Managing Enterprise Cybersecurity MIS 4596

Class 1

Agenda

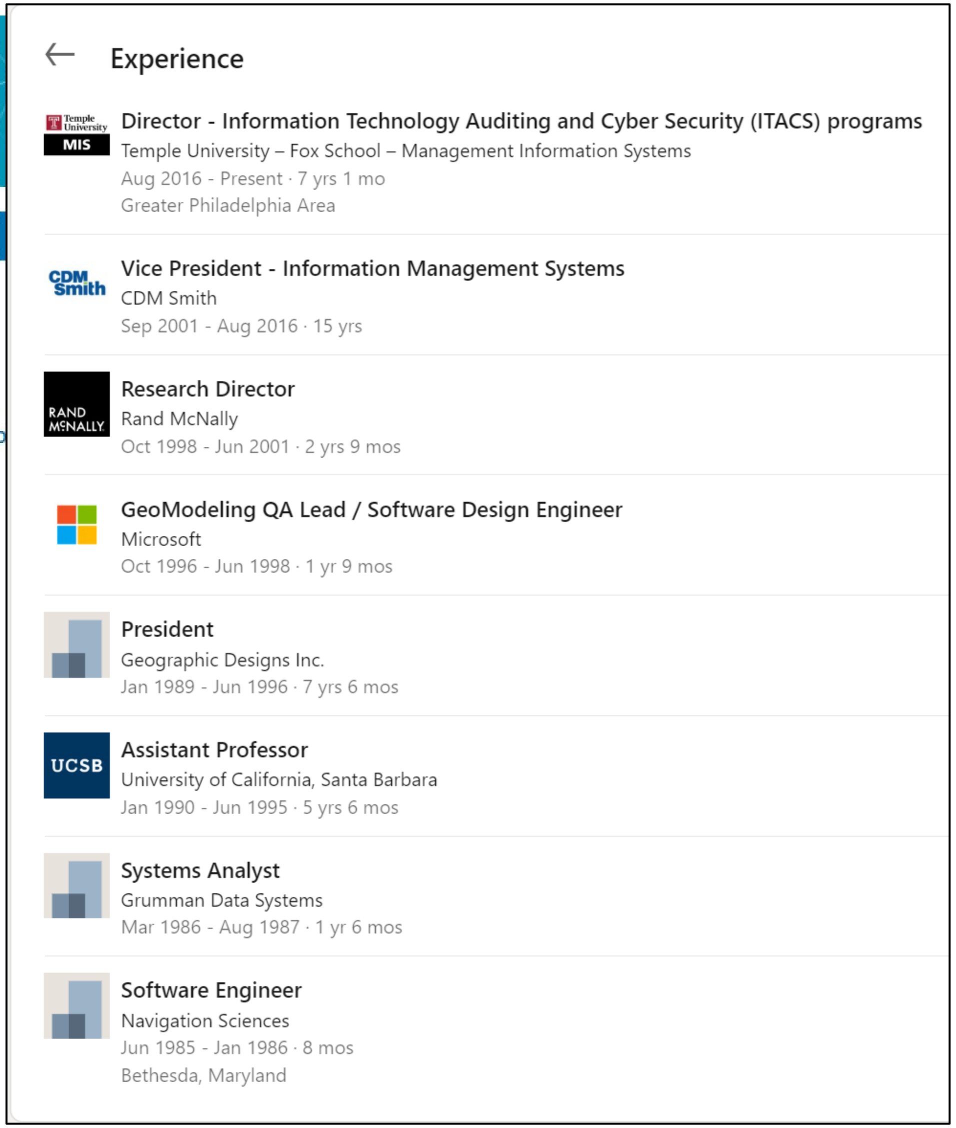
- Instructor
- Course overview
- Introduction
- Need for Cybersecurity Professionals

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 · 7 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

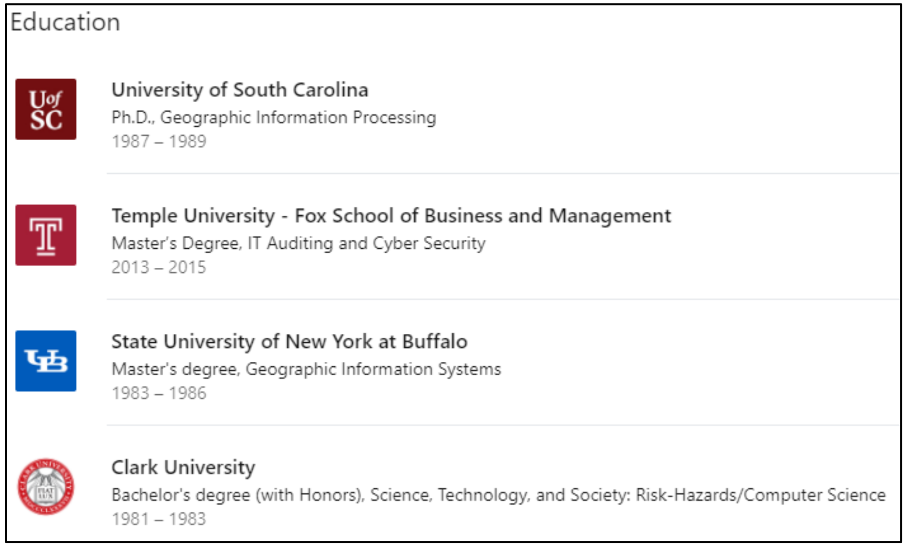
GeoModeling QA Lead / Software Design Engineer
Microsoft
Oct 1996 - Jun 1998 · 1 yr 9 mos

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



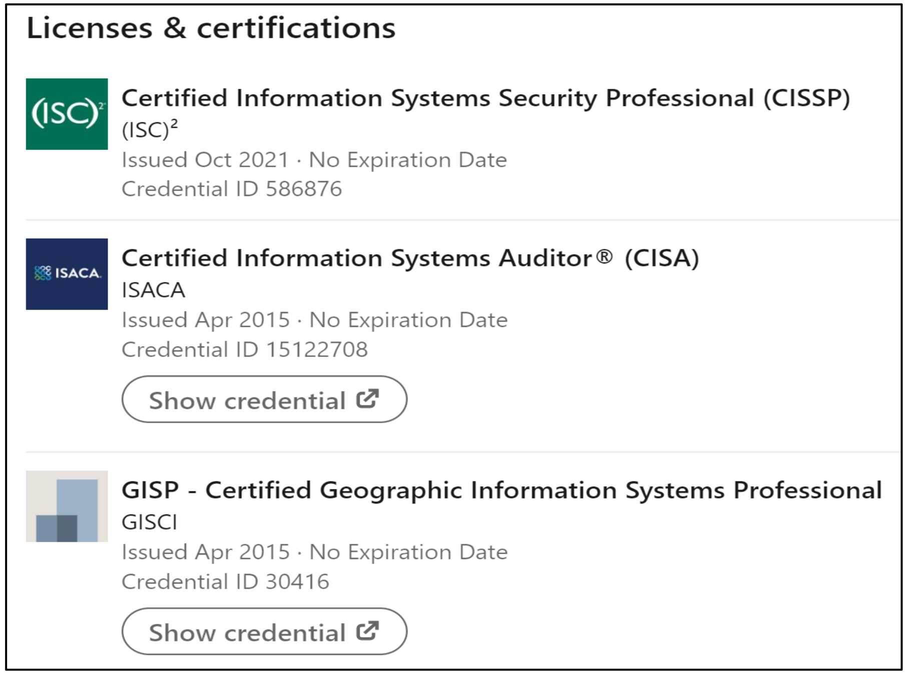
Education

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 Security Professional (CISSP)
(ISC)^2
Issued Oct 2021 · No Expiration Date
Credential ID 586876

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

GISP - Certified Geographic Information Systems Professional
GISCI
Issued Apr 2015 · No Expiration Date
Credential ID 30416
Show credential

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 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:

  - NIST Cybersecurity Framework Version (https://www.nist.gov/cyberframework/framework)
  - NIST Risk Management Framework (https://csrc.nist.gov/projects/risk-management/about-rmf)

- Communicate security risks and responses effectively

  A substantial portion of the course will be devoted to practicing capable, proficient written and verbal communication of cybersecurity risks, threats, mitigations, and responses to relevant stakeholders for their decision making.

Course learning goals

University-Designated Writing-Intensive (W) Course

- This is a University-designated writing-intensive course, and by passing this course, students will fulfill the University requirement that “All undergraduate students must complete at least two writing-intensive courses for a total of at least six credits” (https://bulletin.temple.edu/undergraduate/academic-programs/writing-intensive-courses/).
- This course requires a substantial amount of writing for individual assignments throughout the semester.
- There is no group project in this class; all deliverables are individual assignments. There will be no mid-term and final exams.

Course learning goals

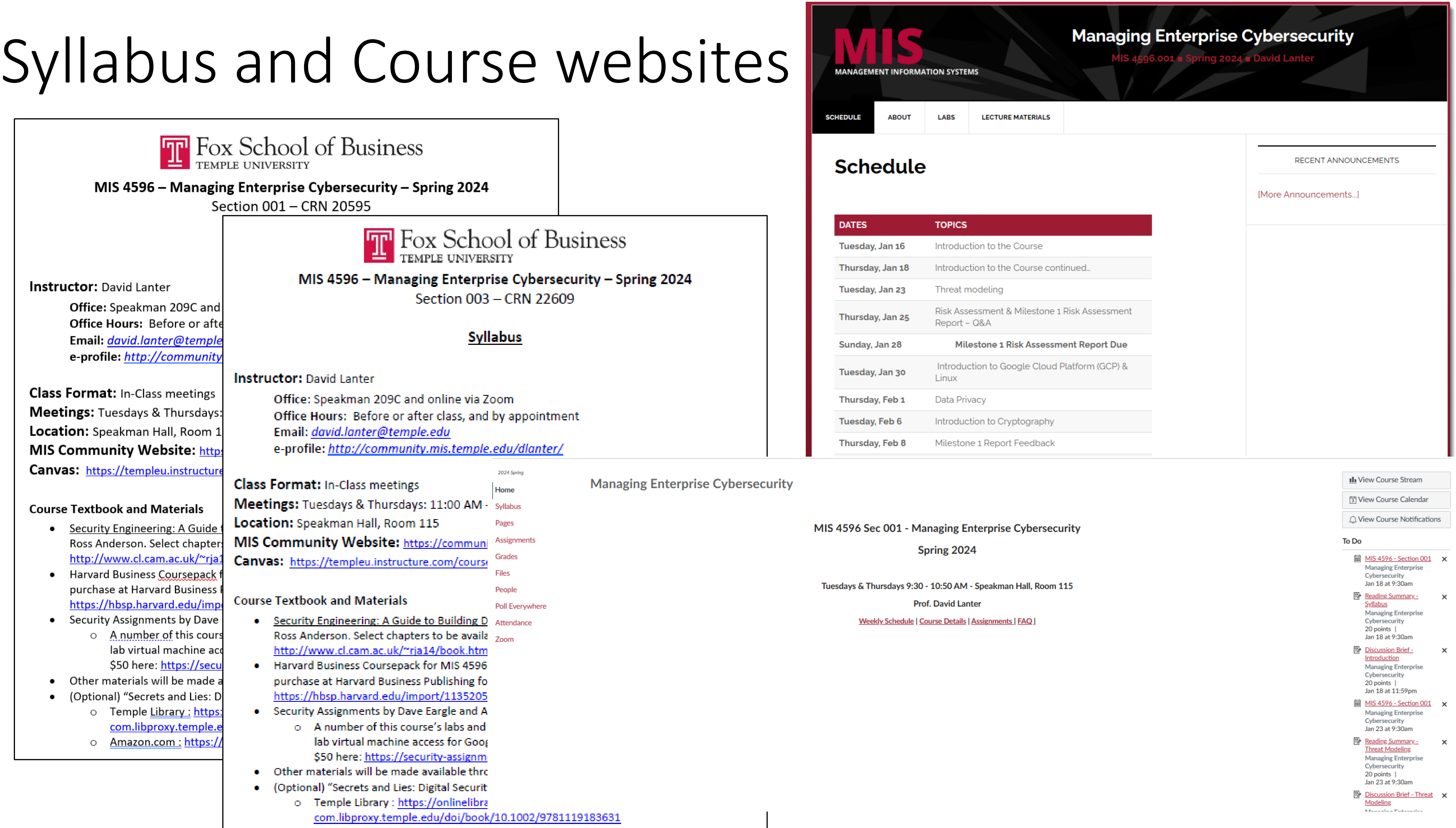
Writing-Related Goals

- Students will learn how to write about highly technical cybersecurity topics for a non-technical audience.
- Students will learn how to explain business implications of cybersecurity risks, threats, mitigations, and responses.
- Students will learn how to organize their writing for impact and actions.
- Students will learn how to produce an executive summary in a concise manner for executive clients/superiors.

Information Literacy Goals

- Students will learn how to discover relevant information on cybersecurity risks, vulnerabilities, and mitigations from credible, reliable, and authoritative sources in a self-directed manner.
- Students will learn how to deploy these information resources effectively in their project reports to advise on cybersecurity risks, vulnerabilities, and mitigations.
- Students will develop the following information literacy skills with in-class instructions and activities:
  - How to identify credible and authoritative sources for cybersecurity matters
  - How to discover relevant information resources
  - How to incorporate the information in their writing assignments

Syllabus and Course websites



Fox School of Business
TEMPLE UNIVERSITY

MIS 4596 – Managing Enterprise Cybersecurity – Spring 2024
Section 001 – CRN 20595

Instructor: David Lanter

Office: Speakman 209C and
Office Hours: Before or afte
Email: *david.lanter@temple*
e-profile: *http://community*

Class Format: In-Class meetings
Meetings: Tuesdays & Thursdays:
Location: Speakman Hall, Room 1
MIS Community Website: https
Canvas: https://templeu.instructure

Course Textbook and Materials

- Security Engineering: A Guide t Ross Anderson. Select chapters http://www.cl.cam.ac.uk/~rja1
- Harvard Business Coursepack f purchase at Harvard Business https://hbsp.harvard.edu/imp
- Security Assignments by Dave
  - A number of this cours lab virtual machine acc $50 here: https://secu
- Other materials will be made a
- (Optional) "Secrets and Lies: D
  - Temple Library : https: com.libproxy.temple.e
  - Amazon.com : https://

Fox School of Business
TEMPLE UNIVERSITY

MIS 4596 – Managing Enterprise Cybersecurity – Spring 2024
Section 003 – CRN 22609

Syllabus

Instructor: David Lanter

Office: Speakman 209C and online via Zoom
Office Hours: Before or after class, and by appointment
Email: *david.lanter@temple.edu*
e-profile: *http://community.mis.temple.edu/dlanter/*

Class Format: In-Class meetings
Meetings: Tuesdays & Thursdays: 11:00 AM -
Location: Speakman Hall, Room 115
MIS Community Website: https://communi
Canvas: https://templeu.instructure.com/course

Course Textbook and Materials

- Security Engineering: A Guide to Building D Ross Anderson. Select chapters to be availa http://www.cl.cam.ac.uk/~rja14/book.htm
- Harvard Business Coursepack for MIS 4596 purchase at Harvard Business Publishing fo https://hbsp.harvard.edu/import/1135205
- Security Assignments by Dave Eargle and A
  - A number of this course's labs and lab virtual machine access for Goo $50 here: https://security-assignm
- Other materials will be made available thro
- (Optional) "Secrets and Lies: Digital Securit
  - Temple Library : https://onlinelibra com.libproxy.temple.edu/doi/book/10.1002/9781119183631

MIS
MANAGEMENT INFORMATION SYSTEMS

Managing Enterprise Cybersecurity
MIS 4596.001 ■ Spring 2024 ■ David Lanter

Schedule

DATES	TOPICS
Tuesday, Jan 16	Introduction to the Course
Thursday, Jan 18	Introduction to the Course continued..
Tuesday, Jan 23	Threat modeling
Thursday, Jan 25	Risk Assessment & Milestone 1 Risk Assessment Report – Q&A
Sunday, Jan 28	Milestone 1 Risk Assessment Report Due
Tuesday, Jan 30	Introduction to Google Cloud Platform (GCP) & Linux
Thursday, Feb 1	Data Privacy
Tuesday, Feb 6	Introduction to Cryptography
Thursday, Feb 8	Milestone 1 Report Feedback

RECENT ANNOUNCEMENTS

[More Announcements...]

Managing Enterprise Cybersecurity

MIS 4596 Sec 001 - Managing Enterprise Cybersecurity

Spring 2024

Tuesdays & Thursdays 9:30 - 10:50 AM - Speakman Hall, Room 115

Prof. David Lanter

Weekly Schedule | Course Details | Assignments | FAQ |

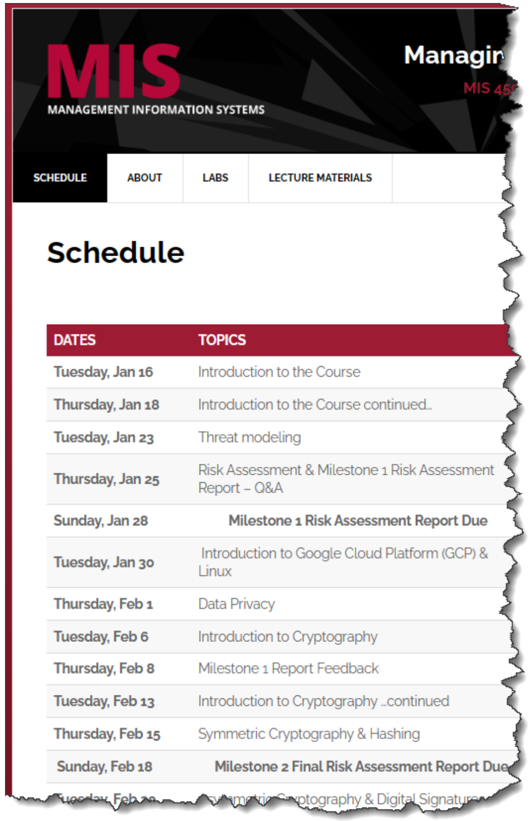
To Do

- MIS 4596 - Section 001
  Managing Enterprise Cybersecurity
  Jan 18 at 9:30am
- Reading Summary - Syllabus
  Managing Enterprise Cybersecurity
  20 points |
  Jan 18 at 9:30am
- Discussion Brief - Introduction
  Managing Enterprise Cybersecurity
  20 points |
  Jan 18 at 11:59pm
- MIS 4596 - Section 001
  Managing Enterprise Cybersecurity
  Jan 23 at 9:30am
- Reading Summary - Threat Modeling
  Managing Enterprise Cybersecurity
  20 points |
  Jan 23 at 9:30am
- Discussion Brief - Threat Modeling

MIS Community Web Site provides easy access to…

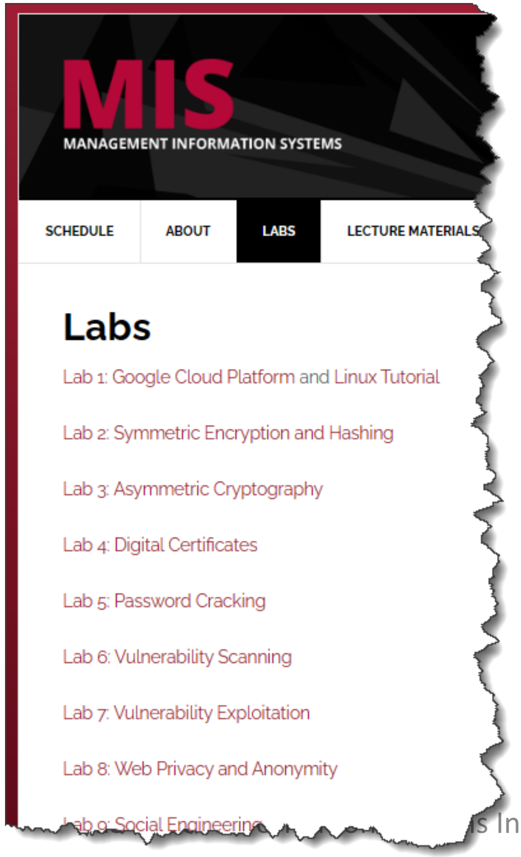
https://community.mis.temple.edu/mis4596sec001spring2024/

1. Updated course schedule
2. Lab links (also found in Canvas assignments)
3. Lecture notes and supporting material



Schedule

DATES	TOPICS
Tuesday, Jan 16	Introduction to the Course
Thursday, Jan 18	Introduction to the Course continued…
Tuesday, Jan 23	Threat modeling
Thursday, Jan 25	Risk Assessment & Milestone 1 Risk Assessment Report – Q&A
Sunday, Jan 28	**Milestone 1 Risk Assessment Report Due**
Tuesday, Jan 30	Introduction to Google Cloud Platform (GCP) & Linux
Thursday, Feb 1	Data Privacy
Tuesday, Feb 6	Introduction to Cryptography
Thursday, Feb 8	Milestone 1 Report Feedback
Tuesday, Feb 13	Introduction to Cryptography …continued
Thursday, Feb 15	Symmetric Cryptography & Hashing
Sunday, Feb 18	**Milestone 2 Final Risk Assessment Report Due**
Tuesday, Feb 20	Symmetric Cryptography & Digital Signatures



Labs

Lab 1: Google Cloud Platform and Linux Tutorial

Lab 2: Symmetric Encryption and Hashing

Lab 3: Asymmetric Cryptography

Lab 4: Digital Certificates

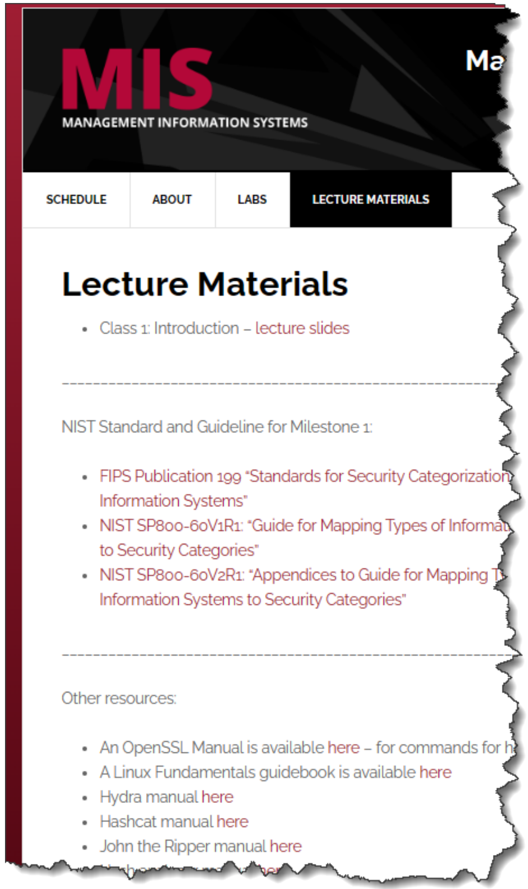
Lab 5: Password Cracking

Lab 6: Vulnerability Scanning

Lab 7: Vulnerability Exploitation

Lab 8: Web Privacy and Anonymity

Lab 9: Social Engineering



Lecture Materials

- Class 1: Introduction – lecture slides

NIST Standard and Guideline for Milestone 1:

- FIPS Publication 199 "Standards for Security Categorization Information Systems"
- NIST SP800-60V1R1: "Guide for Mapping Types of Informat to Security Categories"
- NIST SP800-60V2R1: "Appendices to Guide for Mapping T Information Systems to Security Categories"

Other resources:

- An OpenSSL Manual is available here – for commands for h
- A Linux Fundamentals guidebook is available here
- Hydra manual here
- Hashcat manual here
- John the Ripper manual here

Grading

Grading

Milestones	Individual	40%
Lab Assignments	Individual	25%
Reading Summaries	Individual	10%
Discussion Briefs	Individual	10%
In-Class Participation	Individual	15%
Total		**100%**

Milestones

Milestone Projects (40%)

Students will complete Milestone projects that utilize hands-on skills and apply knowledge from class discussions and lab activities. Each will require submission of a written report for superiors or consulting clients to advise them of important cybersecurity concerns.

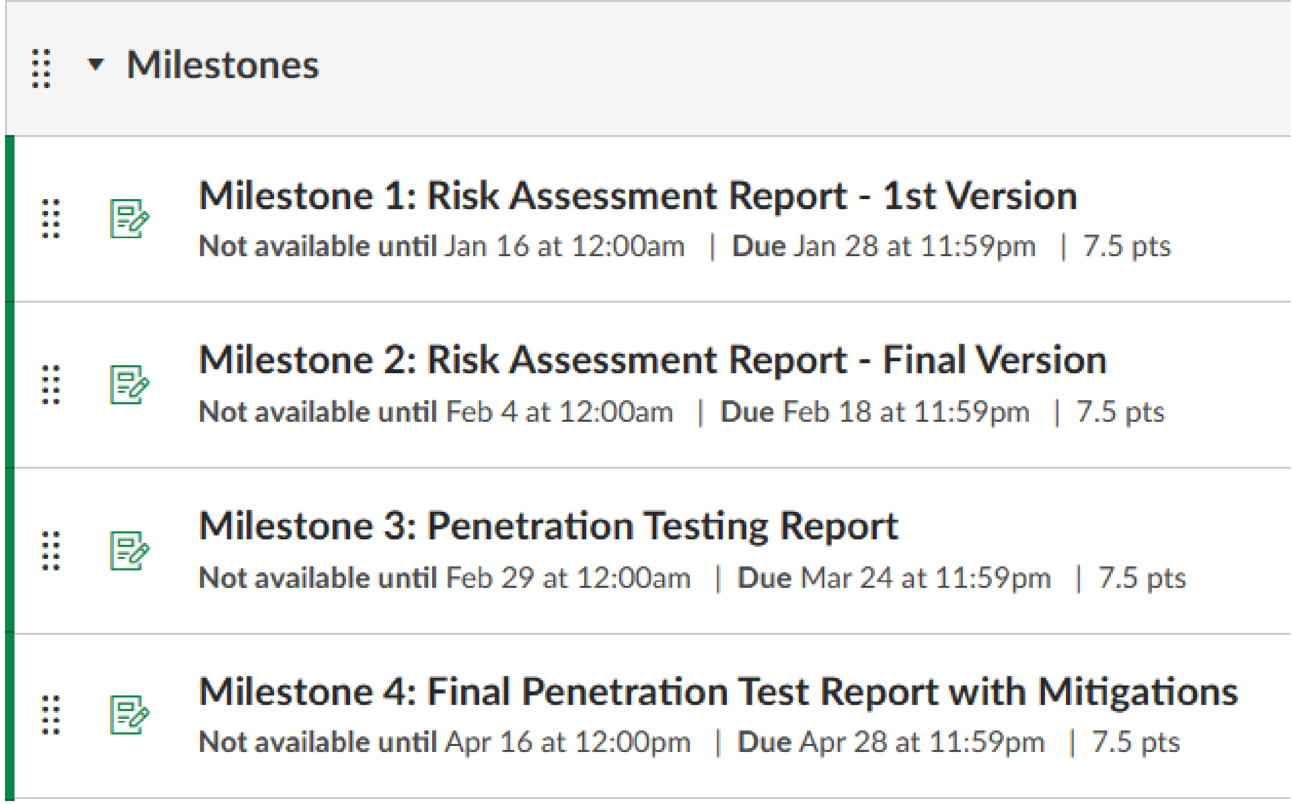
There are four milestone project reports that will help students develop professional written and verbal cybersecurity communication skills.

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

- Late submissions are subject to a 20% deduction in points per each 12 hours late.
- **Note:** *Completing lab assignments 1-7 during the weeks they are assigned will provide you with necessary knowledge and skills that will enable you to complete Milestones 3 & 4.*

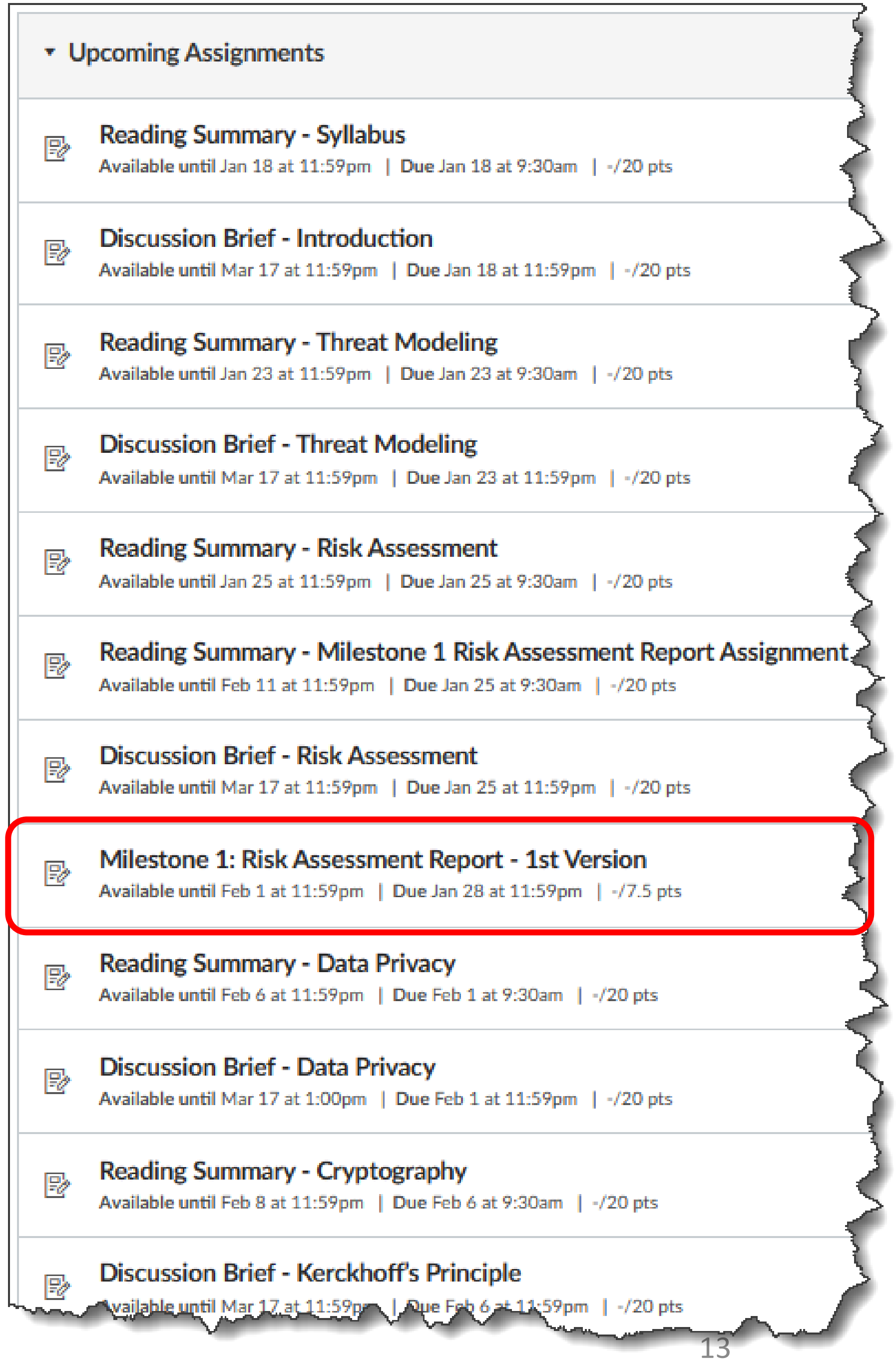
Milestones are found in Canvas

Section 001: https://templeu.instructure.com/courses/139106
Section 003: https://templeu.instructure.com/courses/139394



Milestones

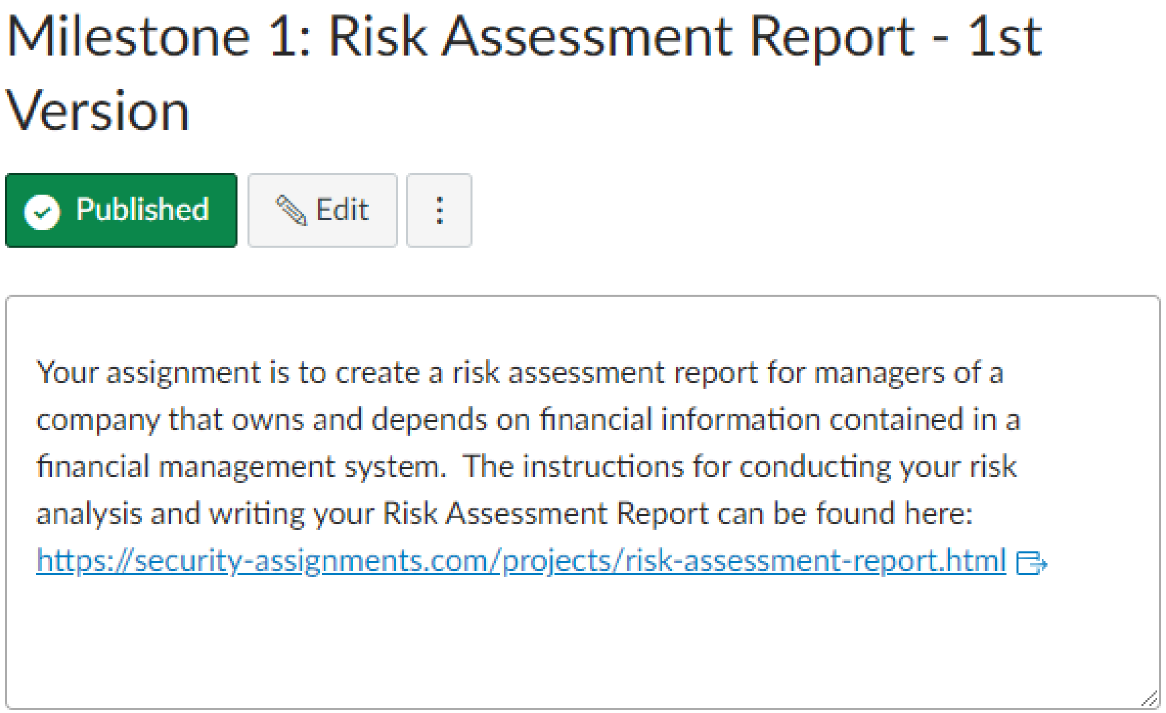
- Milestone 1: Risk Assessment Report - 1st Version
  Not available until Jan 16 at 12:00am | Due Jan 28 at 11:59pm | 7.5 pts
- Milestone 2: Risk Assessment Report - Final Version
  Not available until Feb 4 at 12:00am | Due Feb 18 at 11:59pm | 7.5 pts
- Milestone 3: Penetration Testing Report
  Not available until Feb 29 at 12:00am | Due Mar 24 at 11:59pm | 7.5 pts
- Milestone 4: Final Penetration Test Report with Mitigations
  Not available until Apr 16 at 12:00pm | Due Apr 28 at 11:59pm | 7.5 pts



Upcoming Assignments

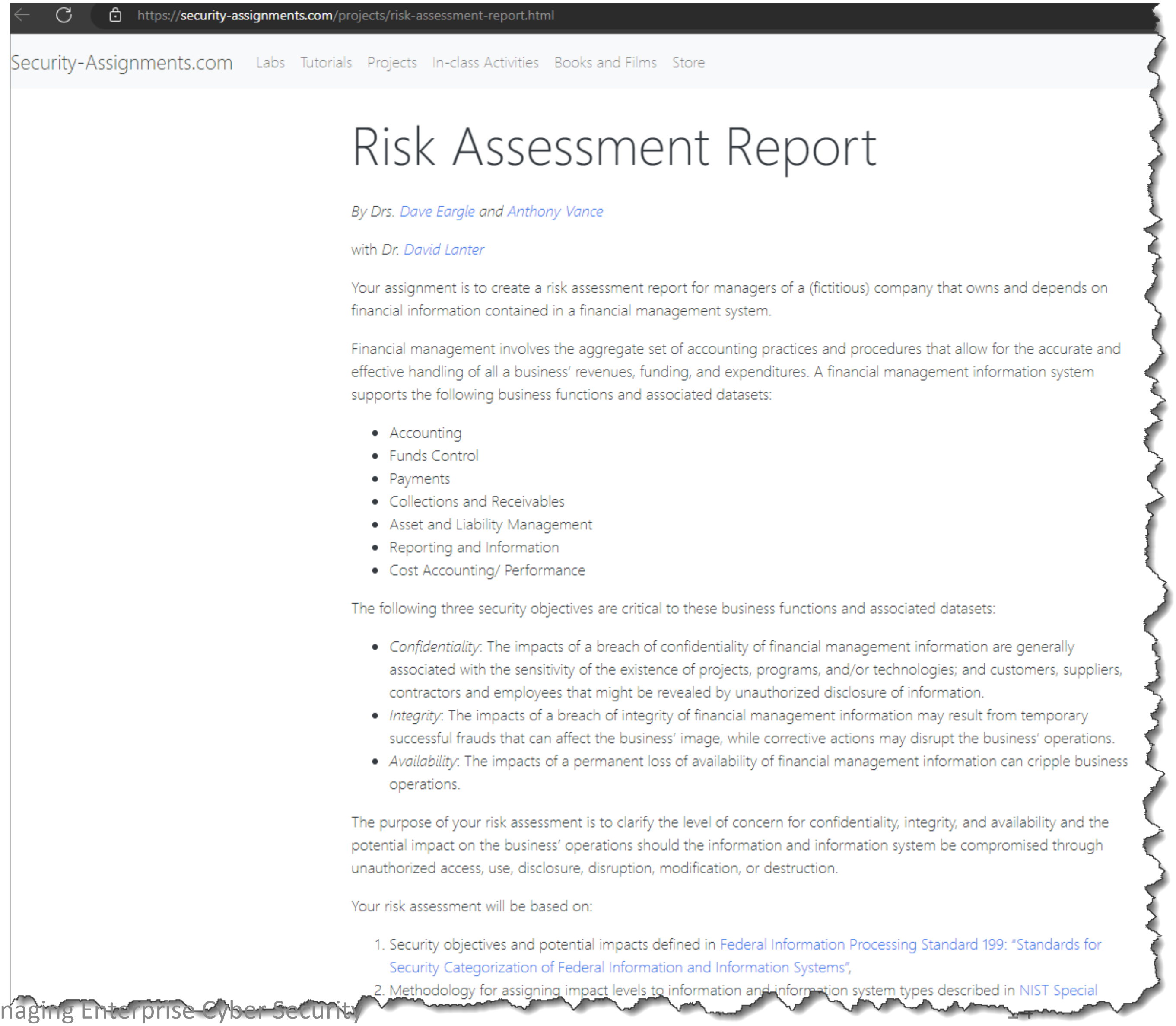
- Reading Summary - Syllabus
  Available until Jan 18 at 11:59pm | Due Jan 18 at 9:30am | -/20 pts
- Discussion Brief - Introduction
  Available until Mar 17 at 11:59pm | Due Jan 18 at 11:59pm | -/20 pts
- Reading Summary - Threat Modeling
  Available until Jan 23 at 11:59pm | Due Jan 23 at 9:30am | -/20 pts
- Discussion Brief - Threat Modeling
  Available until Mar 17 at 11:59pm | Due Jan 23 at 11:59pm | -/20 pts
- Reading Summary - Risk Assessment
  Available until Jan 25 at 11:59pm | Due Jan 25 at 9:30am | -/20 pts
- Reading Summary - Milestone 1 Risk Assessment Report Assignment
  Available until Feb 11 at 11:59pm | Due Jan 25 at 9:30am | -/20 pts
- Discussion Brief - Risk Assessment
  Available until Mar 17 at 11:59pm | Due Jan 25 at 11:59pm | -/20 pts
- Milestone 1: Risk Assessment Report - 1st Version
  Available until Feb 1 at 11:59pm | Due Jan 28 at 11:59pm | -/7.5 pts
- Reading Summary - Data Privacy
  Available until Feb 6 at 11:59pm | Due Feb 1 at 9:30am | -/20 pts
- Discussion Brief - Data Privacy
  Available until Mar 17 at 1:00pm | Due Feb 1 at 11:59pm | -/20 pts
- Reading Summary - Cryptography
  Available until Feb 8 at 11:59pm | Due Feb 6 at 9:30am | -/20 pts
- Discussion Brief - Kerckhoff's Principle
  Available until Mar 17 at 11:59pm | Due Feb 6 at 11:59pm | -/20 pts

Milestones are found in Canvas



Milestone 1: Risk Assessment Report - 1st Version

Your assignment is to create a risk assessment report for managers of a company that owns and depends on financial information contained in a financial management system. The instructions for conducting your risk analysis and writing your Risk Assessment Report can be found here: https://security-assignments.com/projects/risk-assessment-report.html



Risk Assessment Report

By Drs. Dave Eargle and Anthony Vance

with Dr. *David Lanter*

Your assignment is to create a risk assessment report for managers of a (fictitious) company that owns and depends on financial information contained in a financial management system.

Financial management involves the aggregate set of accounting practices and procedures that allow for the accurate and effective handling of all a business' revenues, funding, and expenditures. A financial management information system supports the following business functions and associated datasets:

- Accounting
- Funds Control
- Payments
- Collections and Receivables
- Asset and Liability Management
- Reporting and Information
- Cost Accounting/ Performance

The following three security objectives are critical to these business functions and associated datasets:

- *Confidentiality*: The impacts of a breach of confidentiality of financial management information are generally associated with the sensitivity of the existence of projects, programs, and/or technologies; and customers, suppliers, contractors and employees that might be revealed by unauthorized disclosure of information.
- *Integrity*: The impacts of a breach of integrity of financial management information may result from temporary successful frauds that can affect the business' image, while corrective actions may disrupt the business' operations.
- *Availability*: The impacts of a permanent loss of availability of financial management information can cripple business operations.

The purpose of your risk assessment is to clarify the level of concern for confidentiality, integrity, and availability and the potential impact on the business' operations should the information and information system be compromised through unauthorized access, use, disclosure, disruption, modification, or destruction.

Your risk assessment will be based on:

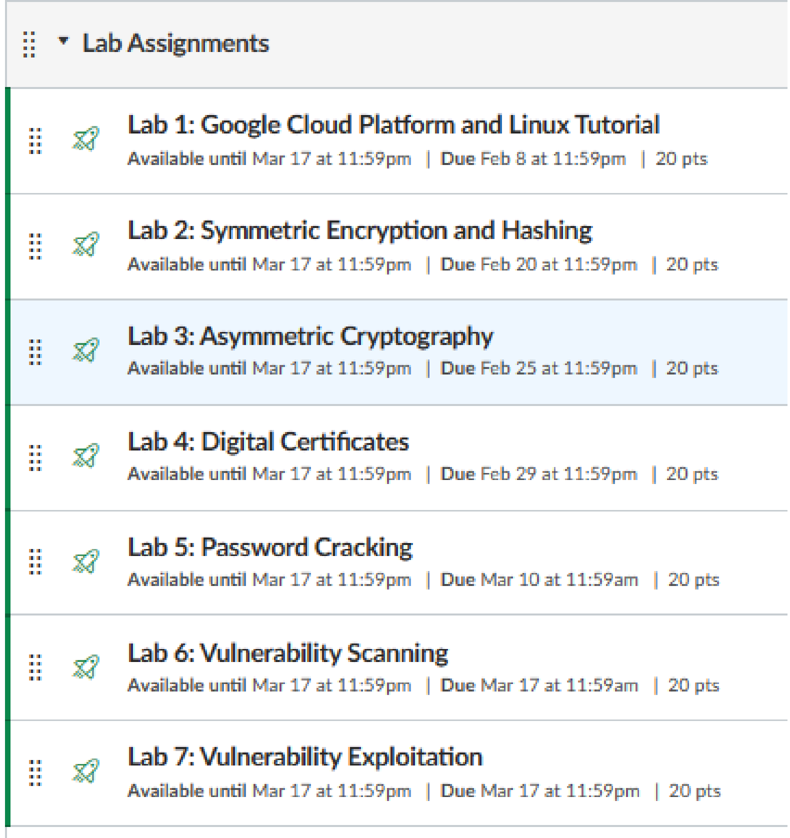
1. Security objectives and potential impacts defined in Federal Information Processing Standard 199: "Standards for Security Categorization of Federal Information and Information Systems",
2. Methodology for assigning impact levels to information and information system types described in NIST Special

Labs

<u>Lab Assignments (25%)</u>

These are hands-on learning activities that are completed by students outside of class.

- There are 9 labs. It is strongly recommended to complete each lab within the week that the corresponding topic is covered in class throughout the semester.
- Notes:
  - ***Completing Lab Assignments 1-7 will provide you with knowledge and skills necessary for completing Milestones 3 & 4.***
  - ***Completing Milestones 2 & 3 will provide you with the knowledge necessary for completing your Milestone 3 & 4 report***
- Labs 1-7 are due by Sunday, March 17, 2024. Labs 8-9 are due by Sunday, April 28, 2024. No late submissions will be accepted.



Lab Assignments

Lab 1: Google Cloud Platform and Linux Tutorial
Available until Mar 17 at 11:59pm | Due Feb 8 at 11:59pm | 20 pts

Lab 2: Symmetric Encryption and Hashing
Available until Mar 17 at 11:59pm | Due Feb 20 at 11:59pm | 20 pts

Lab 3: Asymmetric Cryptography
Available until Mar 17 at 11:59pm | Due Feb 25 at 11:59pm | 20 pts

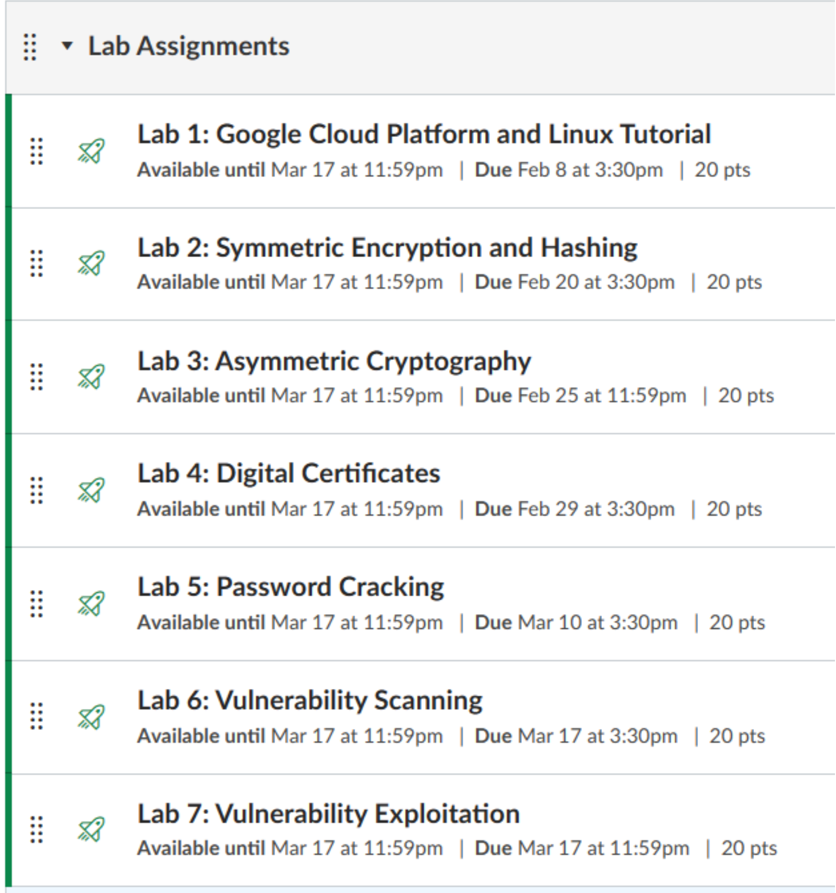
Lab 4: Digital Certificates
Available until Mar 17 at 11:59pm | Due Feb 29 at 11:59pm | 20 pts

Lab 5: Password Cracking
Available until Mar 17 at 11:59pm | Due Mar 10 at 11:59am | 20 pts

Lab 6: Vulnerability Scanning
Available until Mar 17 at 11:59pm | Due Mar 17 at 11:59am | 20 pts

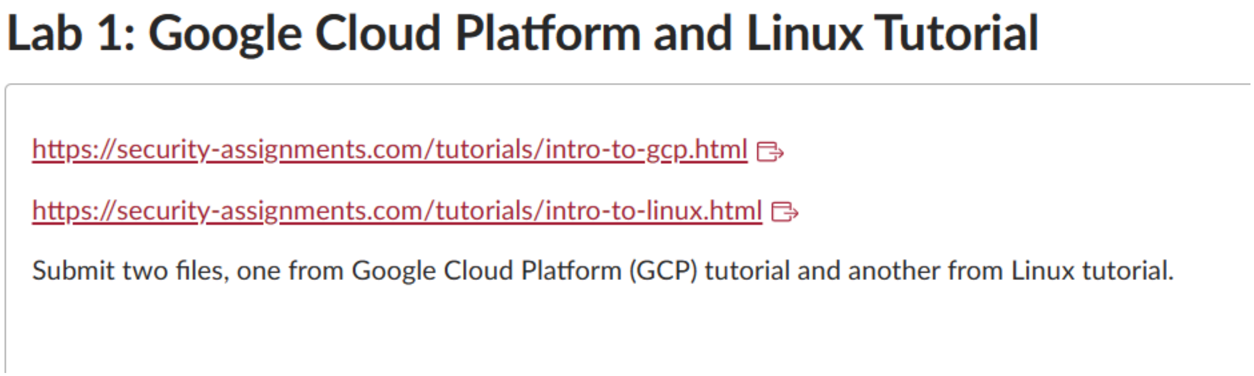
Lab 7: Vulnerability Exploitation
Available until Mar 17 at 11:59pm | Due Mar 17 at 11:59pm | 20 pts

Labs are found in Canvas



Lab Assignments

- **Lab 1: Google Cloud Platform and Linux Tutorial**
  Available until Mar 17 at 11:59pm | **Due** Feb 8 at 3:30pm | 20 pts
- **Lab 2: Symmetric Encryption and Hashing**
  Available until Mar 17 at 11:59pm | **Due** Feb 20 at 3:30pm | 20 pts
- **Lab 3: Asymmetric Cryptography**
  Available until Mar 17 at 11:59pm | **Due** Feb 25 at 11:59pm | 20 pts
- **Lab 4: Digital Certificates**
  Available until Mar 17 at 11:59pm | **Due** Feb 29 at 3:30pm | 20 pts
- **Lab 5: Password Cracking**
  Available until Mar 17 at 11:59pm | **Due** Mar 10 at 3:30pm | 20 pts
- **Lab 6: Vulnerability Scanning**
  Available until Mar 17 at 11:59pm | **Due** Mar 17 at 3:30pm | 20 pts
- **Lab 7: Vulnerability Exploitation**
  Available until Mar 17 at 11:59pm | **Due** Mar 17 at 11:59pm | 20 pts

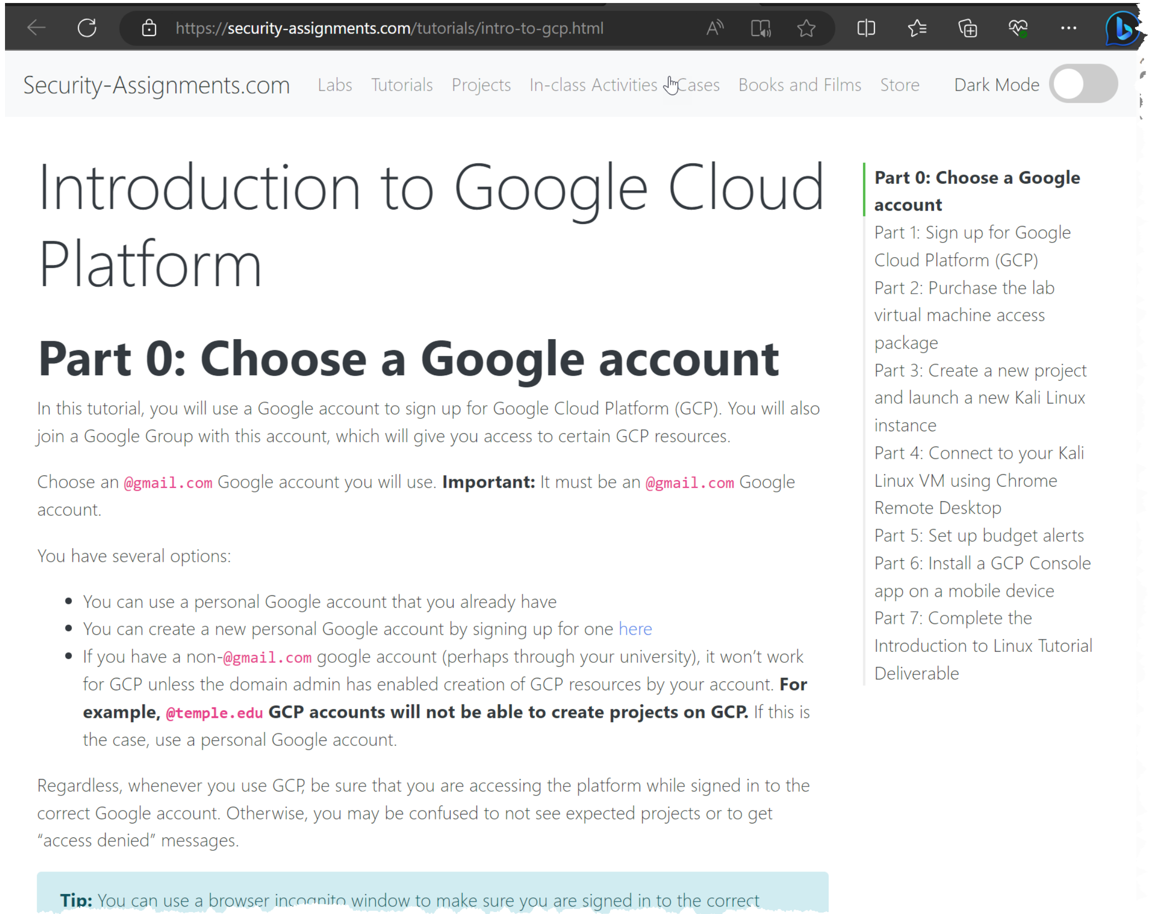


Lab 1: Google Cloud Platform and Linux Tutorial

https://security-assignments.com/tutorials/intro-to-gcp.html

https://security-assignments.com/tutorials/intro-to-linux.html

Submit two files, one from Google Cloud Platform (GCP) tutorial and another from Linux tutorial.



https://security-assignments.com/tutorials/intro-to-gcp.html

Introduction to Google Cloud Platform

Part 0: Choose a Google account

In this tutorial, you will use a Google account to sign up for Google Cloud Platform (GCP). You will also join a Google Group with this account, which will give you access to certain GCP resources.

Choose an `@gmail.com` Google account you will use. **Important:** It must be an `@gmail.com` Google account.

You have several options:

- You can use a personal Google account that you already have
- You can create a new personal Google account by signing up for one here
- If you have a non-`@gmail.com` google account (perhaps through your university), it won't work for GCP unless the domain admin has enabled creation of GCP resources by your account. **For example, `@temple.edu` GCP accounts will not be able to create projects on GCP.** If this is the case, use a personal Google account.

Regardless, whenever you use GCP, be sure that you are accessing the platform while signed in to the correct Google account. Otherwise, you may be confused to not see expected projects or to get "access denied" messages.

Tip: You can use a browser incognito window to make sure you are signed in to the correct

Labs

<u>Lab Peer Support</u>:

Students are encouraged to help each other complete lab and milestone assignments.

ITA – Camryn L. Zavacky

camryn.zavacky@temple.edu

Office Hours – TBA

Grading

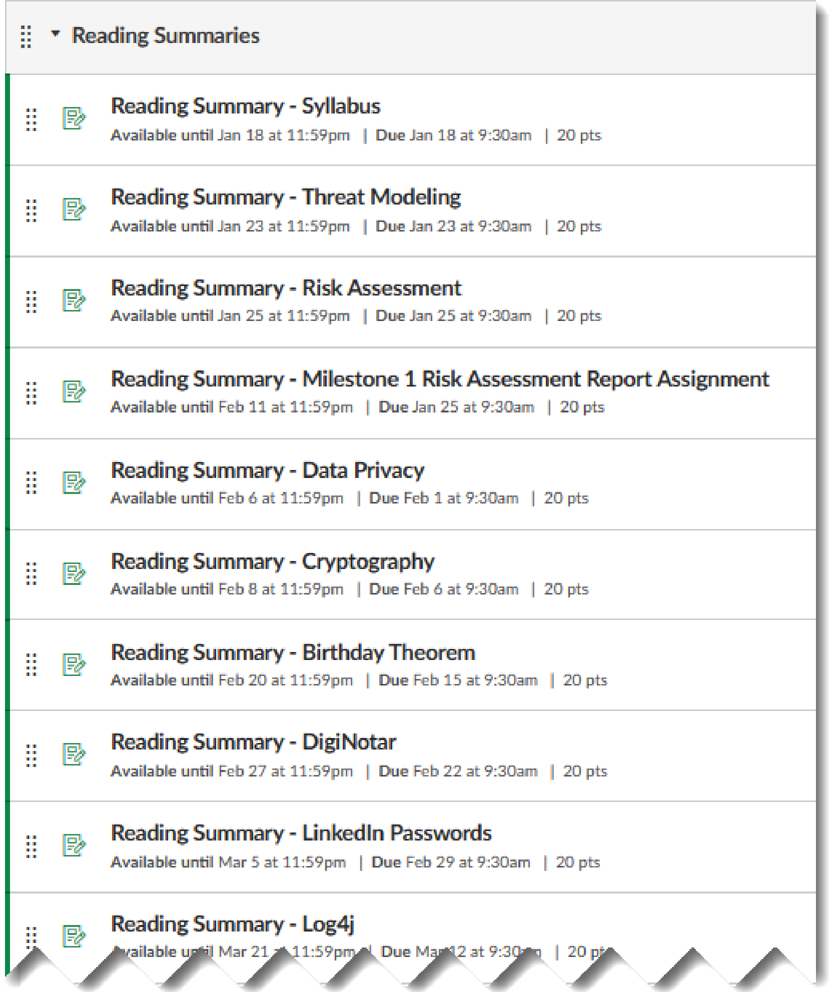
Grading		
Milestones	Individual	40%
Lab Assignments	Individual	25%
Reading Summaries	Individual	10%
Discussion Briefs	Individual	10%
In-Class Participation	Individual	15%
Total		**100%**

Reading Summaries (10%)

Students are to summarize assigned readings (news articles, textbook chapters, or Harvard Business cases) before each week's class.

- Up to 200 words in each summary
- Due before the class on which the reading is assigned
- No late submission will be accepted
- **Goal:** This is to make sure students read assigned readings which promote more effective in-class discussions
- **Grading Criteria:** Clarity, Comprehensiveness, Spelling Grammar, and Organization

Reading Summaries are found in Canvas



Reading Summaries

Reading Summary - Syllabus
Available until Jan 18 at 11:59pm | Due Jan 18 at 9:30am | 20 pts

Reading Summary - Threat Modeling
Available until Jan 23 at 11:59pm | Due Jan 23 at 9:30am | 20 pts

Reading Summary - Risk Assessment
Available until Jan 25 at 11:59pm | Due Jan 25 at 9:30am | 20 pts

Reading Summary - Milestone 1 Risk Assessment Report Assignment
Available until Feb 11 at 11:59pm | Due Jan 25 at 9:30am | 20 pts

Reading Summary - Data Privacy
Available until Feb 6 at 11:59pm | Due Feb 1 at 9:30am | 20 pts

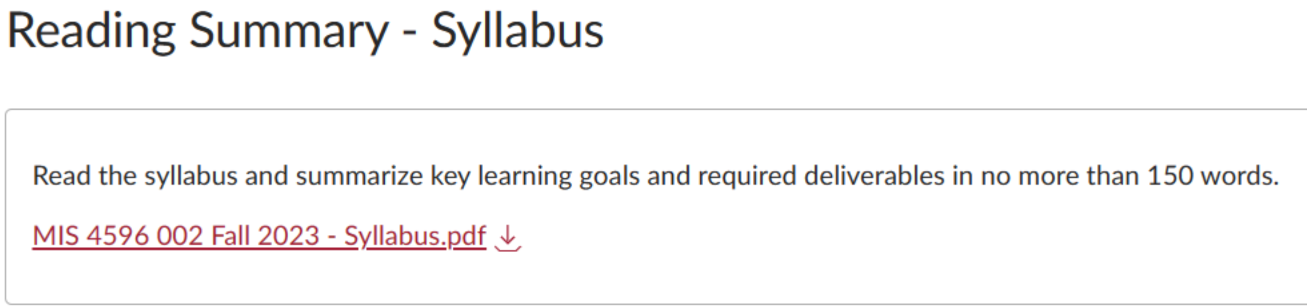
Reading Summary - Cryptography
Available until Feb 8 at 11:59pm | Due Feb 6 at 9:30am | 20 pts

Reading Summary - Birthday Theorem
Available until Feb 20 at 11:59pm | Due Feb 15 at 9:30am | 20 pts

Reading Summary - DigiNotar
Available until Feb 27 at 11:59pm | Due Feb 22 at 9:30am | 20 pts

Reading Summary - LinkedIn Passwords
Available until Mar 5 at 11:59pm | Due Feb 29 at 9:30am | 20 pts

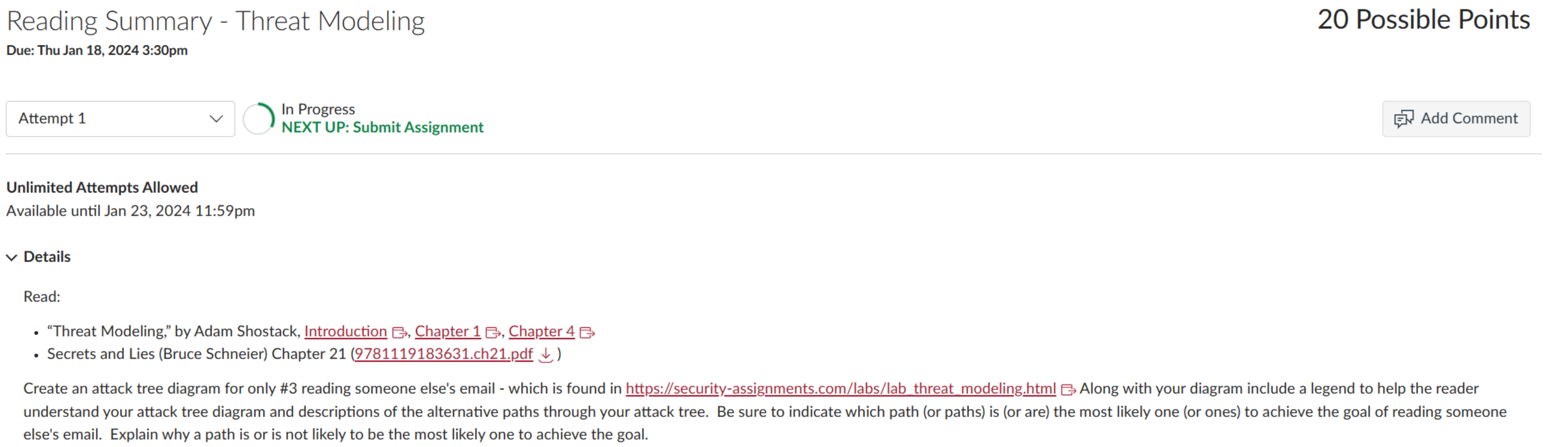
Reading Summary - Log4j
Available until Mar 21 at 11:59pm | Due Mar 12 at 9:30am | 20 pts



Reading Summary - Syllabus

Read the syllabus and summarize key learning goals and required deliverables in no more than 150 words.

MIS 4596 002 Fall 2023 - Syllabus.pdf



Reading Summary - Threat Modeling

Due: Thu Jan 18, 2024 3:30pm

20 Possible Points

Unlimited Attempts Allowed
Available until Jan 23, 2024 11:59pm

Details

Read:

- “Threat Modeling,” by Adam Shostack, Introduction, Chapter 1, Chapter 4
- Secrets and Lies (Bruce Schneier) Chapter 21 (9781119183631.ch21.pdf)

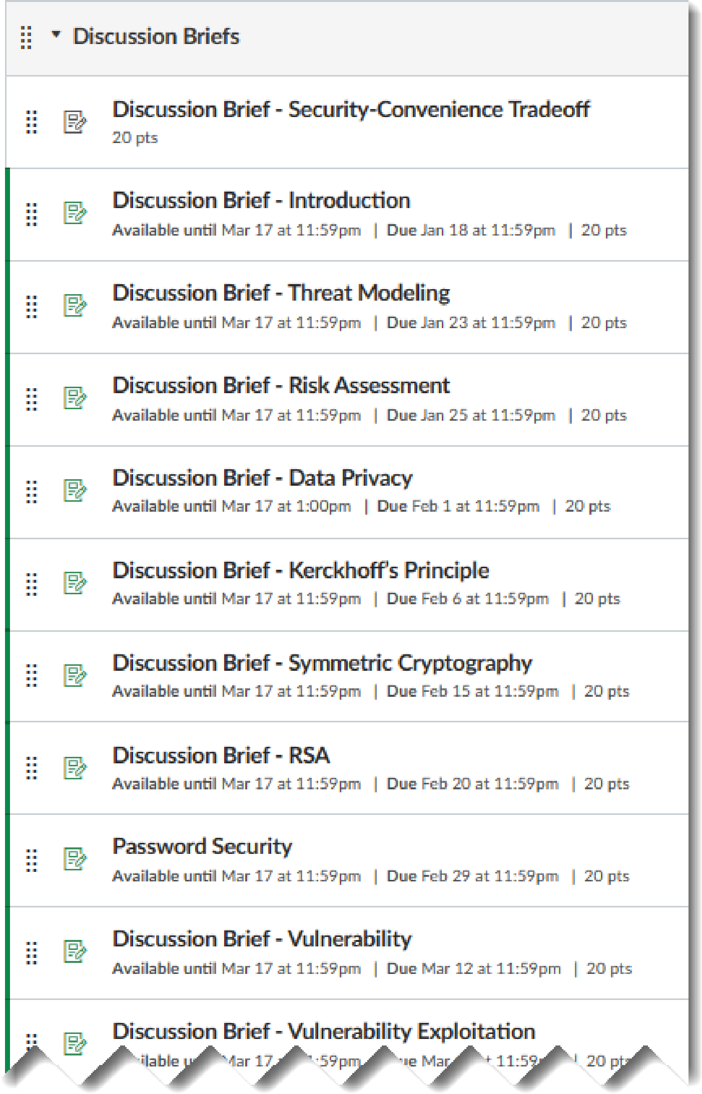
Create an attack tree diagram for only #3 reading someone else's email - which is found in https://security-assignments.com/labs/lab_threat_modeling.html Along with your diagram include a legend to help the reader understand your attack tree diagram and descriptions of the alternative paths through your attack tree. Be sure to indicate which path (or paths) is (or are) the most likely one (or ones) to achieve the goal of reading someone else's email. Explain why a path is or is not likely to be the most likely one to achieve the goal.

Discussion Briefs (10%)

After each week’s class, students are to write a short write-up that is based on in-class lecture & discussions.

- At least 150 words and no more than 300 words in each brief
- Students can skip up to two discussion briefs throughout the semester.
- It is strongly recommended that you write up your discussion brief after the associated class.
- Two deadlines: Sunday, March 17, 2024 is the deadline for discussion briefs for classes covered in weeks 1-8, and Sunday, April 28, 2024 is the deadline for discussion briefs for classes covered in weeks 9-12.
- No late submission is to be accepted.
- Grading Criteria: Clarity, Comprehensiveness, Spelling, Grammar, and Organization

Discussion Briefs are found in Canvas



Discussion Briefs

Discussion Brief - Security-Convenience Tradeoff
20 pts

Discussion Brief - Introduction
Available until Mar 17 at 11:59pm | Due Jan 18 at 11:59pm | 20 pts

Discussion Brief - Threat Modeling
Available until Mar 17 at 11:59pm | Due Jan 23 at 11:59pm | 20 pts

Discussion Brief - Risk Assessment
Available until Mar 17 at 11:59pm | Due Jan 25 at 11:59pm | 20 pts

Discussion Brief - Data Privacy
Available until Mar 17 at 1:00pm | Due Feb 1 at 11:59pm | 20 pts

Discussion Brief - Kerckhoff's Principle
Available until Mar 17 at 11:59pm | Due Feb 6 at 11:59pm | 20 pts

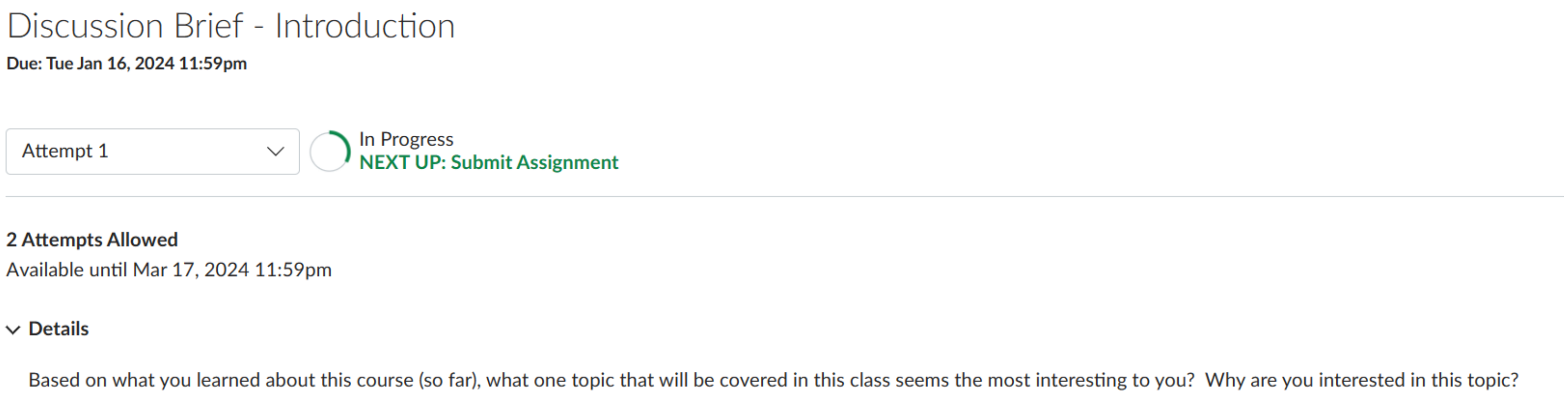
Discussion Brief - Symmetric Cryptography
Available until Mar 17 at 11:59pm | Due Feb 15 at 11:59pm | 20 pts

Discussion Brief - RSA
Available until Mar 17 at 11:59pm | Due Feb 20 at 11:59pm | 20 pts

Password Security
Available until Mar 17 at 11:59pm | Due Feb 29 at 11:59pm | 20 pts

Discussion Brief - Vulnerability
Available until Mar 17 at 11:59pm | Due Mar 12 at 11:59pm | 20 pts

Discussion Brief - Vulnerability Exploitation
ilable u Mar 17 59pm ue Mar 11:59 20 pt



Discussion Brief - Introduction

Due: Tue Jan 16, 2024 11:59pm

In Progress
NEXT UP: Submit Assignment

2 Attempts Allowed
Available until Mar 17, 2024 11:59pm

Details

Based on what you learned about this course (so far), what one topic that will be covered in this class seems the most interesting to you? Why are you interested in this topic?

In-Class Participation (15%)

In-Class Participation (15%)

- Attendance and in-class participation are key components of the learning experiences
- It is strongly encouraged to read/review assigned materials (readings, case studies, labs, milestone assignment, etc.) prior to class to enable you to actively take part in class discussions and activities

Technology requirements

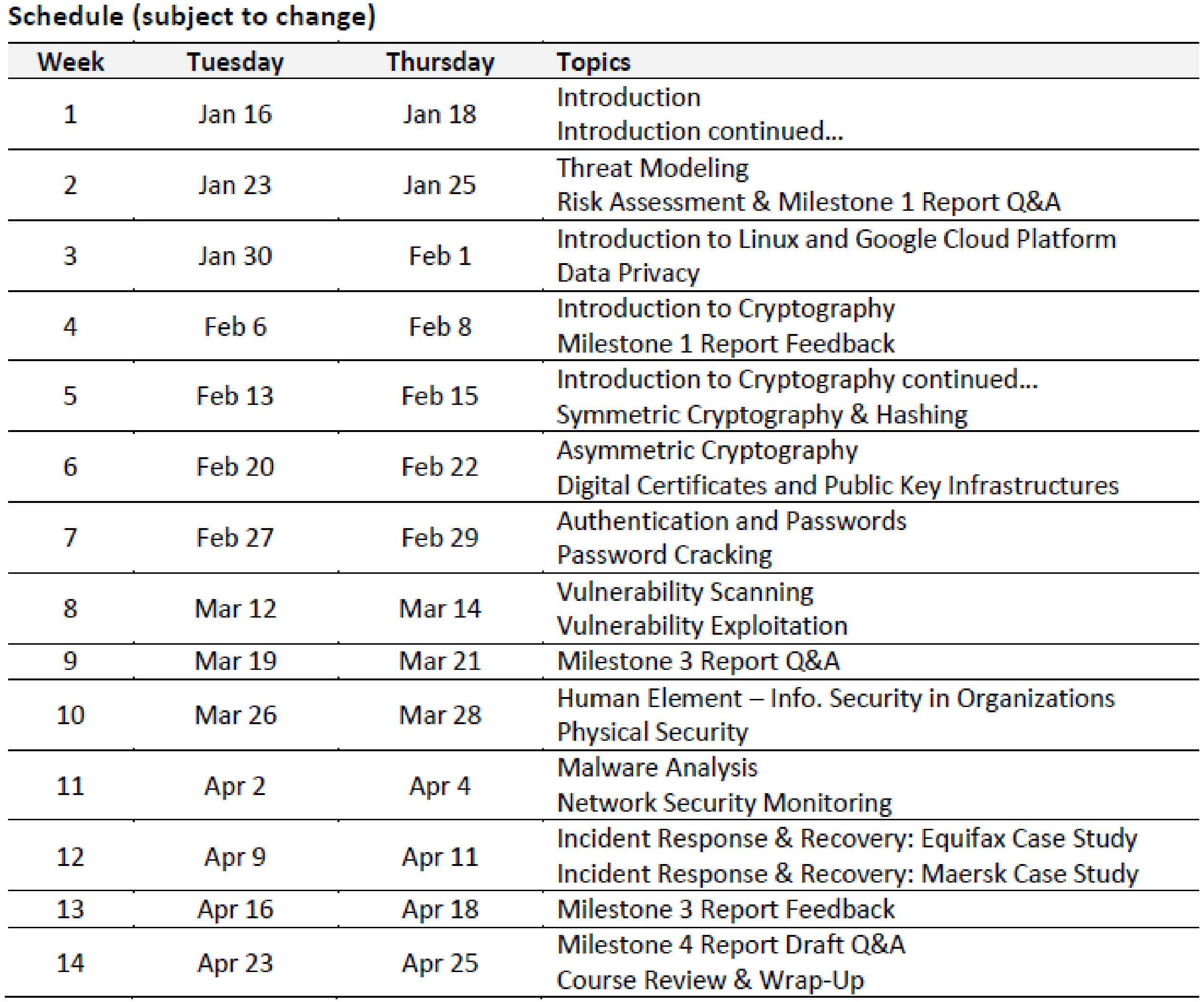
Information Security Assignments: Labs & Milestones 3 & 4

- 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 4 require lab virtual machine access for Google Cloud Platform (GCP) available for purchase for $50 here: https://security-assignments.com/store/

Google Cloud Platform (GCP)

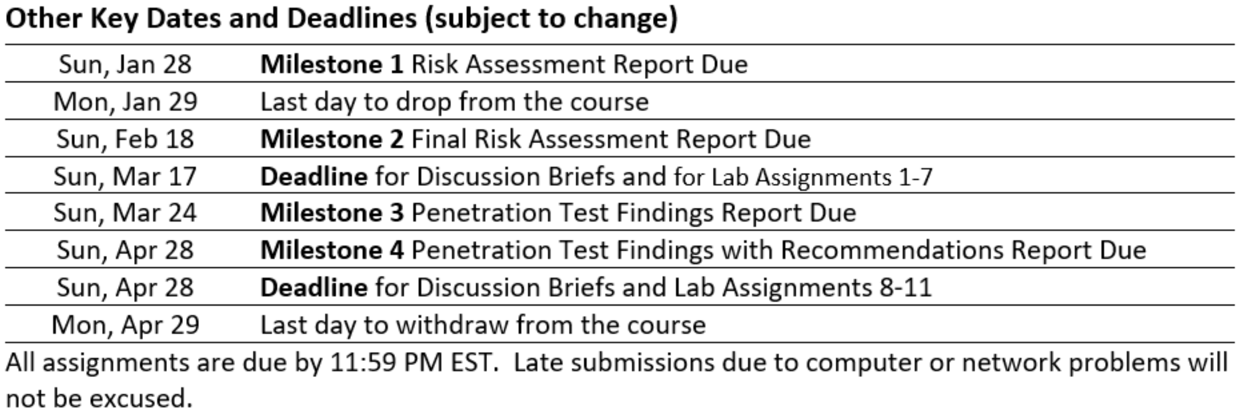
- This course uses GCP to run tools and virtual machines necessary to complete assignments.
- New accounts on GCP receive a $300 credit for no cost.
- Students should be able to complete this class without going over the credit and incurring cost.
- The instructor will have the students launch a Kali 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.

Schedule



Schedule (subject to change)

Week	Tuesday	Thursday	Topics
1	Jan 16	Jan 18	Introduction Introduction continued…
2	Jan 23	Jan 25	Threat Modeling Risk Assessment & Milestone 1 Report Q&A
3	Jan 30	Feb 1	Introduction to Linux and Google Cloud Platform Data Privacy
4	Feb 6	Feb 8	Introduction to Cryptography Milestone 1 Report Feedback
5	Feb 13	Feb 15	Introduction to Cryptography continued… Symmetric Cryptography & Hashing
6	Feb 20	Feb 22	Asymmetric Cryptography Digital Certificates and Public Key Infrastructures
7	Feb 27	Feb 29	Authentication and Passwords Password Cracking
8	Mar 12	Mar 14	Vulnerability Scanning Vulnerability Exploitation
9	Mar 19	Mar 21	Milestone 3 Report Q&A
10	Mar 26	Mar 28	Human Element – Info. Security in Organizations Physical Security
11	Apr 2	Apr 4	Malware Analysis Network Security Monitoring
12	Apr 9	Apr 11	Incident Response & Recovery: Equifax Case Study Incident Response & Recovery: Maersk Case Study
13	Apr 16	Apr 18	Milestone 3 Report Feedback
14	Apr 23	Apr 25	Milestone 4 Report Draft Q&A Course Review & Wrap-Up



Other Key Dates and Deadlines (subject to change)

Sun, Jan 28	**Milestone 1** Risk Assessment Report Due
Mon, Jan 29	Last day to drop from the course
Sun, Feb 18	**Milestone 2** Final Risk Assessment Report Due
Sun, Mar 17	**Deadline** for Discussion Briefs and for Lab Assignments 1-7
Sun, Mar 24	**Milestone 3** Penetration Test Findings Report Due
Sun, Apr 28	**Milestone 4** Penetration Test Findings with Recommendations Report Due
Sun, Apr 28	**Deadline** for Discussion Briefs and Lab Assignments 8-11
Mon, Apr 29	Last day to withdraw from the course

All assignments are due by 11:59 PM EST. Late submissions due to computer or network problems will not be excused.

Agenda

✓Instructor

✓Course overview

- Introduction
- Need for Cybersecurity Professionals

The value of business' data is at a peak

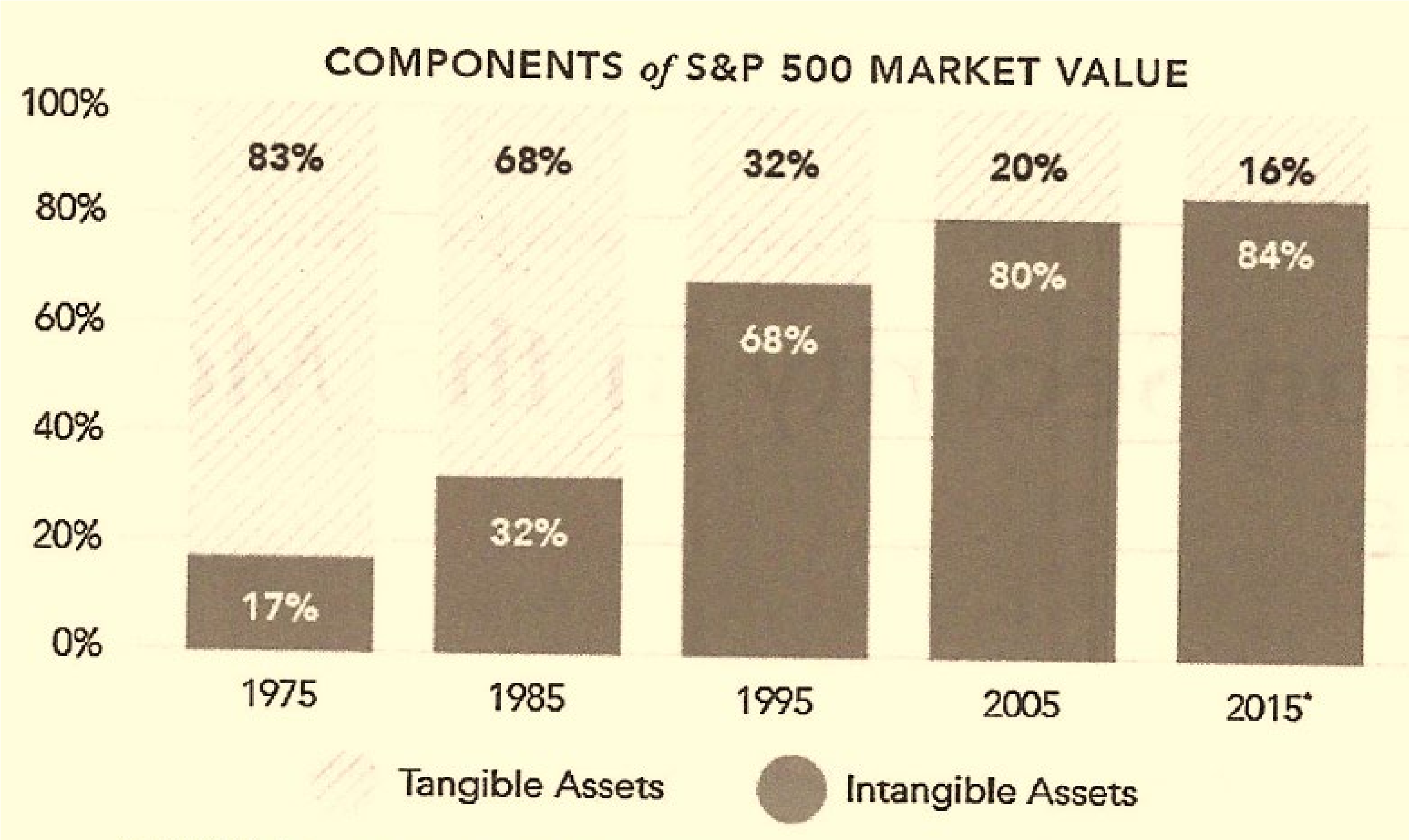


FIGURE 1.1 Change in public company assets from tangible to intangible.

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

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

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

Transformation of Information Security

1970 data security examples

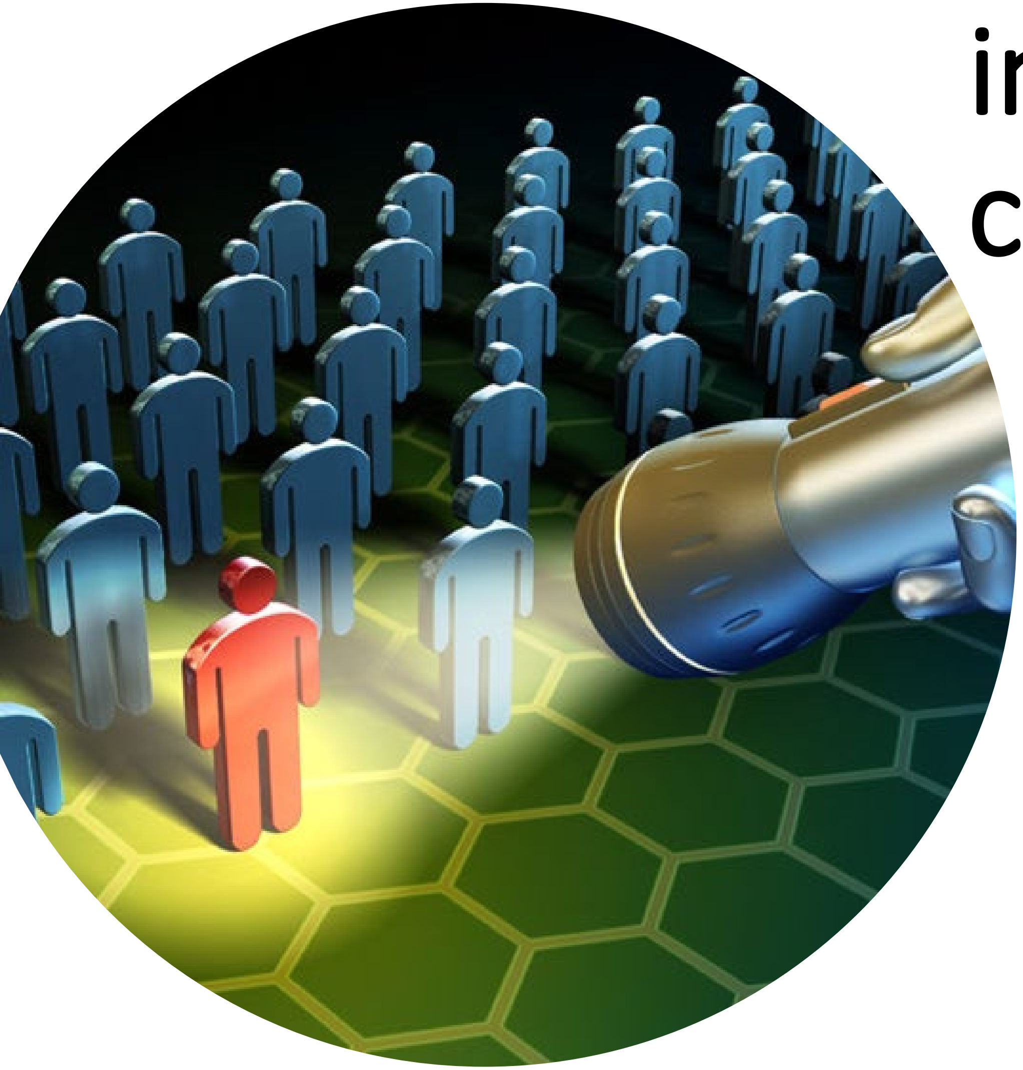
Guarding the photocopier

Watching who went in and out of the front door

Today's data security must consider

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

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

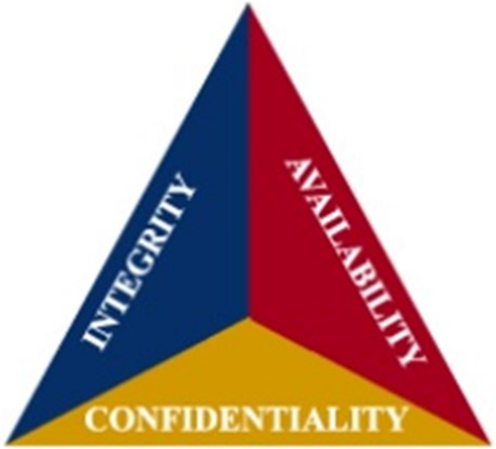


What one thing about information security has not changed over the years?

Human beings remain the primary vector for loss of corporate value

AND

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



Key concepts

Information and Information System security = Cybersecurity

…means protecting information and information systems from unathorized:

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

Key concepts

Threat

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

Vulnerability

Weakness that makes targets susceptible to an attack

Risk

Potential of loss from an attack

Risk Mitigation

Strategy for dealing with risk

What is a threat?

Physical

Technical

Administrative

Anything that has the potential to lead to unauthorized:

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

of an enterprises’ information or information systems

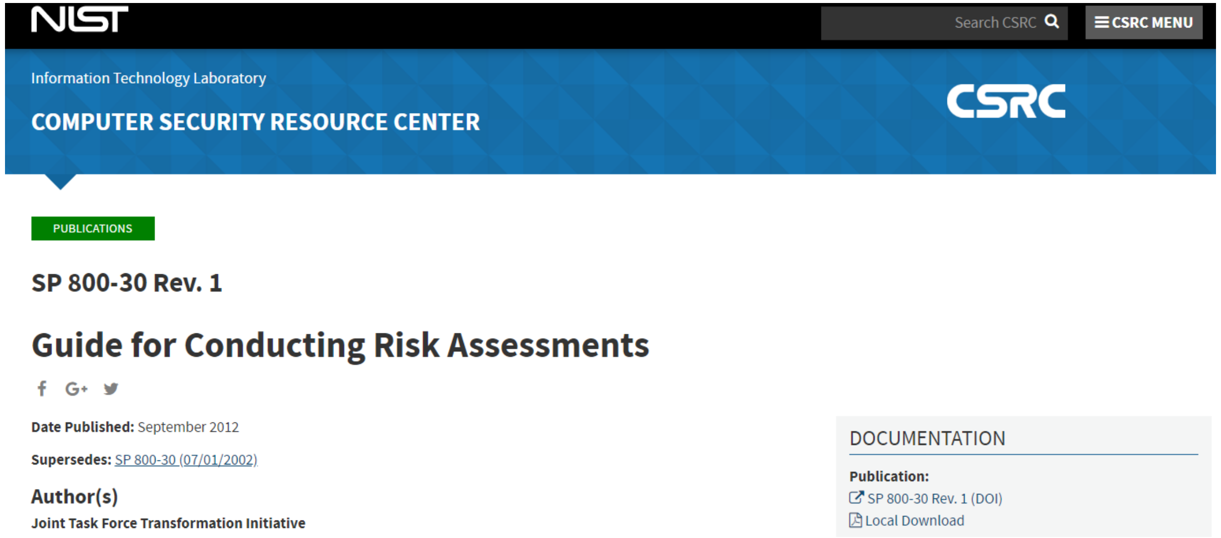
What is a threat…

Threats to information and information systems include:

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

Taxonomy of threat sources

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



Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

PUBLICATIONS

SP 800-30 Rev. 1

Guide for Conducting Risk Assessments

Date Published: September 2012

Supersedes: SP 800-30 (07/01/2002)

Author(s)

Joint Task Force Transformation Initiative

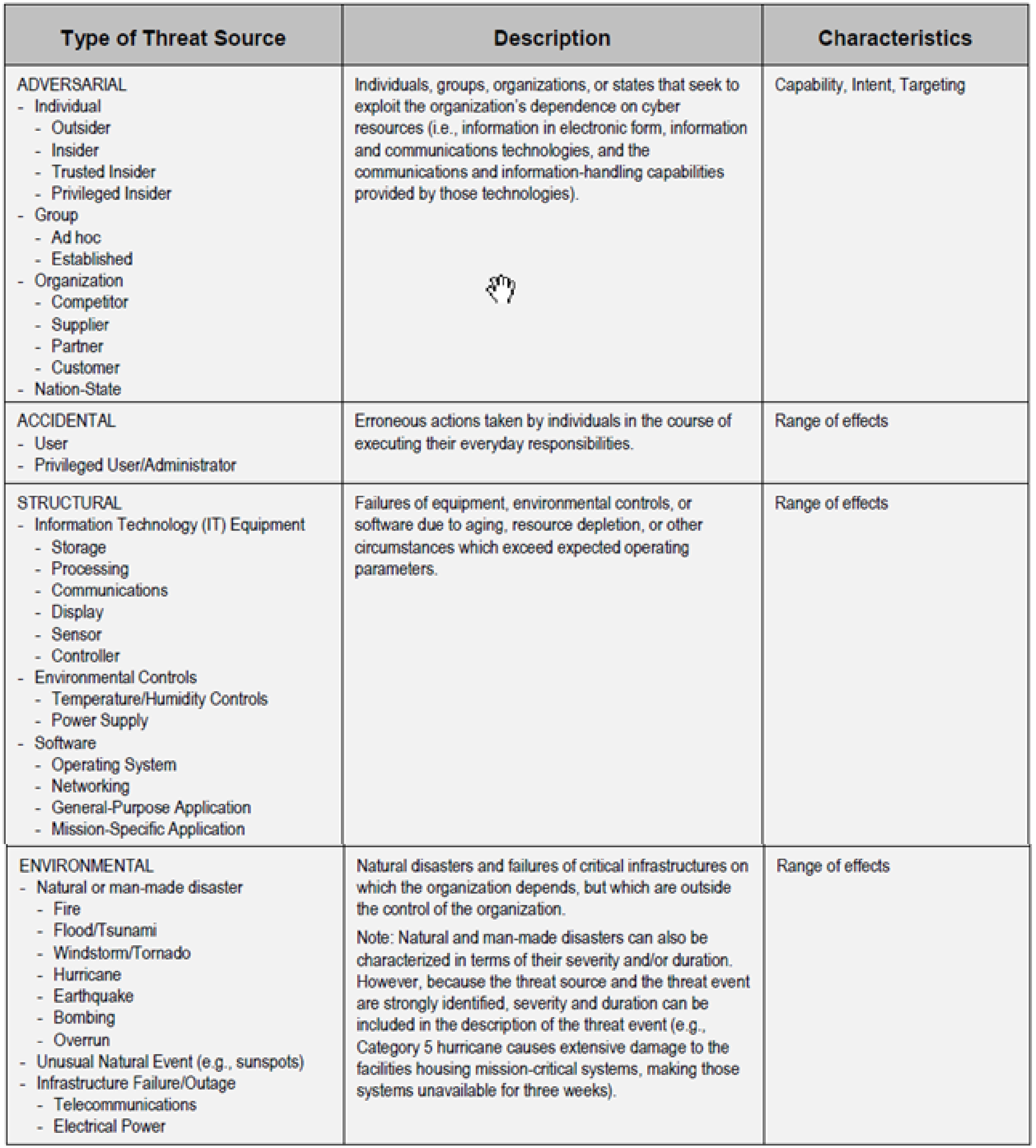
DOCUMENTATION

Publication:

SP 800-30 Rev. 1 (DOI)

Local Download

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

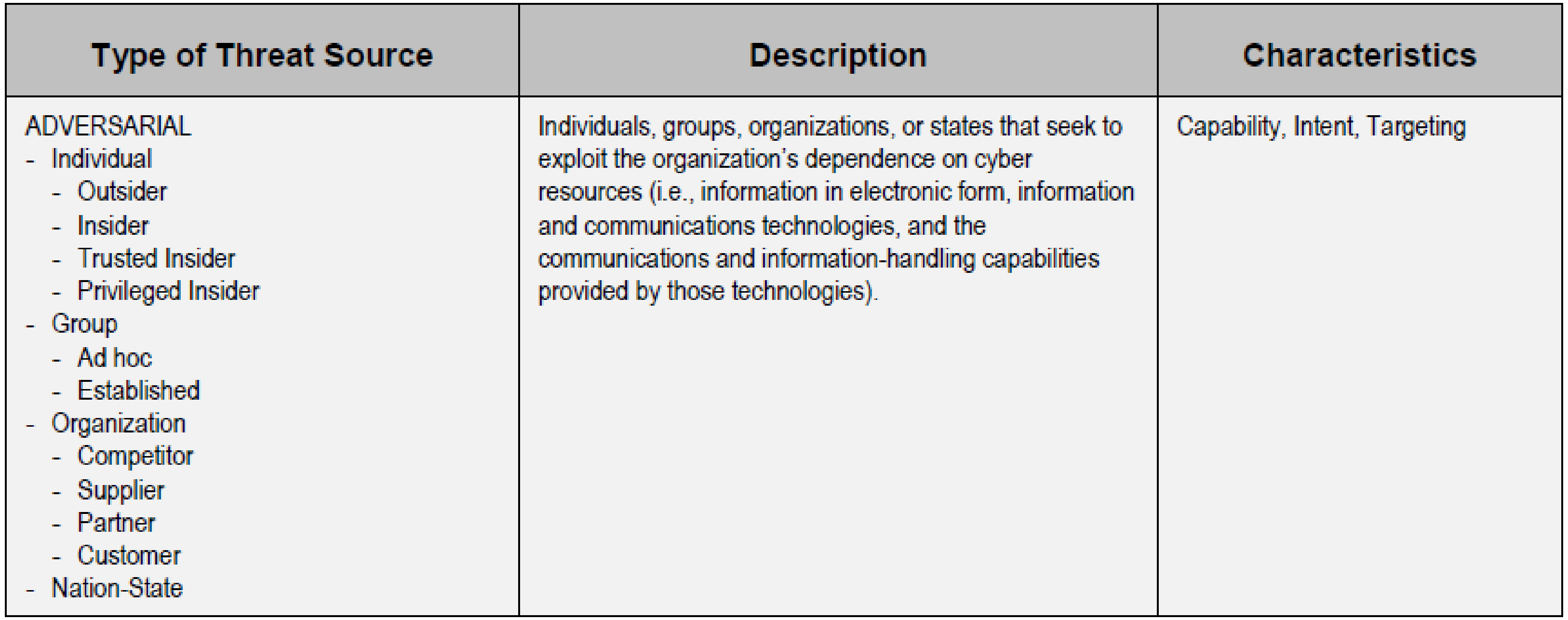


Type of Threat Source	Description	Characteristics
ADVERSARIAL - Individual - Outsider - Insider - Trusted Insider - Privileged Insider - Group - Ad hoc - Established - Organization - Competitor - Supplier - Partner - Customer - Nation-State	Individuals, groups, organizations, or states that seek to exploit 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.”

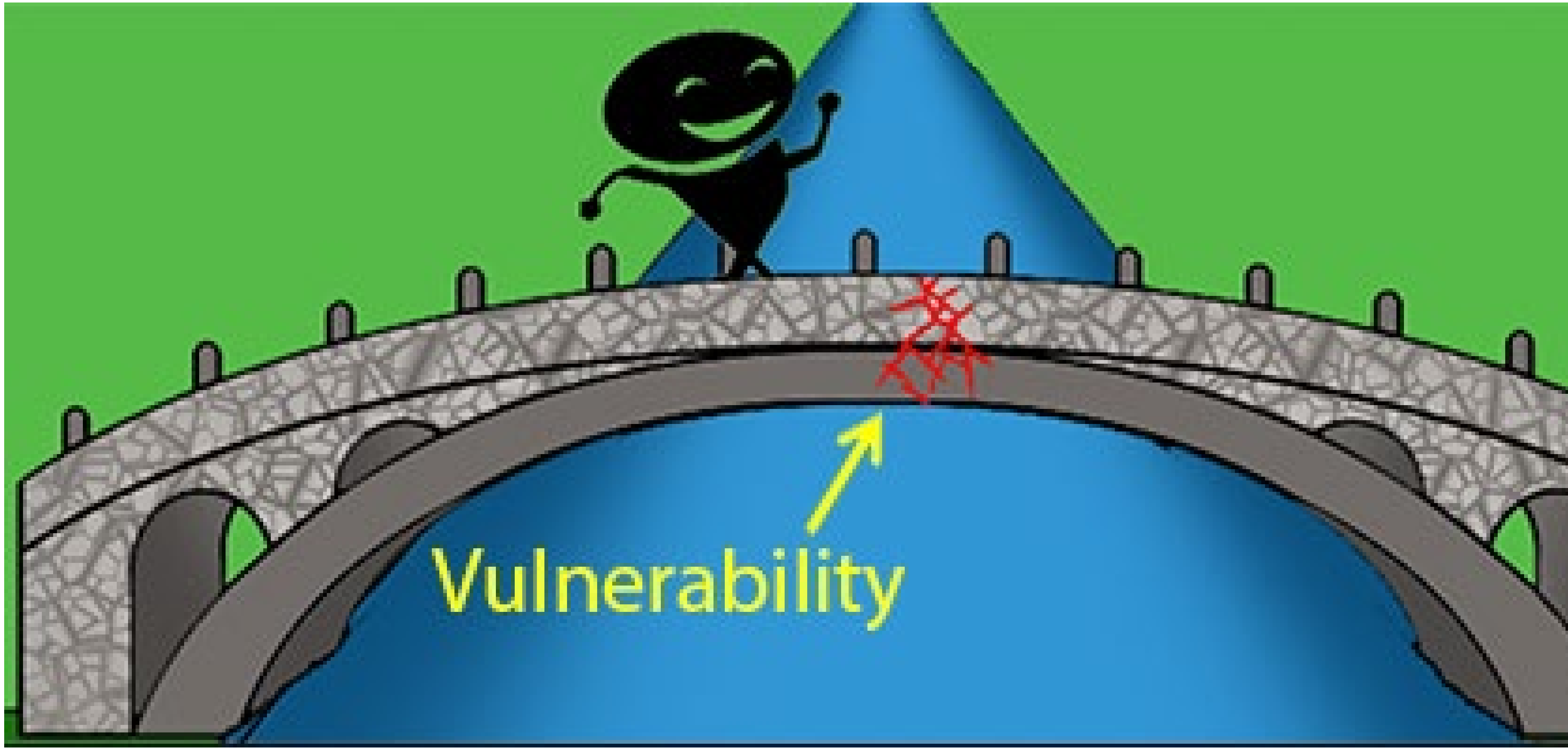
– Bruce Schneier



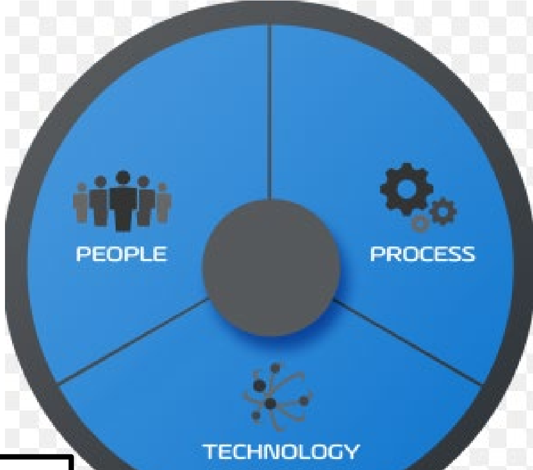
Type of Threat Source	Description	Characteristics
ADVERSARIAL - Individual - Outsider - Insider - Trusted Insider - Privileged Insider - Group - Ad hoc - Established - Organization - Competitor - Supplier - Partner - Customer - Nation-State	Individuals, groups, organizations, or states that seek to exploit 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

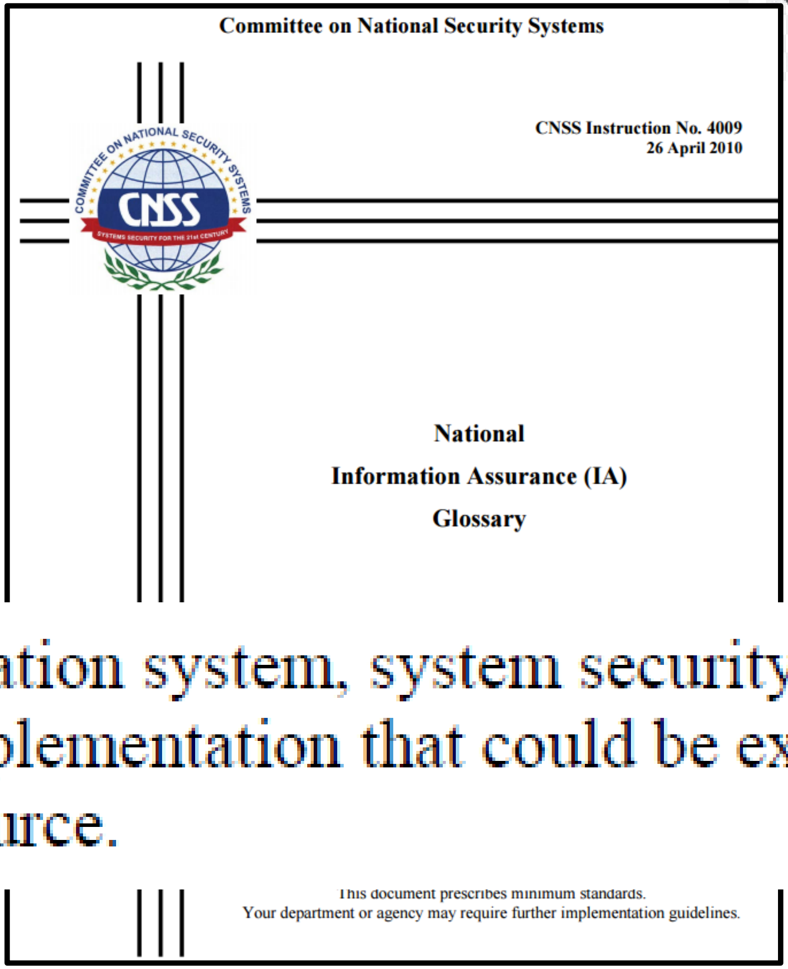
What is a Vulnerability?



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)

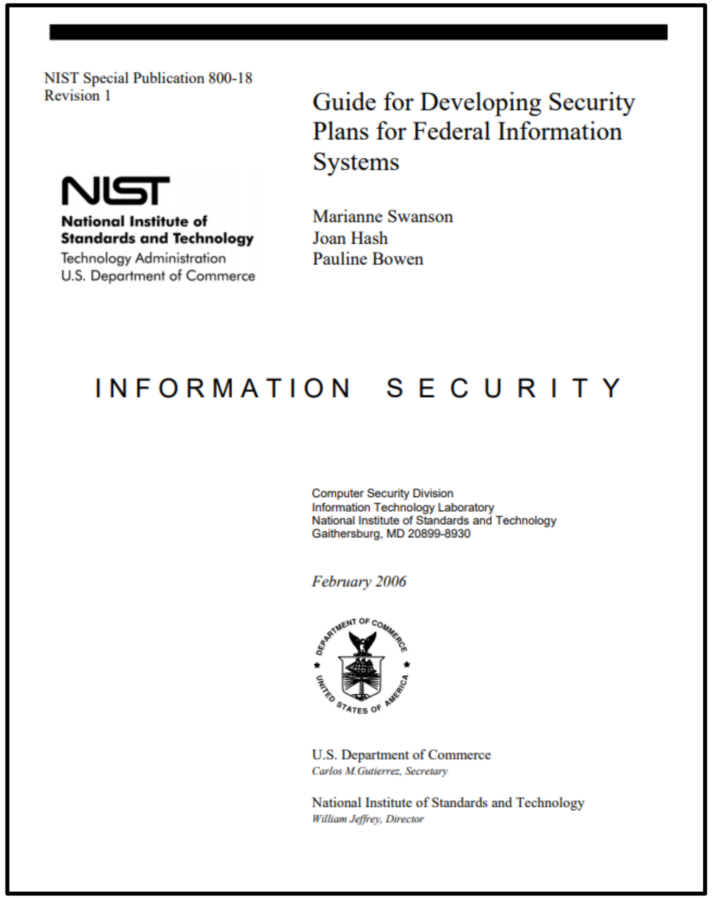
Glossary

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 areas which can lead to negative impacts:



NIST Special Publication 800-18
Revision 1

Guide for Developing Security Plans for Federal Information Systems

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

Marianne Swanson
Joan Hash
Pauline Bowen

INFORMATION SECURITY

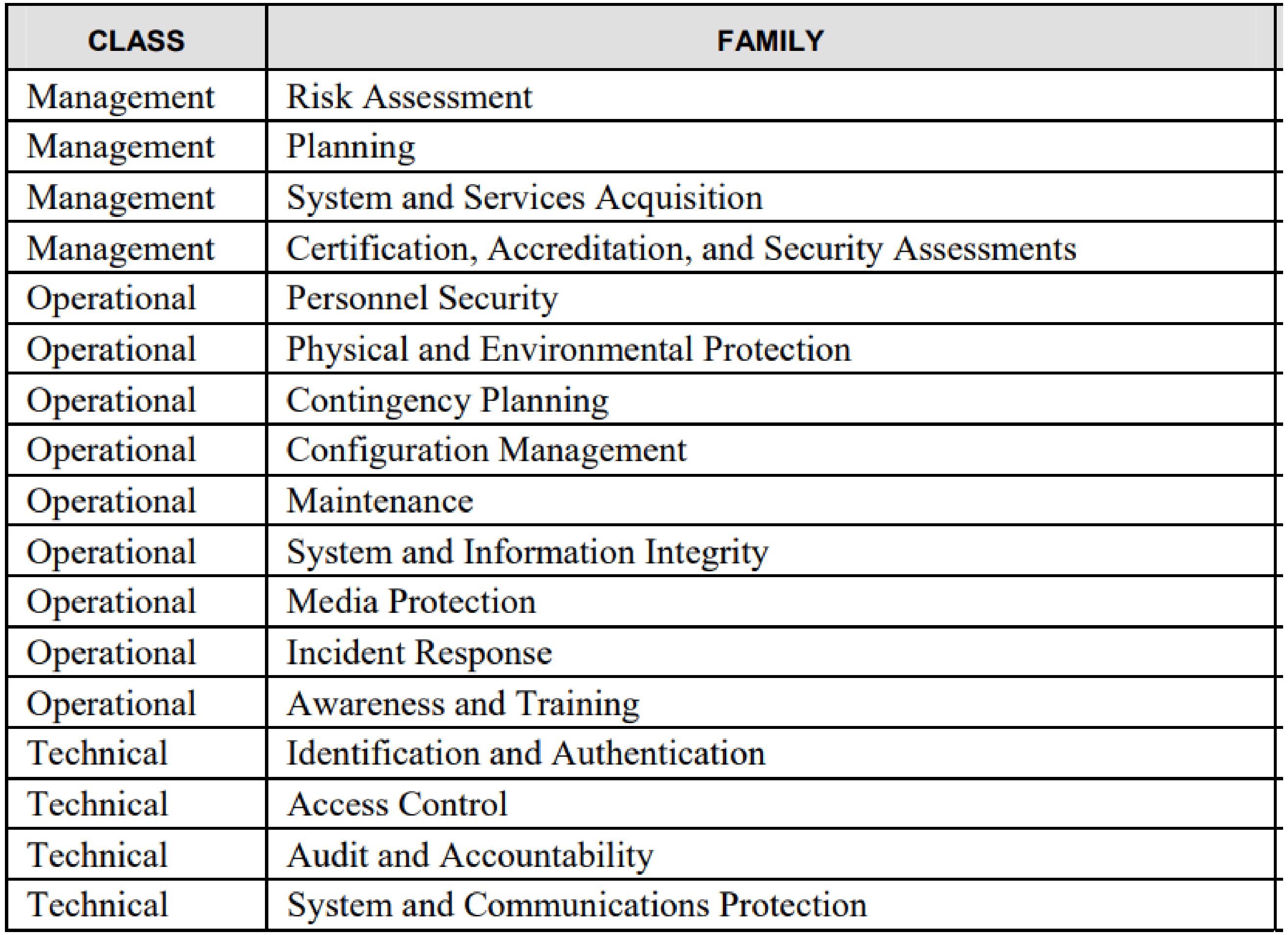
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

February 2006

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

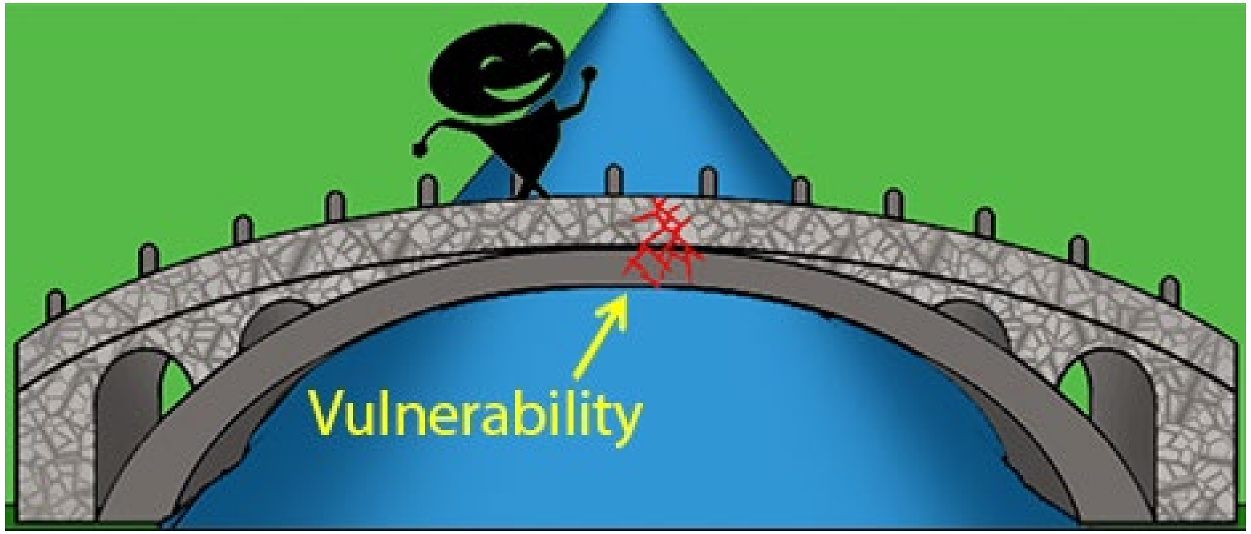
National Institute of Standards and Technology
William Jeffrey, Director

Cybersecurity Controls protect against impacts

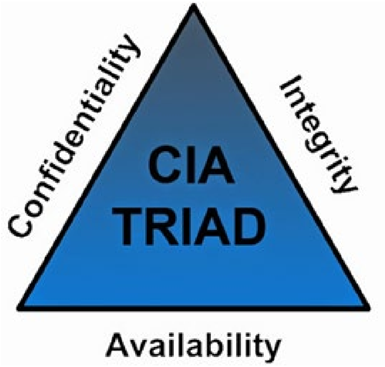


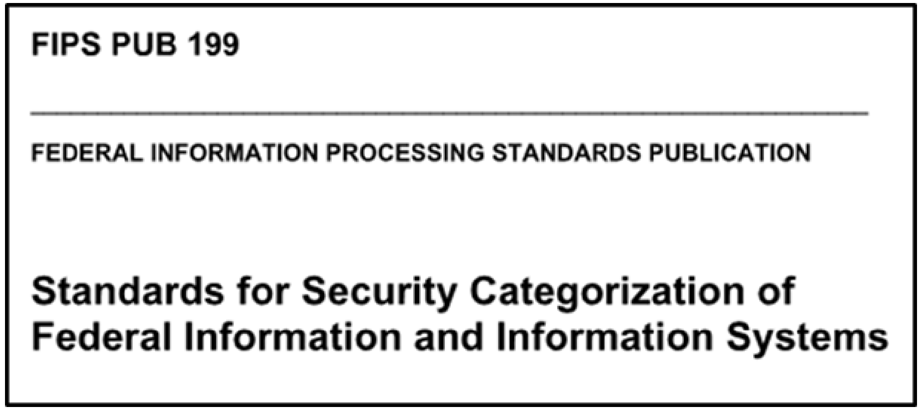
CLASS	FAMILY
Management	Risk Assessment
Management	Planning
Management	System and Services Acquisition
Management	Certification, Accreditation, and Security Assessments
Operational	Personnel Security
Operational	Physical and Environmental Protection
Operational	Contingency Planning
Operational	Configuration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

Vulnerability to what ?



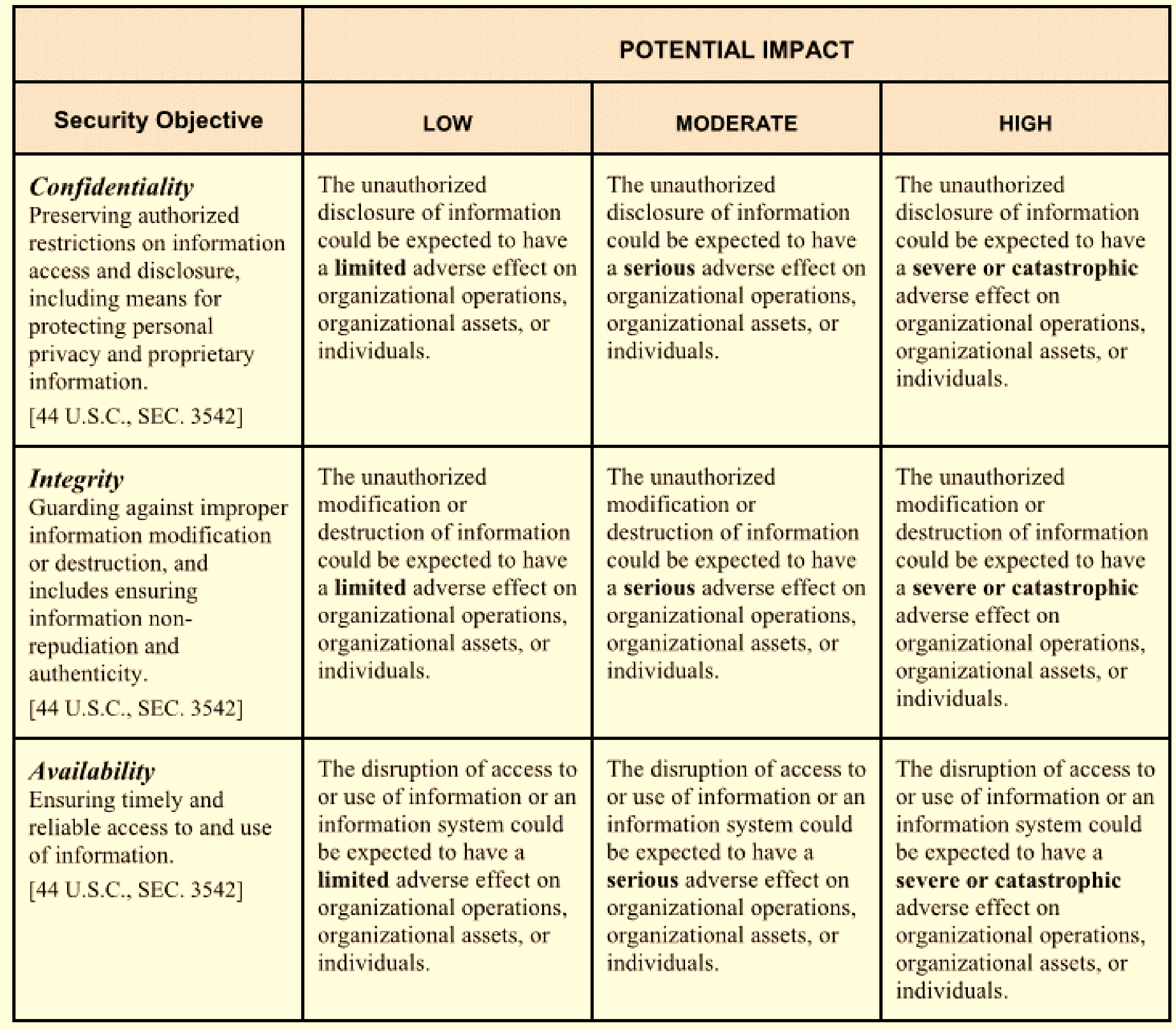
FIPS 199 Standards: Security objectives relate to avoiding negative impacts




FIPS PUB 199

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Standards for Security Categorization of Federal Information and Information Systems

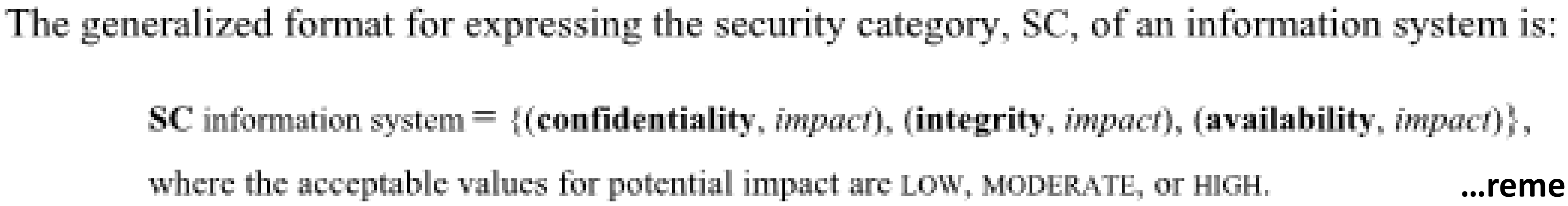


	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could 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.

Impact ratings:

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

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:

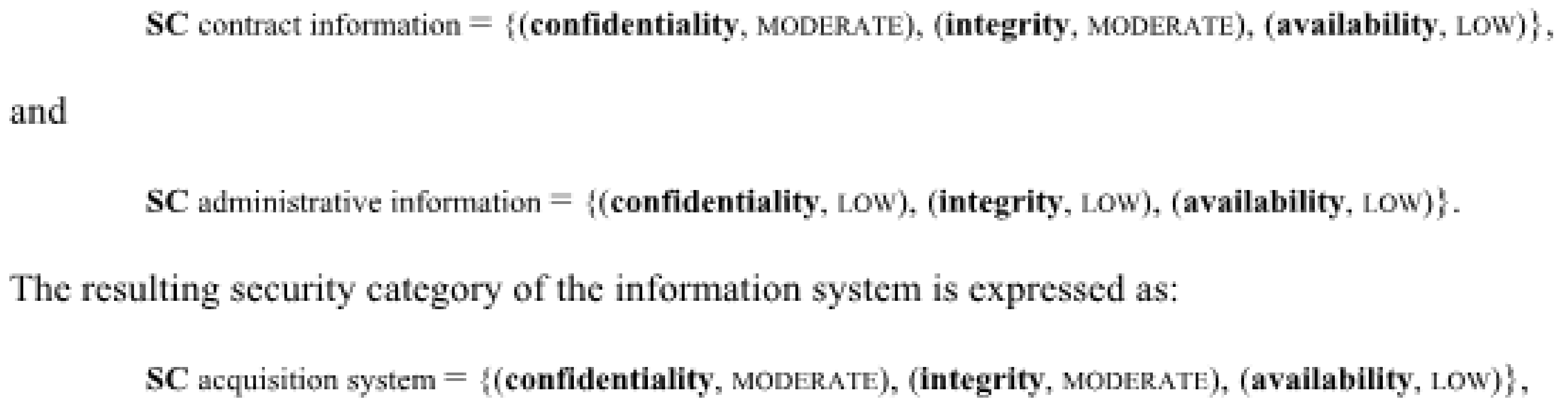
SC information system = {(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *impact*)},

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

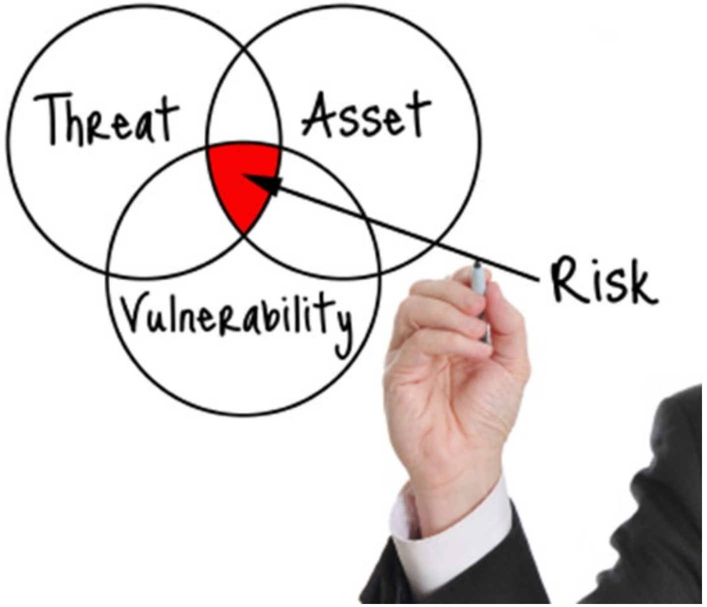
SC administrative information = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}.

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

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

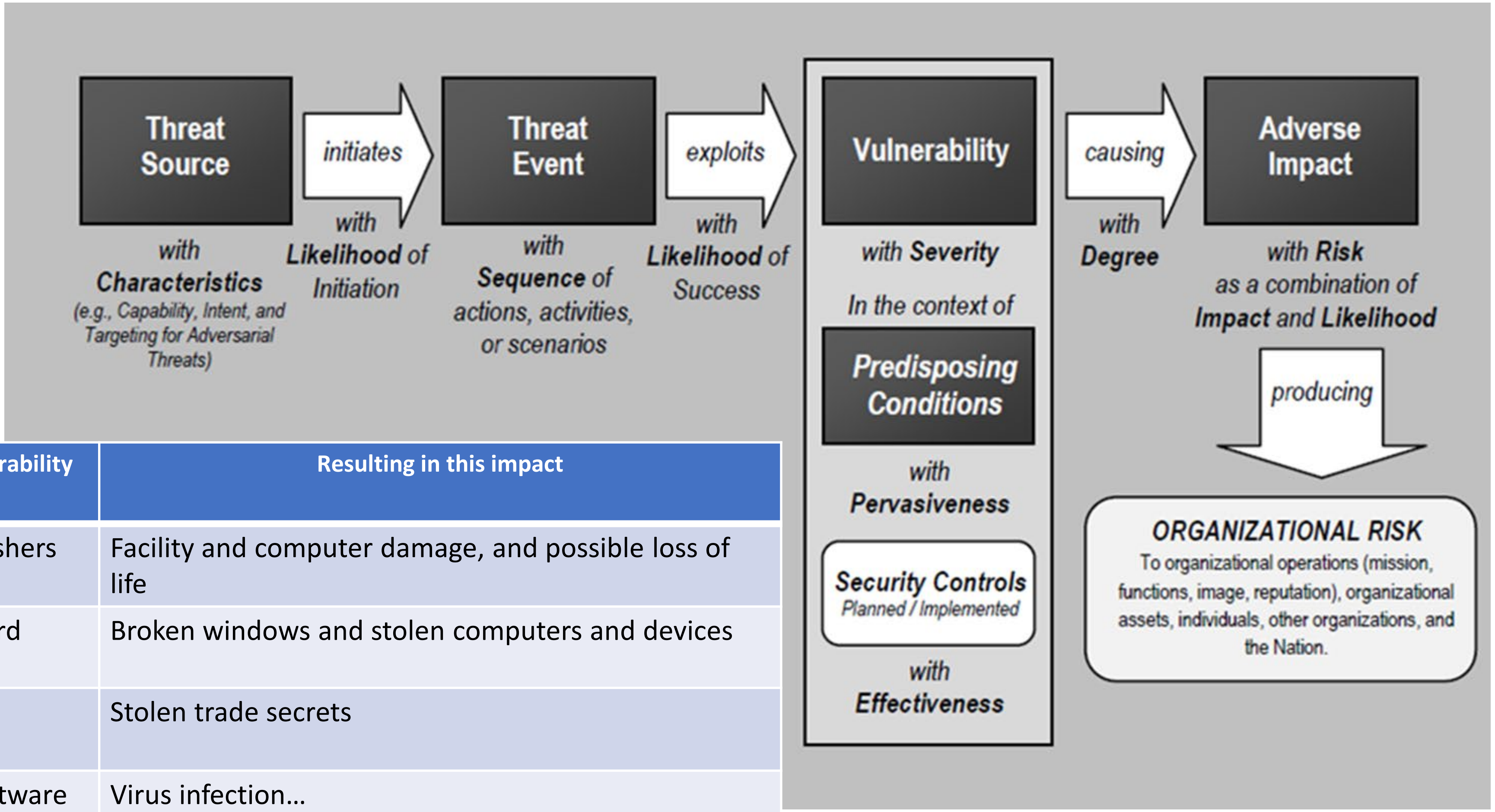
What are examples of Information security risks ?

- 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

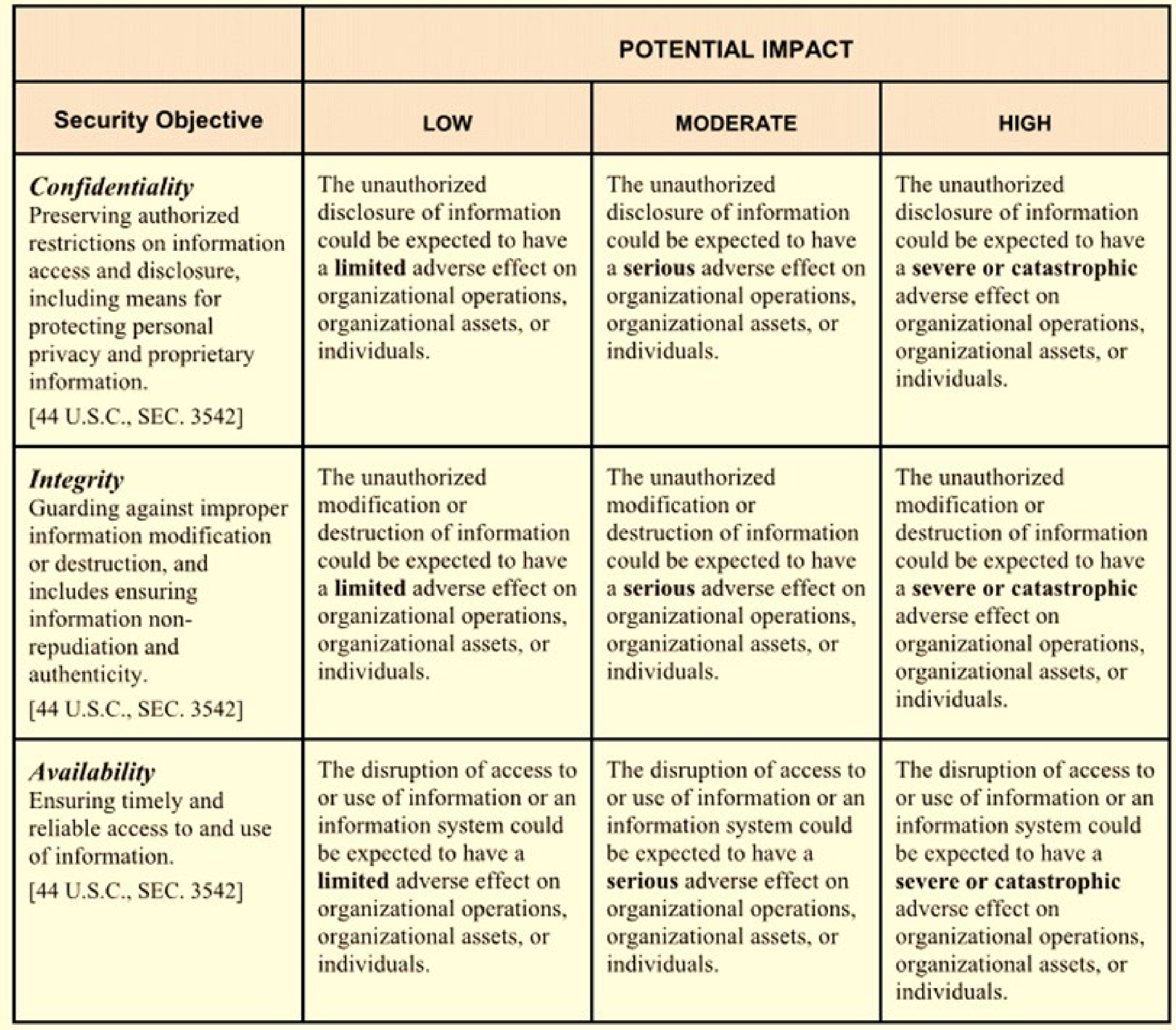

Threat Source
initiates
with Likelihood of Initiation
with Characteristics
(e.g., Capability, Intent, and Targeting for Adversarial Threats)
Threat Event
with Sequence of actions, activities, or scenarios
exploits
with Likelihood of Success
Vulnerability
with Severity
In the context of
Predisposing Conditions
with Pervasiveness
Security Controls
Planned / Implemented
with Effectiveness
causing
with Degree
Adverse Impact
with Risk as a combination of Impact and Likelihood
producing
ORGANIZATIONAL RISK
To organizational operations (mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation.

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



	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.

Quantitative Risk Assessment

$$\textit{Annual Loss Expectancy} = \begin{array}{c}\text{Single Loss Expectancy}\\ \times \\ \text{Annualized Rate of Occurrence}\end{array}$$

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

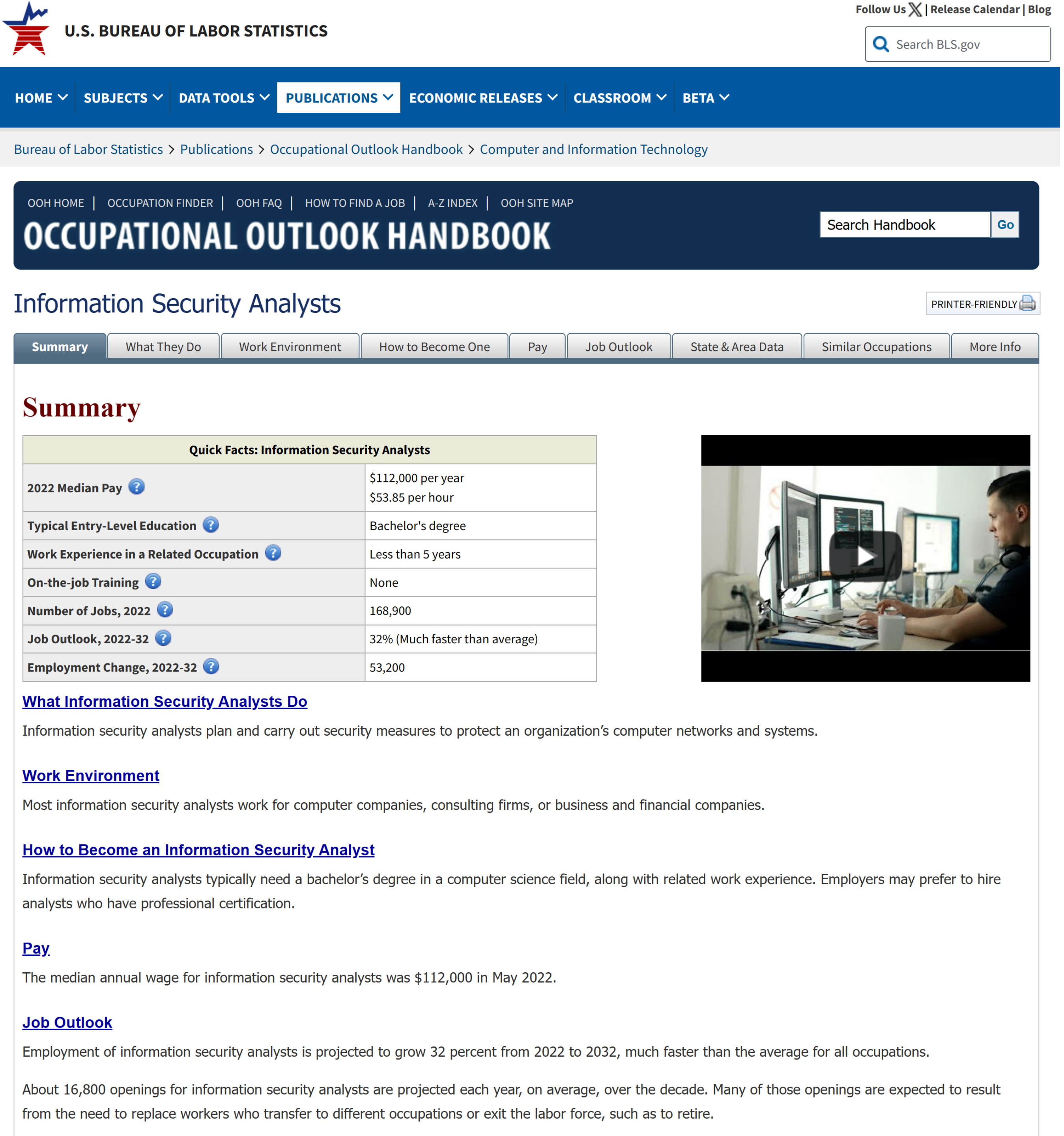
Risk Management Techniques

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

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

Agenda

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


U.S. BUREAU OF LABOR STATISTICS
Follow Us | Release Calendar | Blog
Search BLS.gov
HOME
SUBJECTS
DATA TOOLS
PUBLICATIONS
ECONOMIC RELEASES
CLASSROOM
BETA
Bureau of Labor Statistics > Publications > Occupational Outlook Handbook > Computer and Information Technology
OOH HOME | OCCUPATION FINDER | OOH FAQ | HOW TO FIND A JOB | A-Z INDEX | OOH SITE MAP
OCCUPATIONAL OUTLOOK HANDBOOK
Search Handbook
Go
PRINTER-FRIENDLY
Summary
What They Do
Work Environment
How to Become One
Pay
Job Outlook
State & Area Data
Similar Occupations
More Info

Information Security Analysts

Summary

Quick Facts: Information Security Analysts	
2022 Median Pay	$112,000 per year $53.85 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, 2022	168,900
Job Outlook, 2022-32	32% (Much faster than average)
Employment Change, 2022-32	53,200

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

Information security analysts typically need a bachelor's degree in a computer science field, along with related work experience. Employers may prefer to hire analysts who have professional certification.

Pay

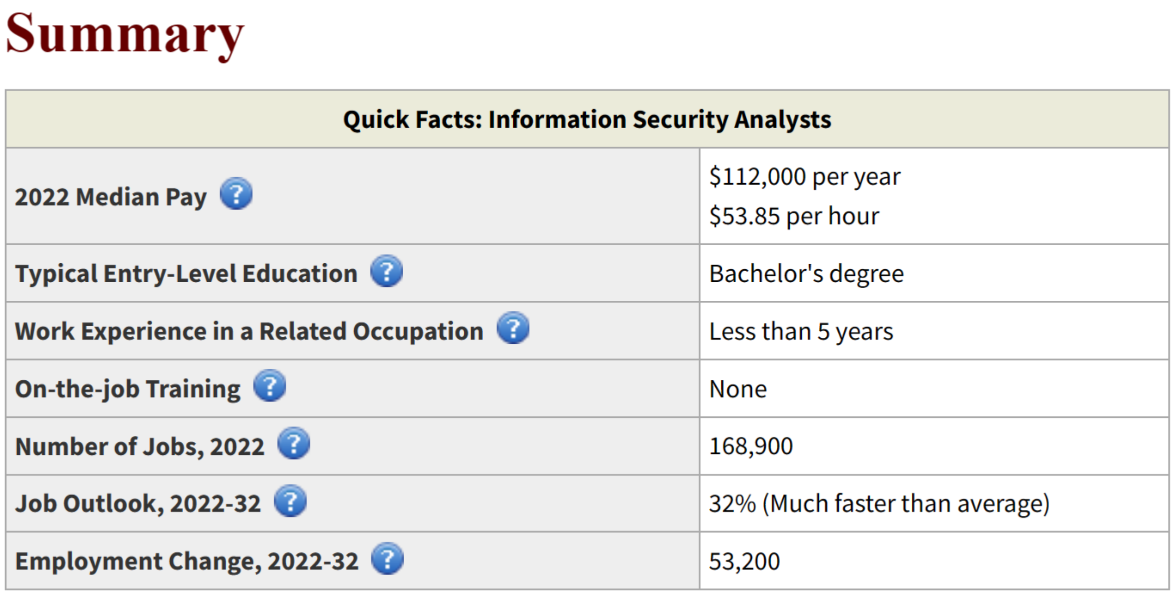
The median annual wage for information security analysts was $112,000 in May 2022.

Job Outlook

Employment of information security analysts is projected to grow 32 percent from 2022 to 2032, much faster than the average for all occupations.

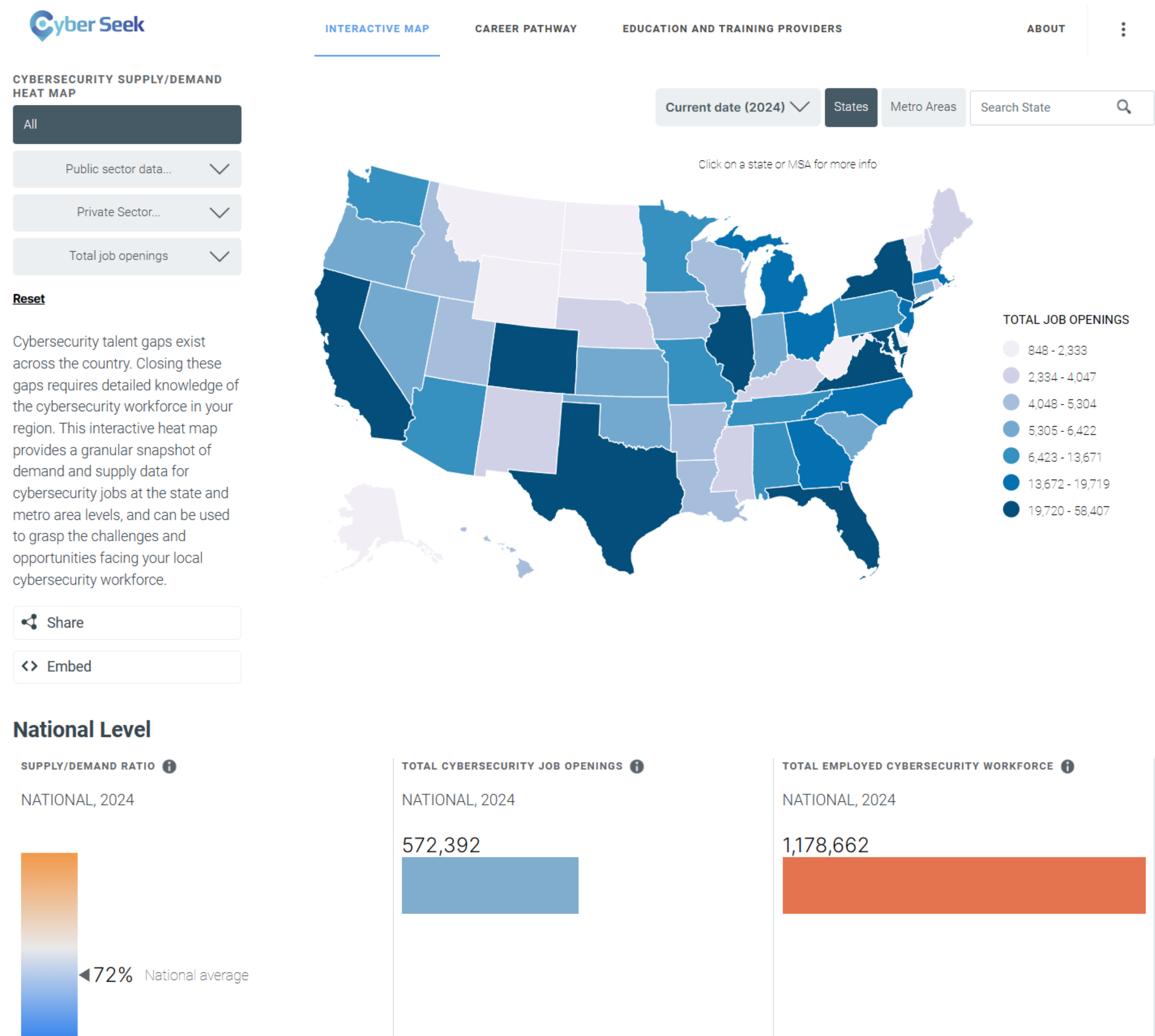
About 16,800 openings for information security analysts are projected each year, on average, over the decade. Many of those openings are expected to result from the need to replace workers who transfer to different occupations or exit the labor force, such as to retire.

https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm



Summary

Quick Facts: Information Security Analysts	
2022 Median Pay	$112,000 per year $53.85 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, 2022	168,900
Job Outlook, 2022-32	32% (Much faster than average)
Employment Change, 2022-32	53,200



CYBERSECURITY SUPPLY/DEMAND HEAT MAP

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.

TOTAL JOB OPENINGS

- ● 848 - 2,333
- ● 2,334 - 4,047
- ● 4,048 - 5,304
- ● 5,305 - 6,422
- ● 6,423 - 13,671
- ● 13,672 - 19,719
- ● 19,720 - 58,407

National Level

SUPPLY/DEMAND RATIO

NATIONAL, 2024

72% National average

TOTAL CYBERSECURITY JOB OPENINGS

NATIONAL, 2024

572,392

TOTAL EMPLOYED CYBERSECURITY WORKFORCE

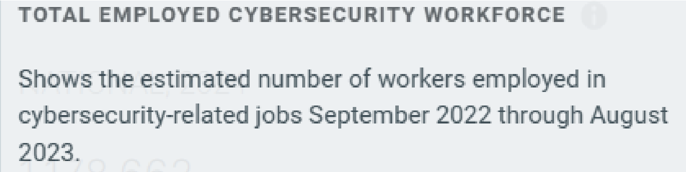
NATIONAL, 2024

1,178,662

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

TOTAL CYBERSECURITY JOB OPENINGS

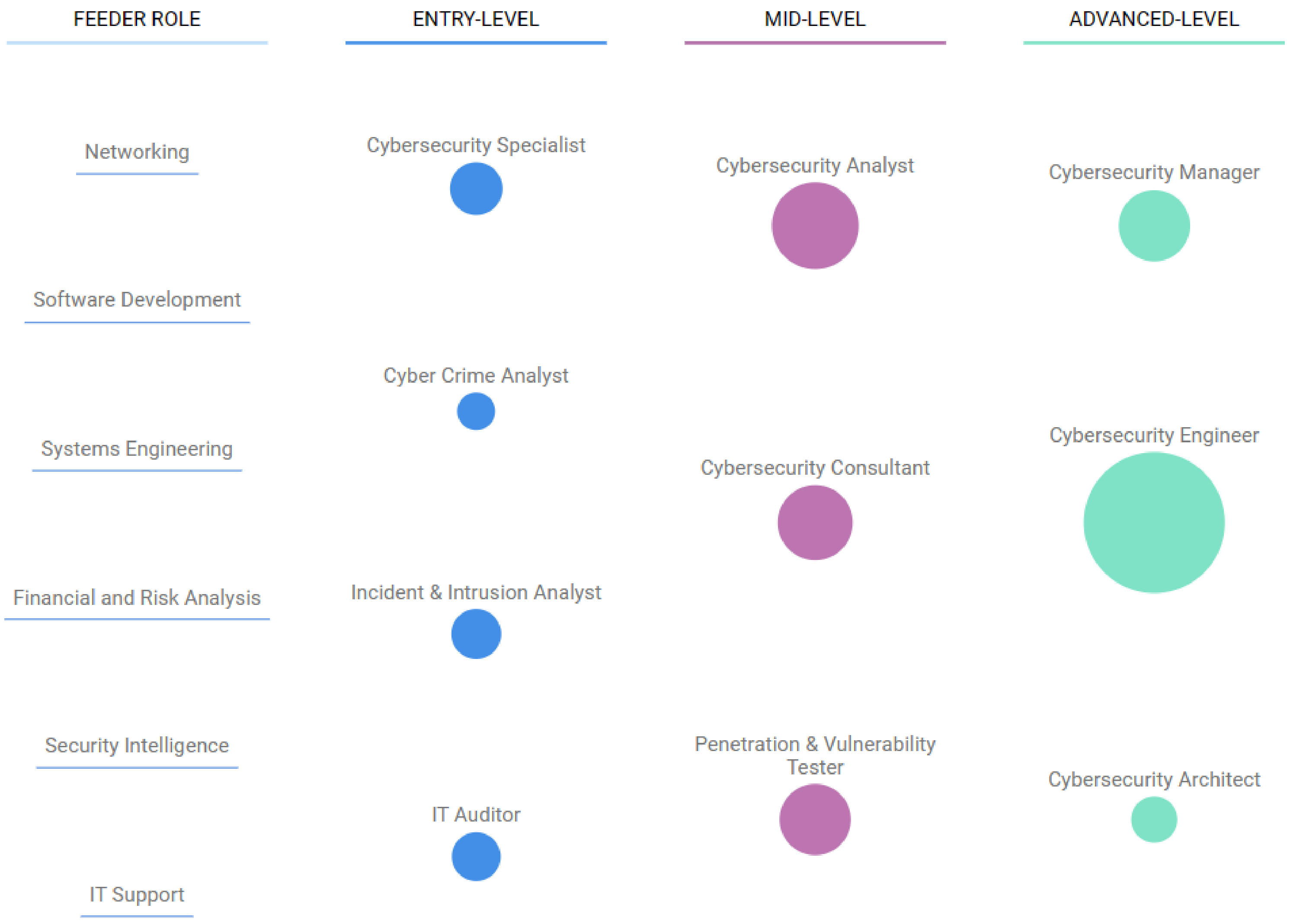
Shows the number of online job listings for cybersecurity-related positions from September 2022 through August 2023.



TOTAL EMPLOYED CYBERSECURITY WORKFORCE

Shows the estimated number of workers employed in cybersecurity-related jobs September 2022 through August 2023.

Example job types



FEEDER ROLE

- Networking
- Software Development
- Systems Engineering
- Financial and Risk Analysis
- Security Intelligence
- IT Support

ENTRY-LEVEL

- Cybersecurity Specialist
- Cyber Crime Analyst
- Incident & Intrusion Analyst
- IT Auditor

MID-LEVEL

- Cybersecurity Analyst
- Cybersecurity Consultant
- Penetration & Vulnerability Tester

ADVANCED-LEVEL

- Cybersecurity Manager
- Cybersecurity Engineer
- Cybersecurity Architect

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

Agenda

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