> - Storage - Processing - Communications - Display - Sensor - Controller - Environmental Controls <ul style="list-style-type: none"> - Temperature/Humidity Controls - Power Supply - Software <ul style="list-style-type: none"> - 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 <ul style="list-style-type: none"> - Natural or man-made disaster <ul style="list-style-type: none"> - Fire - Flood/Tsunami - Windstorm/Tornado - Hurricane - Earthquake - Bombing - Overrun - Unusual Natural Event (e.g., sunspots) - Infrastructure Failure/Outage <ul style="list-style-type: none"> - 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

NIST
Search CSRC 🔍 CSRC MENU

Information Technology Laboratory
CSRC

COMPUTER SECURITY RESOURCE CENTER

PUBLICATIONS

SP 800-30 Rev. 1

Guide for Conducting Risk Assessments

f G+ t

Date Published: September 2012

Supersedes: [SP 800-30 \(07/01/2002\)](#)

Author(s)
Joint Task Force Transformation Initiative

DOCUMENTATION

Publication:

[📄 SP 800-30 Rev. 1 \(DOI\)](#)

[📄 Local Download](#)

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

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
<p>ADVERSARIAL</p> <ul style="list-style-type: none"> - Individual <ul style="list-style-type: none"> - Outsider - Insider - Trusted Insider - Privileged Insider - Group <ul style="list-style-type: none"> - Ad hoc - Established - Organization <ul style="list-style-type: none"> - Competitor - Supplier - Partner - Customer - Nation-State 	<p>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).</p>	<p>Capability, Intent, Targeting</p>



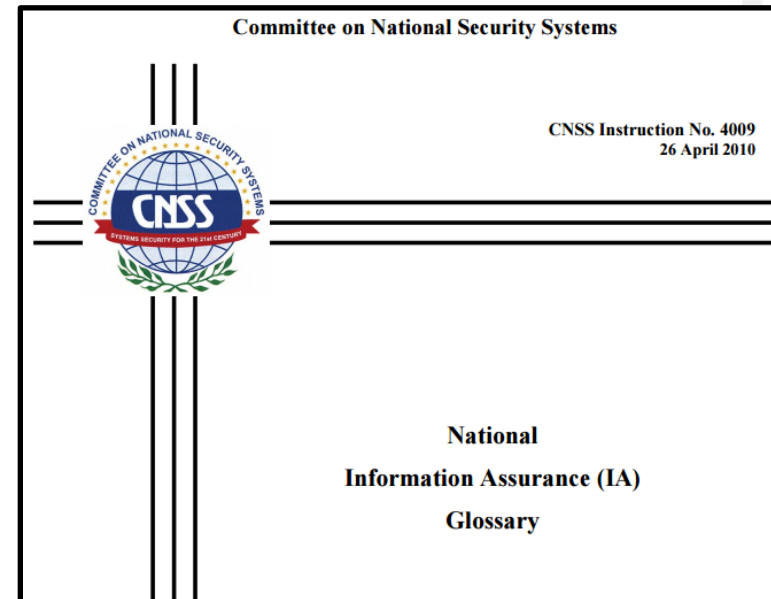
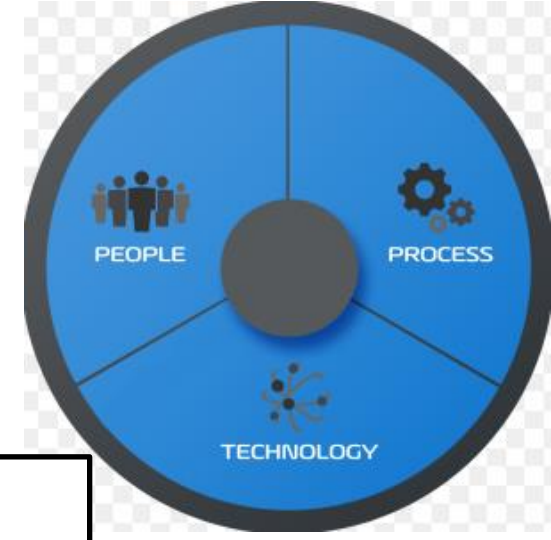
More information can be found in class notes

What is a Vulnerability?



What is a Vulnerability?

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

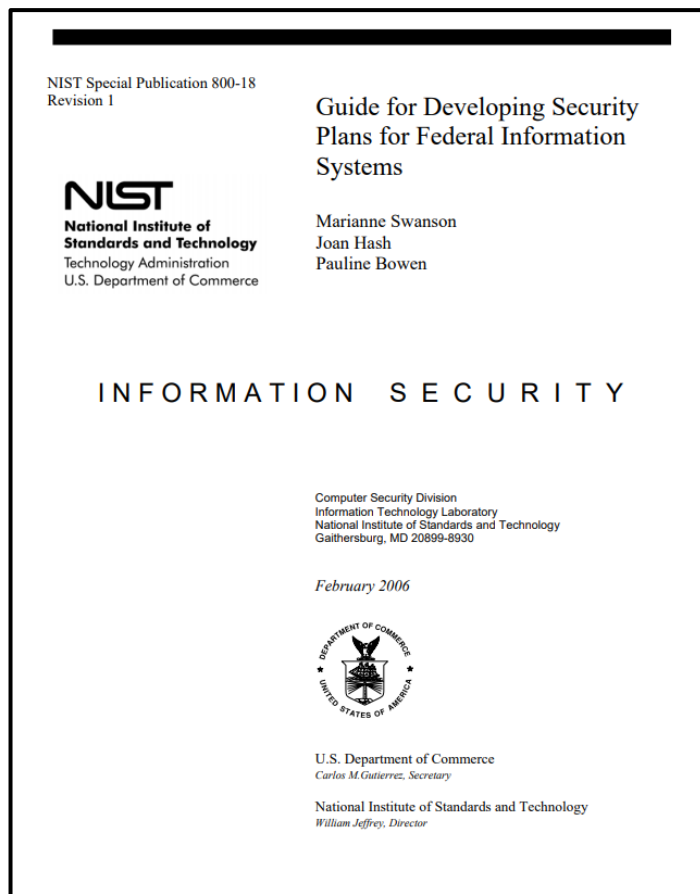


Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Vulnerabilities are...

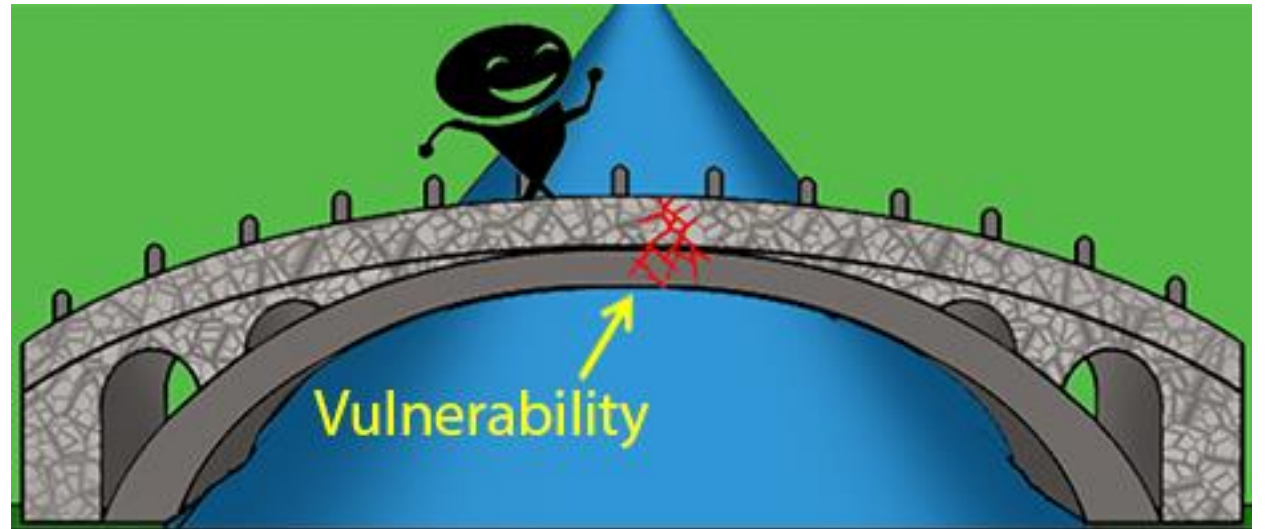
Inadequacies in any of these areas which can lead to negative impacts:

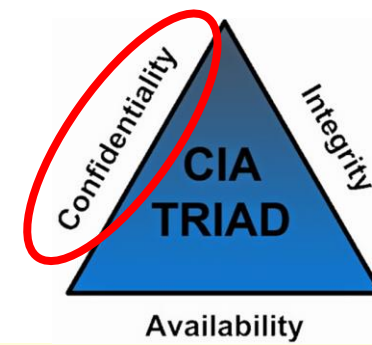
Cybersecurity Controls protect against impacts



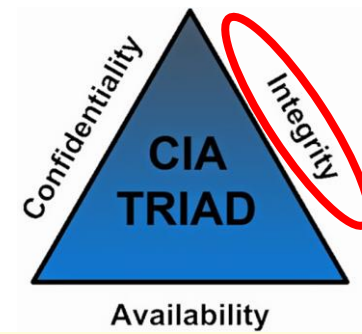
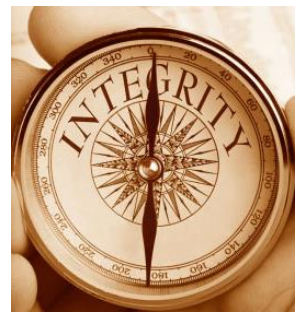
CLASS	FAMILY
Management	Risk Assessment
Management	Planning
Management	System and Services Acquisition
Management	Certification, Accreditation, and Security Assessments
Operational	Personnel Security
Operational	Physical and Environmental Protection
Operational	Contingency Planning
Operational	Configuration 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
<p><i>Confidentiality</i> Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]</p>	<p>The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.</p>



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



	POTENTIAL IMPACT		
Security Objective	LOW	MODERATE	HIGH
<p><i>Availability</i> Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]</p>	<p>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.</p>	<p>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.</p>	<p>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.</p>

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
<p>Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]</p>	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.
<p>Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]</p>	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.
<p>Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]</p>	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)

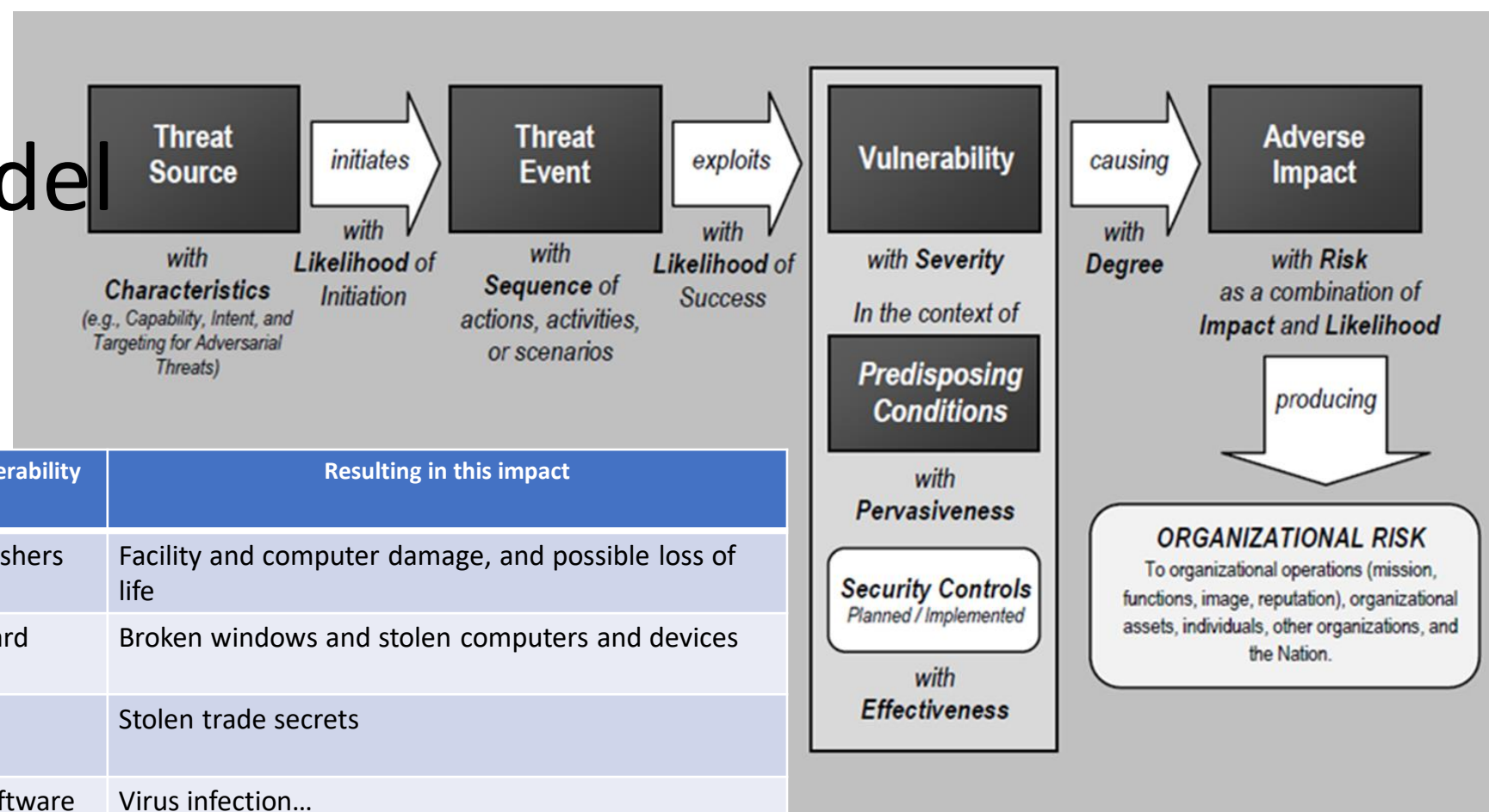
What are examples of Information security risks ?

- 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

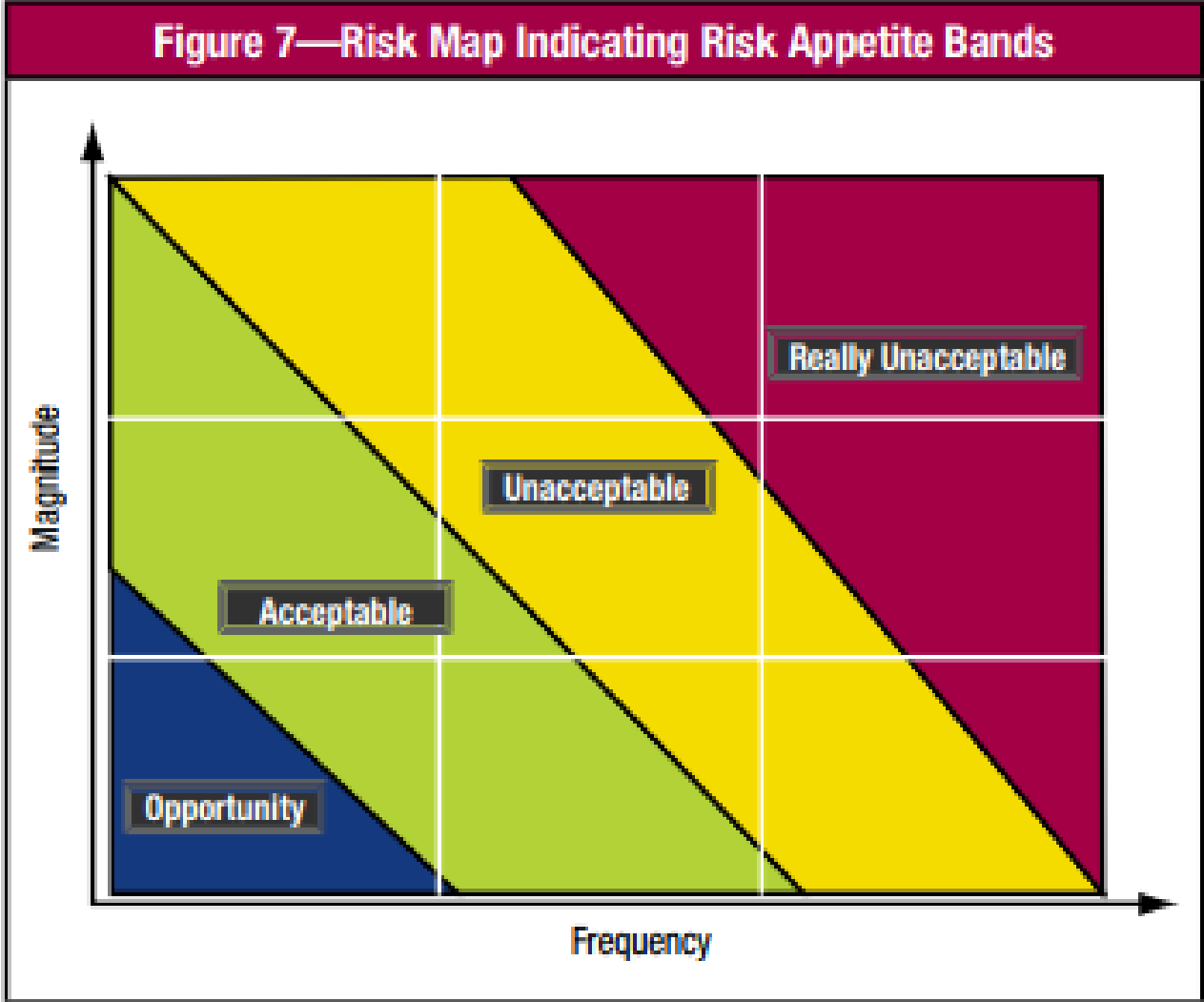
Qualitative Risk Assessment

Quantitative Risk Assessment

$$\begin{aligned}
 \text{Annual Loss Expectancy} &= \\
 &\text{Single Loss Expectancy} \\
 &\quad \times \\
 &\text{Annualized Rate of Occurrence}
 \end{aligned}$$

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

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...



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>

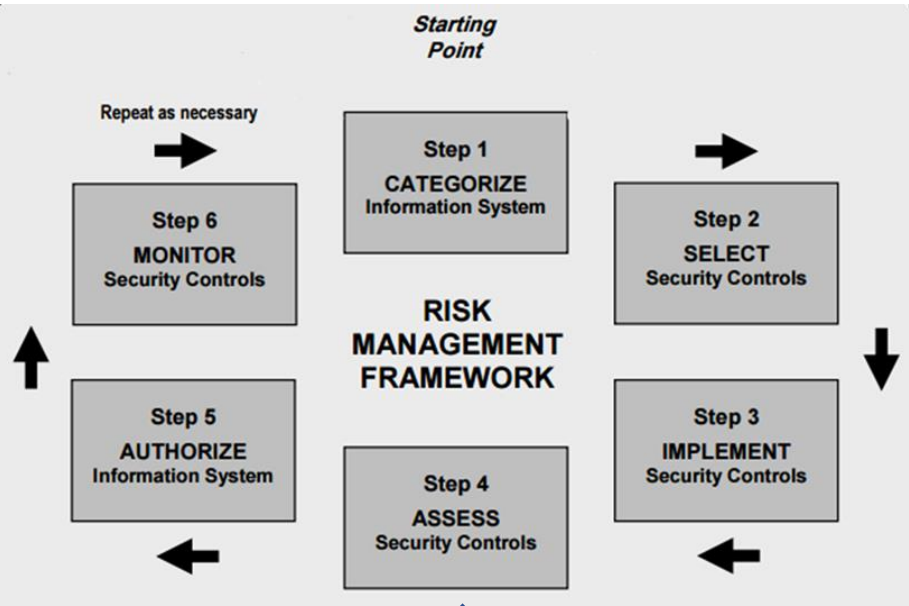
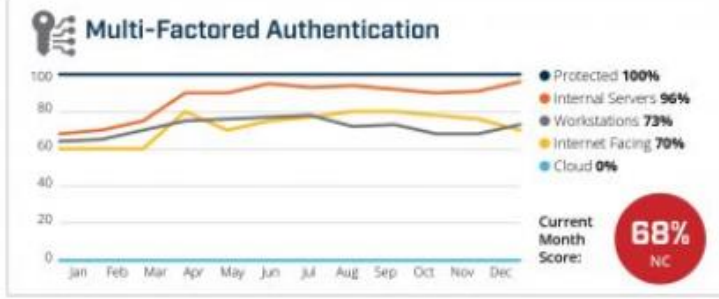
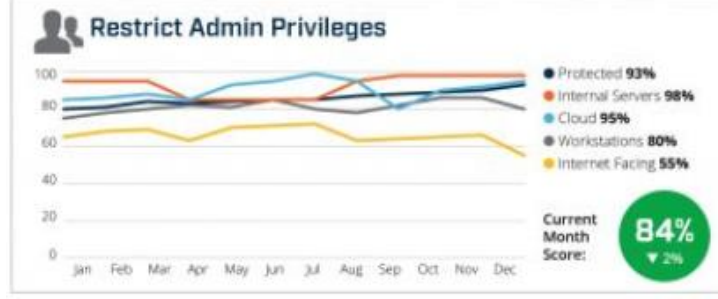
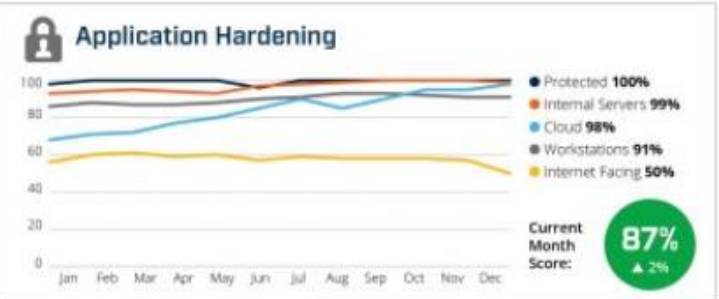
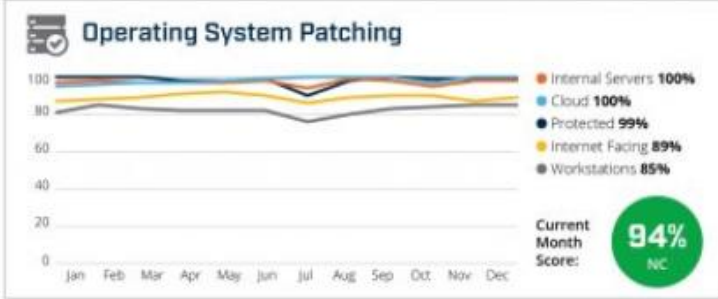
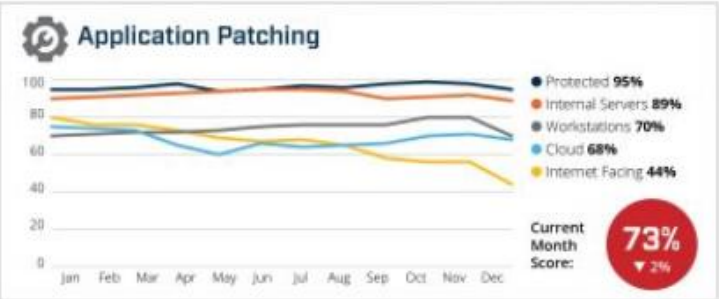
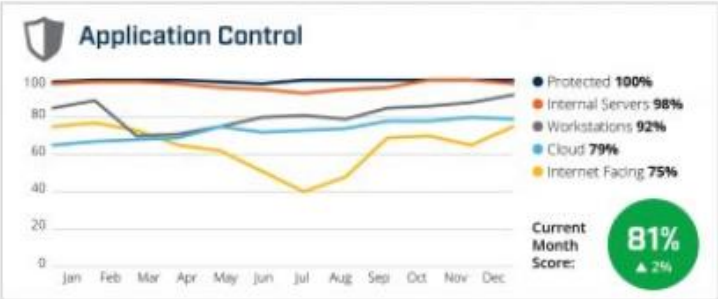
Course objectives

- ✓ 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 websites



MIS 4596 – Managing Enterprise Cybersecurity – Spring 2022
Section 001 – CRN 20595

Syllabus

Instructor: David Lanter

Office: Speakman 209C and online via Zoom

Office Hours: Before and after classes, and by appointment

Email: david.lanter@temple.edu

e-profile: <http://community.mis.temple.edu/dlanter/>

Class Format: We will begin the semester meeting Online through Thursday January 20th and then the plan is to move our class to In-Class meetings COVID-19 permitting.

Meetings: Tuesdays & Thursdays 9:30 – 10:50 AM

Where – Online: [Zoom Meeting](#)

Where – In-Class: Alter Hall, Room 238

MIS Community Website: <https://community.mis.temple.edu/mis4596sec001spring2022/>

Canvas: <https://templeu.instructure.com/courses/108783>

Information Technology Assistant

- Shubhan Patil – shubham.patil@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 case studies are available for purchase at Harvard Business Publishing for \$8.50 here: <https://hbsp.harvard.edu/import/901153>
- Security Assignments by Professors 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://online.library-wiley.com.libproxy.temple.edu/doi/book/10.1002/9781119183631>
 - Amazon.com : <https://www.amazon.com/dp/0471453803/>

MIS MANAGING ENTERPRISE CYBERSECURITY
MIS 4596.001 • Spring 2022 • David Lanter

SCHEDULE ABOUT LABS LECTURE MATERIALS

Schedule

DATES	TOPIC & ASSIGNMENTS DUE	READINGS
Tuesday, 1/11/2022	Introduction to the Course	
Thursday, 1/13/2022	Threat modeling	Anderson, Ch. 1 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, 1/18/2022	Risk Assessment	
Thursday, 1/20/2022	Lab 1: Threat Modeling due Start Milestone 1: Risk Assessment Report Draft Information Privacy	Tim Cook, "Technology can harm, can help"
Tuesday, 1/25/2022	Introduction to Linux Google Cloud Platform (GCP)	
Thursday, 1/27/2022	Lab 2: Web Privacy and Anonymity Lab due Introduction to Cryptography	Anderson, Chapter 5
Saturday, 1/29/2022	Milestone 1: Risk Assessment Report Draft	

- Account
- Dashboard
- Courses
- Calendar
- Inbox
- History
- Help

BU-MIS-4596-001-20595-202203 > Assignments

2022 Spring

Search for Assignment

- Home
- Announcements
- Syllabus
- Pages
- Assignments
- Quizzes
- Grades
- People

Upcoming Assignments

- Lab 1: Threat Modeling**
Available until Mar 26 at 11:59pm | Due Jan 20 at 11:59pm | -/20 pts
- Lab 2: Web Privacy and Anonymity**
Available until Mar 26 at 11:59pm | Due Jan 27 at 11:59pm | -/20 pts
- Milestone 1: Risk Assessment Report Draft**
Not available until Jan 20 at 12:01am | Due Jan 29 at 11:59pm | -/25 pts
- Milestone 2: Final Risk Assessment Report**
Not available until Feb 1 at 12:01am | Due Feb 5 at 11:59pm | -/100 pts
- Lab 3: Introduction to Google Cloud Platform and Linux Tutorial**
Not available until Jan 17 at 12:00am | Due Feb 5 at 11:59pm | -/20 pts
- Lab 4: Symmetric Encryption and Hashing**
Not available until Jan 17 at 12:00am | Due Feb 10 at 11:59pm | -/20 pts
- Lab 5: Asymmetric Cryptography**
Not available until Jan 27 at 12:00am | Due Feb 17 at 11:59pm | -/20 pts
- Lab 6: Digital Certificates and Trust**
Not available until Feb 10 at 12:00am | Due Feb 22 at 11:59pm | -/20 pts
- Lab 7: Password Cracking**
Not available until Feb 10 at 12:00am | Due Feb 24 at 11:59pm | -/20 pts
- Lab 8: Vulnerability Discovery**
Not available until Feb 22 at 12:00am | Due Mar 10 at 11:59pm | -/20 pts
- Lab 9: Vulnerability Exploitation**
Not available until Feb 24 at 12:00am | Due Mar 22 at 11:59pm | -/20 pts
- Milestone 3: Penetration Test Report Draft**

Grading

Milestones	Group	35%
Labs	Individual	25%
Mid-Term Exam	Individual	15%
Final Exam	Individual	20%
Attendance & Participation	Individual	5%
Total		100%

Schedule (subject to change)

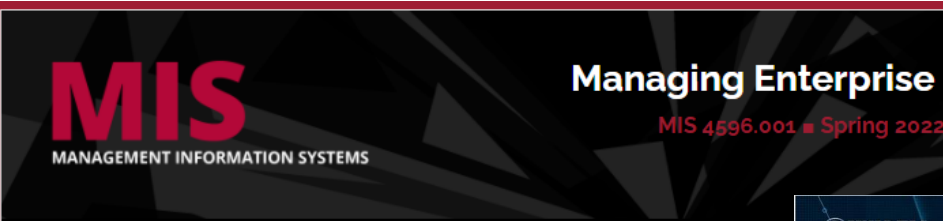
Week	Tuesday	Thursday	Topics
1	Jan 11	Jan 13	Introduction Threat Modeling
2	Jan 18	Jan 20	Risk Assessment Information Privacy
3	Jan 25	Jan 27	Introduction to Linux and Google Cloud Platform Introduction to Cryptography
4	Feb 1	Feb 3	Introduction to Cryptography continued... No Class Meeting
5	Feb 8	Feb 10	Symmetric Cryptography Asymmetric Cryptography
6	Feb 15	Feb 17	Digital Certificates and Public Key Infrastructures Authentication and Passwords
7	Feb 22	Feb 24	Password Cracking Introduction to Networking
8	Mar 8	Mar 10	Vulnerability Scanning
9	Mar 15	Mar 17	Vulnerability Exploitation
10	Mar 22	Mar 24	Human Element–Info. Security in Organizations Physical Security
11	Mar 29	Mar 31	Network Security Monitoring Incident Response – Equifax Case Study
12	Apr 5	Apr 7	Incident Recovery Maersk Case Study
13	Apr 12	Apr 14	Malware Analysis
14	Apr 19	Apr 21	Milestone 4 – Group Work Day Course Wrap-Up

Other Key Dates and Deadlines (subject to change)

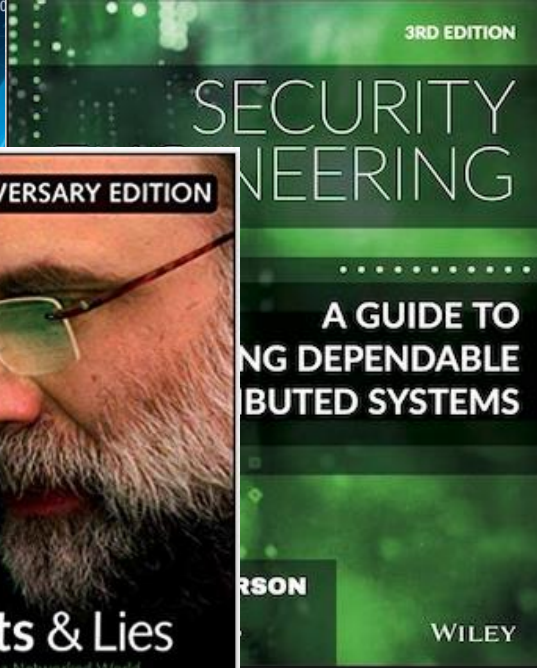
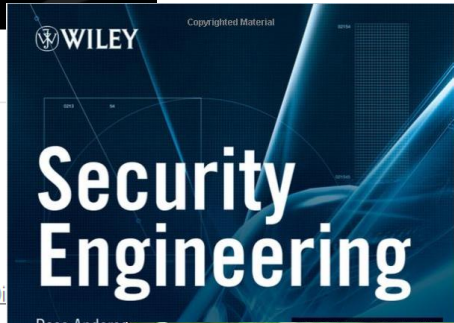
Thu, Jan 20	Start Milestone 1: Risk Assessment Report Draft
Sat, Jan 29	Deadline for Milestone 1: Risk Assessment Report Draft Due
Sat, Feb 5	Deadline for Milestone 2: Risk Assessment Final Report Due
Tue, Feb 22	Midterm Exam opens
Sun, Feb 26	Deadline for Midterm exam
Tue, Mar 15	Start Milestone 3: Penetration Test
Sat, Mar 26	Deadline for completion of lab assignments 1-9
Sat, Apr 2	Deadline for Milestone 3: Penetration Test Report Due
Thu, Apr 21	Final Exam opens
Sat, Apr 23	Deadline for Milestone 4: Penetration Test Report with Mitigations Due
Wed, Apr 28	Deadline for final exam
Sun, May 1	Deadline for completion of lab assignments 10-13

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

Course materials – readings...



SCHEDULE	ABOUT	LABS	LECTURE MATERIALS
	Course overview		
	Course materials		
	Grading and Assignments		
	Instructor		



- Required Case Studies: *Engineering: A Guide to Building Dependable Distributed Systems 2nd or 3rd Edition*, by Ross Anderson.
 - Free PDF of the book: <http://www.cl.cam.ac.uk/~rja14/book.html>
 - Amazon: <http://a.co/gbz6zP>
- **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/901153>
- **Security Assignments:** by Dave Eargle and Anthony Vance at <http://securityassignments.com/>. A number of this course's labs and milestone assignments with Lab 3 require lab virtual machine access for Google Cloud Platform for purchase for \$40 here: <https://security-assignments.com/store/>
- Other materials will be made available throughout the semester
- **Optional Textbook:** *Secrets and Lies: Digital Security in a Networked World* by Bruce Schneier.
 - Available online via Temple Library: <https://onlinelibrary-wiley.com.libproxy.temple.edu/doi/book/10.1002/9781119183631>
 - Amazon: <https://amzn.com/0471453803>

4596
DAVID LANTER
Jan 10, 2022 – May 04, 2022

Student View of Coursepack x

Purchase required to access your materials

PURCHASE COURSEPACK

**MIS 4596 Managing Enterprise
Cybersecurity-I-I** **\$8.50**

Main Case

Data Breach at Equifax **Required \$4.25**

Suraj Srinivasan, Quinn Pitcher, Jonah S. Goldberg

Expiration Date: July 10, 2022 28 page(s)

Main Case

Cyberattack: The Maersk Global Supply-Chain Meltdown **Required \$4.25**

David T.A. Wesley, Luis Alfonso Dau, Alexandra Roth

Expiration Date: July 10, 2022 16 page(s)

HARVARD BUSINESS SCHOOL

SURAJ SRINIVASAN
QUINN PITCHER
JONAH S. GOLDBERG

Data Breach at Equifax

It was October 4, 2017, and Richard Smith, the former CEO of Equifax, was in the U.S. Senate Committee on Banking, Housing, and Urban Affairs. He was there to testify about the data breach at Equifax that had occurred the week before. Smith's replacement, interim CEO Paulino do Rego, had just been named CEO of Equifax. Observers were critical of Equifax's cybersecurity practices and its handling of the breach. The breach had not only exposed the personal information of over 143 million Americans, but it had also caused significant damage to the company's reputation. Smith's replacement, interim CEO Paulino do Rego, had just been named CEO of Equifax. Observers were critical of Equifax's cybersecurity practices and its handling of the breach. The breach had not only exposed the personal information of over 143 million Americans, but it had also caused significant damage to the company's reputation.

Equifax

Founded in 1999, Equifax Inc. (Equifax) was a U.S. credit reporting agency. It was one of the three main credit reporting agencies in the United States, along with Experian and TransUnion. Equifax was known for its credit reporting services, which provided information on the creditworthiness of individuals and businesses. Equifax was a major player in the credit reporting industry, and its services were used by a wide range of financial institutions and businesses.

IVEY Publishing

D'Amore-McKim
Northeastern University

W19132

CYBERATTACK: THE MAERSK GLOBAL SUPPLY-CHAIN MELTDOWN¹

David Wesley and Professors Luis Dau and Alexandra Roth write 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, M6J 1B1; (519) 661-2200; ivy.cases@ivey.uwo.ca. 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 at the next meeting on global risks and uncertainty at Stanford University's Directors' College. As he was getting ready to speak, he was informed that the Maersk Global Supply-Chain Meltdown had just occurred. Snabe was a member of the Maersk Global Supply-Chain Meltdown task force, and he was one of the few people who had been involved in the investigation. Snabe was a member of the Maersk Global Supply-Chain Meltdown task force, and he was one of the few people who had been involved in the investigation.

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 table, which read "4:00 a.m." in a dim blue digital font. Who could be calling at this hour, he wondered?

"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 Narsarsuaq, 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.

A self-described "nerd," Snabe attended Aarhus University in the late 1980s, where he studied mathematical proof. 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."

Upon receiving his master's degree in 1990, Snabe became a trainee at software giant SAP, Germany's second-largest company after Siemens. 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. permissions@temple.edu or 610.763.7650

Course materials – schedule...

The screenshot shows the course website header with the MIS logo and navigation tabs. The 'Schedule' tab is active, displaying a table with columns for Dates, Topic & Assignments Due, and Readings. The table content is as follows:

DATES	TOPIC & ASSIGNMENTS DUE	READINGS
Tuesday, 1/11/2022	Introduction to the Course	Anderson, Ch. 1
Thursday, 1/13/2022	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, 1/18/2022	Risk Assessment	
Thursday, 1/20/2022	Start Milestone 1: Risk Assessment Report Draft	Tim Cook, "Technology can harm, can help"
Thursday, 1/20/2022	Information Privacy	
Tuesday, 1/25/2022	Introduction to Linux Google Cloud Platform (GCP)	
Thursday, 1/27/2022	Introduction to Cryptography	Anderson, Chapter 5
Saturday, 1/29/2022	Milestone 1: Risk Assessment Report Draft	

DATES	TOPIC & ASSIGNMENTS DUE	READINGS
Tuesday, 1/11/2022	Introduction to the Course	Anderson, Ch. 1
Thursday, 1/13/2022	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, 1/18/2022	Risk Assessment	
Thursday, 1/20/2022	Start Milestone 1: Risk Assessment Report Draft	Tim Cook, "Technology can harm, can help"
Thursday, 1/20/2022	Information Privacy	
Tuesday, 1/25/2022	Introduction to Linux Google Cloud Platform (GCP)	
Thursday, 1/27/2022	Introduction to Cryptography	Anderson, Chapter 5
Saturday, 1/29/2022	Milestone 1: Risk Assessment Report Draft due	
Tuesday, 2/1/2022	Introduction to Cryptography continued...	Anderson, Chapter 5

Grading...

Milestones (35%)

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
- Late submissions are subject to a 10% deduction in points per each 12 hours late.

You and your team 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.)

MIS
MANAGEMENT INFORMATION SYSTEMS

Managing Enterprise
MIS 4596.001 - Spring

SCHEDULE ABOUT **LABS** LECTURE MATERIALS

Labs

Lab1: Threat Modeling with Attack Trees

Lab2: Web Privacy and Anonymity

Lab3: See Tutorials - Introduction to Google Cloud Platform & Introduction to Linux

Lab4: Symmetric Encryption and Hashing

Lab5: Asymmetric Encryption

Lab6: Digital Certificates

Lab7: Password Cracking

Lab8: Vulnerability Scanning

Lab9: Exploitation

Lab10: Physical Security Scavenger Hunt

Lab11: Social Engineering

Lab12: Network Security Monitoring and Security Onion

Lab13: Malware Analysis

Tutorials

Tutorial: Introduction to Google Cloud Platform

Tutorial: Introduction to Linux

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 April 19.

Agenda

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



OOH HOME | OCCUPATION FINDER | OOH FAQ | OOH GLOSSARY | A-Z INDEX | OOH SITE MAP

OCCUPATIONAL OUTLOOK HANDBOOK

Search Handbook

On-the-job Training

Additional training needed (postemployment) to attain competency in the skills needed in this occupation.

Information Security Analysts

PRINTER-FRIENDLY

Summary | What They Do | Work Environment | How to Become One | Pay | Job Outlook | State & Area Data | Similar Occupations | More Info

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, 2020	141,200
Job Outlook, 2020-30	33% (Much faster)
Employment Change, 2020-30	47,100

What Information Security Analysts Do
Information security analysts plan and carry out security measures to

Work Environment
Most information security analysts work for computer companies, cons

How to Become an Information Security Analyst
Most information security analyst positions require a bachelor's degree related occupation.

Pay
The median annual wage for information security analysts was \$103,5

Job Outlook
Employment of information security analysts is projected to grow 33 percent from 2020 to 2030, much faster than the average for all occupations.

About 16,300 openings for information security analysts are projected each year, on average, over the decade. Many of those openings are expected to result from the need to replace workers who transfer to different occupations or exit the labor force, such as to retire.

Summary

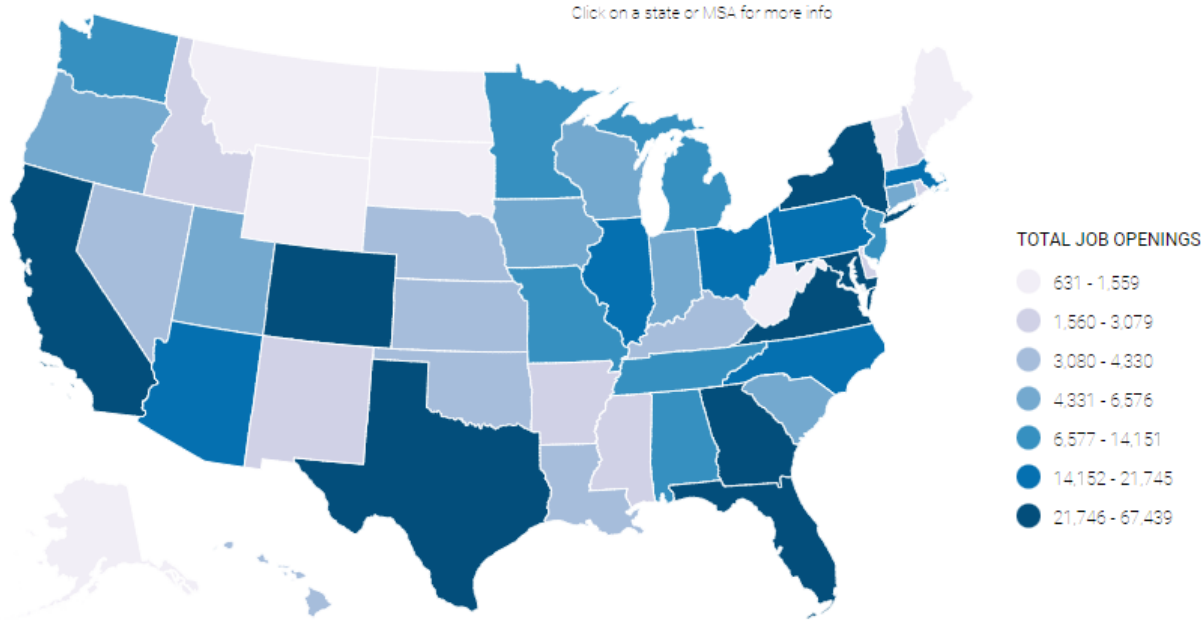
Quick Facts: Information Security Analysts	
2020 Median Pay	\$103,590 per year \$49.80 per hour
Typical Entry-Level Education	Bachelor's degree
Work Experience in a Related Occupation	Less than 5 years
On-the-job Training	None
Number of Jobs, 2020	141,200
Job Outlook, 2020-30	33% (Much faster than average)
Employment Change, 2020-30	47,100

CYBERSECURITY SUPPLY/DEMAND HEAT MAP

States Metro Areas Search State 🔍

- 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.



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

- Share
- Embed

National level

<p>TOTAL CYBERSECURITY JOB OPENINGS ⓘ</p> <p>597,767</p> <hr/> <p>TOTAL EMPLOYED CYBERSECURITY WORKFORCE ⓘ</p> <p>1,053,468</p>	<p>SUPPLY/DEMAND RATIO ⓘ</p> <p>68% National average</p>	<p>GEOGRAPHIC CONCENTRATION ⓘ</p> <p>Average</p> <p>LOCATION QUOTIENT</p> <p>National average</p>	<p>TOP CYBERSECURITY JOB TITLES ⓘ</p> <ul style="list-style-type: none"> ■ Cybersecurity Analyst ■ Cybersecurity Manager ■ Cybersecurity Consultant ■ Software Developer ■ Systems Engineer ■ Network Engineer ■ Penetration & Vulnerability Tester ■ Systems Administrator ■ Cybersecurity Specialist
---	---	---	--

Example job types



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

Agenda

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