

MIS5206

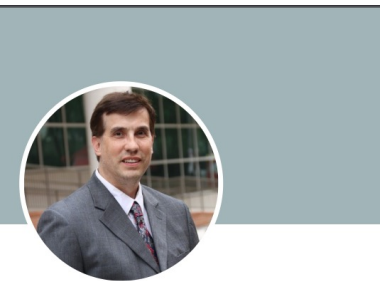
Protection of Information Assets

Unit #1

Agenda

- Instructor
- Course objectives, Class topics and Schedule
- Textbook and Readings
- Grading
- Assignments
 - Readings
 - Answering questions
 - Case studies
- Participation
 - Comments
 - In the News
- Team Project
- Exams
- *Quizzes*
- Next

Instructor



Experience



Cyber Security Consultant

Freelance

Jun 2020 - Present · 2 yrs 3 mos

Manage Information Assurance efforts for selected systems supporting national infrastructure. Serve as Information Security DSME to system managers and mentor second level engineers.



Adjunct Faculty

Management Information Systems at the Fox School of Business, Temple University

May 2017 - Present · 5 yrs 4 mos

Greater Philadelphia Area

Revamped graduate-level Cybersecurity Capstone course, adding a risk assessment capstone project, and update the course annually to reflect current cybersecurity topics, threat models, as well ...see more



Senior Cybersecurity Instructor

Simplilearn · Freelance

Aug 2012 - Present · 10 yrs 1 mo

Teach cybersecurity (CEH, CISA, CISM, CRISC, CISSP, Security+,), ITIL, and project management courses, in-person and on-line. ...see more



Simplilearn Certified Faculty

Deliver In-Person and On-Line Information Technology & Security Classes.

Topics included CISA, CISSP, ITIL, PMP



VP Information Security

Police and Fire Federal Credit Union · Full-time

Jul 2016 - Jun 2020 · 4 yrs

Greater Philadelphia Area

Developed Information Security Program for \$7.2b credit union, to address FFIEC requirements and NCUA examinations, collaborating with system owners to align business processes to regulat ...see more



Manager, Information Security & Privacy

Protiviti · Full-time

Feb 2015 - Jun 2016 · 1 yr 5 mos

Performed gap analysis, privacy, risk, and third-party service provider assessments utilizing varied frameworks. ...see more



Certified Information Privacy Manager

IAPP - International Association of Privacy Professionals

Issued Jun 2015 · No Expiration Date



PCIQSA Payment Card Industry Qualified Security Assessor

PCI Security Standards Council

Issued May 2015 · No Expiration Date

Credential ID 203-827

Show credential [↗](#)



Certified Information Privacy Professional - CIPP/IT, CIPP/US, CIPP/G

IAPP - International Association of Privacy Professionals

Issued Jun 2012 · No Expiration Date



A+ / Net+ / Project+ / Security+ / Server+ / Storage+

CompTIA



CAP® - Certified Authorization Professional

(ISC)2



CISA / CISM / CGEIT / CRISC

ISACA



CISSP - Certified Information System Security Professional

(ISC)2



CPHIMS - Certified Professional in Healthcare Information and Management Systems

HIMSS



PMP - Project Management Professional

Project Management Institute



SSCP® - Systems Security Certified Practitioner

(ISC)2

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 manage risk

Course website and syllabus

Instructor

William Bailey
online via Zoom
Office Hours: by appointment
Email: william.bailey@temple.edu

Course Format: Online, via Zoom.

Class Meetings: Wednesdays 5:30 PM – 8:00 PM

Where: Online, via Zoom. Access Zoom via Canvas

Website: <https://community.mis.temple.edu/mis5206sec701fall2022/category/welcome/>

Canvas: <https://temple.instructure.com/courses/116863>

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

temple.edu/mis5206sec701fall2022/

Assets Log Out Customize 1 New Edit Page Test Schema

MIS

MANAGEMENT INFORMATION SYSTEMS

Protection of Information Assets

MIS 5206.701 • Fall 2022 • William Bailey

- HOME PAGE
- INSTRUCTOR
- SYLLABUS
- SCHEDULE
- DELIVERABLES
- CLASS CAPTURE VIDEOS

Welcome!

AUGUST 1, 2022 BY WILLIAM BAILEY

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

- > Gain an overview of the nature of information security vulnerabilities and threats
- > Learn how information security risks are identified, classified and prioritized
- > Develop an understanding of how information security risks are managed, mitigated and controlled
- > Gain experience working as part of team, developing and delivering a professional presentation

WEEKLY DISCUSSIONS

- > Unit 01: Understanding an Organization's Risk Environment (4)
- > Unit 02: Data Classification Process and Models (5)
- > Welcome (1)

Class topics and schedule

Unit	Assignment Topics	Date
1	Introduction to MIS5206	Aug. 24
	Understanding an Organization's Risk Environment	
2	Case Study 1: <i>Snowfall and a stolen laptop</i>	Aug. 31
	Data Classification Process and Models	
3	Risk Evaluation	Sept. 7
4	Case Study 2: <i>Autopsy of a Data Breach: The Target Case</i>	Sept. 14
5	Creating a Security Aware Organization	Sept. 21
6	Physical and Environmental Security	Sept. 28
7	Midterm Exam	Oct. 5
8	Case Study 3: <i>A Hospital Catches the "Millennium Bug"</i>	Oct. 12
9	Business Continuity and Disaster Recovery Planning	Oct. 19
10	Network Security	Oct. 26
11	Cryptography, Public Key Encryption and Digital Signatures	Nov. 2
12	Identity Management and Access Control	Nov.9
13	Computer Application Security	Nov. 16
	Team Project Presentations (if needed)	
14	Team Project Presentations	Nov. 30
	Review	
15	Final Exam	Dec. 14

Class topics and schedule

MIS

MANAGEMENT INFORMATION SYSTEMS

Protection of Information Assets

MIS 5206.701 • Fall 2022 • William Bailey

HOMEPAGE	INSTRUCTOR	SYLLABUS	SCHEDULE	DELIVERABLES	CLASS CAPTURE VIDEOS
--------------------------	----------------------------	--------------------------	--------------------------	------------------------------	--------------------------------------

Unit #1: Understanding an Organization's Risk Environment

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: "Framework for Improving Critical Infrastructure"
- ISACA "Risk IT Framework" pp. 1-30

Due before Week (Unit) 2:

- Post your answers** to the weekly reading/discussion question(s) for Unit #2 by the due date according to the Weekly Cycle schedule
- Post your answers** to the case study questions in Canvas by the due date according to 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

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

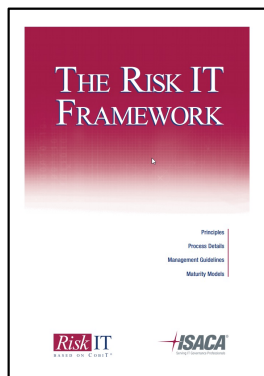
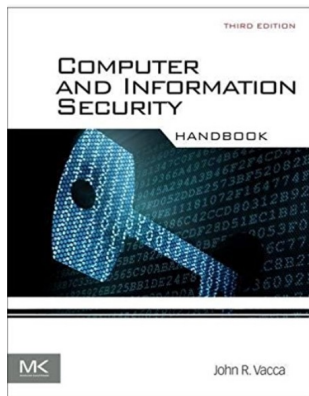
Unit #5: Creating a Security Aware Organization

Unit #6: Physical and Environmental Security

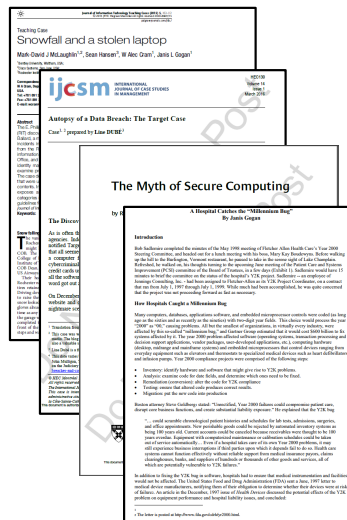
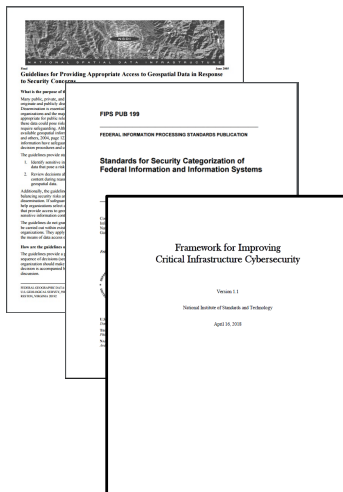
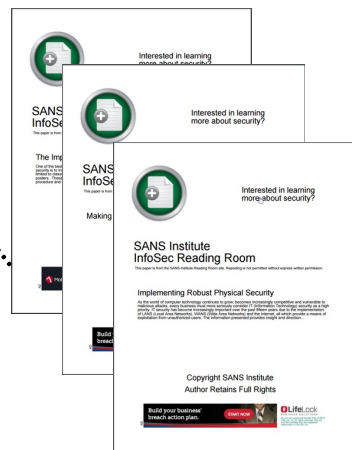
WEEKLY DISCUSSIONS

- > [Unit 01: Understanding an Organization's Risk Environment \(4\)](#)
- > [Unit 02: Data Classification Process and Models \(5\)](#)
- > [Welcome \(1\)](#)

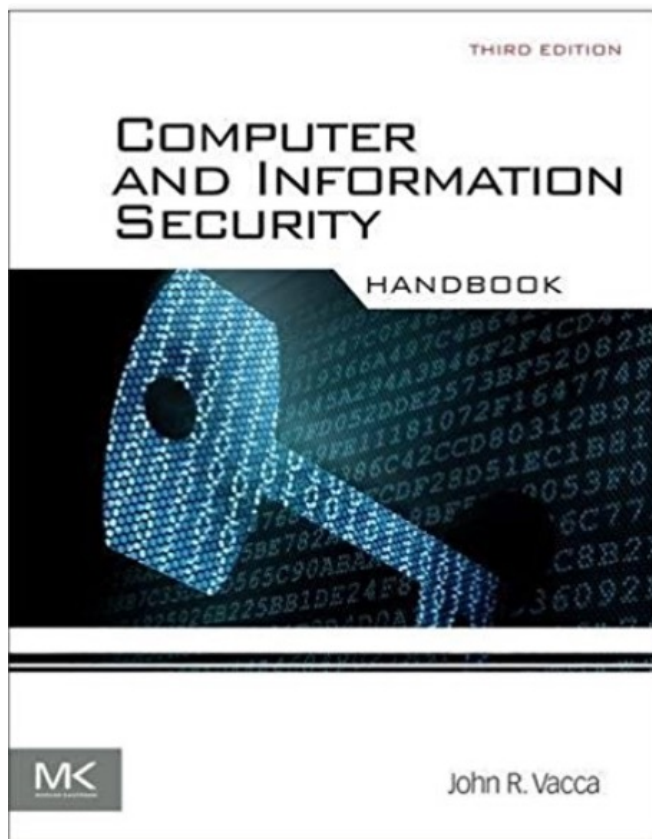
Textbook and readings



Textbook	Computer and Information Security Handbook - Third Edition, 2017, John R. Vacca, Elsevier, Inc. ISBN: 978-0-12-803843-7 Available online at O'Reilly 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/853285 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'"

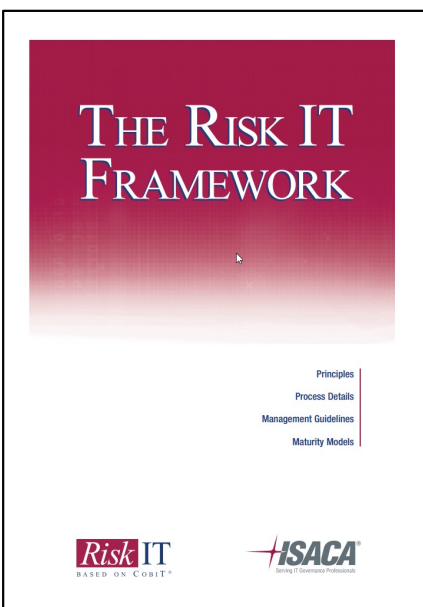


Textbook and readings



Textbook	<u>Computer and Information Security Handbook - Third Edition</u> , 2017, John R. Vacca, Elsevier, Inc. ISBN: 978-0-12-803843-7 Available online at O'Reilly 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. Masaji, CISA, CGA, CISSP

With the recent suspected everywh and chaos are com have come to unfo The question th happen.

Failure to propa theoretical name as the discharge of its the horrors of disas dents of a perfect of crisis they could be

As the experie just technology bu the recognition th through superior p positive, strategic, tough, touchy, sens disaster, organizati problems involv campaigns, corpora crisis communicati building, ethics/ons management, mana relations strategy an management, and a controversy, comm

In the aftermath began to build the ing, restoring and ery planning that fo centers was far fro These plans did not of key business pro ment. The requirem ness, web-speed we Web-based and dist processes too comp Business contin ness success that the department alone. If the responsibility es must become the sh entire senior manag executives in charge

INFORMATION SYL

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.

Figure 1—Recovery Principles

- Identify and test critical applications.
- Create a recovery team with roles and responsibilities.
- Provide a backup for all essential components of corporate 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 (OS), applications and data. From system 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.

Textbook	Computer and Information Security Handbook - Third Edition, 2017, John R. Vacca, Elsevier, Inc. ISBN: 978-0-12-803843-7 Available online at O'Reilly 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?

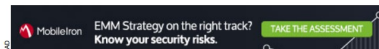
SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

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 webcasts, 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.

Copyright SANS Institute
Author Retains Full Rights



Interested in learning more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Making Security Awareness Efforts Work for You



Interested in learning more about security?

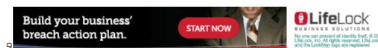
SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

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...


Copyright SANS Institute
Author Retains Full Rights



Textbook	Computer and Information Security Handbook - Third Edition, 2017, John R. Vacca, Elsevier, Inc. ISBN: 978-0-12-803843-7 Available online at O'Reilly 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



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

June 2005

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

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

Framework for Improving Critical Infrastructure Cybersecurity

Version 1.0

National Institute of Standards and Technology


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
Philip J. Bond, Under Secretary for Technology
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Arden L. Bemont, Jr., Director

Textbook	Computer and Information Security Handbook - Third Edition, 2017, John R. Vacca, Elsevier, Inc. ISBN: 978-0-12-803843-7 Available online at O'Reilly 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, 102-110
© 2015 IJTC, Taylor & Francis Ltd. <http://www.tandfonline.com/doi/full/10.1080/15393101.2015.1021101>

Teaching Case
Snowfall and a stolen laptop
Mark-David J McLaughlin^{1,2}, Sean Hansen³, W Alec Cram¹, Janis L Gogan¹

¹Bentley University, Waltham, USA,
²Claro Systems, San Jose, USA,
³Rochester Inst

Correspondence
W A Cram, Dept
USA
Tel: +781 891 20
Fax: +781 891 2
E-mail: wacram@

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 DUBÉ³

Abstract
The E. Philip (EP) discover Ballard, a m incidents in from the P information, Office, and F identity may examine per The case de that work of contents. In expose an categories of guidelines for Journal of Inf Keywords:

The Discov
As is often the agencies. Inde notified Target that all seeme a computer r cybercriminal credit cards us all the softwar word got out a

On December website and c nightmare see

Snowfalling
The vast Rochest might h COB. The College of I Institute of I COB Dean, US Airways Their loc Rochester ne tires remains Driving dow to raise the snow looko gloves ahead time as any the garage w completed i front of the steps and wa

¹ Translation from
² This case was ne media. The blog also a valuable so
³ Line Dubé is a fu
⁴ This date varies b Julia Mulligan, 7 on the Judiciary [branches-and-co](#)

CC BY-NC
All rights reserved
The International J This case is in an administrative situ in Case-Studies-Cas This document is authorize

The Myth of Secure Computing
by R

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 Boudevsyns. 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 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. 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/y2000.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'Reilly 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/853285 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%

Assignments

1. Readings

Week	Readings
1	<ul style="list-style-type: none"> • Vacca Chapter 1 "Information Security in the Modern Enterprise" • Vacca Chapter 2 "Building a Secure Organization" • NIST Reading 1: "Framework for Improving Critical Infrastructure Cybersecurity" • ISACA Risk IT Framework, pp. 1-42
2	<ul style="list-style-type: none"> • 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)"

Week	Readings
1	<ul style="list-style-type: none"> • Vacca Chapter 1 "Information Security in the Modern Enterprise" • Vacca Chapter 2 "Building a Secure Organization" • NIST Reading 1: "Framework for Improving Critical Infrastructure Cybersecurity" • ISACA Risk IT Framework, pp. 1-42
2	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Vacca Chapter 25 "Security Management Systems" • Vacca Chapter 34 "Risk Management" • ISACA Reading 1: "Risk IT Framework" pp. 47-96
4	<ul style="list-style-type: none"> • Case Study 2: "Autopsy of a Data Breach: The Target Case"
5	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • HBR Reading 1: "The Myth of Security Computing" • Vacca Chapter 69 "Physical Security Essentials" • SANS Reading 3: "Implementing Robust Physical Security"
8	<ul style="list-style-type: none"> • Case Study 2: "A Hospital Catches the Millennium Bug"
9	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 MIS5206 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 5206 Protecting Information Assets

The screenshot displays a Moodle LMS interface for the course 'Protection of Information Assets'. The page title is 'MIS MANAGEMENT INFORMATION SYSTEMS' and 'Protection of Information Assets'. The course code is 'MIS 5206.702' and the semester is 'Fall 2020' by 'David Lanter'. The navigation menu includes 'HOMEPAGE', 'INSTRUCTOR', 'SYLLABUS', 'SCHEDULE', 'DELIVERABLES', 'ZOOM MEETINGS', and 'GRADEBOOK'. The current unit is 'Unit 01: Understanding an Organization's Risk Environment'. The page shows a list of 'All Questions' under the unit, with three questions visible. The first question is 'Do ITACS students represent information security vulnerabilities to each other, or both? Explain your answer.' The second question is 'Is information security a technical problem, a business problem, or both? Explain your answer.' The third question is 'What challenges are involved in performing a quantitative information security analysis?'. A detailed view of 'Question 2' is shown, with the text 'Is information security a technical problem or a business problem? Explain your answer.' Below the question, it says 'FILED UNDER: UNIT 01: UNDERSTANDING AN ORGANIZATION'S RISK ENVIRONMENT' and 'TAGGED WITH:'. A comment from 'Wenyao Ma' is displayed, dated 'AUGUST 23, 2020 AT 3:31 AM'. The comment text reads: '(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 build 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.' There is a 'Reply' button below the comment.

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.

- 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...*

Journal of Information Technology Teaching Cases (2015) 1, 1-11
DOI: 10.1002/it2.1001
Copyright © 2015, John Wiley & Sons, Ltd.

Teaching Case
Snowfall and a stolen laptop

Mark-David J McLaughlin^{1,2}, Sean Hansen^{1,2}, W Alec Cram¹, Janis L Gogan¹

¹Yorkshire University, Wetherby, UK;
²York Business School, UK;
³Rockefeller Institute of Technology, Rochester, USA

Correspondence:
M-D J Gogan, Department of Information and Process Management, Bentley University, 175 Forest Street, Waltham, MA 02452, USA.
Tel: +1 978 881 2811;
Fax: +1 978 881 2842;
E-mail: mclaughin@bentley.edu

Abstract
The Dr. Philip Saunders College of Business (COB) Dean at Rockefeller Institute of Technology (RIT) discovers that his PPT caused 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 PPT 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 explore 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 threat of a competing choice compels an organization to raise of inadvertent disclosure of information in different categories (such as private, confidential, internal, or public), and students can discuss useful guidelines for effective information security incident response.

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 Dr. Philip Saunders College of Business, one of eight colleges of the Rockefeller Institute of Technology (RIT) in the driver's seat was the EPS COB Dean. He said goodbye to his wife who would head 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 tire 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 tapping off, this was in good time as any to get a little exercise, or be grabbed a shower 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 Carlton 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? There he felt another chill from the sudden realization that his laptop, which he'd left on the couch in the den before taking his life to the airport, was no longer there. After darting and kicking 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 – now, here, he called.

A Hospital Catches the "Millennium Bug"
By Janis Gogan

Introduction
Bob Sadlemier 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 Roadways. Before walking up the hill to the Burlington, Vermont restaurant, he passed 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). Sadlemier would have 15 minutes to brief the committee on the status of the hospital's Y2K project. Sadlemier – an employee of Jennings Consulting, Inc. – had been assigned to Fletcher-Alten 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, non-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.
• Analytic: 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 stated: "Unnoticed, 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. 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 The letter is posted at <http://www.fda.gov/ohrt/y2000.html>.

ijcsm INTERNATIONAL JOURNAL OF CASE STUDIES IN MANAGEMENT

Volume 14 Issue 1 March 2014

Autopsy of a Data Breach: The Target Case
Case 2 prepared by Line DUBE¹

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 18.²

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 wanted 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 10, 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 Andrew Schneider of case #9 01 2014 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 public. The blog by the investigators reporter Erika Zardo (Investmentcase.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 Dube is a PhD professor in ISEC Montreal's Department of Information Technologies.

⁴ This data refers to December 15 and 16, depending on the source. December 15 is used here because it is the date given by John McKinley, Target's Executive Vice-President and Chief Financial Officer, in testimony before the U.S. Senate Committee on the Judiciary on February 4, 2014 (<http://www.judiciary.senate.gov/record/testimony.aspx?in-the-digital-age-part-2>).

⁵ ISEC Montreal 2014. All rights reserved for all countries. Any reproduction or translation in any form whatsoever is prohibited.

⁶ The International Journal of Case Studies in Management is published on-line (http://www.ijcsm.com/online_content.html), ISSN 1911-2396. This case is intended to be used in the classroom for an educational discussion and does not imply any judgement on the administration's situation presented. Deposited under number # 02 2014 0017 with the ISEC Montreal Case Centre, 2006, chemin de la Cité Sainte-Catherine, Montréal (Québec) H3T 1J4, Canada.

This document is authorized for educator review use only by David Lurie, Toronto University until August 2017. Copying or posting is an infringement of copyright. Permission@ijcsm.com or case.centre@ijcsm.com

Assignments

3. Three case studies (continued...)

- 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.



Journal of Management Inquiry
Volume 14
Number 3
September 2005

Teaching Case
Snowfall and a stolen laptop
 Mark David J. McLaughlin,^{1,2} Sean Hansen,³ W Alec Crain,¹ Jenni L. Gogan¹

Teaching Case
 Copyright © 2005, Sage Publications
 10.1177/1056492605279993

Abstract
 This case study illustrates the challenges of protecting information assets in a hospital setting. It discusses the challenges of protecting information assets in a hospital setting. It discusses the challenges of protecting information assets in a hospital setting. It discusses the challenges of protecting information assets in a hospital setting. It discusses the challenges of protecting information assets in a hospital setting.

Keywords
 information security, incident response, risk management, IT governance

A Hospital Catches the "Millennium Bug"
 By Jamn Gogan

Introduction
 In the minutes of the minutes of the May 1998 meeting of the Board of Trustees, a committee was formed to study the Y2K problem. The committee was formed to study the Y2K problem. The committee was formed to study the Y2K problem. The committee was formed to study the Y2K problem.

How Hospitals Caught a Millennium Bug
 Many computers, databases, applications software, and embedded microprocessor controls were coded for long ago in the 1970s and 80s. These systems 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 General Electric estimated that it would cost \$600 million to fix its systems affected by it. The year 2000 problem affected software (operating systems, transaction processing and database support applications, vendor packages, non-developed applications, etc.), computing hardware (desktop, laptops and mainframe systems) and embedded microprocessors that control devices ranging from everyday equipment such as elevators and turbines 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.
- Analyze, examine code for date fields, and determine which ones need to be fixed.
- Remediation (corrective) also the code for Y2K compliance.
- Testing: ensure that altered code produces correct results.
- Migration: put the new code into production.

Business attorney Steve Goldberg stated: "Unmodified, Year 2000 factories could compromise patient care, disrupt core business functions, and create substantial liability exposure." This explained that the Y2K bug "... could scramble chronological patient histories and schedules for lab tests, admissions, surgeries, and office appointments. New, potentially good, could be rejected by automated inventory systems as being 100 years old. Current accounts could be canceled because expirables were thought to be 100 years overdue. Equipment with compressed 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 critical support from medical insurance payors, claims clearinghouses, banks, and suppliers of hardware 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) used a June 1997 letter to medical device manufacturers, reminding them of their obligation to determine whether their devices were at risk of failure. An article in the December, 1997 issue of *Hospital HealthCare* discussed the potential effects of the Y2K problem on equipment performance and hospital liability issues, and concluded:

"... the letter is posted at <http://www.fda.gov/oc/y2k00.html>.

iJCSM INTERNATIONAL JOURNAL OF STUDIES IN MANAGEMENT
 Volume 14
 Number 3
 September 2005

Autopsy of a Data Breach: The Target Case
 Case¹ prepared by Lisa DeBBE¹

Abstract
 On December 19, 2013, Target, the second-largest retailer in the United States, announced a breach involving the theft of 40.1 million credit and debit cards used to make purchases in Target U.S. stores between December 2nd and December 15th.

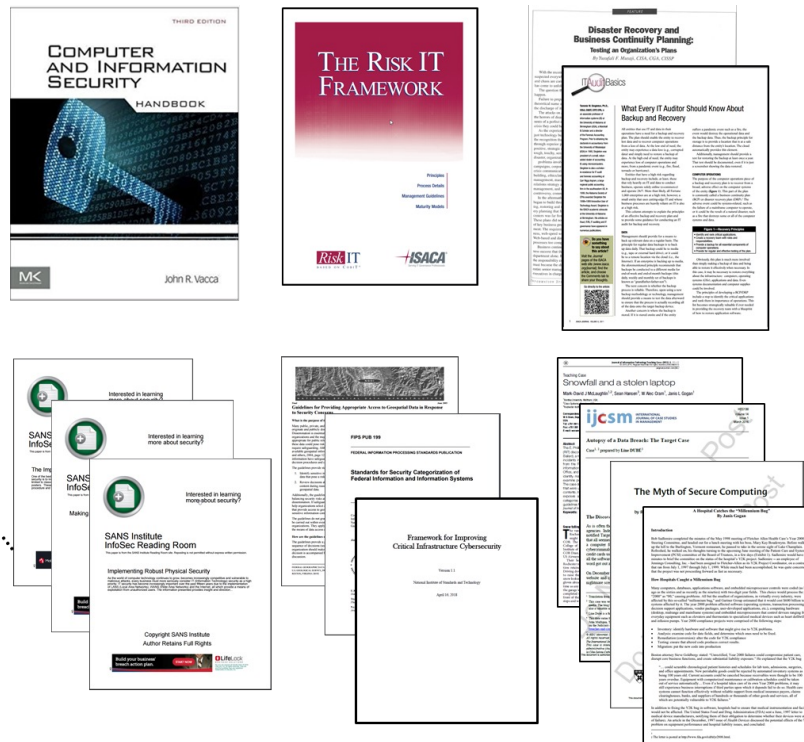
Introduction
 As is often the case in such situations, Target learned of the data breach from law enforcement agencies. Indeed, on December 13, 2013, representatives from the U.S. Department of Justice notified Target a management of a large number of fraudulent debit and credit card transactions that all seemed to share a link to transactions made at Target. Following the notification, Target hired a computer forensic firm to investigate the breach. The results confirmed as worst fear: cybercriminals had been tracking data from Target's systems and installing data from its million debit and credit cards used in its U.S. establishments since November 27. Target wanted to take immediate action to prevent further data theft. But despite the company's eagerness to solve the puzzle, what 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 centers were quickly inundated with calls from outraged customers, creating a nightmare scenario for its customer service department. To make matters even worse, the breach was not limited to Target's U.S. operations. Instead, it had spread to its Canadian, Mexican, and U.K. operations.

Target's CEO, Brian Cornell, announced the breach on December 19 in a prepared statement. He said: "We have been notified by law enforcement agencies that our systems were breached. The breach involved the theft of 40.1 million credit and debit cards used in our U.S. stores between December 2nd and December 15th. The breach also involved the theft of approximately 100 million names, addresses, and phone numbers of our customers in the United States and Canada. This breach is a significant violation of our privacy policy and our commitment to our customers. We are taking immediate steps to protect our customers' information and to prevent further breaches. We are working with law enforcement agencies to identify the perpetrators of this breach and to bring them to justice. We are also reviewing our security measures to ensure that we can prevent such breaches in the future. We will provide a more detailed update as more information becomes available."

Assignments


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



MIS 5206 Protecting Information Assets

Unit #	Readings
1	<ul style="list-style-type: none"> • Vacca Chapter 1 "Information Security in the Modern Enterprise" • Vacca Chapter 2 "Building a Secure Organization" • NIST Reading 1: "Framework for Improving Critical Infrastructure Cybersecurity" • ISACA Risk IT Framework, pp. 1-42
2	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Vacca Chapter 25 "Security Management Systems" • Vacca Chapter 34 "Risk Management" • ISACA Reading 1: "Risk IT Framework" pp. 47-96
4	<ul style="list-style-type: none"> • Case Study 2: "Autopsy of a Data Breach: The Target Case"
5	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • HBR Reading 1: "The Myth of Security Computing" • Vacca Chapter 69 "Physical Security Essentials" • SANS Reading 3: "Implementing Robust Physical Security"
8	<ul style="list-style-type: none"> • Case Study 2: "A Hospital Catches the 'Millennium Bug'"
9	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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"


Deliverables



Protection of Information Assets

MIS 5206.701 • Fall 2022 • William Bailey

- HOME PAGE
- INSTRUCTOR
- SYLLABUS
- SCHEDULE
- DELIVERABLES
- CLASS CAPTURE VIDEOS



Welcome!

AUGUST 1, 2022 BY WILLIAM BAILEY

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

- > Gain an overview of the nature of information security vulnerabilities and threats
- > Learn how information security risks are identified, classified and prioritized
- > Develop an understanding of how information security risks are managed, mitigated and controlled
- > Gain experience working as part of team, developing and delivering a professional presentation

- 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

- > Unit 01: Understanding an Organization's Risk Environment (4)
- > Unit 02: Data Classification Process and Models (5)
- > Welcome (1)

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](#)

Participation

2. “In the News” articles



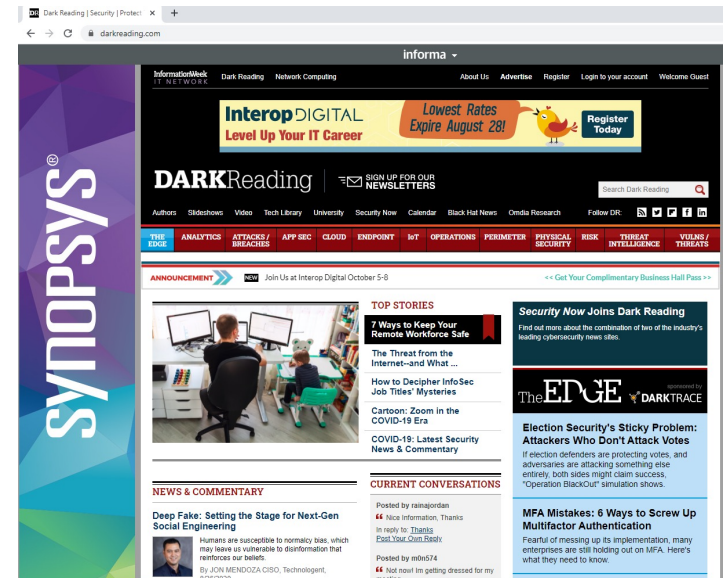
- <https://www.theregister.co.uk/security/>
- <http://www.eweek.com/security>
- <https://www.computerworld.com/category/security/>
- <https://krebsonsecurity.com/>
- ⋮

MIS 5206 Protecting Information Assets

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



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 dont 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. 5	Midterm
Dec. 14	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

Weekly Cycle

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

Next...

Week	Assignment Topics
1 ✓	Introduction to MIS5206
1 →	Understanding an Organization's Risk Environment
2	Case Study 1: <i>Snowfall and a stolen laptop</i>

Unit #	Readings
1	<ul style="list-style-type: none">• Vacca Chapter 1 "Information Security in the Modern Enterprise"• Vacca Chapter 2 "Building a Secure Organization"• NIST Reading 1: "Framework for Improving Critical Infrastructure Cybersecurity"• ISACA Risk IT Framework, pp. 1-42• Case Study 1: "Snowfall and a Stolen Laptop"

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