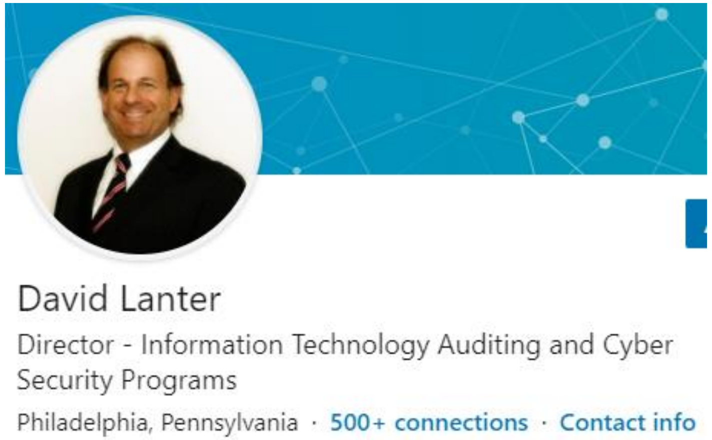
MIS5206
Protection of Information Assets
Unit #1

Agenda

- Introductions
- Course objectives, Class topics and Schedule
- Textbook and Readings
- Grading
- Assignments
- Participation
- Team Project
- Exams
- *Quizzes*

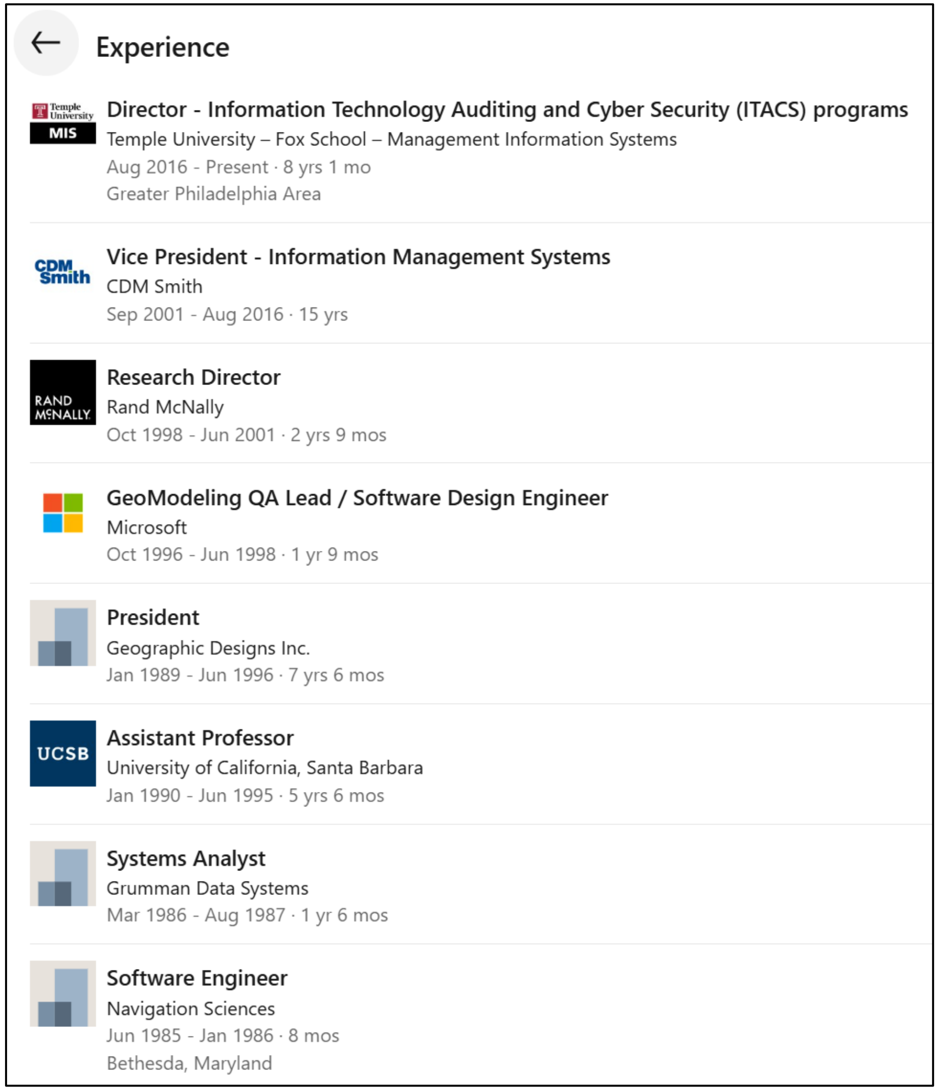
Instructor



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 · 8 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

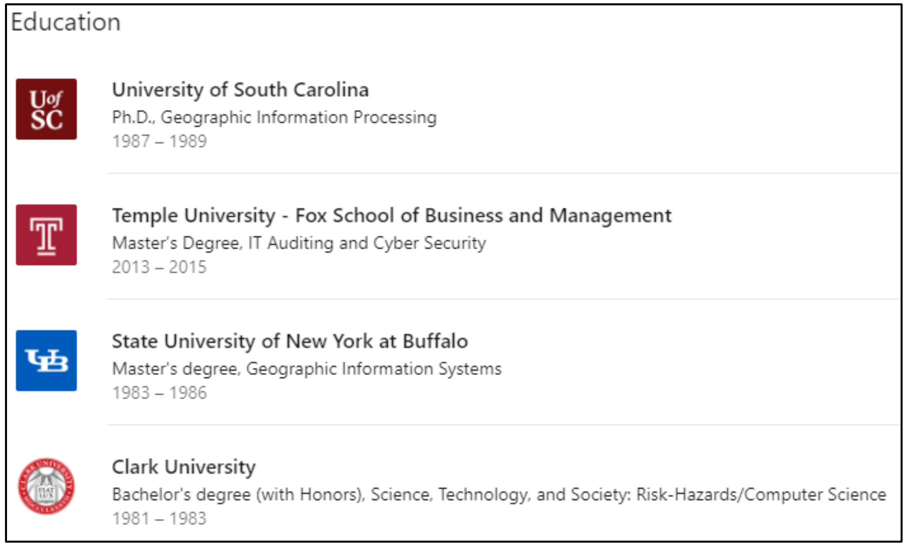
GeoModeling QA Lead / Software Design Engineer
Microsoft
Oct 1996 - Jun 1998 · 1 yr 9 mos

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



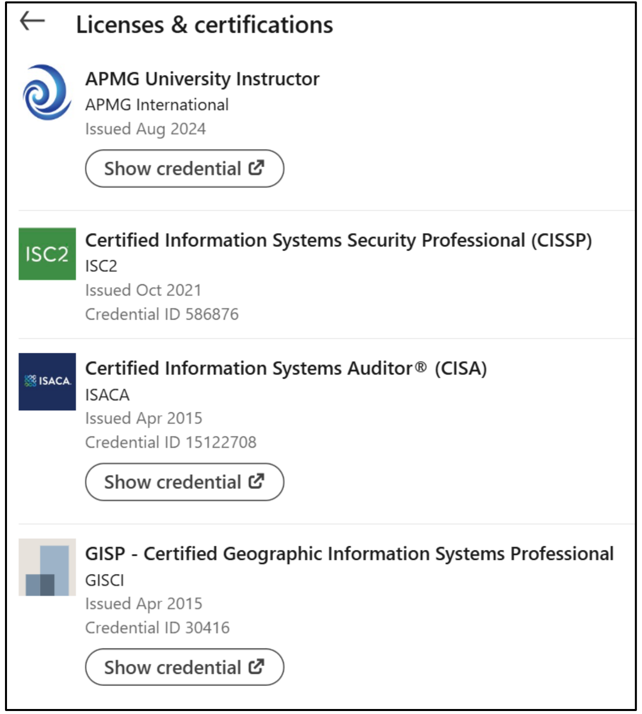
Education

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

APMG University Instructor
APMG International
Issued Aug 2024
Show credential

Certified Information Systems Security Professional (CISSP)
ISC2
Issued Oct 2021
Credential ID 586876

Certified Information Systems Auditor® (CISA)
ISACA
Issued Apr 2015
Credential ID 15122708
Show credential

GISP - Certified Geographic Information Systems Professional
GISCI
Issued Apr 2015
Credential ID 30416
Show credential

Course objectives

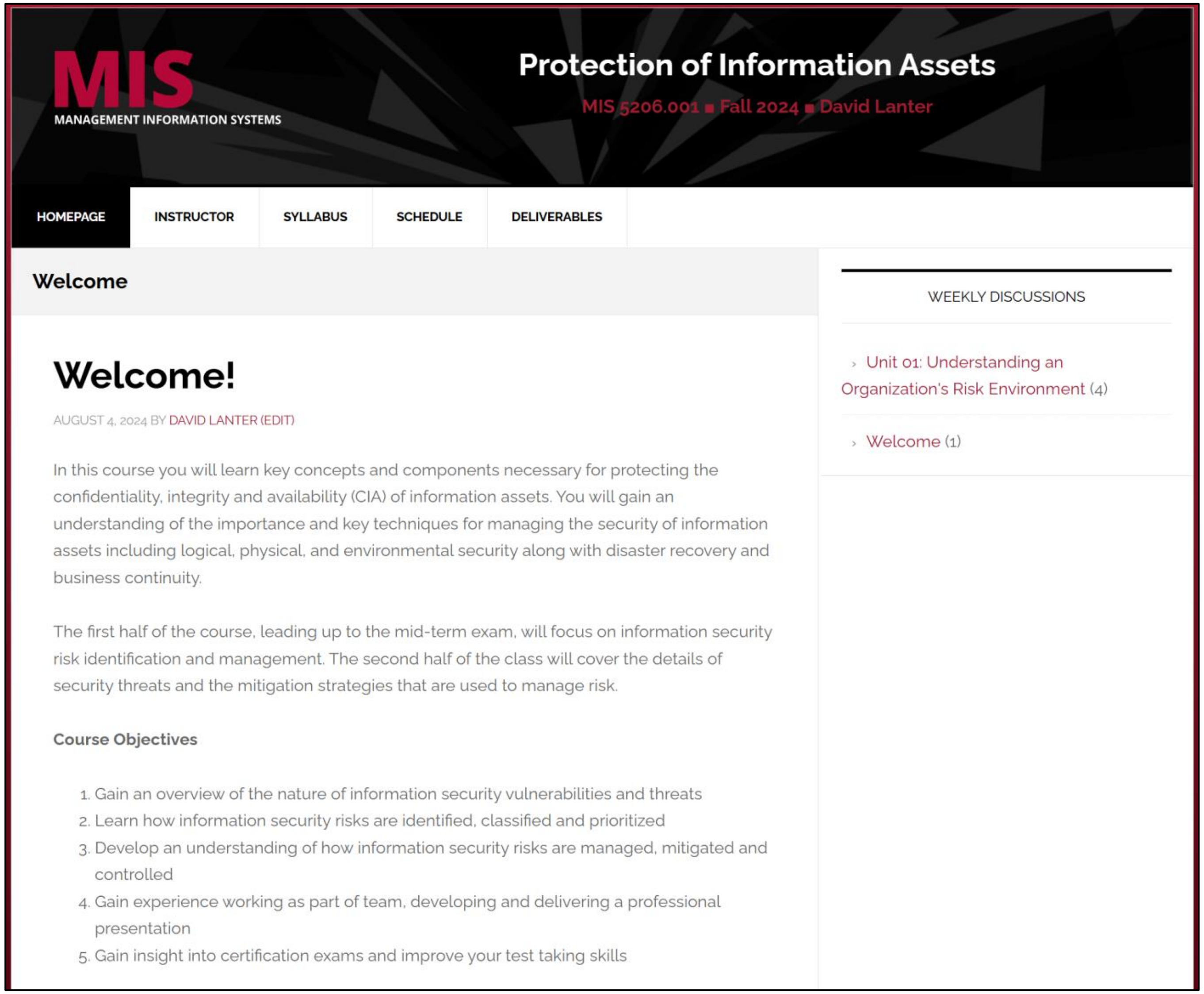
In this course you will gain an understanding of how information assets are managed, in terms of logical, physical, and administrative information systems security controls along with disaster recovery and business continuity

Key subject areas covered in the course are:

- Information Security Risk Identification and Management
- Security Threats and Mitigation Strategies

- First half of the course, leading up to the mid-term exam, will focus on Information Security Risk Identification and Management
- Second half of the class will cover the details of security threats and the mitigation strategies used to mange risk

Course website and syllabus



Protection of Information Assets

MIS 5206.001 ■ Fall 2024 ■ David Lanter

Welcome

Welcome!

AUGUST 4, 2024 BY DAVID LANTER (EDIT)

In this course you will learn key concepts and components necessary for protecting the confidentiality, integrity and availability (CIA) of information assets. You will gain an understanding of the importance and key techniques for managing the security of information assets including logical, physical, and environmental security along with disaster recovery and business continuity.

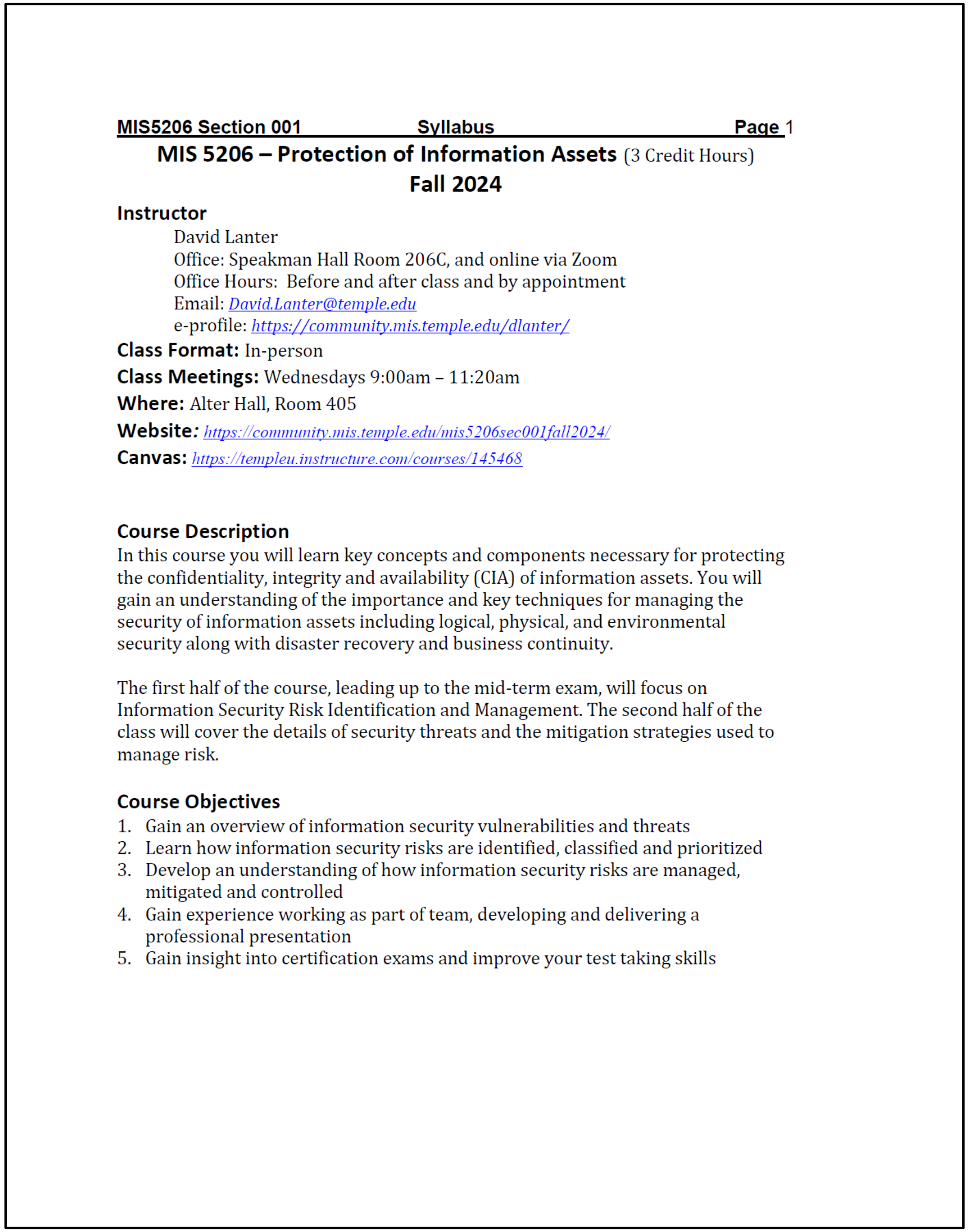
The first half of the course, leading up to the mid-term exam, will focus on information security risk identification and management. The second half of the class will cover the details of security threats and the mitigation strategies that are used to manage risk.

Course Objectives

1. Gain an overview of the nature of information security vulnerabilities and threats
2. Learn how information security risks are identified, classified and prioritized
3. Develop an understanding of how information security risks are managed, mitigated and controlled
4. Gain experience working as part of team, developing and delivering a professional presentation
5. Gain insight into certification exams and improve your test taking skills

WEEKLY DISCUSSIONS

- Unit 01: Understanding an Organization's Risk Environment (4)
- Welcome (1)



MIS5206 Section 001 Syllabus Page 1

MIS 5206 – Protection of Information Assets (3 Credit Hours)

Fall 2024

Instructor

David Lanter
Office: Speakman Hall Room 206C, and online via Zoom
Office Hours: Before and after class and by appointment
Email: David.Lanter@temple.edu
e-profile: https://community.mis.temple.edu/dlanter/

Class Format: In-person
Class Meetings: Wednesdays 9:00am – 11:20am
Where: Alter Hall, Room 405
Website: https://community.mis.temple.edu/mis5206sec001fall2024/
Canvas: https://templeu.instructure.com/courses/145468

Course Description

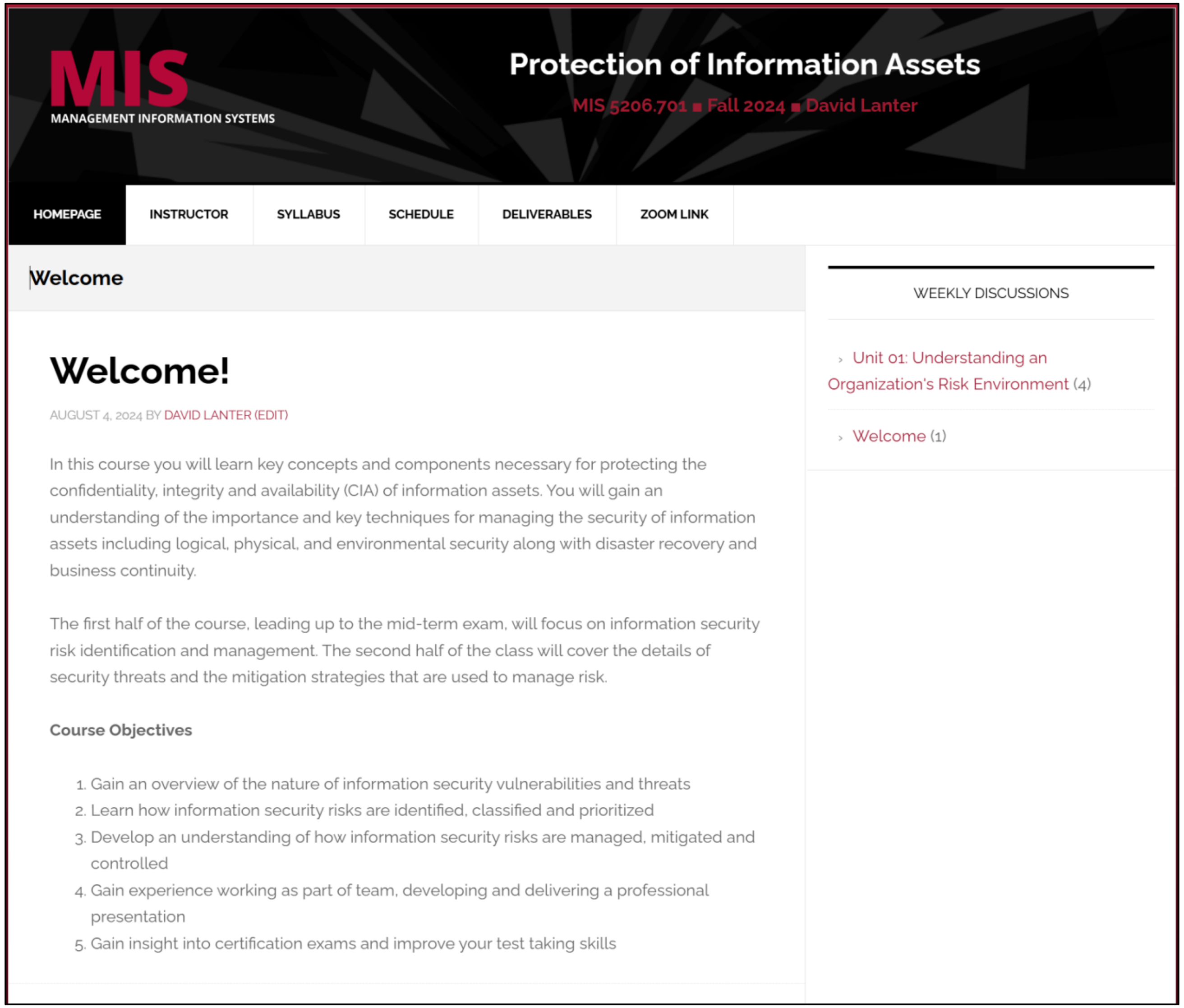
In this course you will learn key concepts and components necessary for protecting the confidentiality, integrity and availability (CIA) of information assets. You will gain an understanding of the importance and key techniques for managing the security of information assets including logical, physical, and environmental security along with disaster recovery and business continuity.

The first half of the course, leading up to the mid-term exam, will focus on Information Security Risk Identification and Management. The second half of the class will cover the details of security threats and the mitigation strategies used to manage risk.

Course Objectives

1. Gain an overview of information security vulnerabilities and threats
2. Learn how information security risks are identified, classified and prioritized
3. Develop an understanding of how information security risks are managed, mitigated and controlled
4. Gain experience working as part of team, developing and delivering a professional presentation
5. Gain insight into certification exams and improve your test taking skills

Course website and syllabus



MIS
MANAGEMENT INFORMATION SYSTEMS

Protection of Information Assets

MIS 5206.701 ■ Fall 2024 ■ David Lanter

Welcome

Welcome!

AUGUST 4, 2024 BY DAVID LANTER (EDIT)

In this course you will learn key concepts and components necessary for protecting the confidentiality, integrity and availability (CIA) of information assets. You will gain an understanding of the importance and key techniques for managing the security of information assets including logical, physical, and environmental security along with disaster recovery and business continuity.

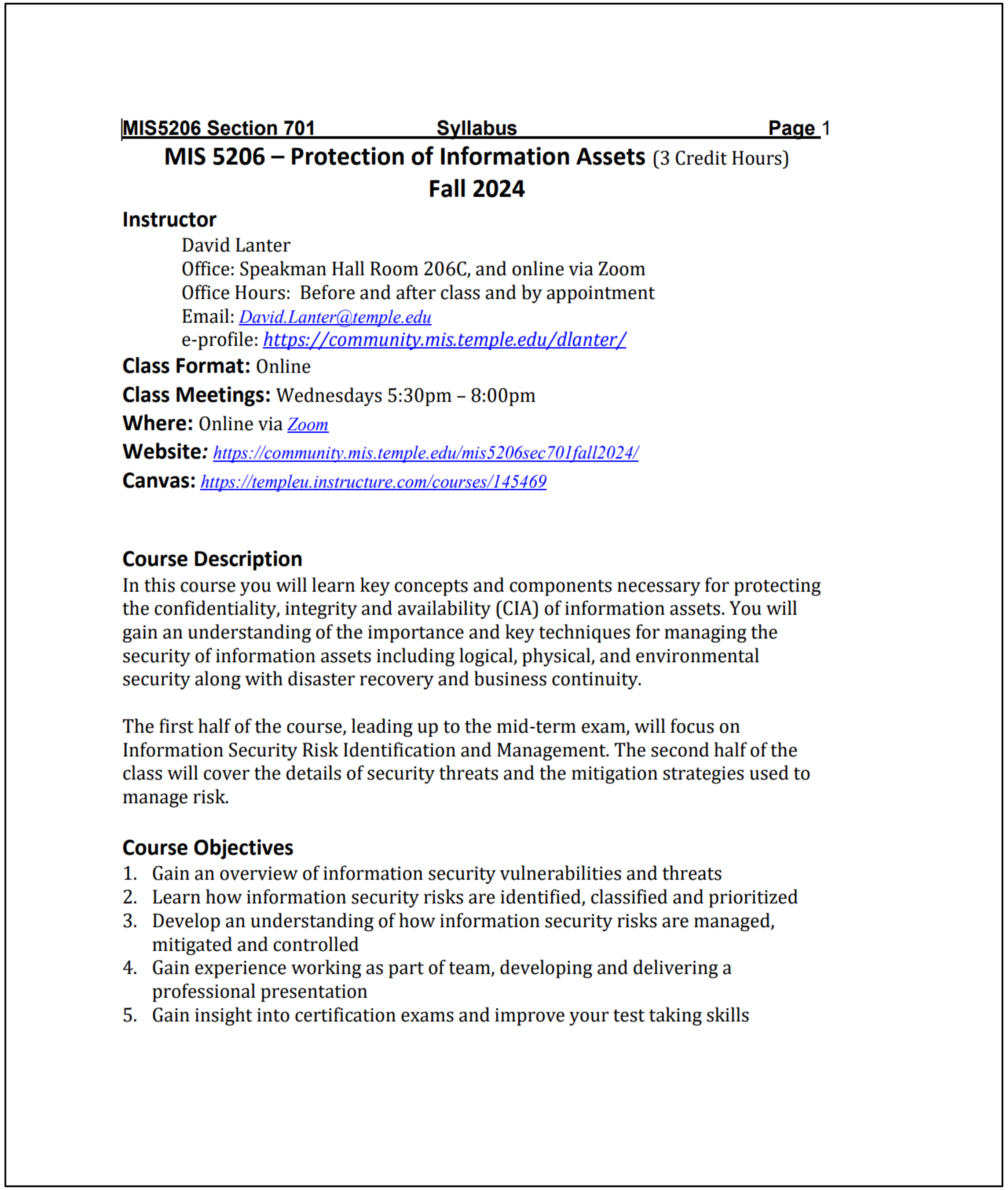
The first half of the course, leading up to the mid-term exam, will focus on information security risk identification and management. The second half of the class will cover the details of security threats and the mitigation strategies that are used to manage risk.

Course Objectives

1. Gain an overview of the nature of information security vulnerabilities and threats
2. Learn how information security risks are identified, classified and prioritized
3. Develop an understanding of how information security risks are managed, mitigated and controlled
4. Gain experience working as part of team, developing and delivering a professional presentation
5. Gain insight into certification exams and improve your test taking skills

WEEKLY DISCUSSIONS

- Unit 01: Understanding an Organization's Risk Environment (4)
- Welcome (1)



MIS5206 Section 701 Syllabus Page 1

MIS 5206 – Protection of Information Assets (3 Credit Hours)
Fall 2024

Instructor
David Lanter
Office: Speakman Hall Room 206C, and online via Zoom
Office Hours: Before and after class and by appointment
Email: David.Lanter@temple.edu
e-profile: https://community.mis.temple.edu/dlanter/

Class Format: Online
Class Meetings: Wednesdays 5:30pm – 8:00pm
Where: Online via Zoom
Website: https://community.mis.temple.edu/mis5206sec701fall2024/
Canvas: https://templeu.instructure.com/courses/145469

Course Description

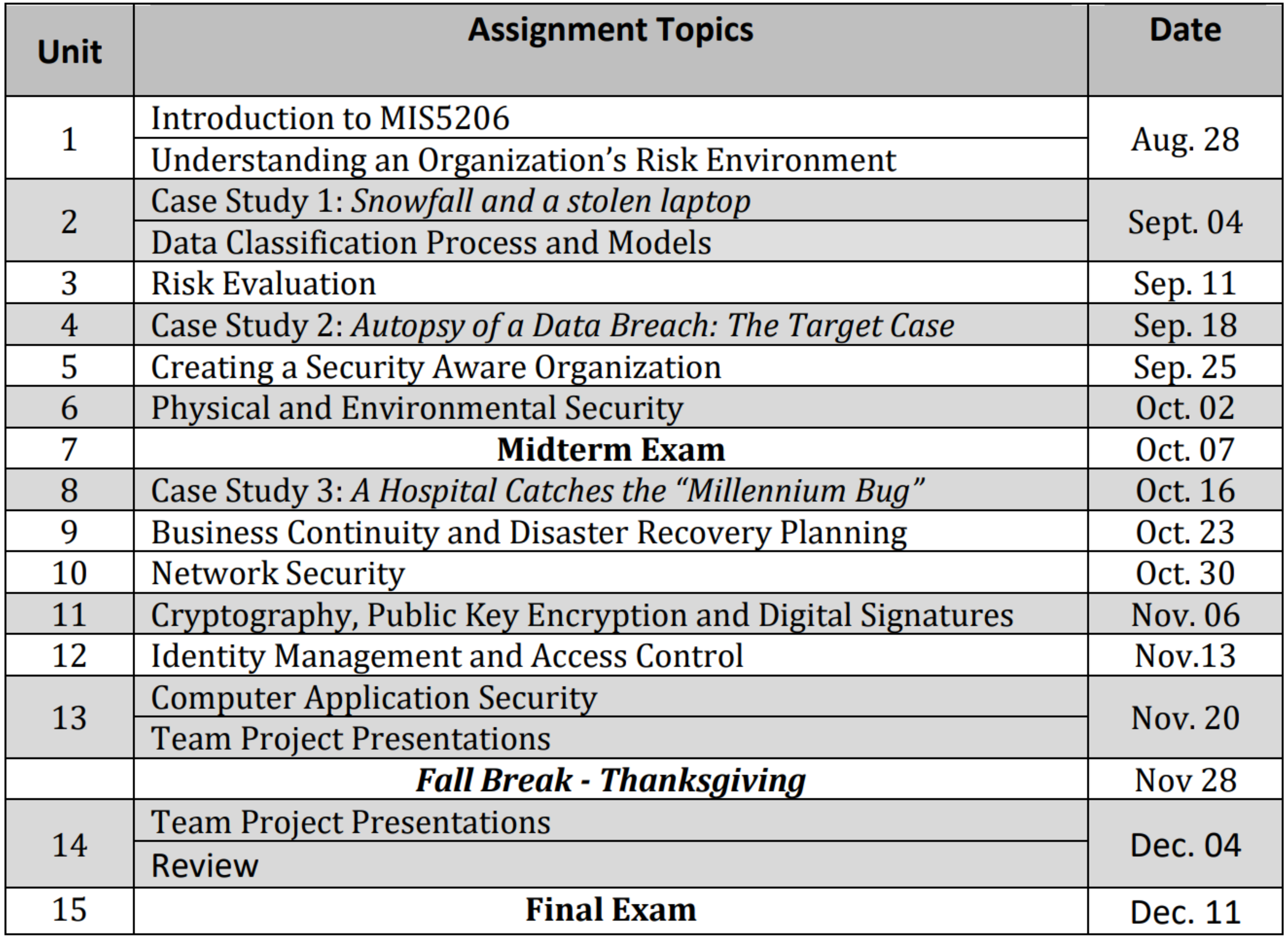
In this course you will learn key concepts and components necessary for protecting the confidentiality, integrity and availability (CIA) of information assets. You will gain an understanding of the importance and key techniques for managing the security of information assets including logical, physical, and environmental security along with disaster recovery and business continuity.

The first half of the course, leading up to the mid-term exam, will focus on Information Security Risk Identification and Management. The second half of the class will cover the details of security threats and the mitigation strategies used to manage risk.

Course Objectives

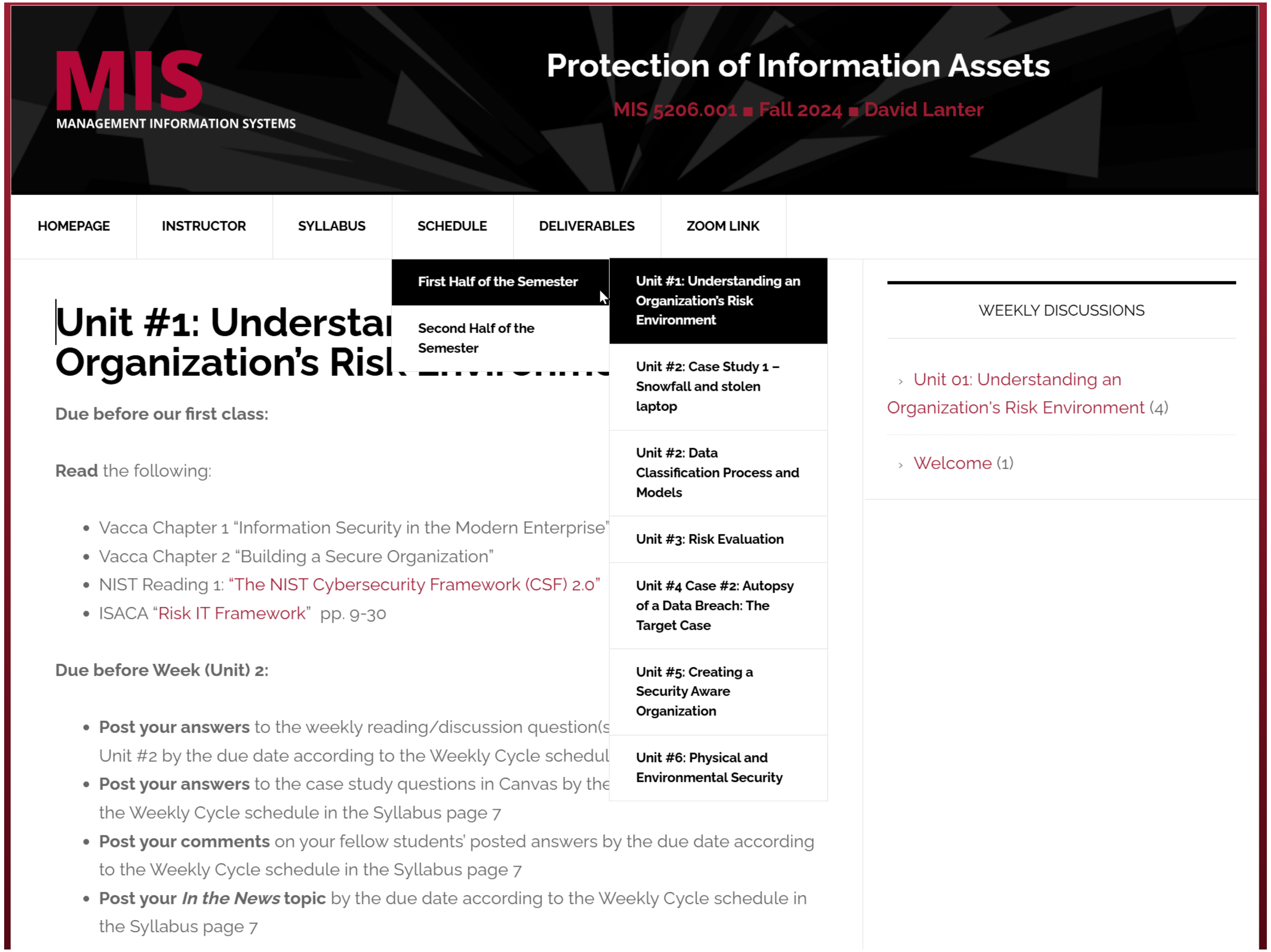
1. Gain an overview of information security vulnerabilities and threats
2. Learn how information security risks are identified, classified and prioritized
3. Develop an understanding of how information security risks are managed, mitigated and controlled
4. Gain experience working as part of team, developing and delivering a professional presentation
5. Gain insight into certification exams and improve your test taking skills

Class topics and schedule



Unit	Assignment Topics	Date
1	Introduction to MIS5206	Aug. 28
	Understanding an Organization’s Risk Environment	
2	Case Study 1: *Snowfall and a stolen laptop*	Sept. 04
	Data Classification Process and Models	
3	Risk Evaluation	Sep. 11
4	Case Study 2: *Autopsy of a Data Breach: The Target Case*	Sep. 18
5	Creating a Security Aware Organization	Sep. 25
6	Physical and Environmental Security	Oct. 02
7	**Midterm Exam**	Oct. 07
8	Case Study 3: *A Hospital Catches the “Millennium Bug”*	Oct. 16
9	Business Continuity and Disaster Recovery Planning	Oct. 23
10	Network Security	Oct. 30
11	Cryptography, Public Key Encryption and Digital Signatures	Nov. 06
12	Identity Management and Access Control	Nov.13
13	Computer Application Security	Nov. 20
	Team Project Presentations	
	Fall Break - Thanksgiving	Nov 28
14	Team Project Presentations	Dec. 04
	Review	
15	**Final Exam**	Dec. 11

Class topics and schedule


MIS
MANAGEMENT INFORMATION SYSTEMS
Protection of Information Assets
MIS 5206.001 ■ Fall 2024 ■ David Lanter
HOMEPAGE
INSTRUCTOR
SYLLABUS
SCHEDULE
DELIVERABLES
ZOOM LINK
First Half of the Semester
Second Half of the Semester
Unit #1: Understanding an Organization's Risk Environment
Unit #2: Case Study 1 – Snowfall and stolen laptop
Unit #2: Data Classification Process and Models
Unit #3: Risk Evaluation
Unit #4 Case #2: Autopsy of a Data Breach: The Target Case
Unit #5: Creating a Security Aware Organization
Unit #6: Physical and Environmental Security
WEEKLY DISCUSSIONS
› Unit 01: Understanding an Organization's Risk Environment (4)
› Welcome (1)

Unit #1: Understandi Organization's Risk

Due before our first class:

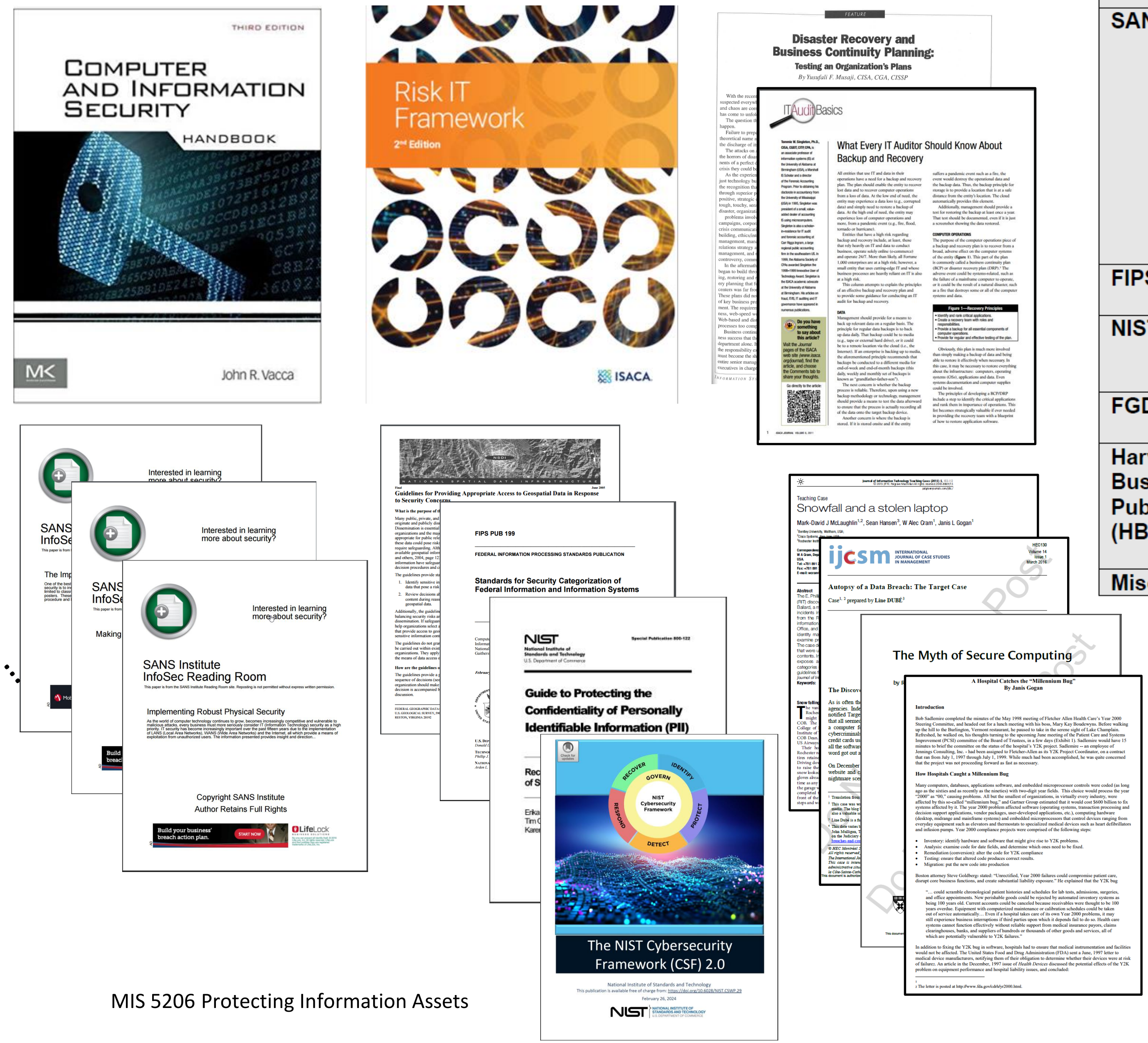
Read the following:

- Vacca Chapter 1 "Information Security in the Modern Enterprise"
- Vacca Chapter 2 "Building a Secure Organization"
- NIST Reading 1: "The NIST Cybersecurity Framework (CSF) 2.0"
- ISACA "Risk IT Framework" pp. 9-30

Due before Week (Unit) 2:

- **Post your answers** to the weekly reading/discussion question(s Unit #2 by the due date according to the Weekly Cycle schedul
- **Post your answers** to the case study questions in Canvas by the the Weekly Cycle schedule in the Syllabus page 7
- **Post your comments** on your fellow students' posted answers by the due date according to the Weekly Cycle schedule in the Syllabus page 7
- **Post your *In the News* topic** by the due date according to the Weekly Cycle schedule in the Syllabus page 7

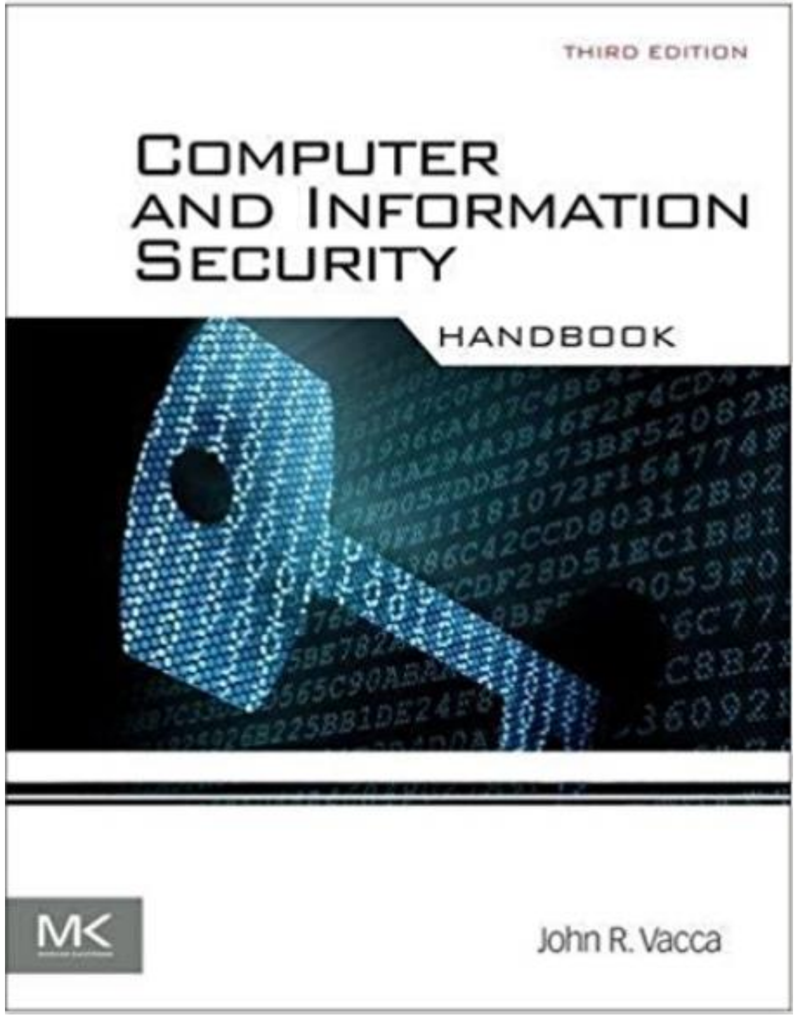
Textbook and readings

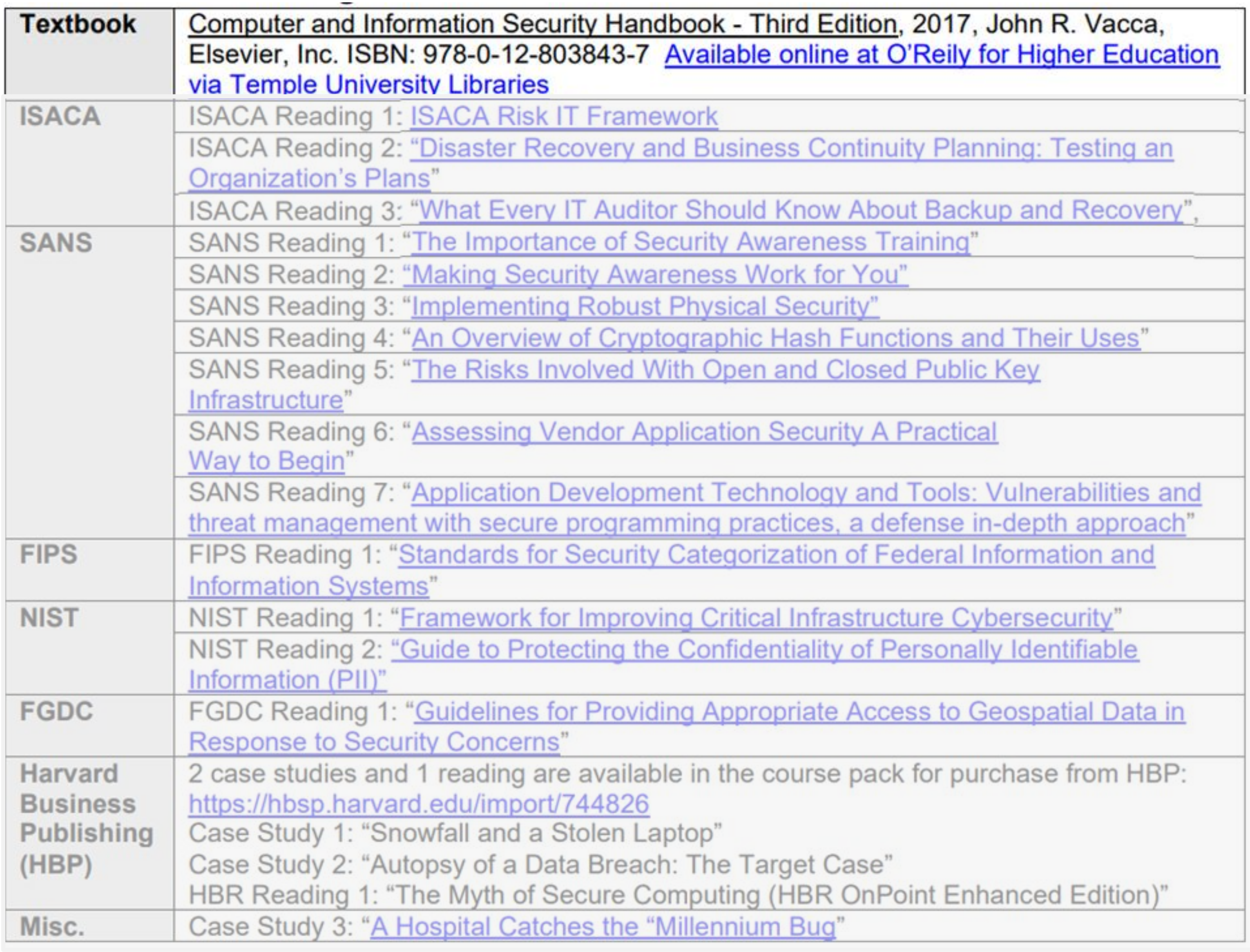


THIRD EDITION
COMPUTER AND INFORMATION SECURITY HANDBOOK
John R. Vacca
Risk IT Framework
2nd Edition
ISACA
Disaster Recovery and Business Continuity Planning: Testing an Organization's Plans
IT Audit Basics
What Every IT Auditor Should Know About Backup and Recovery
Interested in learning more about security?
SANS Institute InfoSec Reading Room
Implementing Robust Physical Security
Copyright SANS Institute
Author Retains Full Rights
Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns
FIPS PUB 199
FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION
Standards for Security Categorization of Federal Information and Information Systems
NIST Special Publication 800-122
Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
The NIST Cybersecurity Framework (CSF) 2.0
Teaching Case
Snowfall and a stolen laptop
ijcsm
Autopsy of a Data Breach: The Target Case
The Myth of Secure Computing
A Hospital Catches the "Millennium Bug"
By Janis Gogan
…

Textbook	Computer and Information Security Handbook - Third Edition, 2017, John R. Vacca, Elsevier, Inc. ISBN: 978-0-12-803843-7 Available online via Temple University Libraries
ISACA	ISACA Reading 1: ISACA Risk IT Framework
	ISACA Reading 2: "Disaster Recovery and Business Continuity Planning: Testing an Organization's Plans"
	ISACA Reading 3: "What Every IT Auditor Should Know About Backup and Recovery",
SANS	SANS Reading 1: "The Importance of Security Awareness Training"
	SANS Reading 2: "Making Security Awareness Work for You"
	SANS Reading 3: "Implementing Robust Physical Security"
	SANS Reading 4: "An Overview of Cryptographic Hash Functions and Their Uses"
	SANS Reading 5: "The Risks Involved With Open and Closed Public Key Infrastructure"
	SANS Reading 6: "Assessing Vendor Application Security A Practical Way to Begin"
	SANS Reading 7: "Application Development Technology and Tools: Vulnerabilities and threat management with secure programming practices, a defense in-depth approach"
FIPS	FIPS Reading 1: "Standards for Security Categorization of Federal Information and Information Systems"
NIST	NIST Reading 1: "The NIST Cybersecurity Framework (CSF) 2.0"
	NIST Reading 2: "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)"
FGDC	FGDC Reading 1: "Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns"
Harvard Business Publishing (HBP)	2 case studies and 1 reading are available in the course pack for purchase from HBP: https://hbsp.harvard.edu/import/1196217 Case Study 1: "Snowfall and a Stolen Laptop" Case Study 2: "Autopsy of a Data Breach: The Target Case" HBR Reading 1: "The Myth of Secure Computing (HBR OnPoint Enhanced Edition)"
Misc.	Case Study 3: "A Hospital Catches the "Millennium Bug"

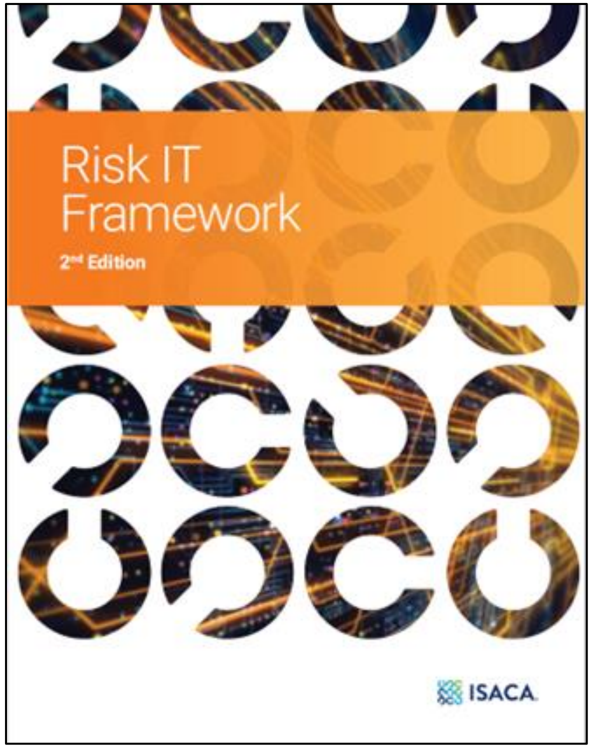
Textbook and readings





Textbook	Computer and Information Security Handbook - Third Edition, 2017, John R. Vacca, Elsevier, Inc. ISBN: 978-0-12-803843-7 Available online at O'Reily for Higher Education via Temple University Libraries
ISACA	ISACA Reading 1: ISACA Risk IT Framework
	ISACA Reading 2: “Disaster Recovery and Business Continuity Planning: Testing an Organization's Plans”
	ISACA Reading 3: “What Every IT Auditor Should Know About Backup and Recovery”,
SANS	SANS Reading 1: “The Importance of Security Awareness Training”
	SANS Reading 2: “Making Security Awareness Work for You”
	SANS Reading 3: “Implementing Robust Physical Security”
	SANS Reading 4: “An Overview of Cryptographic Hash Functions and Their Uses”
	SANS Reading 5: “The Risks Involved With Open and Closed Public Key Infrastructure”
	SANS Reading 6: “Assessing Vendor Application Security A Practical Way to Begin”
	SANS Reading 7: “Application Development Technology and Tools: Vulnerabilities and threat management with secure programming practices, a defense in-depth approach”
FIPS	FIPS Reading 1: “Standards for Security Categorization of Federal Information and Information Systems”
NIST	NIST Reading 1: “Framework for Improving Critical Infrastructure Cybersecurity”
	NIST Reading 2: “Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)”
FGDC	FGDC Reading 1: “Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns”
Harvard Business Publishing (HBP)	2 case studies and 1 reading are available in the course pack for purchase from HBP: https://hbsp.harvard.edu/import/744826 Case Study 1: “Snowfall and a Stolen Laptop” Case Study 2: “Autopsy of a Data Breach: The Target Case” HBR Reading 1: “The Myth of Secure Computing (HBR OnPoint Enhanced Edition)”
Misc.	Case Study 3: “A Hospital Catches the “Millennium Bug”

Textbook and readings



FEATURE

Disaster Recovery and Business Continuity Planning: Testing an Organization's Plans

By Yusufali F. Musaji, CISA, CGA, CISSP

IT Audit Basics

Tommie W. Singleton, Ph.D., CISA, CGEIT, CITP, CPA, is an associate professor of information systems (IS) at the University of Alabama at Birmingham (USA), a Marshall IS Scholar and a director of the Forensic Accounting Program. Prior to obtaining his doctorate in accountancy from the University of Mississippi (USA) in 1995, Singleton was president of a small, value-added dealer of accounting IS using microcomputers. Singleton is also a scholar-in-residence for IT audit and forensic accounting at Carr Riggs Ingram, a large regional public accounting firm in the southeastern US. In 1999, the Alabama Society of CPAs awarded Singleton the 1998–1999 Innovative User of Technology Award. Singleton is the ISACA academic advocate at the University of Alabama at Birmingham. His articles on fraud, IT/IS, IT auditing and IT governance have appeared in numerous publications.

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article, and choose the Comments tab to share your thoughts.

Go directly to the article:

What Every IT Auditor Should Know About Backup and Recovery

All entities that use IT and data in their operations have a need for a backup and recovery plan. The plan should enable the entity to recover lost data and to recover computer operations from a loss of data. At the low end of need, the entity may experience a data loss (e.g., corrupted data) and simply need to restore a backup of data. At the high end of need, the entity may experience loss of computer operations and more, from a pandemic event (e.g., fire, flood, tornado or hurricane).

Entities that have a high risk regarding backup and recovery include, at least, those that rely heavily on IT and data to conduct business, operate solely online (e-commerce) and operate 24/7. More than likely, all Fortune 1,000 enterprises are at a high risk; however, a small entity that uses cutting-edge IT and whose business processes are heavily reliant on IT is also at a high risk.

This column attempts to explain the principles of an effective backup and recovery plan and to provide some guidance for conducting an IT audit for backup and recovery.

DATA

Management should provide for a means to back up relevant data on a regular basis. The principle for regular data backups is to back up data daily. That backup could be to media (e.g., tape or external hard drive), or it could be to a remote location via the cloud (i.e., the Internet). If an enterprise is backing up to media, the aforementioned principle recommends that backups be conducted to a different media for end-of-week and end-of-month backups (this daily, weekly and monthly set of backups is known as "grandfather-father-son").

The next concern is whether the backup process is reliable. Therefore, upon using a new backup methodology or technology, management should provide a means to test the data afterward to ensure that the process is actually recording all of the data onto the target backup device.

Another concern is where the backup is stored. If it is stored onsite and if the entity suffers a pandemic event such as a fire, the event would destroy the operational data and the backup data. Thus, the backup principle for storage is to provide a location that is at a safe distance from the entity's location. The cloud automatically provides this element.

Additionally, management should provide a test for restoring the backup at least once a year. That test should be documented, even if it is just a screenshot showing the data restored.

COMPUTER OPERATIONS

The purpose of the computer operations piece of a backup and recovery plan is to recover from a broad, adverse effect on the computer systems of the entity (**figure 1**). This part of the plan is commonly called a business continuity plan (BCP) or disaster recovery plan (DRP).[1] The adverse event could be systems-related, such as the failure of a mainframe computer to operate, or it could be the result of a natural disaster, such as a fire that destroys some or all of the computer systems and data.

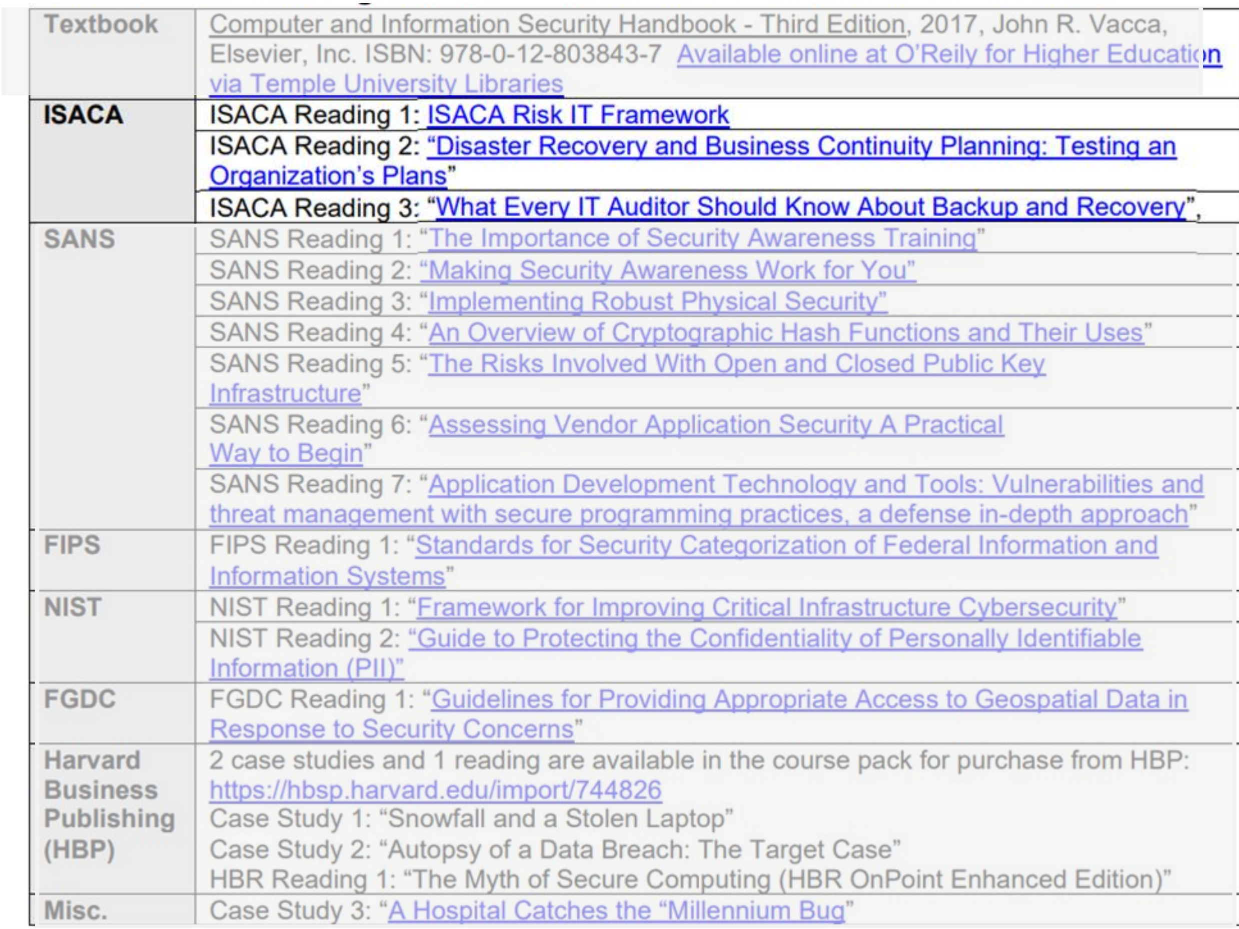
Figure 1—Recovery Principles

- Identify and rank critical applications.
- Create a recovery team with roles and responsibilities.
- Provide a backup for all essential components of computer operations.
- Provide for regular and effective testing of the plan.

Obviously, this plan is much more involved than simply making a backup of data and being able to restore it effectively when necessary. In this case, it may be necessary to restore everything about the infrastructure: computers, operating systems (OSs), applications and data. Even systems documentation and computer supplies could be involved.

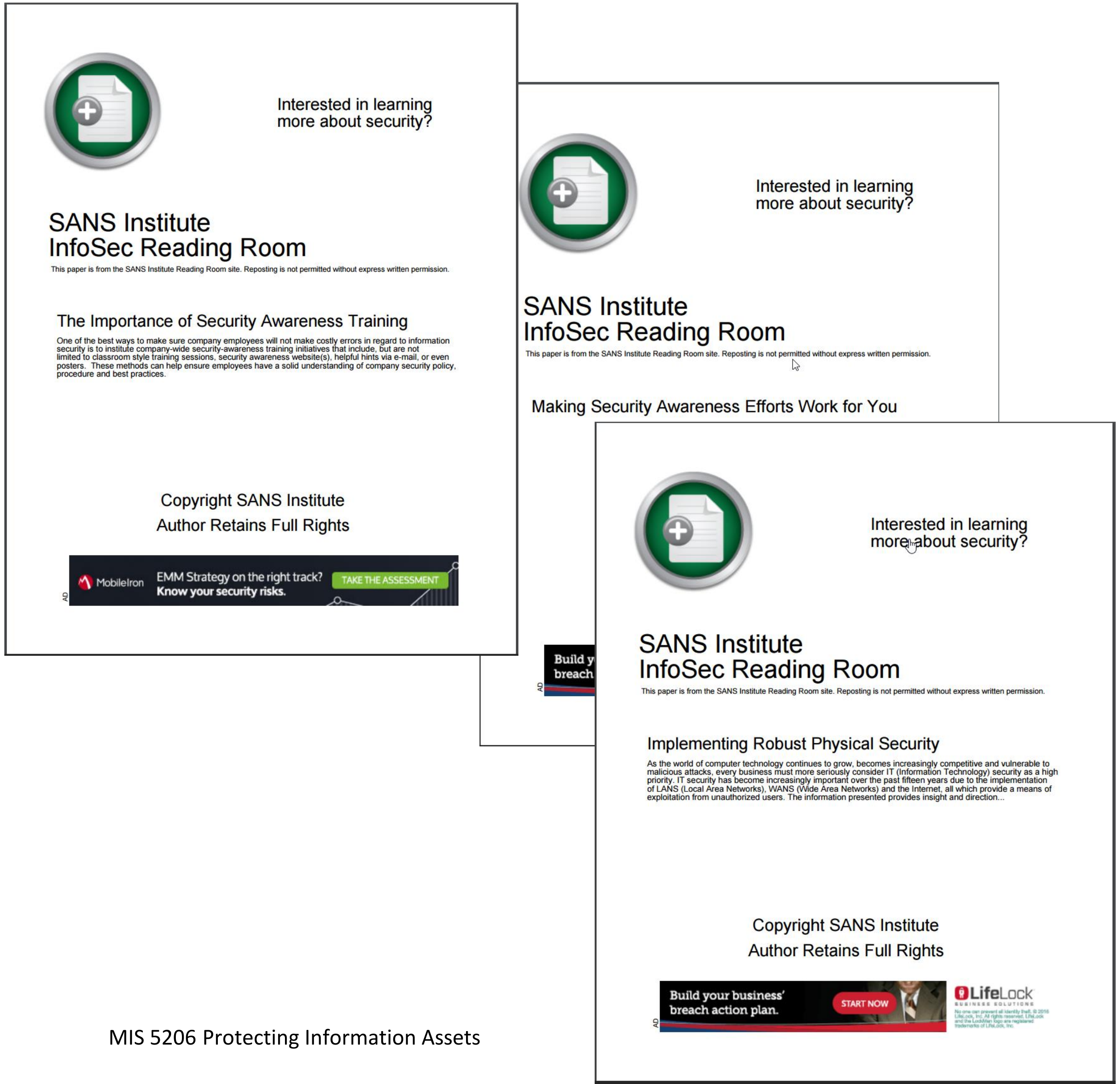
The principles of developing a BCP/DRP include a step to identify the critical applications and rank them in importance of operations. This list becomes strategically valuable if ever needed in providing the recovery team with a blueprint of how to restore application software.

1 ISACA JOURNAL VOLUME 6, 2011



Textbook	Computer and Information Security Handbook - Third Edition, 2017, John R. Vacca, Elsevier, Inc. ISBN: 978-0-12-803843-7 Available online at O'Reily for Higher Education via Temple University Libraries
ISACA	ISACA Reading 1: ISACA Risk IT Framework ISACA Reading 2: "Disaster Recovery and Business Continuity Planning: Testing an Organization's Plans" ISACA Reading 3: "What Every IT Auditor Should Know About Backup and Recovery",
SANS	SANS Reading 1: "The Importance of Security Awareness Training" SANS Reading 2: "Making Security Awareness Work for You" SANS Reading 3: "Implementing Robust Physical Security" SANS Reading 4: "An Overview of Cryptographic Hash Functions and Their Uses" SANS Reading 5: "The Risks Involved With Open and Closed Public Key Infrastructure" SANS Reading 6: "Assessing Vendor Application Security A Practical Way to Begin" SANS Reading 7: "Application Development Technology and Tools: Vulnerabilities and threat management with secure programming practices, a defense in-depth approach"
FIPS	FIPS Reading 1: "Standards for Security Categorization of Federal Information and Information Systems"
NIST	NIST Reading 1: "Framework for Improving Critical Infrastructure Cybersecurity" NIST Reading 2: "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)"
FGDC	FGDC Reading 1: "Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns"
Harvard Business Publishing (HBP)	2 case studies and 1 reading are available in the course pack for purchase from HBP: https://hbsp.harvard.edu/import/744826 Case Study 1: "Snowfall and a Stolen Laptop" Case Study 2: "Autopsy of a Data Breach: The Target Case" HBR Reading 1: "The Myth of Secure Computing (HBR OnPoint Enhanced Edition)"
Misc.	Case Study 3: "A Hospital Catches the "Millennium Bug"

Textbook and readings



Interested in learning more about security?

SANS Institute
InfoSec Reading Room

The Importance of Security Awareness Training

One of the best ways to make sure company employees will not make costly errors in regard to information security is to institute company-wide security-awareness training initiatives that include, but are not limited to classroom style training sessions, security awareness website(s), helpful hints via e-mail, or even posters. These methods can help ensure employees have a solid understanding of company security policy, procedure and best practices.

Interested in learning more about security?

SANS Institute
InfoSec Reading Room

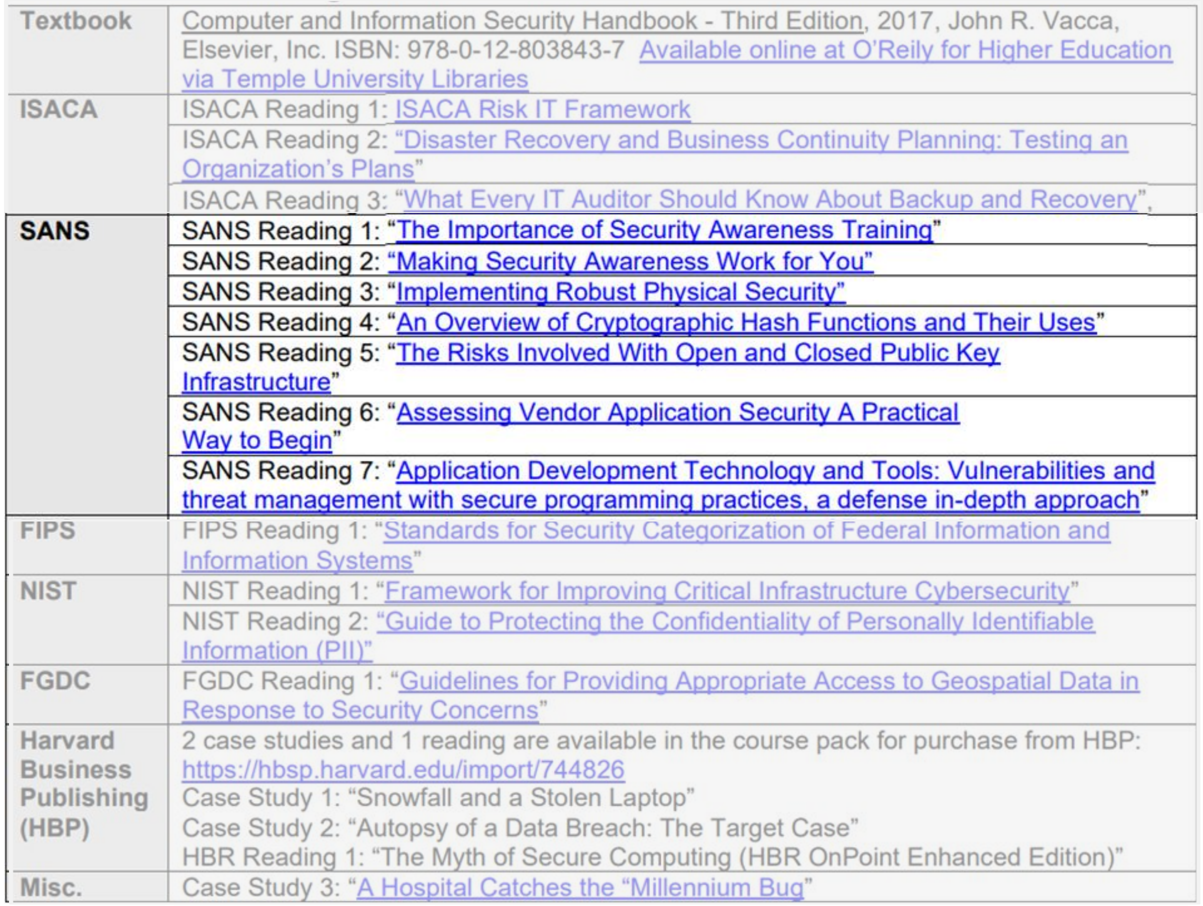
Making Security Awareness Efforts Work for You

Interested in learning more about security?

SANS Institute
InfoSec Reading Room

Implementing Robust Physical Security

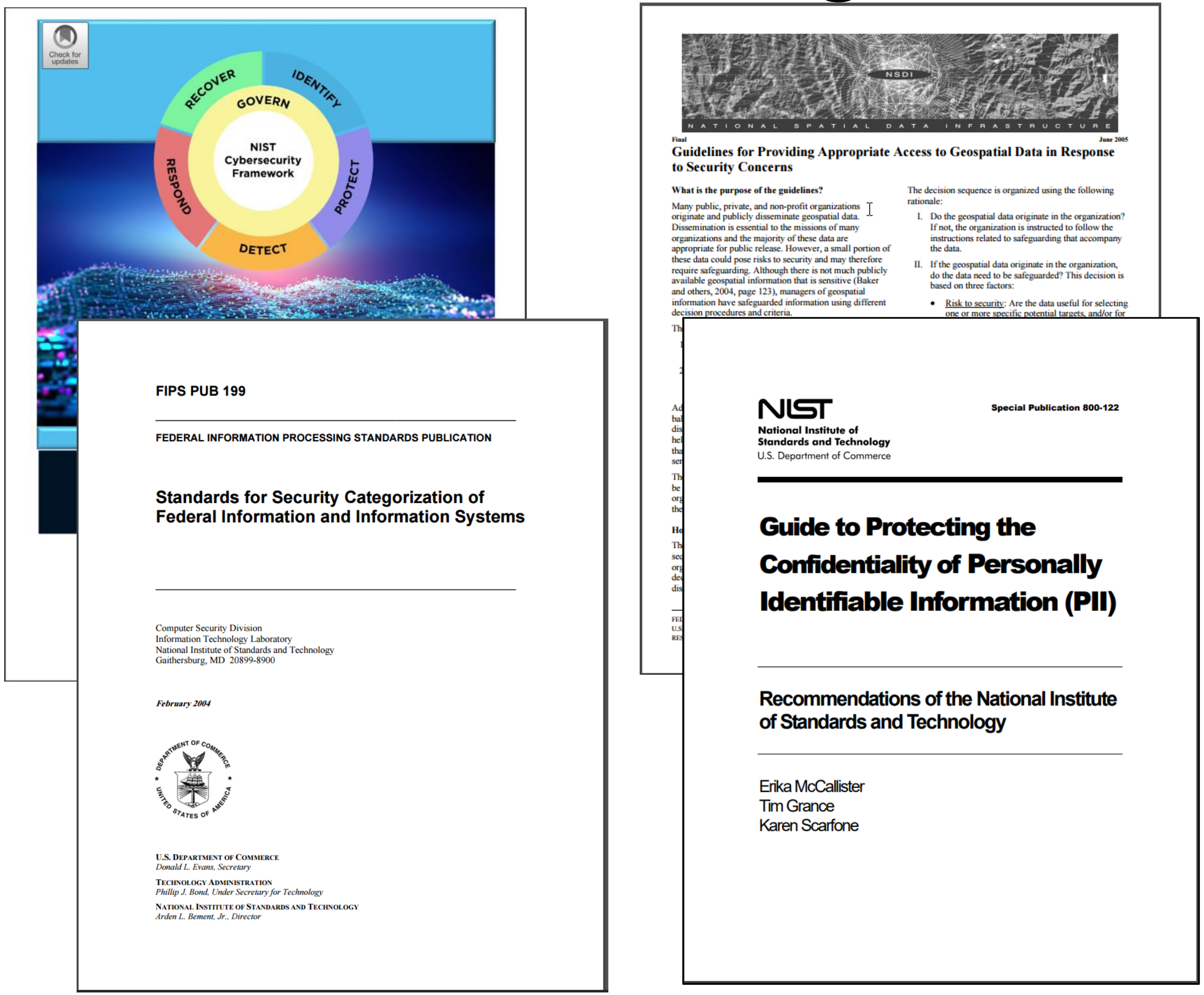
As the world of computer technology continues to grow, becomes increasingly competitive and vulnerable to malicious attacks, every business must more seriously consider IT (Information Technology) security as a high priority. IT security has become increasingly important over the past fifteen years due to the implementation of LANS (Local Area Networks), WANS (Wide Area Networks) and the Internet, all which provide a means of exploitation from unauthorized users. The information presented provides insight and direction...



Textbook	Computer and Information Security Handbook - Third Edition, 2017, John R. Vacca, Elsevier, Inc. ISBN: 978-0-12-803843-7 Available online at O'Reily for Higher Education via Temple University Libraries
ISACA	ISACA Reading 1: ISACA Risk IT Framework
	ISACA Reading 2: "Disaster Recovery and Business Continuity Planning: Testing an Organization's Plans"
	ISACA Reading 3: "What Every IT Auditor Should Know About Backup and Recovery",
SANS	SANS Reading 1: "The Importance of Security Awareness Training"
	SANS Reading 2: "Making Security Awareness Work for You"
	SANS Reading 3: "Implementing Robust Physical Security"
	SANS Reading 4: "An Overview of Cryptographic Hash Functions and Their Uses"
	SANS Reading 5: "The Risks Involved With Open and Closed Public Key Infrastructure"
	SANS Reading 6: "Assessing Vendor Application Security A Practical Way to Begin"
	SANS Reading 7: "Application Development Technology and Tools: Vulnerabilities and threat management with secure programming practices, a defense in-depth approach"
FIPS	FIPS Reading 1: "Standards for Security Categorization of Federal Information and Information Systems"
NIST	NIST Reading 1: "Framework for Improving Critical Infrastructure Cybersecurity"
	NIST Reading 2: "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)"
FGDC	FGDC Reading 1: "Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns"
Harvard Business Publishing (HBP)	2 case studies and 1 reading are available in the course pack for purchase from HBP: https://hbsp.harvard.edu/import/744826 Case Study 1: "Snowfall and a Stolen Laptop" Case Study 2: "Autopsy of a Data Breach: The Target Case" HBR Reading 1: "The Myth of Secure Computing (HBR OnPoint Enhanced Edition)"
Misc.	Case Study 3: "A Hospital Catches the "Millennium Bug"

…

Textbook and readings



NATIONAL SPATIAL DATA INFRASTRUCTURE

NSDI

Final June 2005

Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns

What is the purpose of the guidelines?

Many public, private, and non-profit organizations originate and publicly disseminate geospatial data. Dissemination is essential to the missions of many organizations and the majority of these data are appropriate for public release. However, a small portion of these data could pose risks to security and may therefore require safeguarding. Although there is not much publicly available geospatial information that is sensitive (Baker and others, 2004, page 123), managers of geospatial information have safeguarded information using different decision procedures and criteria.

The decision sequence is organized using the following rationale:

I. Do the geospatial data originate in the organization? If not, the organization is instructed to follow the instructions related to safeguarding that accompany the data.

II. If the geospatial data originate in the organization, do the data need to be safeguarded? This decision is based on three factors:

- Risk to security: Are the data useful for selecting one or more specific potential targets, and/or for

FIPS PUB 199

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Standards for Security Categorization of Federal Information and Information Systems

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

February 2004

U.S. DEPARTMENT OF COMMERCE
Donald L. Evans, Secretary
TECHNOLOGY ADMINISTRATION
Phillip J. Bond, Under Secretary for Technology
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Arden L. Bement, Jr., Director

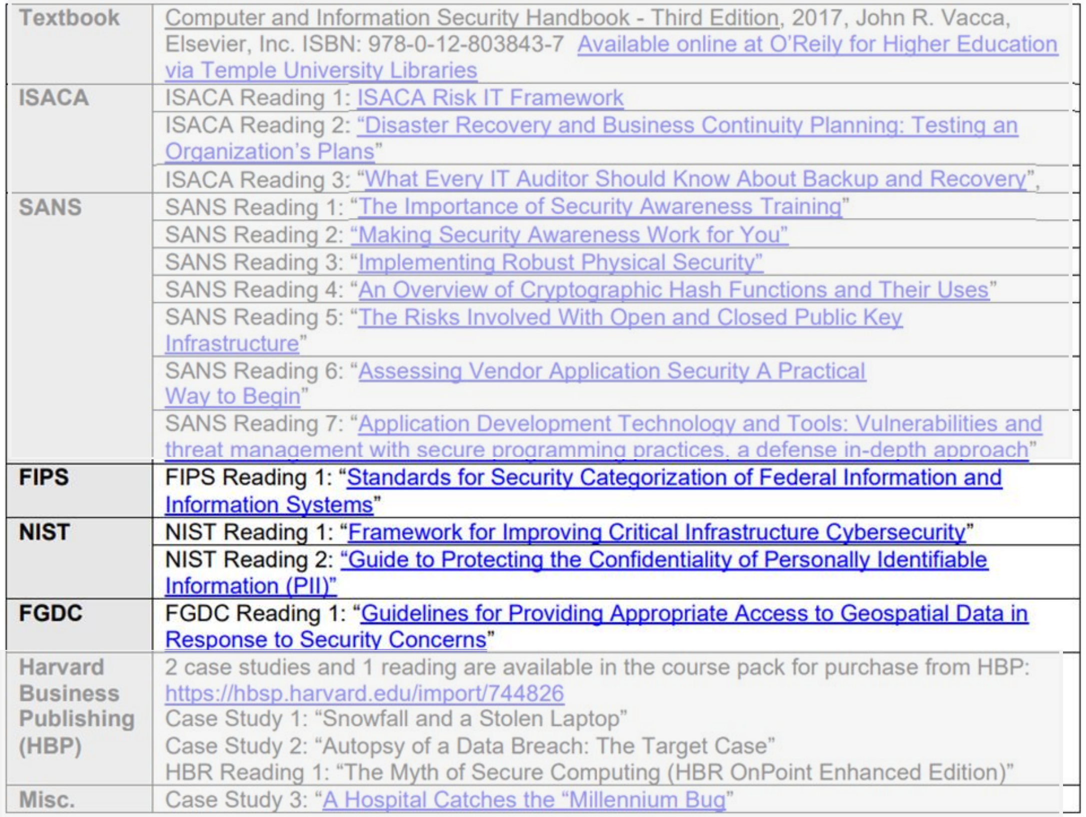
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-122

Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)

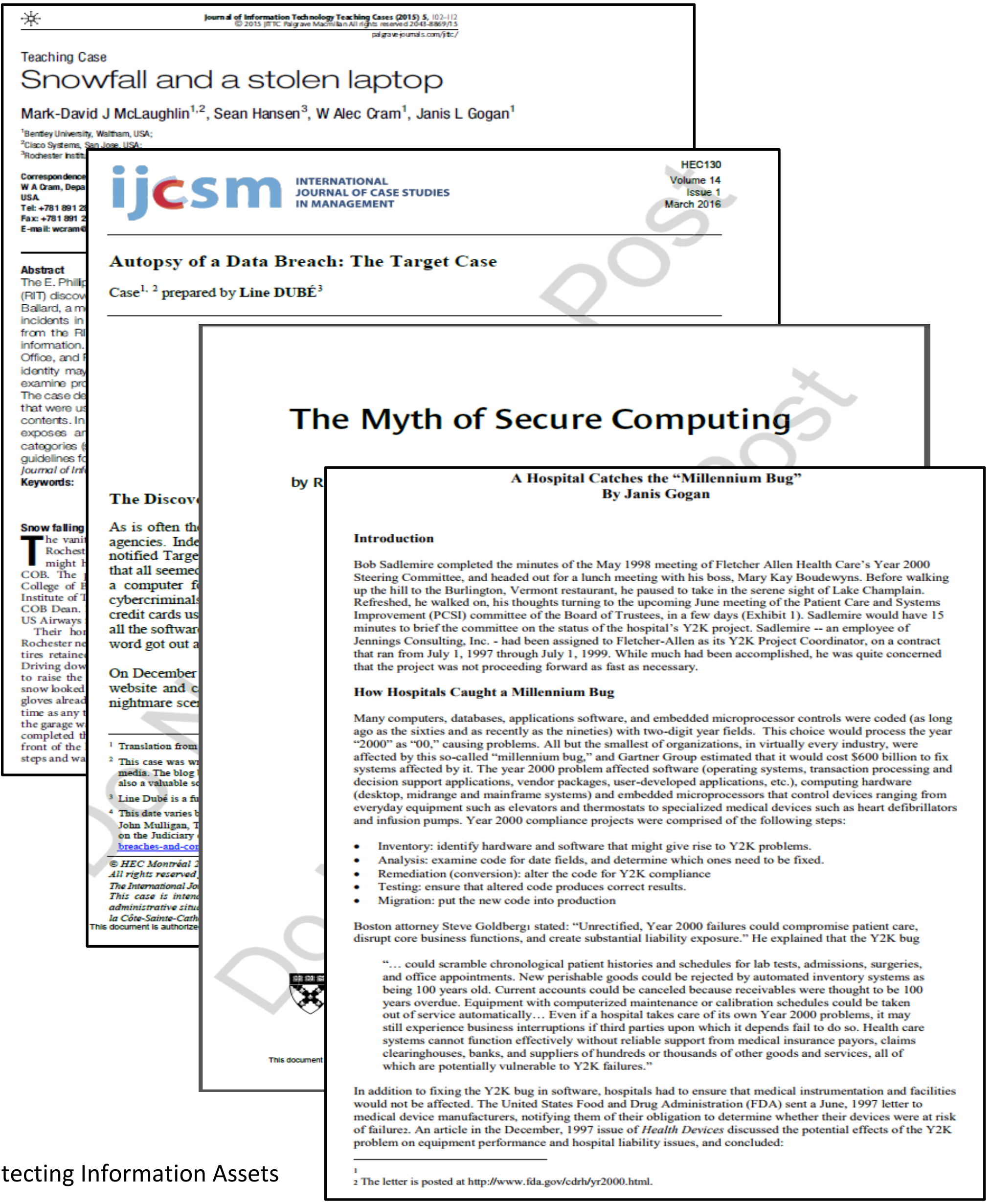
Recommendations of the National Institute of Standards and Technology

Erika McCallister
Tim Grance
Karen Scarfone



Textbook	Computer and Information Security Handbook - Third Edition, 2017, John R. Vacca, Elsevier, Inc. ISBN: 978-0-12-803843-7 Available online at O'Reily for Higher Education via Temple University Libraries
ISACA	ISACA Reading 1: ISACA Risk IT Framework
	ISACA Reading 2: "Disaster Recovery and Business Continuity Planning: Testing an Organization's Plans"
	ISACA Reading 3: "What Every IT Auditor Should Know About Backup and Recovery",
SANS	SANS Reading 1: "The Importance of Security Awareness Training"
	SANS Reading 2: "Making Security Awareness Work for You"
	SANS Reading 3: "Implementing Robust Physical Security"
	SANS Reading 4: "An Overview of Cryptographic Hash Functions and Their Uses"
	SANS Reading 5: "The Risks Involved With Open and Closed Public Key Infrastructure"
	SANS Reading 6: "Assessing Vendor Application Security A Practical Way to Begin"
	SANS Reading 7: "Application Development Technology and Tools: Vulnerabilities and threat management with secure programming practices, a defense in-depth approach"
FIPS	FIPS Reading 1: "Standards for Security Categorization of Federal Information and Information Systems"
NIST	NIST Reading 1: "Framework for Improving Critical Infrastructure Cybersecurity"
	NIST Reading 2: "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)"
FGDC	FGDC Reading 1: "Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns"
Harvard Business Publishing (HBP)	2 case studies and 1 reading are available in the course pack for purchase from HBP: https://hbsp.harvard.edu/import/744826 Case Study 1: "Snowfall and a Stolen Laptop" Case Study 2: "Autopsy of a Data Breach: The Target Case" HBR Reading 1: "The Myth of Secure Computing (HBR OnPoint Enhanced Edition)"
Misc.	Case Study 3: "A Hospital Catches the "Millennium Bug"

Textbook and readings



Journal of Information Technology Teaching Cases (2015) 5, 102–112
© 2015 JITTC Palgrave Macmillan All rights reserved 2043-8869/15
palgrave-journals.com/jittc/

Teaching Case

Snowfall and a stolen laptop

Mark-David J McLaughlin[1,2], Sean Hansen[3], W Alec Cram[1], Janis L Gogan[1]

ijcsm INTERNATIONAL JOURNAL OF CASE STUDIES IN MANAGEMENT

HEC130
Volume 14
Issue 1
March 2016

Autopsy of a Data Breach: The Target Case

Case[1, 2] prepared by Line DUBÉ[3]

The Myth of Secure Computing

A Hospital Catches the "Millennium Bug"
By Janis Gogan

Introduction

Bob Sadlemire completed the minutes of the May 1998 meeting of Fletcher Allen Health Care's Year 2000 Steering Committee, and headed out for a lunch meeting with his boss, Mary Kay Boudewyns. Before walking up the hill to the Burlington, Vermont restaurant, he paused to take in the serene sight of Lake Champlain. Refreshed, he walked on, his thoughts turning to the upcoming June meeting of the Patient Care and Systems Improvement (PCSI) committee of the Board of Trustees, in a few days (Exhibit 1). Sadlemire would have 15 minutes to brief the committee on the status of the hospital's Y2K project. Sadlemire -- an employee of Jennings Consulting, Inc. - had been assigned to Fletcher-Allen as its Y2K Project Coordinator, on a contract that ran from July 1, 1997 through July 1, 1999. While much had been accomplished, he was quite concerned that the project was not proceeding forward as fast as necessary.

How Hospitals Caught a Millennium Bug

Many computers, databases, applications software, and embedded microprocessor controls were coded (as long ago as the sixties and as recently as the nineties) with two-digit year fields. This choice would process the year "2000" as "00," causing problems. All but the smallest of organizations, in virtually every industry, were affected by this so-called "millennium bug," and Gartner Group estimated that it would cost $600 billion to fix systems affected by it. The year 2000 problem affected software (operating systems, transaction processing and decision support applications, vendor packages, user-developed applications, etc.), computing hardware (desktop, midrange and mainframe systems) and embedded microprocessors that control devices ranging from everyday equipment such as elevators and thermostats to specialized medical devices such as heart defibrillators and infusion pumps. Year 2000 compliance projects were comprised of the following steps:

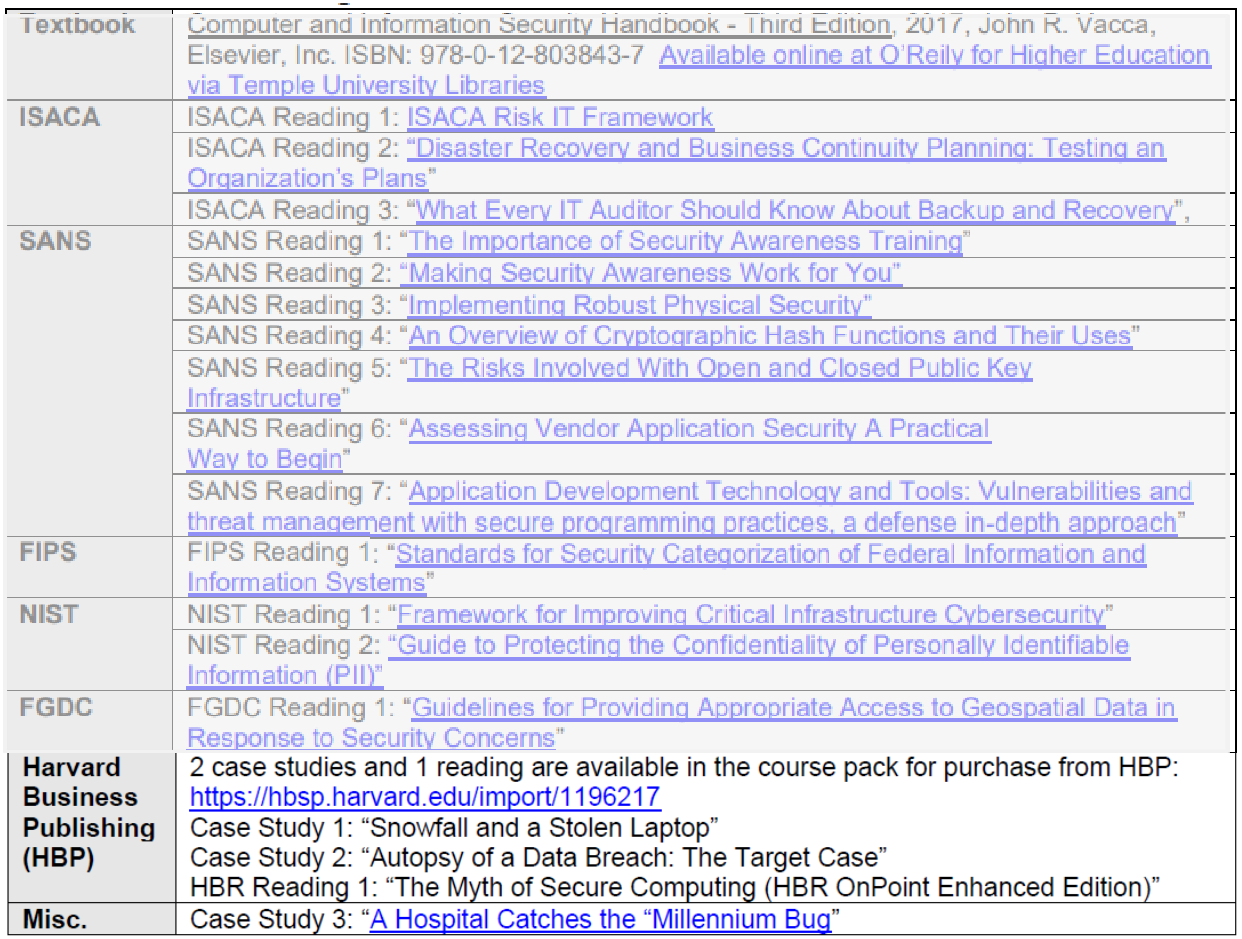
- Inventory: identify hardware and software that might give rise to Y2K problems.
- Analysis: examine code for date fields, and determine which ones need to be fixed.
- Remediation (conversion): alter the code for Y2K compliance
- Testing: ensure that altered code produces correct results.
- Migration: put the new code into production

Boston attorney Steve Goldberg[1] stated: "Unrectified, Year 2000 failures could compromise patient care, disrupt core business functions, and create substantial liability exposure." He explained that the Y2K bug

> "… could scramble chronological patient histories and schedules for lab tests, admissions, surgeries, and office appointments. New perishable goods could be rejected by automated inventory systems as being 100 years old. Current accounts could be canceled because receivables were thought to be 100 years overdue. Equipment with computerized maintenance or calibration schedules could be taken out of service automatically… Even if a hospital takes care of its own Year 2000 problems, it may still experience business interruptions if third parties upon which it depends fail to do so. Health care systems cannot function effectively without reliable support from medical insurance payors, claims clearinghouses, banks, and suppliers of hundreds or thousands of other goods and services, all of which are potentially vulnerable to Y2K failures."

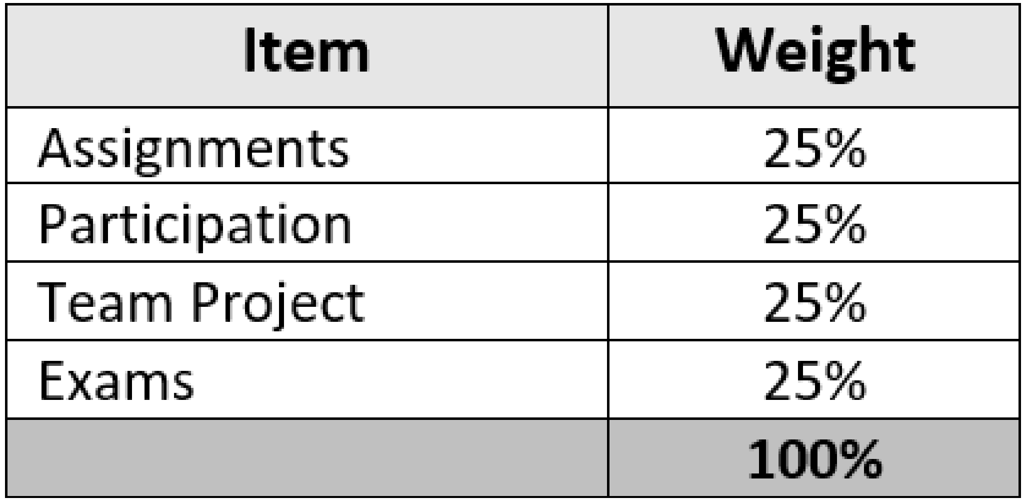
In addition to fixing the Y2K bug in software, hospitals had to ensure that medical instrumentation and facilities would not be affected. The United States Food and Drug Administration (FDA) sent a June, 1997 letter to medical device manufacturers, notifying them of their obligation to determine whether their devices were at risk of failure[2]. An article in the December, 1997 issue of *Health Devices* discussed the potential effects of the Y2K problem on equipment performance and hospital liability issues, and concluded:

[1]
[2] The letter is posted at http://www.fda.gov/cdrh/yr2000.html.



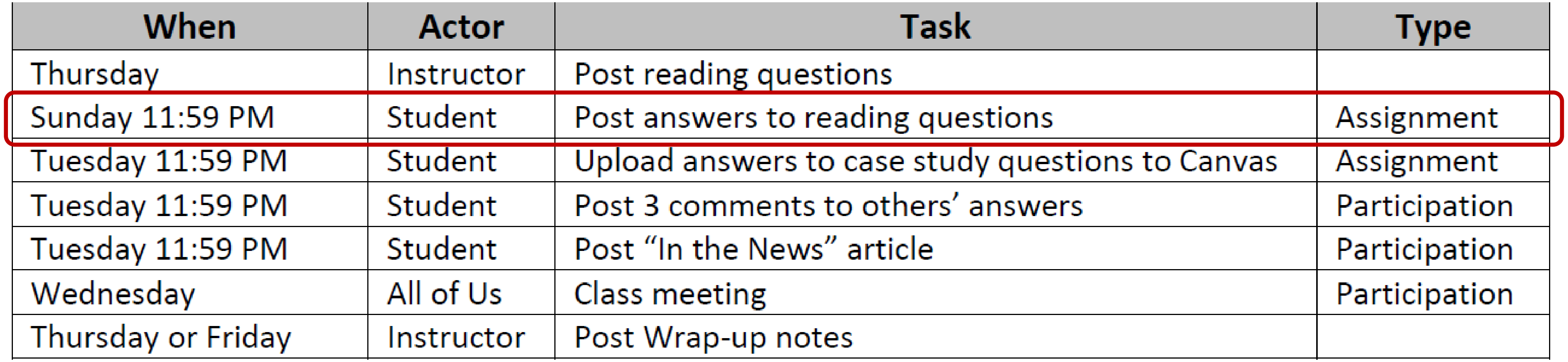
Textbook	Computer and Information Security Handbook - Third Edition, 2017, John R. Vacca, Elsevier, Inc. ISBN: 978-0-12-803843-7 Available online at O'Reily for Higher Education via Temple University Libraries
ISACA	ISACA Reading 1: ISACA Risk IT Framework
	ISACA Reading 2: "Disaster Recovery and Business Continuity Planning: Testing an Organization's Plans"
	ISACA Reading 3: "What Every IT Auditor Should Know About Backup and Recovery",
SANS	SANS Reading 1: "The Importance of Security Awareness Training"
	SANS Reading 2: "Making Security Awareness Work for You"
	SANS Reading 3: "Implementing Robust Physical Security"
	SANS Reading 4: "An Overview of Cryptographic Hash Functions and Their Uses"
	SANS Reading 5: "The Risks Involved With Open and Closed Public Key Infrastructure"
	SANS Reading 6: "Assessing Vendor Application Security A Practical Way to Begin"
	SANS Reading 7: "Application Development Technology and Tools: Vulnerabilities and threat management with secure programming practices, a defense in-depth approach"
FIPS	FIPS Reading 1: "Standards for Security Categorization of Federal Information and Information Systems"
NIST	NIST Reading 1: "Framework for Improving Critical Infrastructure Cybersecurity"
	NIST Reading 2: "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)"
FGDC	FGDC Reading 1: "Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns"
Harvard Business Publishing (HBP)	2 case studies and 1 reading are available in the course pack for purchase from HBP: https://hbsp.harvard.edu/import/1196217 Case Study 1: "Snowfall and a Stolen Laptop" Case Study 2: "Autopsy of a Data Breach: The Target Case" HBR Reading 1: "The Myth of Secure Computing (HBR OnPoint Enhanced Edition)"
Misc.	Case Study 3: "A Hospital Catches the "Millennium Bug"

Grading



Item	Weight
Assignments	25%
Participation	25%
Team Project	25%
Exams	25%
	100%

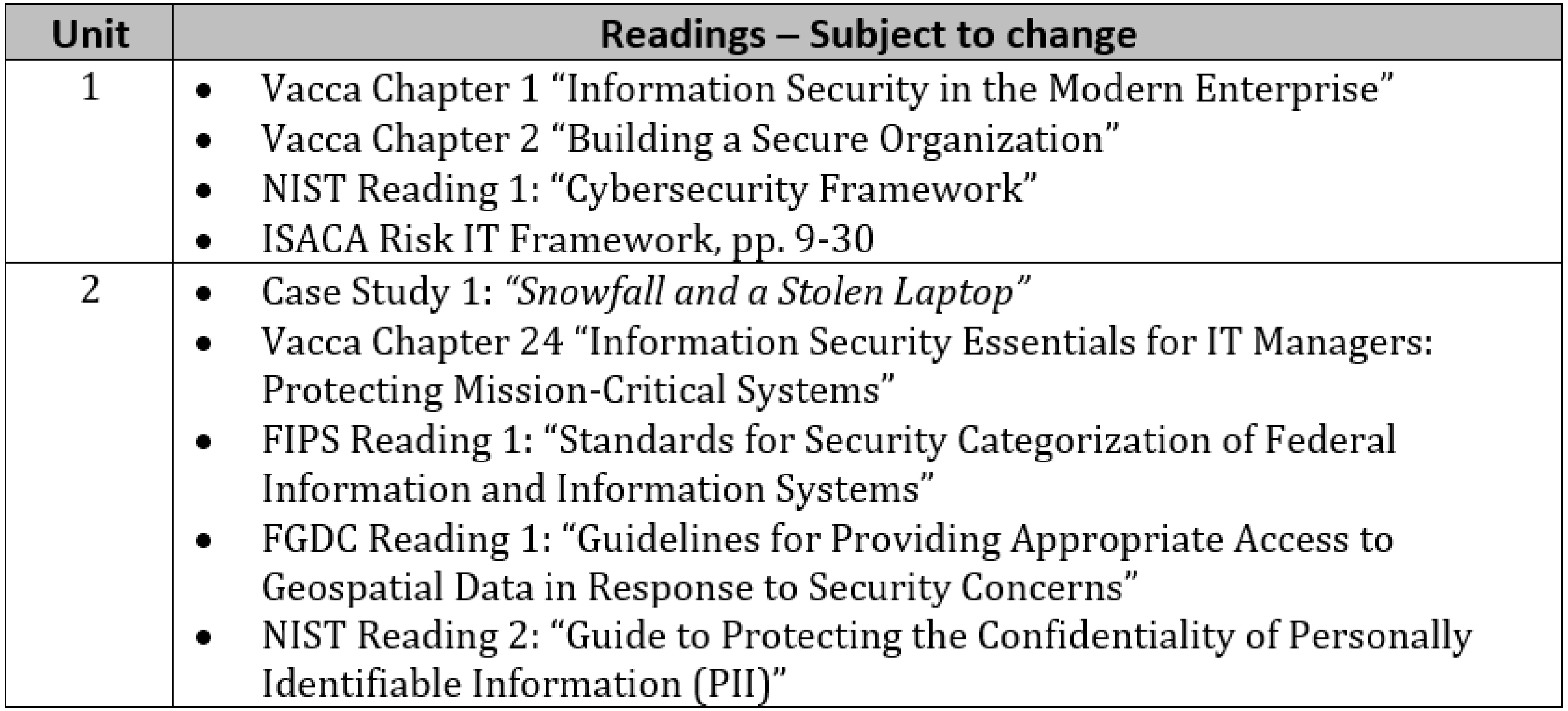
Weekly Cycle



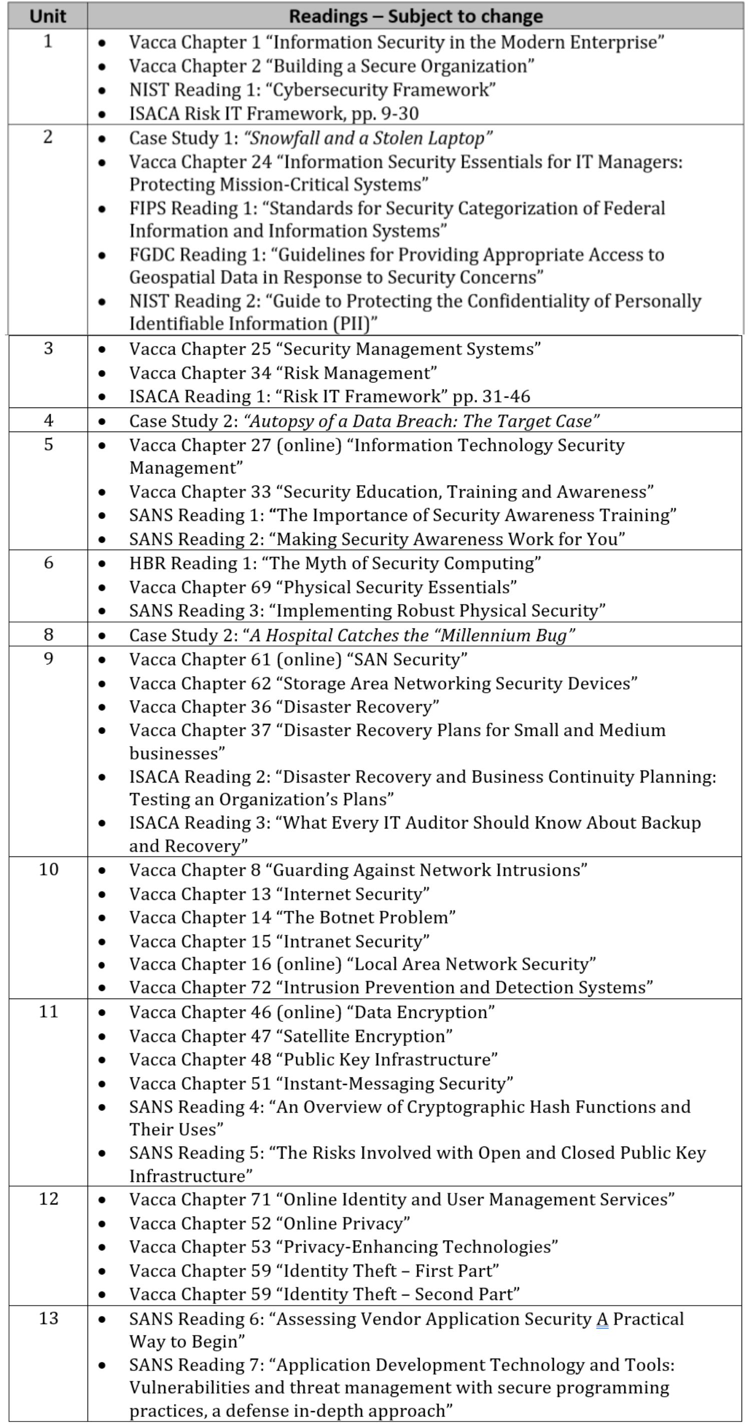
When	Actor	Task	Type
Thursday	Instructor	Post reading questions	
Sunday 11:59 PM	Student	Post answers to reading questions	Assignment
Tuesday 11:59 PM	Student	Upload answers to case study questions to Canvas	Assignment
Tuesday 11:59 PM	Student	Post 3 comments to others’ answers	Participation
Tuesday 11:59 PM	Student	Post “In the News” article	Participation
Wednesday	All of Us	Class meeting	Participation
Thursday or Friday	Instructor	Post Wrap-up notes	

Assignments

1. Readings



Unit	Readings – Subject to change
1	• Vacca Chapter 1 "Information Security in the Modern Enterprise" • Vacca Chapter 2 "Building a Secure Organization" • NIST Reading 1: "Cybersecurity Framework" • ISACA Risk IT Framework, pp. 9-30
2	• Case Study 1: *"Snowfall and a Stolen Laptop"* • Vacca Chapter 24 "Information Security Essentials for IT Managers: Protecting Mission-Critical Systems" • FIPS Reading 1: "Standards for Security Categorization of Federal Information and Information Systems" • FGDC Reading 1: "Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns" • NIST Reading 2: "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)"



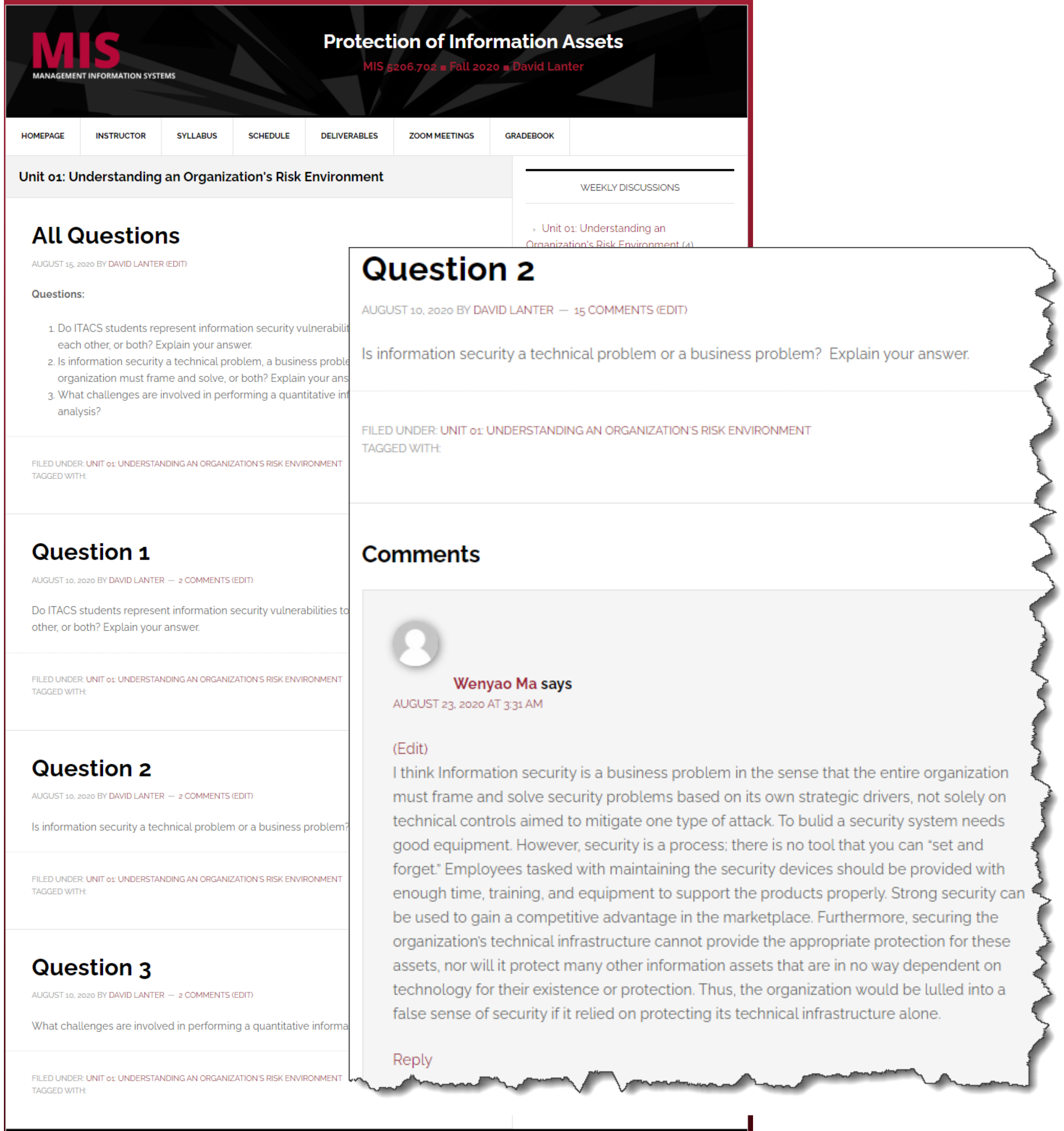
Unit	Readings – Subject to change
1	• Vacca Chapter 1 "Information Security in the Modern Enterprise" • Vacca Chapter 2 "Building a Secure Organization" • NIST Reading 1: "Cybersecurity Framework" • ISACA Risk IT Framework, pp. 9-30
2	• Case Study 1: *"Snowfall and a Stolen Laptop"* • Vacca Chapter 24 "Information Security Essentials for IT Managers: Protecting Mission-Critical Systems" • FIPS Reading 1: "Standards for Security Categorization of Federal Information and Information Systems" • FGDC Reading 1: "Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns" • NIST Reading 2: "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)"
3	• Vacca Chapter 25 "Security Management Systems" • Vacca Chapter 34 "Risk Management" • ISACA Reading 1: "Risk IT Framework" pp. 31-46
4	• Case Study 2: *"Autopsy of a Data Breach: The Target Case"*
5	• Vacca Chapter 27 (online) "Information Technology Security Management" • Vacca Chapter 33 "Security Education, Training and Awareness" • SANS Reading 1: "The Importance of Security Awareness Training" • SANS Reading 2: "Making Security Awareness Work for You"
6	• HBR Reading 1: "The Myth of Security Computing" • Vacca Chapter 69 "Physical Security Essentials" • SANS Reading 3: "Implementing Robust Physical Security"
8	• Case Study 2: *"A Hospital Catches the "Millennium Bug"*
9	• Vacca Chapter 61 (online) "SAN Security" • Vacca Chapter 62 "Storage Area Networking Security Devices" • Vacca Chapter 36 "Disaster Recovery" • Vacca Chapter 37 "Disaster Recovery Plans for Small and Medium businesses" • ISACA Reading 2: "Disaster Recovery and Business Continuity Planning: Testing an Organization's Plans" • ISACA Reading 3: "What Every IT Auditor Should Know About Backup and Recovery"
10	• Vacca Chapter 8 "Guarding Against Network Intrusions" • Vacca Chapter 13 "Internet Security" • Vacca Chapter 14 "The Botnet Problem" • Vacca Chapter 15 "Intranet Security" • Vacca Chapter 16 (online) "Local Area Network Security" • Vacca Chapter 72 "Intrusion Prevention and Detection Systems"
11	• Vacca Chapter 46 (online) "Data Encryption" • Vacca Chapter 47 "Satellite Encryption" • Vacca Chapter 48 "Public Key Infrastructure" • Vacca Chapter 51 "Instant-Messaging Security" • SANS Reading 4: "An Overview of Cryptographic Hash Functions and Their Uses" • SANS Reading 5: "The Risks Involved with Open and Closed Public Key Infrastructure"
12	• Vacca Chapter 71 "Online Identity and User Management Services" • Vacca Chapter 52 "Online Privacy" • Vacca Chapter 53 "Privacy-Enhancing Technologies" • Vacca Chapter 59 "Identity Theft – First Part" • Vacca Chapter 59 "Identity Theft – Second Part"
13	• SANS Reading 6: "Assessing Vendor Application Security A Practical Way to Begin" • SANS Reading 7: "Application Development Technology and Tools: Vulnerabilities and threat management with secure programming practices, a defense in-depth approach"

Assignments

2. Answer reading questions

Questions are posted on the MIS5214 class web site questions organized by Unit # for the readings. You are expected to post your answers to the questions as you complete each unit.

- *A paragraph or two of thoughtful analysis is expected for your answer to each question*
- *Post your answer to the class assignment blog*
- *Come to class prepared to discuss all of the questions in detail when we meet*


MIS
MANAGEMENT INFORMATION SYSTEMS
Protection of Information Assets
MIS 5206.702 ■ Fall 2020 ■ David Lanter
HOMEPAGE
INSTRUCTOR
SYLLABUS
SCHEDULE
DELIVERABLES
ZOOM MEETINGS
GRADEBOOK
WEEKLY DISCUSSIONS
› Unit 01: Understanding an Organization's Risk Environment (4)

Unit 01: Understanding an Organization's Risk Environment

All Questions

AUGUST 15, 2020 BY DAVID LANTER (EDIT)

Questions:

1. Do ITACS students represent information security vulnerabilit
each other, or both? Explain your answer.
2. Is information security a technical problem, a business proble
organization must frame and solve, or both? Explain your ans
3. What challenges are involved in performing a quantitative inf
analysis?

FILED UNDER: UNIT 01: UNDERSTANDING AN ORGANIZATION'S RISK ENVIRONMENT
TAGGED WITH:

Question 1

AUGUST 10, 2020 BY DAVID LANTER — 2 COMMENTS (EDIT)

Do ITACS students represent information security vulnerabilities to
other, or both? Explain your answer.

FILED UNDER: UNIT 01: UNDERSTANDING AN ORGANIZATION'S RISK ENVIRONMENT
TAGGED WITH:

Question 2

AUGUST 10, 2020 BY DAVID LANTER — 2 COMMENTS (EDIT)

Is information security a technical problem or a business problem?

FILED UNDER: UNIT 01: UNDERSTANDING AN ORGANIZATION'S RISK ENVIRONMENT
TAGGED WITH:

Question 3

AUGUST 10, 2020 BY DAVID LANTER — 2 COMMENTS (EDIT)

What challenges are involved in performing a quantitative informa

FILED UNDER: UNIT 01: UNDERSTANDING AN ORGANIZATION'S RISK ENVIRONMENT
TAGGED WITH:

Question 2

AUGUST 10, 2020 BY DAVID LANTER — 15 COMMENTS (EDIT)

Is information security a technical problem or a business problem? Explain your answer.

FILED UNDER: UNIT 01: UNDERSTANDING AN ORGANIZATION'S RISK ENVIRONMENT
TAGGED WITH:

Comments

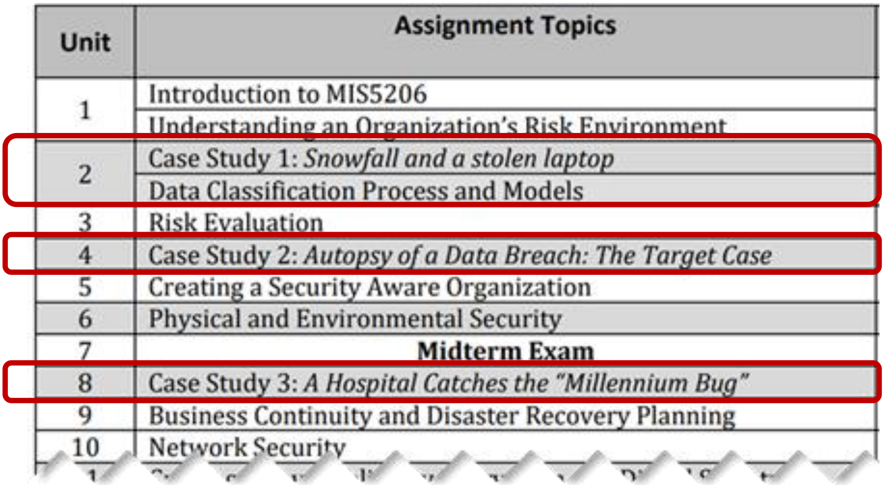
Wenyao Ma says
AUGUST 23, 2020 AT 3:31 AM

(Edit)
I think Information security is a business problem in the sense that the entire organization must frame and solve security problems based on its own strategic drivers, not solely on technical controls aimed to mitigate one type of attack. To bulid a security system needs good equipment. However, security is a process; there is no tool that you can "set and forget." Employees tasked with maintaining the security devices should be provided with enough time, training, and equipment to support the products properly. Strong security can be used to gain a competitive advantage in the marketplace. Furthermore, securing the organization's technical infrastructure cannot provide the appropriate protection for these assets, nor will it protect many other information assets that are in no way dependent on technology for their existence or protection. Thus, the organization would be lulled into a false sense of security if it relied on protecting its technical infrastructure alone.

Reply

Weekly Cycle

When	Actor	Task	Type
Thursday	Instructor	Post reading questions	
Sunday 11:59 PM	Student	Post answers to reading questions	Assignment
Tuesday 11:59 PM	Student	Upload answers to case study questions to Canvas	Assignment
Tuesday 11:59 PM	Student	Post 3 comments to others' answers	Participation
Tuesday 11:59 PM	Student	Post "In the News" article	Participation
Wednesday	All of Us	Class meeting	Participation
Thursday or Friday	Instructor	Post Wrap-up notes	



Unit	Assignment Topics
1	Introduction to MIS5206
	Understanding an Organization's Risk Environment
2	Case Study 1: *Snowfall and a stolen laptop*
	Data Classification Process and Models
3	Risk Evaluation
4	Case Study 2: *Autopsy of a Data Breach: The Target Case*
5	Creating a Security Aware Organization
6	Physical and Environmental Security
7	**Midterm Exam**
8	Case Study 3: *A Hospital Catches the "Millennium Bug"*
9	Business Continuity and Disaster Recovery Planning
10	Network Security

Assignments

3. Three case studies

You will find discussion questions for each case study posted on the class web site).

Answer each question in depth as part of your individual preparation.

Journal of Information Technology Teaching Cases (2015) 5, 102–112
© 2015 JITTC Palgrave Macmillan All rights reserved 2043-8869/15
palgrave-journals.com/jittc/

Teaching Case

Snowfall and a stolen laptop

Mark-David J McLaughlin[1,2], Sean Hansen[3], W Alec Cram[1], Janis L Gogan[1]

[1]Bentley University, Waltham, USA;
[2]Cisco Systems, San Jose, USA;
[3]Rochester Institute of Technology, Rochester, USA

Correspondence:
W A Cram, Department of Information and Process Management, Bentley University, 175 Forest Street, Waltham, MA 02452, USA.
Tel: +781 891 2811;
Fax: +781 891 2949;
E-mail: wcram@bentley.edu

Abstract
The E. Phillip Saunders College of Business (COB) Dean at Rochester Institute of Technology (RIT) discovers that his RIT-issued laptop has been stolen from his home. He notifies Dave Ballard, a member of the College of Business IT staff. Ballard, still acutely aware of two recent incidents in which laptops containing thousands of Social Security numbers were stolen from the RIT campus, hopes the Dean's laptop does not contain personally identifiable information. If so, the incident would need to be reported to the New York Attorney General's Office, and RIT would be required to pay for a credit monitoring service for individuals whose identity may have been compromised. The case provides an opportunity for students to examine processes that should be triggered when an information security incident occurs. The case describes incident response processes that were triggered at RIT and technologies that were used or could have been used by COB IT staff to track the laptop and protect its contents. In discussing the case, students can consider how the theft of a computing device exposes an organization to risks of inadvertent disclosure of information in different categories (such as private, confidential, internal, or public), and students can derive useful guidelines for effective information security incident response.

Journal of Information Technology Teaching Cases (2015) **5**, 102–112. doi:10.1057/jittc.2015.12
Keywords: information security; incident response; risk management; IT governance

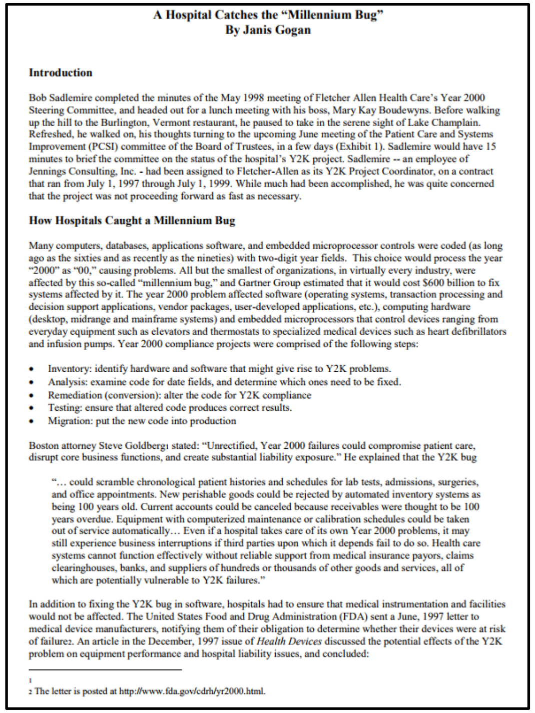
Snow falling on Rochester

The vanity plates on the Lexus pulling up to the curb at Rochester New York International Airport in February might have seemed cryptic to a casual onlooker: EPS COB. The plates' acronym stood for E. Phillip Saunders College of Business, one of eight colleges of the Rochester Institute of Technology (RIT). In the driver's seat was the EPS COB Dean. He said goodbye to his wife, who would board a US Airways flight to Boston, where she worked.

Their home sat on a corner lot in a quiet residential Rochester neighborhood. The Dean was grateful that his snow tires retained their grip; it had again been snowing all day. Driving down Villanova Street, he clicked the remote control to raise the garage door and pulled into his driveway. The snow looked to be four or five inches deep. With his jacket and gloves already on and the snow tapering off, this was as good a time as any to get a little exercise, so he grabbed a shovel from the garage wall and set to work. It was light, fluffy snow and he completed the job in 10 or 15 min. He walked around to the front of the house (facing Carleton Road) to shovel the front steps and walk. A few minutes later, after depositing the shovel in the garage, he headed into the house through the back door, wiping his snowy boots on the doormat.

And that's when he noticed a trail of wet boot prints. 'What the …?' At first he could not make sense of what he saw, but he soon realized those were not his wet boot prints; someone had been in his house! He stepped into the kitchen and through to the den, where he had planned to spend the evening answering emails and reviewing some materials in preparation for several upcoming meetings. The intruder's trail led through the den and into the front hall. He felt a cold wind blowing through the front door – why was it open? Then he felt another chill: from the sudden realization that his laptop, which he'd left on the couch in the den before taking his wife to the airport, was no longer there. After shutting and locking the front door, he raced through the house to verify that the laptop was not in another room. Nothing else seemed amiss, but the laptop was definitely gone. Its power cord dangled from the wall.

The Saunders College Dean realized he'd better call the police – and Dave Ballard.



A Hospital Catches the "Millennium Bug"
By Janis Gogan

Introduction

Bob Sadlemire completed the minutes of the May 1998 meeting of Fletcher Allen Health Care's Year 2000 Steering Committee, and headed out for a lunch meeting with his boss, Mary Kay Boudewyns. Before walking up the hill to the Burlington, Vermont restaurant, he paused to take in the serene sight of Lake Champlain. Refreshed, he walked on, his thoughts turning to the upcoming June meeting of the Patient Care and Systems Improvement (PCSI) committee of the Board of Trustees, in a few days (Exhibit 1). Sadlemire would have 15 minutes to brief the committee on the status of the hospital's Y2K project. Sadlemire -- an employee of Jennings Consulting, Inc. - had been assigned to Fletcher-Allen as its Y2K Project Coordinator, on a contract that ran from July 1, 1997 through July 1, 1999. While much had been accomplished, he was quite concerned that the project was not proceeding forward as fast as necessary.

How Hospitals Caught a Millennium Bug

Many computers, databases, applications software, and embedded microprocessor controls were coded (as long ago as the sixties and as recently as the nineties) with two-digit year fields. This choice would process the year "2000" as "00," causing problems. All but the smallest of organizations, in virtually every industry, were affected by this so-called "millennium bug," and Gartner Group estimated that it would cost $600 billion to fix systems affected by it. The year 2000 problem affected software (operating systems, transaction processing and decision support applications, vendor packages, user-developed applications, etc.), computing hardware (desktop, midrange and mainframe systems) and embedded microprocessors that control devices ranging from everyday equipment such as elevators and thermostats to specialized medical devices such as heart defibrillators and infusion pumps. Year 2000 compliance projects were comprised of the following steps:

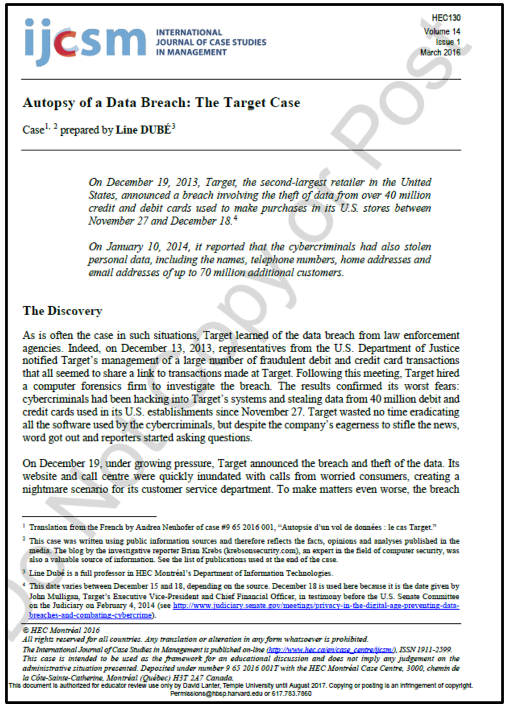
- Inventory: identify hardware and software that might give rise to Y2K problems.
- Analysis: examine code for date fields, and determine which ones need to be fixed.
- Remediation (conversion): alter the code for Y2K compliance
- Testing: ensure that altered code produces correct results.
- Migration: put the new code into production

Boston attorney Steve Goldberg[1] stated: "Unrectified, Year 2000 failures could compromise patient care, disrupt core business functions, and create substantial liability exposure." He explained that the Y2K bug

> "… could scramble chronological patient histories and schedules for lab tests, admissions, surgeries, and office appointments. New perishable goods could be rejected by automated inventory systems as being 100 years old. Current accounts could be canceled because receivables were thought to be 100 years overdue. Equipment with computerized maintenance or calibration schedules could be taken out of service automatically… Even if a hospital takes care of its own Year 2000 problems, it may still experience business interruptions if third parties upon which it depends fail to do so. Health care systems cannot function effectively without reliable support from medical insurance payors, claims clearinghouses, banks, and suppliers of hundreds or thousands of other goods and services, all of which are potentially vulnerable to Y2K failures."

In addition to fixing the Y2K bug in software, hospitals had to ensure that medical instrumentation and facilities would not be affected. The United States Food and Drug Administration (FDA) sent a June, 1997 letter to medical device manufacturers, notifying them of their obligation to determine whether their devices were at risk of failure[2]. An article in the December, 1997 issue of *Health Devices* discussed the potential effects of the Y2K problem on equipment performance and hospital liability issues, and concluded:

[1]
[2] The letter is posted at http://www.fda.gov/cdrh/yr2000.html.



ijcsm INTERNATIONAL JOURNAL OF CASE STUDIES IN MANAGEMENT

HEC130
Volume 14
Issue 1
March 2016

Autopsy of a Data Breach: The Target Case

Case[1, 2] prepared by **Line DUBÉ**[3]

> *On December 19, 2013, Target, the second-largest retailer in the United States, announced a breach involving the theft of data from over 40 million credit and debit cards used to make purchases in its U.S. stores between November 27 and December 18.*[4]
>
> *On January 10, 2014, it reported that the cybercriminals had also stolen personal data, including the names, telephone numbers, home addresses and email addresses of up to 70 million additional customers.*

The Discovery

As is often the case in such situations, Target learned of the data breach from law enforcement agencies. Indeed, on December 13, 2013, representatives from the U.S. Department of Justice notified Target's management of a large number of fraudulent debit and credit card transactions that all seemed to share a link to transactions made at Target. Following this meeting, Target hired a computer forensics firm to investigate the breach. The results confirmed its worst fears: cybercriminals had been hacking into Target's systems and stealing data from 40 million debit and credit cards used in its U.S. establishments since November 27. Target wasted no time eradicating all the software used by the cybercriminals, but despite the company's eagerness to stifle the news, word got out and reporters started asking questions.

On December 19, under growing pressure, Target announced the breach and theft of the data. Its website and call centre were quickly inundated with calls from worried consumers, creating a nightmare scenario for its customer service department. To make matters even worse, the breach

[1] Translation from the French by Andrea Neuhofer of case #9 65 2016 001, "Autopsie d'un vol de données : le cas Target."

[2] This case was written using public information sources and therefore reflects the facts, opinions and analyses published in the media. The blog by the investigative reporter Brian Krebs (krebsonsecurity.com), an expert in the field of computer security, was also a valuable source of information. See the list of publications used at the end of the case.

[3] Line Dubé is a full professor in HEC Montréal's Department of Information Technologies.

[4] This date varies between December 15 and 18, depending on the source. December 18 is used here because it is the date given by John Mulligan, Target's Executive Vice-President and Chief Financial Officer, in testimony before the U.S. Senate Committee on the Judiciary on February 4, 2014 (see http://www.judiciary.senate.gov/meetings/privacy-in-the-digital-age-preventing-data-breaches-and-combating-cybercrime).

The International Journal of Case Studies in Management is published on-line (http://www.hec.ca/en/case_centre/ijcsm/), ISSN 1911-2599.

This case is intended to be used as the framework for an educational discussion and does not imply any judgement on the administrative situation presented. Deposited under number 9 65 2016 001T with the HEC Montréal Case Centre, 3000, chemin de la Côte-Sainte-Catherine, Montréal (Québec) H3T 2A7 Canada.

i. Individual preparation is done as homework assignments that will prepare you to contribute in group discussion meetings. It will prepare you to learn from what others say.

To fully benefit from the interchange of ideas about a case's problem, however, you must possess a good understanding of the facts of the case and have your own ideas.

Studying the case, doing your homework and answering the questions readies you to react to what others say. *This is how we learn…*

Assignments

3. Three case studies (continued…)

Journal of Information Technology Teaching Cases (2015) 5, 102–112
© 2015 JITTC Palgrave Macmillan All rights reserved 2043-8869/15
palgrave-journals.com/jittc/

Teaching Case

Snowfall and a stolen laptop

Mark-David J McLaughlin[1,2], Sean Hansen[3], W Alec Cram[1], Janis L Gogan[1]

[1]Bentley University, Waltham, USA;
[2]Cisco Systems, San Jose, USA;
[3]Rochester Institute of Technology, Rochester, USA

Correspondence:
W A Cram, Department of Information and Process Management, Bentley University, 175 Forest Street, Waltham, MA 02452, USA.
Tel: +781 891 2811;
Fax: +781 891 2949;
E-mail: wcram@bentley.edu

Abstract
The E. Phillip Saunders College of Business (COB) Dean at Rochester Institute of Technology (RIT) discovers that his RIT-issued laptop has been stolen from his home. He notifies Dave Ballard, a member of the College of Business IT staff. Ballard, still acutely aware of two recent incidents in which laptops containing thousands of Social Security numbers were stolen from the RIT campus, hopes the Dean's laptop does not contain personally identifiable information. If so, the incident would need to be reported to the New York Attorney General's Office, and RIT would be required to pay for a credit monitoring service for individuals whose identity may have been compromised. The case provides an opportunity for students to examine processes that should be triggered when an information security incident occurs. The case describes incident response processes that were triggered at RIT and technologies that were used or could have been used by COB IT staff to track the laptop and protect its contents. In discussing the case, students can consider how the theft of a computing device exposes an organization to risks of inadvertent disclosure of information in different categories (such as private, confidential, internal, or public), and students can derive useful guidelines for effective information security incident response.

Journal of Information Technology Teaching Cases (2015) **5**, 102–112. doi:10.1057/jittc.2015.12
Keywords: information security; incident response; risk management; IT governance

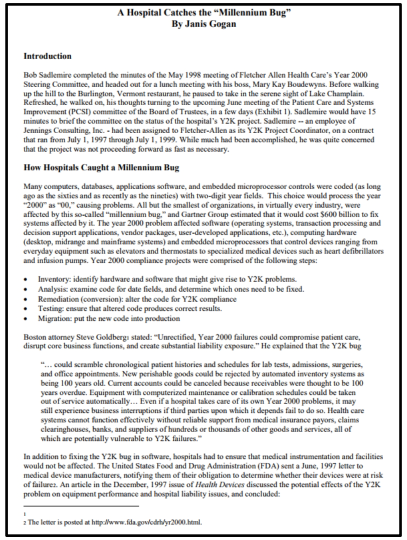
Snow falling on Rochester

The vanity plates on the Lexus pulling up to the curb at Rochester New York International Airport in February might have seemed cryptic to a casual onlooker: EPS COB. The plates' acronym stood for E. Phillip Saunders College of Business, one of eight colleges of the Rochester Institute of Technology (RIT). In the driver's seat was the EPS COB Dean. He said goodbye to his wife, who would board a US Airways flight to Boston, where she worked.

Their home sat on a corner lot in a quiet residential Rochester neighborhood. The Dean was grateful that his snow tires retained their grip; it had again been snowing all day. Driving down Villanova Street, he clicked the remote control to raise the garage door and pulled into his driveway. The snow looked to be four or five inches deep. With his jacket and gloves already on and the snow tapering off, this was as good a time as any to get a little exercise, so he grabbed a shovel from the garage wall and set to work. It was light, fluffy snow and he completed the job in 10 or 15 min. He walked around to the front of the house (facing Carleton Road) to shovel the front steps and walk. A few minutes later, after depositing the shovel in the garage, he headed into the house through the back door, wiping his snowy boots on the doormat.

And that's when he noticed a trail of wet boot prints. 'What the …?' At first he could not make sense of what he saw, but he soon realized those were not his wet boot prints; someone had been in his house! He stepped into the kitchen and through to the den, where he had planned to spend the evening answering emails and reviewing some materials in preparation for several upcoming meetings. The intruder's trail led through the den and into the front hall. He felt a cold wind blowing through the front door – why was it open? Then he felt another chill: from the sudden realization that his laptop, which he'd left on the couch in the den before taking his wife to the airport, was no longer there. After shutting and locking the front door, he raced through the house to verify that the laptop was not in another room. Nothing else seemed amiss, but the laptop was definitely gone. Its power cord dangled from the wall.

The Saunders College Dean realized he'd better call the police – and Dave Ballard.



A Hospital Catches the "Millennium Bug"
By Janis Gogan

Introduction

Bob Sadlemire completed the minutes of the May 1998 meeting of Fletcher Allen Health Care's Year 2000 Steering Committee, and headed out for a lunch meeting with his boss, Mary Kay Boudewyns. Before walking up the hill to the Burlington, Vermont restaurant, he paused to take in the serene sight of Lake Champlain. Refreshed, he walked on, his thoughts turning to the upcoming June meeting of the Patient Care and Systems Improvement (PCSI) committee of the Board of Trustees, in a few days (Exhibit 1). Sadlemire would have 15 minutes to brief the committee on the status of the hospital's Y2K project. Sadlemire -- an employee of Jennings Consulting, Inc. - had been assigned to Fletcher-Allen as its Y2K Project Coordinator, on a contract that ran from July 1, 1997 through July 1, 1999. While much had been accomplished, he was quite concerned that the project was not proceeding forward as fast as necessary.

How Hospitals Caught a Millennium Bug

Many computers, databases, applications software, and embedded microprocessor controls were coded (as long ago as the sixties and as recently as the nineties) with two-digit year fields. This choice would process the year "2000" as "00," causing problems. All but the smallest of organizations, in virtually every industry, were affected by this so-called "millennium bug," and Gartner Group estimated that it would cost $600 billion to fix systems affected by it. The year 2000 problem affected software (operating systems, transaction processing and decision support applications, vendor packages, user-developed applications, etc.), computing hardware (desktop, midrange and mainframe systems) and embedded microprocessors that control devices ranging from everyday equipment such as elevators and thermostats to specialized medical devices such as heart defibrillators and infusion pumps. Year 2000 compliance projects were comprised of the following steps:

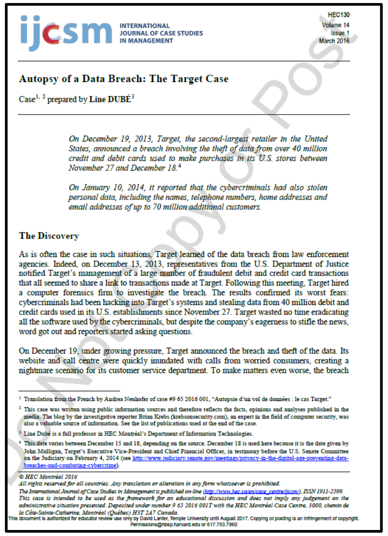
- Inventory: identify hardware and software that might give rise to Y2K problems.
- Analysis: examine code for date fields, and determine which ones need to be fixed.
- Remediation (conversion): alter the code for Y2K compliance
- Testing: ensure that altered code produces correct results.
- Migration: put the new code into production

Boston attorney Steve Goldberg[1] stated: "Unrectified, Year 2000 failures could compromise patient care, disrupt core business functions, and create substantial liability exposure." He explained that the Y2K bug

> "… could scramble chronological patient histories and schedules for lab tests, admissions, surgeries, and office appointments. New perishable goods could be rejected by automated inventory systems as being 100 years old. Current accounts could be canceled because receivables were thought to be 100 years overdue. Equipment with computerized maintenance or calibration schedules could be taken out of service automatically… Even if a hospital takes care of its own Year 2000 problems, it may still experience business interruptions if third parties upon which it depends fail to do so. Health care systems cannot function effectively without reliable support from medical insurance payors, claims clearinghouses, banks, and suppliers of hundreds or thousands of other goods and services, all of which are potentially vulnerable to Y2K failures."

In addition to fixing the Y2K bug in software, hospitals had to ensure that medical instrumentation and facilities would not be affected. The United States Food and Drug Administration (FDA) sent a June, 1997 letter to medical device manufacturers, notifying them of their obligation to determine whether their devices were at risk of failure[2]. An article in the December, 1997 issue of *Health Devices* discussed the potential effects of the Y2K problem on equipment performance and hospital liability issues, and concluded:

[1]
[2] The letter is posted at http://www.fda.gov/cdrh/yr2000.html.



ijcsm INTERNATIONAL JOURNAL OF CASE STUDIES IN MANAGEMENT

HEC130
Volume 14
Issue 1
March 2016

Autopsy of a Data Breach: The Target Case

Case[1, 2] prepared by **Line DUBÉ**[3]

On December 19, 2013, Target, the second-largest retailer in the United States, announced a breach involving the theft of data from over 40 million credit and debit cards used to make purchases in its U.S. stores between November 27 and December 18.[4]

On January 10, 2014, it reported that the cybercriminals had also stolen personal data, including the names, telephone numbers, home addresses and email addresses of up to 70 million additional customers.

The Discovery

As is often the case in such situations, Target learned of the data breach from law enforcement agencies. Indeed, on December 13, 2013, representatives from the U.S. Department of Justice notified Target's management of a large number of fraudulent debit and credit card transactions that all seemed to share a link to transactions made at Target. Following this meeting, Target hired a computer forensics firm to investigate the breach. The results confirmed its worst fears: cybercriminals had been hacking into Target's systems and stealing data from 40 million debit and credit cards used in its U.S. establishments since November 27. Target wasted no time eradicating all the software used by the cybercriminals, but despite the company's eagerness to stifle the news, word got out and reporters started asking questions.

On December 19, under growing pressure, Target announced the breach and theft of the data. Its website and call centre were quickly inundated with calls from worried consumers, creating a nightmare scenario for its customer service department. To make matters even worse, the breach

[1] Translation from the French by Andrea Neuhofer of case #9 65 2016 001, "Autopsie d'un vol de données : le cas Target."

[2] This case was written using public information sources and therefore reflects the facts, opinions and analyses published in the media. The blog by the investigative reporter Brian Krebs (krebsonsecurity.com), an expert in the field of computer security, was also a valuable source of information. See the list of publications used at the end of the case.

[3] Line Dubé is a full professor in HEC Montréal's Department of Information Technologies.

[4] This date varies between December 15 and 18, depending on the source. December 18 is used here because it is the date given by John Mulligan, Target's Executive Vice-President and Chief Financial Officer, in testimony before the U.S. Senate Committee on the Judiciary on February 4, 2014 (see http://www.judiciary.senate.gov/meetings/privacy-in-the-digital-age-preventing-data-breaches-and-combating-cybercrime).

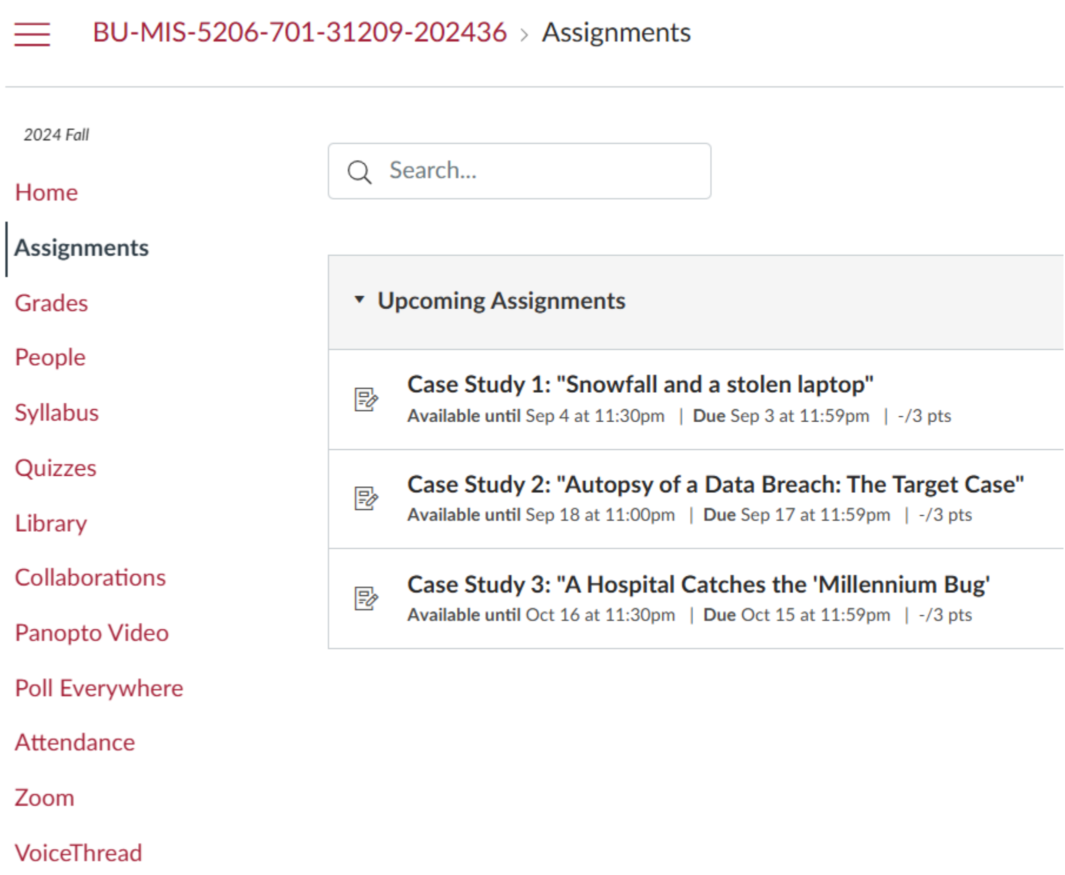
The International Journal of Case Studies in Management is published on-line (http://www.hec.ca/en/case_centre/ijcsm/), ISSN 1911-2599.
This case is intended to be used as the framework for an educational discussion and does not imply any judgement on the administrative situation presented. Deposited under number 9 65 2016 001T with the HEC Montréal Case Centre, 3000, chemin de la Côte-Sainte-Catherine, Montréal (Québec) H3T 2A7 Canada.

ii. Group discussions are informal sessions of give and take. Come with your own ideas and leave with better understanding. By combining your insights with those of the group you advance your own analysis. Discussions within small groups is also helpful for those uncomfortable talking in large classes to express their views and gain feedback.

iii. Class discussion advances learning from the case, but does not necessarily solve the case. Rather it helps develop your understanding of why you need to gain more knowledge and learn concepts that provide the basis of your intellectual toolkit you develop in class and apply in practice.

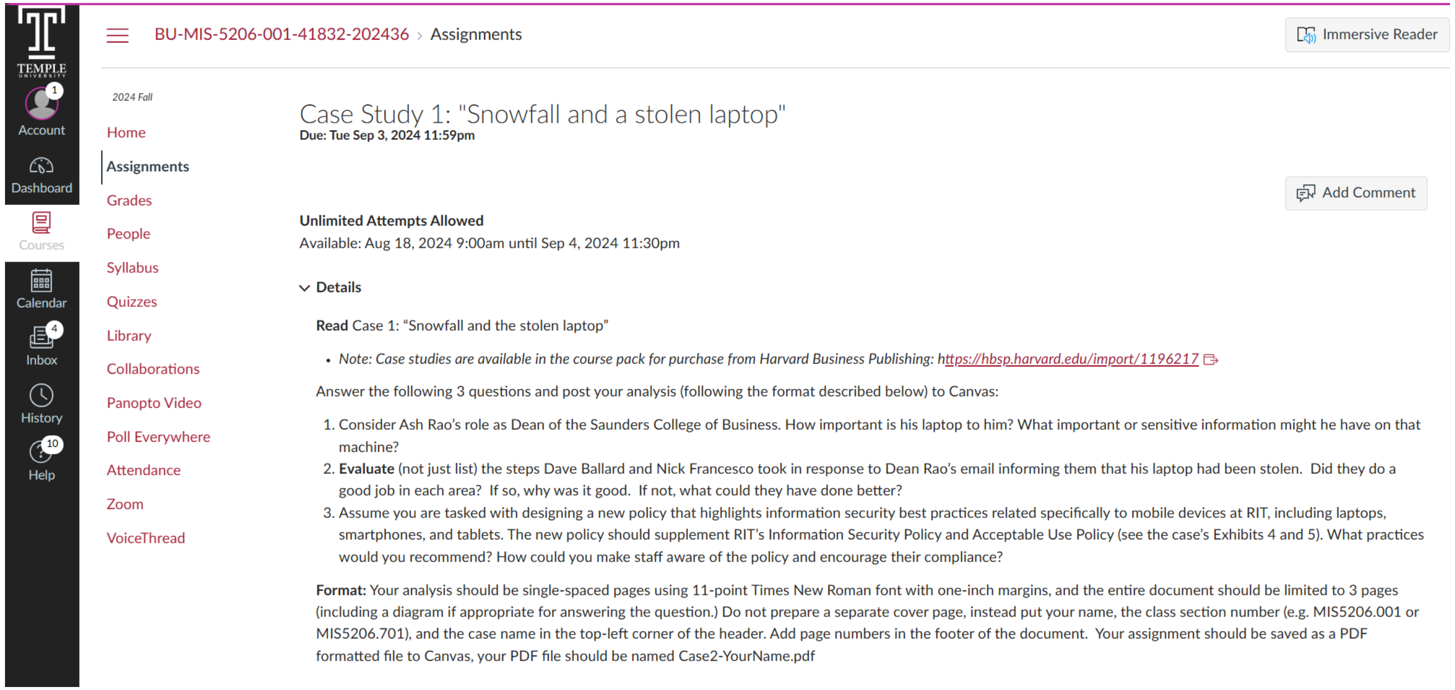
Assignments

3. Three case studies (continued…)



▾ Upcoming Assignments

- Case Study 1: "Snowfall and a stolen laptop"
  Available until Sep 4 at 11:30pm | **Due** Sep 3 at 11:59pm | -/3 pts
- Case Study 2: "Autopsy of a Data Breach: The Target Case"
  Available until Sep 18 at 11:00pm | **Due** Sep 17 at 11:59pm | -/3 pts
- Case Study 3: "A Hospital Catches the 'Millennium Bug'
  Available until Oct 16 at 11:30pm | **Due** Oct 15 at 11:59pm | -/3 pts



Case Study 1: "Snowfall and a stolen laptop"
Due: Tue Sep 3, 2024 11:59pm

Unlimited Attempts Allowed
Available: Aug 18, 2024 9:00am until Sep 4, 2024 11:30pm

Details

Read Case 1: “Snowfall and the stolen laptop”

- *Note: Case studies are available in the course pack for purchase from Harvard Business Publishing: https://hbsp.harvard.edu/import/1196217*

Answer the following 3 questions and post your analysis (following the format described below) to Canvas:

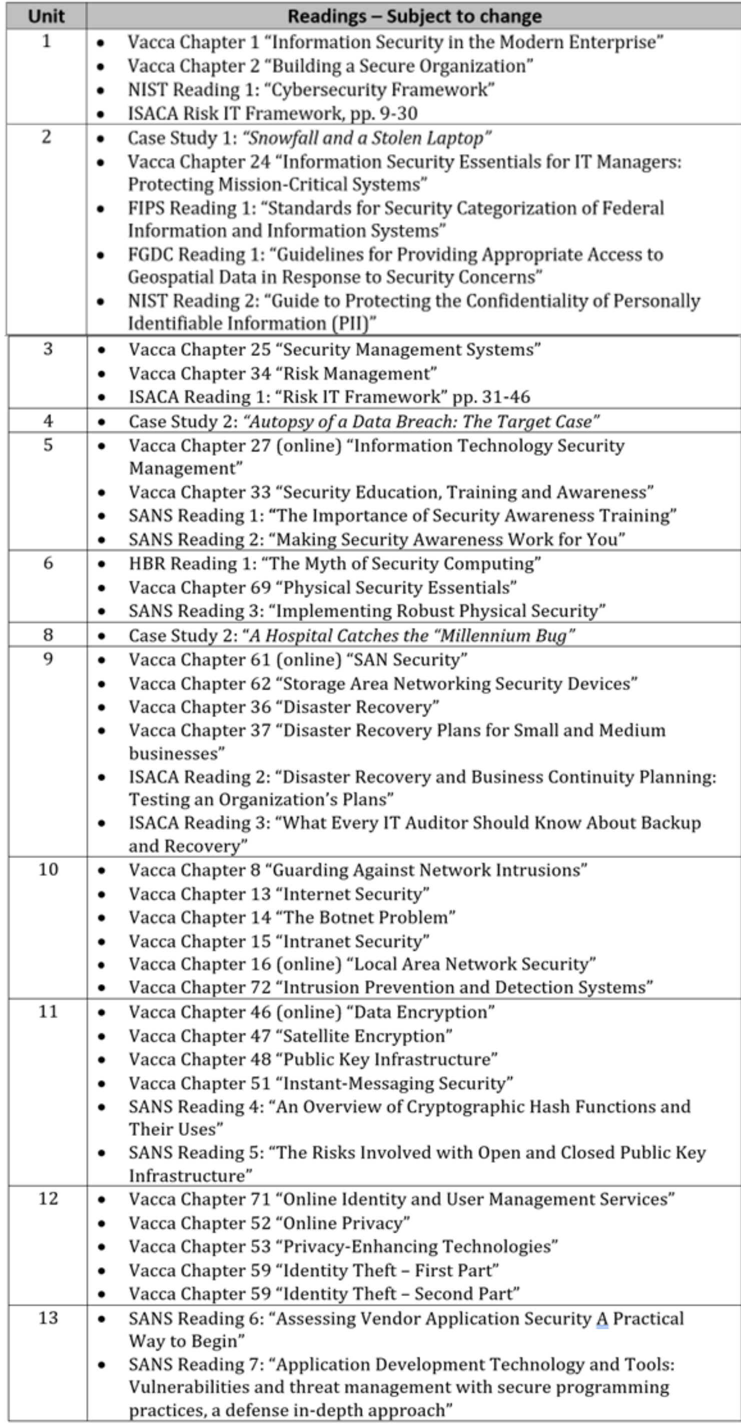
1. Consider Ash Rao’s role as Dean of the Saunders College of Business. How important is his laptop to him? What important or sensitive information might he have on that machine?
2. **Evaluate** (not just list) the steps Dave Ballard and Nick Francesco took in response to Dean Rao’s email informing them that his laptop had been stolen. Did they do a good job in each area? If so, why was it good. If not, what could they have done better?
3. Assume you are tasked with designing a new policy that highlights information security best practices related specifically to mobile devices at RIT, including laptops, smartphones, and tablets. The new policy should supplement RIT’s Information Security Policy and Acceptable Use Policy (see the case’s Exhibits 4 and 5). What practices would you recommend? How could you make staff aware of the policy and encourage their compliance?

Format: Your analysis should be single-spaced pages using 11-point Times New Roman font with one-inch margins, and the entire document should be limited to 3 pages (including a diagram if appropriate for answering the question.) Do not prepare a separate cover page, instead put your name, the class section number (e.g. MIS5206.001 or MIS5206.701), and the case name in the top-left corner of the header. Add page numbers in the footer of the document. Your assignment should be saved as a PDF formatted file to Canvas, your PDF file should be named Case2-YourName.pdf

Assignments

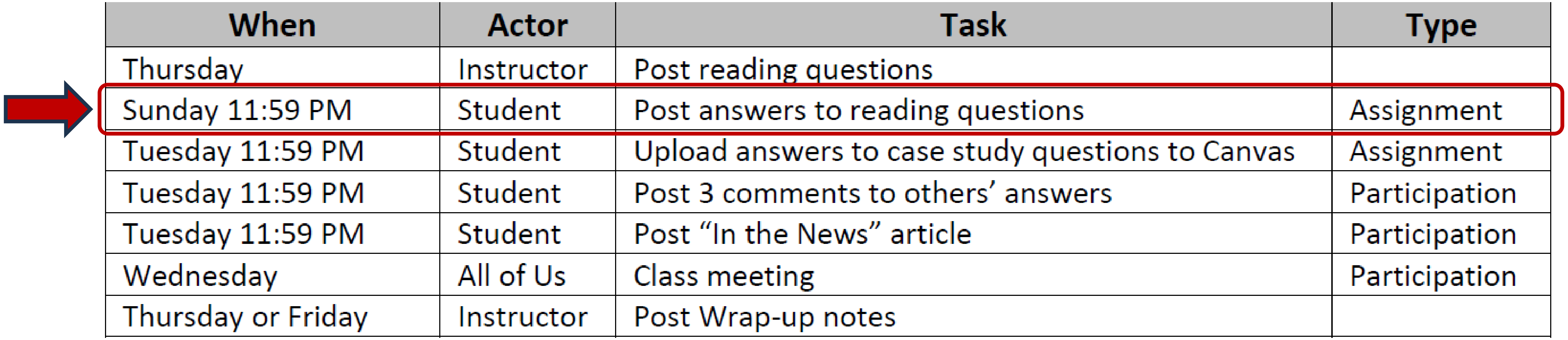
1. **Readings**
2. **Answers to questions**
3. **Case study analyses**

Computer and Information Security Handbook
Third Edition
John R. Vacca
Risk IT Framework
2nd Edition
ISACA
Disaster Recovery and Business Continuity Planning: Testing an Organization's Plans
IT Audit Basics
What Every IT Auditor Should Know About Backup and Recovery
SANS Institute InfoSec Reading Room
Implementing Robust Physical Security
Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns
FIPS PUB 199
Standards for Security Categorization of Federal Information and Information Systems
NIST
Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
The NIST Cybersecurity Framework (CSF) 2.0
Snowfall and a stolen laptop
ijcsm
Autopsy of a Data Breach: The Target Case
The Myth of Secure Computing
A Hospital Catches the "Millennium Bug"



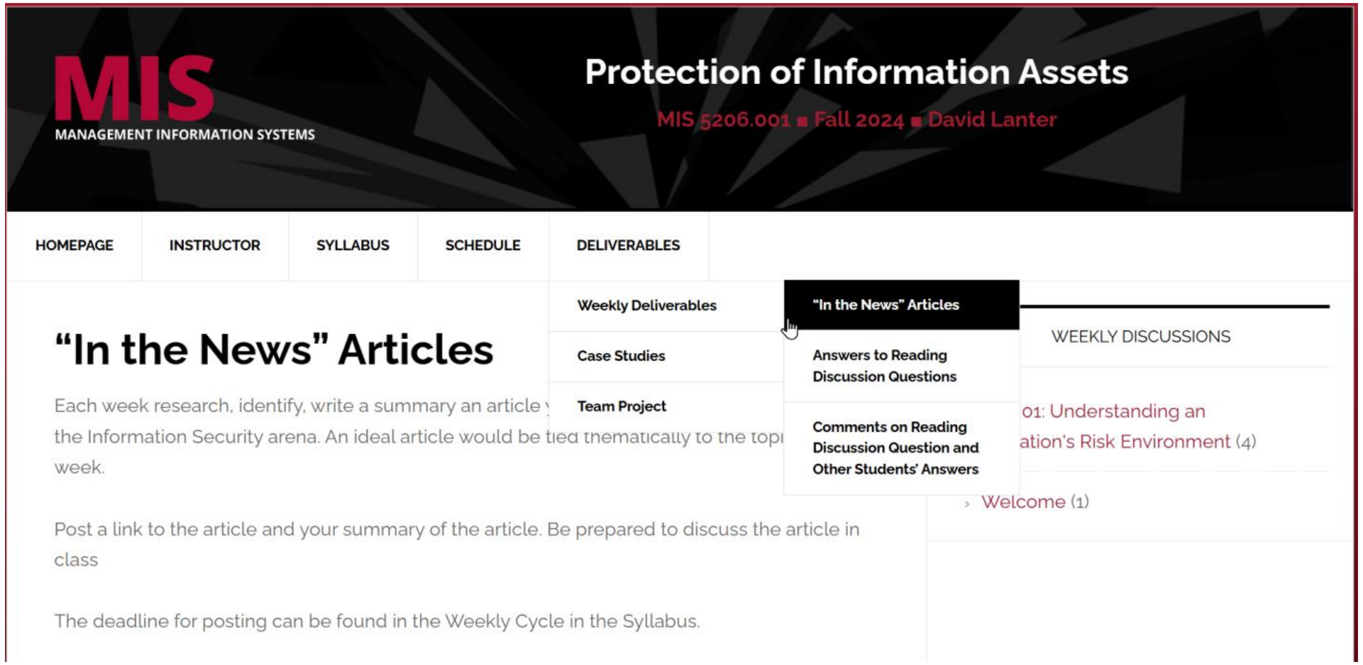
Unit	Readings – Subject to change
1	• Vacca Chapter 1 "Information Security in the Modern Enterprise" • Vacca Chapter 2 "Building a Secure Organization" • NIST Reading 1: "Cybersecurity Framework" • ISACA Risk IT Framework, pp. 9-30
2	• Case Study 1: *"Snowfall and a Stolen Laptop"* • Vacca Chapter 24 "Information Security Essentials for IT Managers: Protecting Mission-Critical Systems" • FIPS Reading 1: "Standards for Security Categorization of Federal Information and Information Systems" • FGDC Reading 1: "Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns" • NIST Reading 2: "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)"
3	• Vacca Chapter 25 "Security Management Systems" • Vacca Chapter 34 "Risk Management" • ISACA Reading 1: "Risk IT Framework" pp. 31-46
4	• Case Study 2: *"Autopsy of a Data Breach: The Target Case"*
5	• Vacca Chapter 27 (online) "Information Technology Security Management" • Vacca Chapter 33 "Security Education, Training and Awareness" • SANS Reading 1: "The Importance of Security Awareness Training" • SANS Reading 2: "Making Security Awareness Work for You"
6	• HBR Reading 1: "The Myth of Security Computing" • Vacca Chapter 69 "Physical Security Essentials" • SANS Reading 3: "Implementing Robust Physical Security"
8	• Case Study 2: *"A Hospital Catches the "Millennium Bug"*
9	• Vacca Chapter 61 (online) "SAN Security" • Vacca Chapter 62 "Storage Area Networking Security Devices" • Vacca Chapter 36 "Disaster Recovery" • Vacca Chapter 37 "Disaster Recovery Plans for Small and Medium businesses" • ISACA Reading 2: "Disaster Recovery and Business Continuity Planning: Testing an Organization's Plans" • ISACA Reading 3: "What Every IT Auditor Should Know About Backup and Recovery"
10	• Vacca Chapter 8 "Guarding Against Network Intrusions" • Vacca Chapter 13 "Internet Security" • Vacca Chapter 14 "The Botnet Problem" • Vacca Chapter 15 "Intranet Security" • Vacca Chapter 16 (online) "Local Area Network Security" • Vacca Chapter 72 "Intrusion Prevention and Detection Systems"
11	• Vacca Chapter 46 (online) "Data Encryption" • Vacca Chapter 47 "Satellite Encryption" • Vacca Chapter 48 "Public Key Infrastructure" • Vacca Chapter 51 "Instant-Messaging Security" • SANS Reading 4: "An Overview of Cryptographic Hash Functions and Their Uses" • SANS Reading 5: "The Risks Involved with Open and Closed Public Key Infrastructure"
12	• Vacca Chapter 71 "Online Identity and User Management Services" • Vacca Chapter 52 "Online Privacy" • Vacca Chapter 53 "Privacy-Enhancing Technologies" • Vacca Chapter 59 "Identity Theft – First Part" • Vacca Chapter 59 "Identity Theft – Second Part"
13	• SANS Reading 6: "Assessing Vendor Application Security A Practical Way to Begin" • SANS Reading 7: "Application Development Technology and Tools: Vulnerabilities and threat management with secure programming practices, a defense in-depth approach"

Weekly Cycle



When	Actor	Task	Type
Thursday	Instructor	Post reading questions	
Sunday 11:59 PM	Student	Post answers to reading questions	Assignment
Tuesday 11:59 PM	Student	Upload answers to case study questions to Canvas	Assignment
Tuesday 11:59 PM	Student	Post 3 comments to others’ answers	Participation
Tuesday 11:59 PM	Student	Post “In the News” article	Participation
Wednesday	All of Us	Class meeting	Participation
Thursday or Friday	Instructor	Post Wrap-up notes	

Deliverables

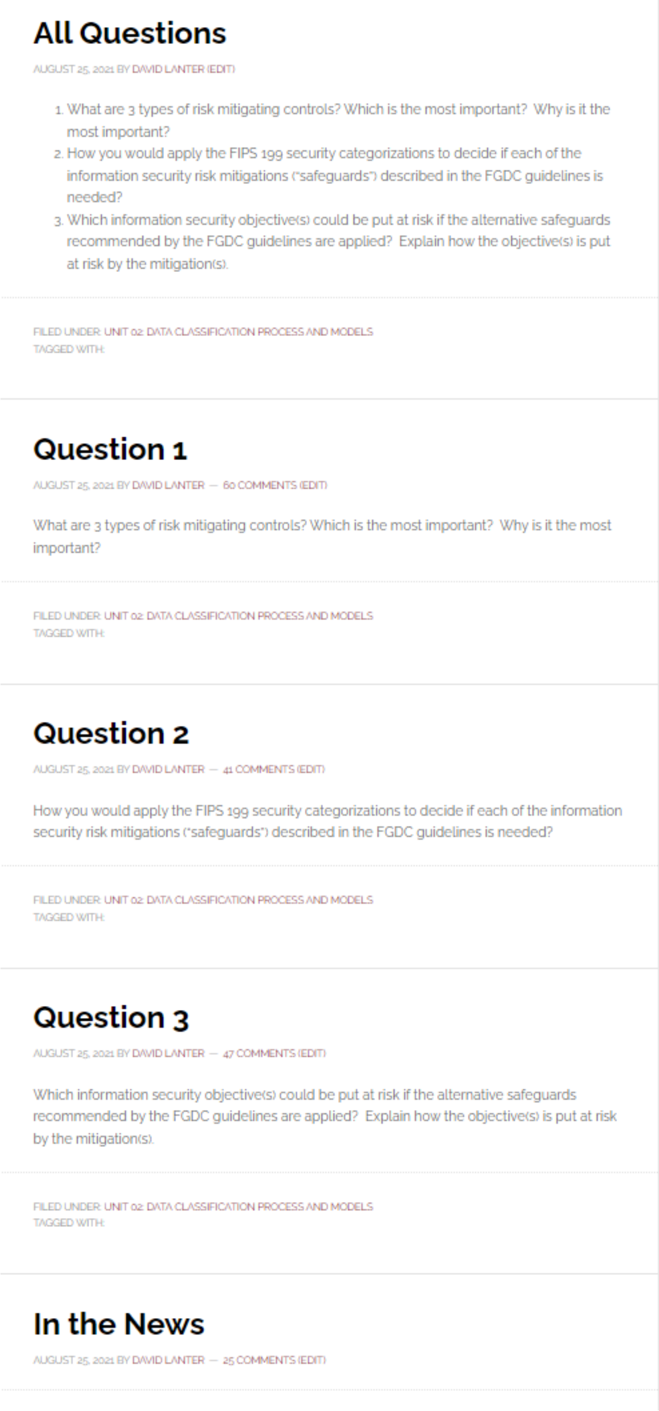

MIS
MANAGEMENT INFORMATION SYSTEMS
Protection of Information Assets
MIS 5206.001 ■ Fall 2024 ■ David Lanter
HOMEPAGE
INSTRUCTOR
SYLLABUS
SCHEDULE
DELIVERABLES
Weekly Deliverables
Case Studies
Team Project
"In the News" Articles
Answers to Reading Discussion Questions
Comments on Reading Discussion Question and Other Students' Answers
WEEKLY DISCUSSIONS
01: Understanding an
ation's Risk Environment (4)
Welcome (1)

"In the News" Articles

Each week research, identify, write a summary an article
the Information Security arena. An ideal article would be tied thematically to the topi
week.

Post a link to the article and your summary of the article. Be prepared to discuss the article in class

The deadline for posting can be found in the Weekly Cycle in the Syllabus.



All Questions

AUGUST 25, 2021 BY DAVID LANTER (EDIT)

1. What are 3 types of risk mitigating controls? Which is the most important? Why is it the most important?
2. How you would apply the FIPS 199 security categorizations to decide if each of the information security risk mitigations ("safeguards") described in the FGDC guidelines is needed?
3. Which information security objective(s) could be put at risk if the alternative safeguards recommended by the FGDC guidelines are applied? Explain how the objective(s) is put at risk by the mitigation(s).

FILED UNDER: UNIT 02: DATA CLASSIFICATION PROCESS AND MODELS
TAGGED WITH:

Question 1

AUGUST 25, 2021 BY DAVID LANTER — 60 COMMENTS (EDIT)

What are 3 types of risk mitigating controls? Which is the most important? Why is it the most important?

FILED UNDER: UNIT 02: DATA CLASSIFICATION PROCESS AND MODELS
TAGGED WITH:

Question 2

AUGUST 25, 2021 BY DAVID LANTER — 41 COMMENTS (EDIT)

How you would apply the FIPS 199 security categorizations to decide if each of the information security risk mitigations ("safeguards") described in the FGDC guidelines is needed?

FILED UNDER: UNIT 02: DATA CLASSIFICATION PROCESS AND MODELS
TAGGED WITH:

Question 3

AUGUST 25, 2021 BY DAVID LANTER — 47 COMMENTS (EDIT)

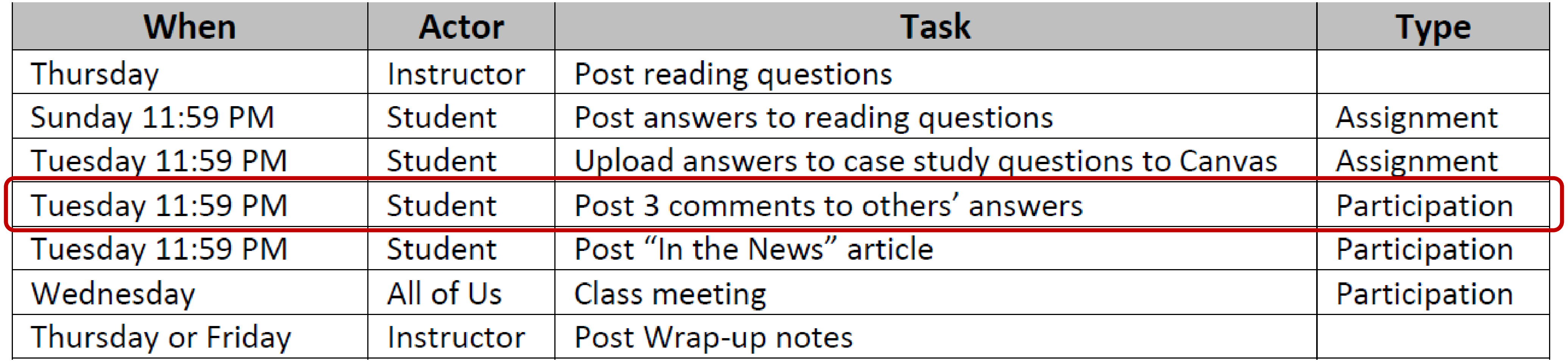
Which information security objective(s) could be put at risk if the alternative safeguards recommended by the FGDC guidelines are applied? Explain how the objective(s) is put at risk by the mitigation(s).

FILED UNDER: UNIT 02: DATA CLASSIFICATION PROCESS AND MODELS
TAGGED WITH:

In the News

AUGUST 25, 2021 BY DAVID LANTER — 25 COMMENTS (EDIT)

Weekly Cycle

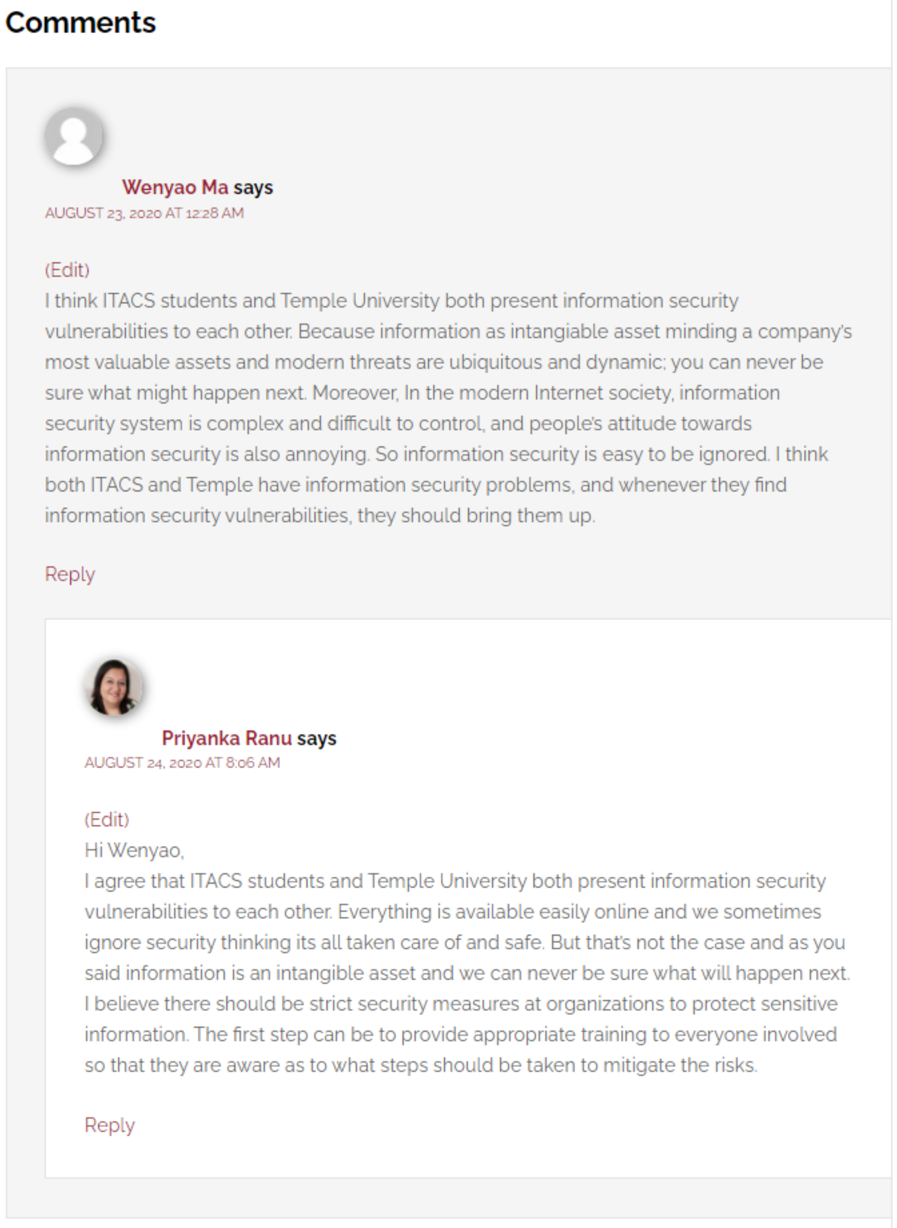


When	Actor	Task	Type
Thursday	Instructor	Post reading questions	
Sunday 11:59 PM	Student	Post answers to reading questions	Assignment
Tuesday 11:59 PM	Student	Upload answers to case study questions to Canvas	Assignment
Tuesday 11:59 PM	Student	Post 3 comments to others’ answers	Participation
Tuesday 11:59 PM	Student	Post “In the News” article	Participation
Wednesday	All of Us	Class meeting	Participation
Thursday or Friday	Instructor	Post Wrap-up notes	

Participation

1. **Comment on weekly discussion question answers and comments posted by other students**

Read the responses of others to the discussion questions and contribute at least three (3) substantive posts that include your thoughtful comments as you participate in the discussion of the questions with your classmates



Comments

Wenyao Ma says
AUGUST 23, 2020 AT 12:28 AM

(Edit)
I think ITACS students and Temple University both present information security vulnerabilities to each other. Because information as intangible asset minding a company's most valuable assets and modern threats are ubiquitous and dynamic; you can never be sure what might happen next. Moreover, In the modern Internet society, information security system is complex and difficult to control, and people's attitude towards information security is also annoying. So information security is easy to be ignored. I think both ITACS and Temple have information security problems, and whenever they find information security vulnerabilities, they should bring them up.

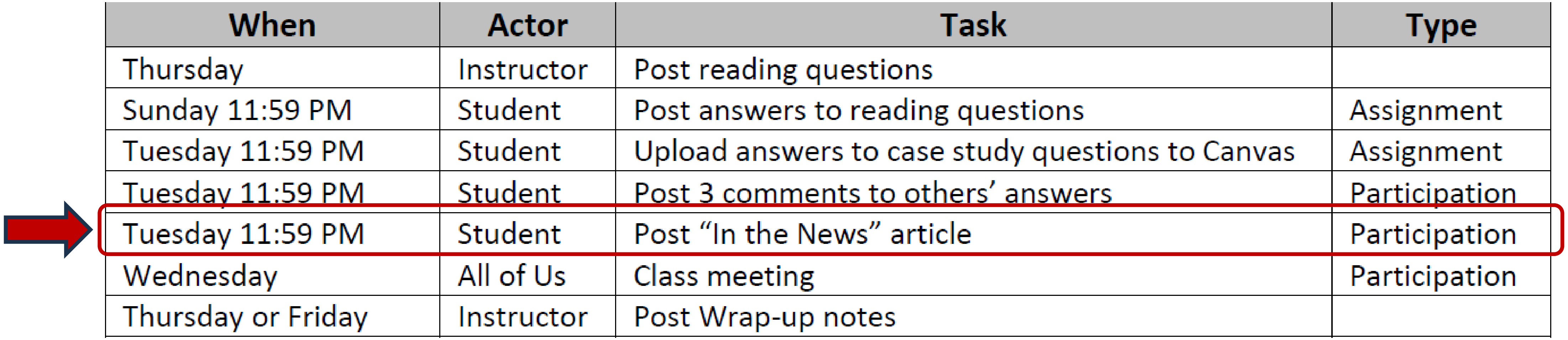
Reply

Priyanka Ranu says
AUGUST 24, 2020 AT 8:06 AM

(Edit)
Hi Wenyao,
I agree that ITACS students and Temple University both present information security vulnerabilities to each other. Everything is available easily online and we sometimes ignore security thinking its all taken care of and safe. But that's not the case and as you said information is an intangible asset and we can never be sure what will happen next. I believe there should be strict security measures at organizations to protect sensitive information. The first step can be to provide appropriate training to everyone involved so that they are aware as to what steps should be taken to mitigate the risks.

Reply

Weekly Cycle



When	Actor	Task	Type
Thursday	Instructor	Post reading questions	
Sunday 11:59 PM	Student	Post answers to reading questions	Assignment
Tuesday 11:59 PM	Student	Upload answers to case study questions to Canvas	Assignment
Tuesday 11:59 PM	Student	Post 3 comments to others’ answers	Participation
Tuesday 11:59 PM	Student	Post “In the News” article	Participation
Wednesday	All of Us	Class meeting	Participation
Thursday or Friday	Instructor	Post Wrap-up notes	

Participation

2. “In the News” articles

https://www.theregister.co.uk/security/

https://thehackernews.com/

https://cybernews.com/

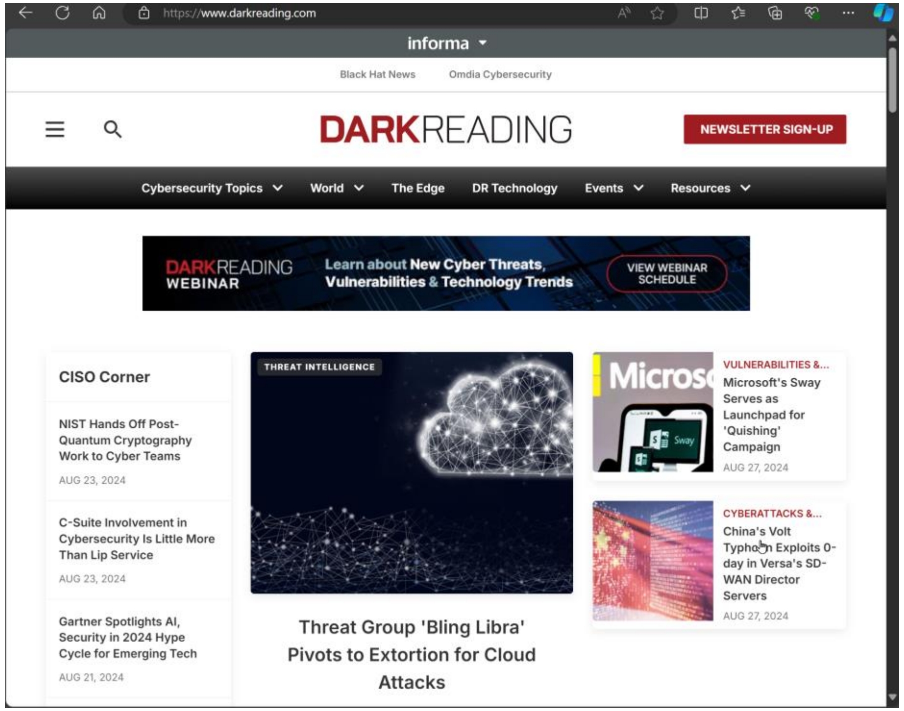
https://krebsonsecurity.com/

⋮

Research article you found about a current event in the Information Security arena

Identify, write a summary, post a link to your summary, and be prepared to discuss in class

An ideal article would be tied thematically to the topic of the week. However, any article you find interesting and would like to share is welcome



CISO Corner

NIST Hands Off Post-Quantum Cryptography Work to Cyber Teams

AUG 23, 2024

C-Suite Involvement in Cybersecurity Is Little More Than Lip Service

AUG 23, 2024

Gartner Spotlights AI, Security in 2024 Hype Cycle for Emerging Tech

AUG 21, 2024

Threat Group 'Bling Libra' Pivots to Extortion for Cloud Attacks

Microsoft's Sway Serves as Launchpad for 'Quishing' Campaign

AUG 27, 2024

China's Volt Typhoon Exploits 0-day in Versa's SD-WAN Director Servers

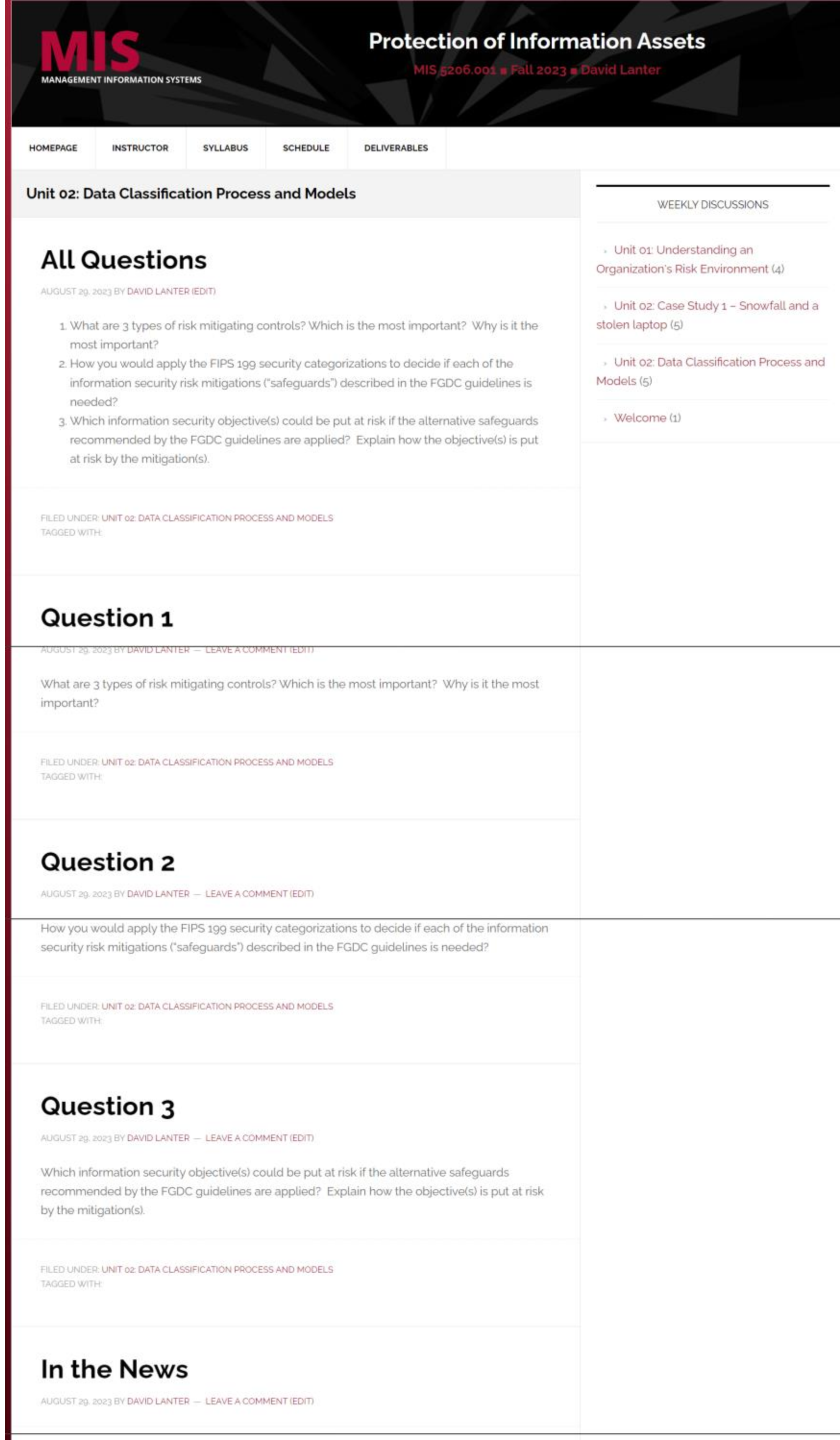
AUG 27, 2024

Participation

2. “In the News” articles

In the News

AUGUST 29, 2023 BY DAVID LANTER — LEAVE A COMMENT (EDIT)



Protection of Information Assets

MIS 5206.001 ■ Fall 2023 ■ David Lanter

Unit 02: Data Classification Process and Models

All Questions

AUGUST 29, 2023 BY DAVID LANTER (EDIT)

1. What are 3 types of risk mitigating controls? Which is the most important? Why is it the most important?
2. How you would apply the FIPS 199 security categorizations to decide if each of the information security risk mitigations (“safeguards”) described in the FGDC guidelines is needed?
3. Which information security objective(s) could be put at risk if the alternative safeguards recommended by the FGDC guidelines are applied? Explain how the objective(s) is put at risk by the mitigation(s).

FILED UNDER: UNIT 02: DATA CLASSIFICATION PROCESS AND MODELS
TAGGED WITH:

Question 1

AUGUST 29, 2023 BY DAVID LANTER — LEAVE A COMMENT (EDIT)

What are 3 types of risk mitigating controls? Which is the most important? Why is it the most important?

FILED UNDER: UNIT 02: DATA CLASSIFICATION PROCESS AND MODELS
TAGGED WITH:

Question 2

AUGUST 29, 2023 BY DAVID LANTER — LEAVE A COMMENT (EDIT)

How you would apply the FIPS 199 security categorizations to decide if each of the information security risk mitigations (“safeguards”) described in the FGDC guidelines is needed?

FILED UNDER: UNIT 02: DATA CLASSIFICATION PROCESS AND MODELS
TAGGED WITH:

Question 3

AUGUST 29, 2023 BY DAVID LANTER — LEAVE A COMMENT (EDIT)

Which information security objective(s) could be put at risk if the alternative safeguards recommended by the FGDC guidelines are applied? Explain how the objective(s) is put at risk by the mitigation(s).

FILED UNDER: UNIT 02: DATA CLASSIFICATION PROCESS AND MODELS
TAGGED WITH:

In the News

AUGUST 29, 2023 BY DAVID LANTER — LEAVE A COMMENT (EDIT)

WEEKLY DISCUSSIONS

- Unit 01: Understanding an Organization’s Risk Environment (4)
- Unit 02: Case Study 1 – Snowfall and a stolen laptop (5)
- Unit 02: Data Classification Process and Models (5)
- Welcome (1)

Participation

3. During class

We will often begin a class with a discussion of your In The News article or answers to questions about assigned readings or the case study

When you are called on, you should summarize the key issues, opportunities, and challenges in the reading or question

Be prepared to answer all the assigned questions

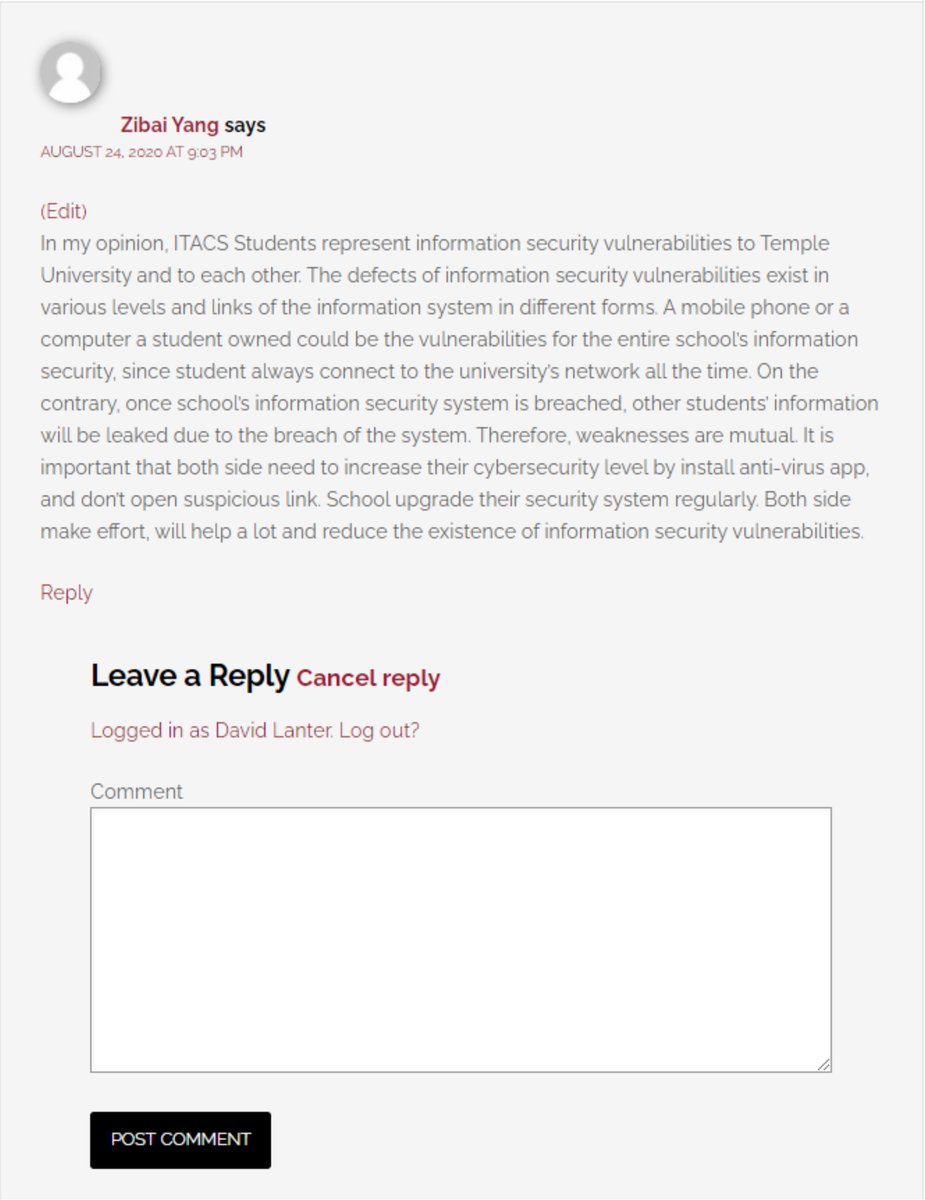
Another important aspect of in-class participation is completion of in-class assignments and contribution to group and team activities

Participation

1. **Comment & participate in discussions of questions on blog site**

2. **Research, summarize and discuss "In the News" article in class**

3. **Participate in discussions during class**



Zibai Yang says
AUGUST 24, 2020 AT 9:03 PM

(Edit)
In my opinion, ITACS Students represent information security vulnerabilities to Temple University and to each other. The defects of information security vulnerabilities exist in various levels and links of the information system in different forms. A mobile phone or a computer a student owned could be the vulnerabilities for the entire school's information security, since student always connect to the university's network all the time. On the contrary, once school's information security system is breached, other students' information will be leaked due to the breach of the system. Therefore, weaknesses are mutual. It is important that both side need to increase their cybersecurity level by install anti-virus app, and don't open suspicious link. School upgrade their security system regularly. Both side make effort, will help a lot and reduce the existence of information security vulnerabilities.

Reply

Leave a Reply Cancel reply

Logged in as David Lanter. Log out?

Comment

POST COMMENT

Team project

Students will be organized into presentation development and delivery teams

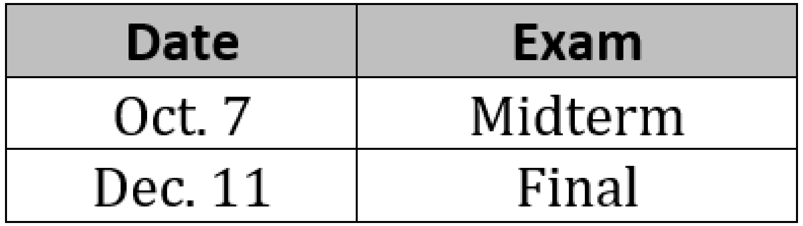
Each team will be assigned a topic and will work together to develop a presentation covering the assigned topic

During Units #13 and #14 each team will have 15 minutes to present their results of working on the topic, following by a brief session of questions and answers (Q&A) from the other teams

Teams not presenting are responsible for asking thoughtful and insightful questions at the end of each presentation

Exams

There will be two exams, together these exams are weighted 25% of each student’s final grade



Date	Exam
Oct. 7	Midterm
Dec. 11	Final

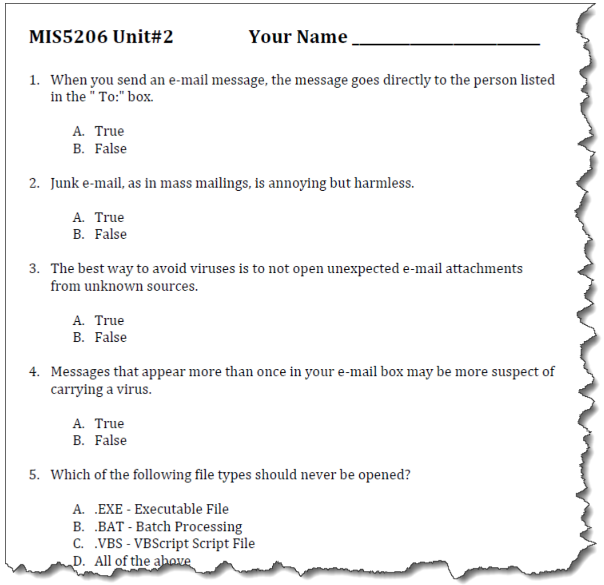
The exams will consist of multiple-choice, and possibly fill in the blank or short answer questions

The Midterm Exam will occur during Week #7 and the Final Exam will occur during finals week

The final exam will be cumulative, but more focused on the course materials since the beginning of the midterm exam

Expect important concepts highlighted in class to appear on both exams

Quizzes



MIS5206 Unit#2 **Your Name ______________________**

1. When you send an e-mail message, the message goes directly to the person listed in the " To:" box.

   A. True
   B. False

2. Junk e-mail, as in mass mailings, is annoying but harmless.

   A. True
   B. False

3. The best way to avoid viruses is to not open unexpected e-mail attachments from unknown sources.

   A. True
   B. False

4. Messages that appear more than once in your e-mail box may be more suspect of carrying a virus.

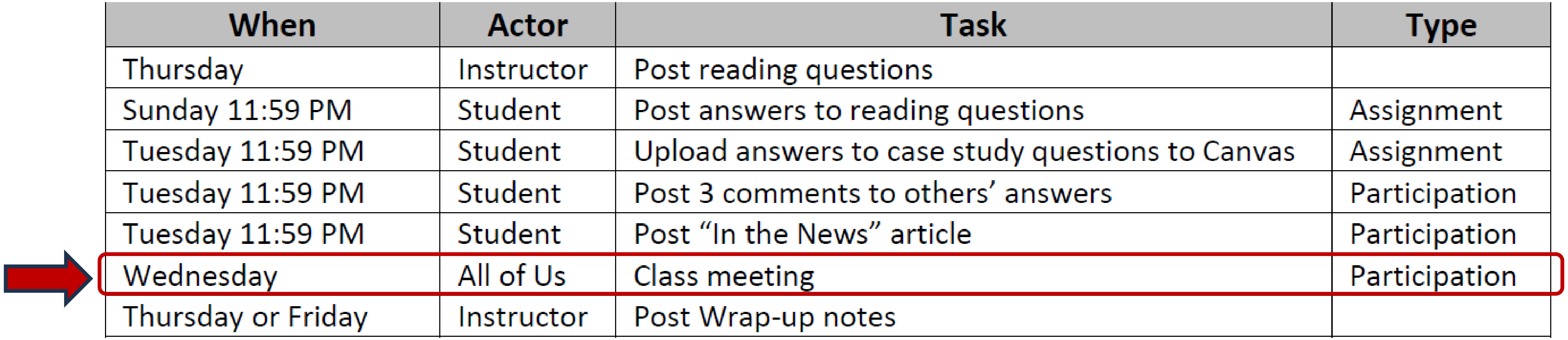
   A. True
   B. False

5. Which of the following file types should never be opened?

   A. .EXE - Executable File
   B. .BAT - Batch Processing
   C. .VBS - VBScript Script File
   D. All of the above

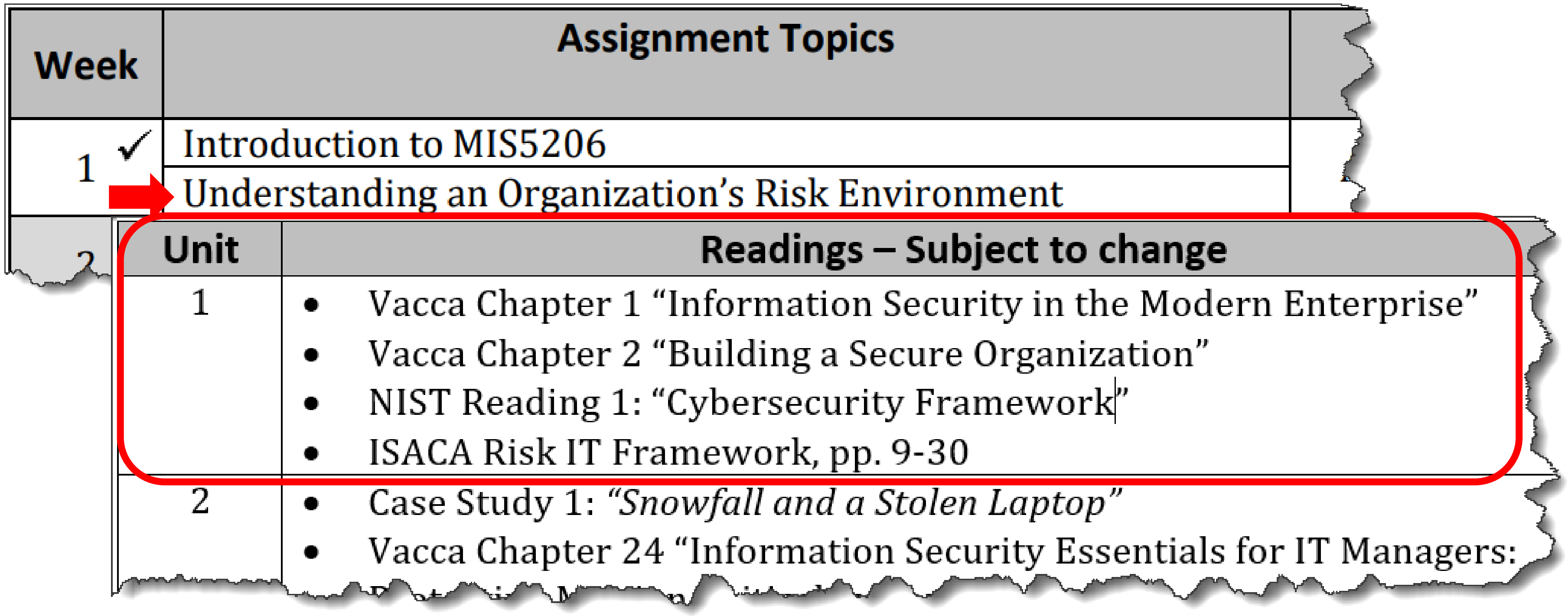
- Quizzes typically conducted in-class interactively
- Quiz consists of practice exam questions
- Test taking tip provided before each quiz
- Grades for quizzes do not count towards your final grade
- Taking quizzes counts toward participation score
- *Each quiz includes <u>additional</u> terminology, acronyms and material for you to research and study on your own*

Weekly Cycle



When	Actor	Task	Type
Thursday	Instructor	Post reading questions	
Sunday 11:59 PM	Student	Post answers to reading questions	Assignment
Tuesday 11:59 PM	Student	Upload answers to case study questions to Canvas	Assignment
Tuesday 11:59 PM	Student	Post 3 comments to others' answers	Participation
Tuesday 11:59 PM	Student	Post "In the News" article	Participation
Wednesday	All of Us	Class meeting	Participation
Thursday or Friday	Instructor	Post Wrap-up notes	

Next…



Week	Assignment Topics
1 ✓	Introduction to MIS5206
	Understanding an Organization's Risk Environment
2	

Unit	Readings – Subject to change
1	• Vacca Chapter 1 "Information Security in the Modern Enterprise" • Vacca Chapter 2 "Building a Secure Organization" • NIST Reading 1: "Cybersecurity Framework" • ISACA Risk IT Framework, pp. 9-30
2	• Case Study 1: *"Snowfall and a Stolen Laptop"* • Vacca Chapter 24 "Information Security Essentials for IT Managers:

1. Do ITACS students represent information security vulnerabilities to the University, each other, or both? Explain the nature of the vulnerabilities
2. Is information security a technical problem, a business problem that the entire organization must frame and solve, or both? Explain your answer
3. What challenges are involved in performing a quantitative information security risk analysis?

Agenda

- ✓ Course objectives
- ✓ Instructor
- ✓ Class topics and schedule
- ✓ Textbook and readings
- ✓ Grading
- ✓ Assignments
  - ✓ Readings
  - ✓ Answering questions
  - ✓ Case studies
- ✓ Participation
- ✓ Team project
- ✓ Exams
- ✓ *quizzes*
- ✓ Next

Protecting Information Assets
Week #1a