Protecting Information Assets
Week 1
Secure Computing is a Myth

When it comes to digital security, there’s no such thing as an impenetrable defense. But you can mitigate risks by following sound operating practices.

Robert D. Austin and Christopher A.R. Darby
2003 Harvard Business School
Agenda

• Welcome - introductions
• Course Objectives
• Textbook and Readings
• Grading
  – Assignments
  – Participation in class and online
  – Team Presentation
  – Exams
• Class Web Site “Blog”
• Quizzes
• Semester Schedule
• Weekly Rhythm
• Typical Class Session
• Week 1: Risk Management
• Next time
Introductions - Instructor

MIS 5206 Protecting Information Assets
Course Objectives

In this course you will gain an understanding the importance of and techniques related to managing information assets including logical, physical, and environmental security along with disaster recovery and business continuity.

The Key subject areas that are covered in the course are:
  – Information Security Risk Identification and Management
  – Security Threats and Mitigation Strategies

• 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.
Textbook and Readings

**MIS 5206 Protecting Information Assets**

**Required Textbook and Readings**

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ISACA Reading 3: “Implementing Robust Physical Security” [Link]</td>
<td>SANS Reading 1: “The Importance of Security Awareness Training” [Link]</td>
</tr>
<tr>
<td>FGDC FGDC Reading 1: “Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns”, [Link]</td>
<td>Harvard Business Publishing (HBP) The 2 case studies and 1 reading listed below are available in the course pack for purchase from HBP: [Link]</td>
</tr>
</tbody>
</table>
Grading

<table>
<thead>
<tr>
<th>Item</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assignments</td>
<td>25%</td>
</tr>
<tr>
<td>Participation (in class and online)</td>
<td>20%</td>
</tr>
<tr>
<td>Team Presentation</td>
<td>25%</td>
</tr>
<tr>
<td>Exams</td>
<td>30%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>
Assignments

1. Readings

<table>
<thead>
<tr>
<th>Class #</th>
<th>Readings</th>
<th>Class Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>• Vacca Ch.1 “Building a Secure Organization”</td>
<td>9/7</td>
</tr>
<tr>
<td></td>
<td>• ISACA Risk IT Framework, pp. 1-42</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• NIST Reading 1: “Framework for Improving Critical Infrastructure Cybersecurity”</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>• Vacca Ch.21 “Information Security Essentials for IT Managers: Protecting Mission-Critical Systems”</td>
<td>9/14</td>
</tr>
<tr>
<td></td>
<td>• FIPS Reading 1: “Standards for Security Categorization of Federal Information and Information Systems”</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• FGDC Reading 1: “Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns”</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ISO 27001 Reading 1: ISO 27001 Data Security Classifications Model Policy</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>• Vacca Ch.22 “Security Management Systems”</td>
<td>9/21</td>
</tr>
<tr>
<td></td>
<td>• Vacca Ch.53 “Risk Management”</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ISACA Risk IT Framework pp. 47-96</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>• Vacca Ch. 24 “Information Technology Security Management”</td>
<td>9/28</td>
</tr>
<tr>
<td></td>
<td>• SANS Reading 1: “The Importance of Security Awareness Training”</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SANS Reading 2: “Making Security Awareness Work for You”</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>• HBR Reading 1: “The Myth of Secure Computing”</td>
<td>10/5</td>
</tr>
<tr>
<td></td>
<td>• Vacca Ch.54 “Physical Security Essentials”</td>
<td></td>
</tr>
</tbody>
</table>
Assignments

2. Answers to weekly reading discussion questions

Each Friday you will find a post that includes several discussion questions about the coming week’s readings. You will be expected to post your answer to one of the discussion questions on the week’s readings by **Sunday @11:59 PM**.

A paragraph or two of thoughtful analysis is expected for your initial answer to the question.

Post your answer to the weekly class assignment blog.

You must come to class prepared to discuss all of these questions in detail when we meet.
Assignments

2. Answers to weekly reading discussion questions
Assignments

3. Two case study writes ups

For each case study I will provide several discussion questions which will be posted to the class site. Pick one question and respond to it in depth.

Your analysis should not exceed one single-spaced page using 11 point Times New Roman font with one-inch margins. Do not prepare a separate cover page, instead put your name, the class section number and the case name in the top-left corner of the header.

To submit your case study analysis, you must post it on the class blog no later than Monday at 9:00 AM of the week it is due. Please copy your analysis in clear text onto the blog.
### Assignments

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

#### Required Textbook and Readings

|----------|-------------------------------------------------------------------------------------------------------------------|

#### ITACS 5206

**Week 2 – All Questions**

**Coursework:**
- ISACA students represent information security vulnerabilities to Temple University, each other or both.
- Students are encouraged to use the course materials to enhance their understanding.

**Question:**
1. Do ISACA students represent information security vulnerabilities to Temple University, each other or both?
2. Explain the nature of the problem of information security failure.

**Case Study Analysis:**
- ISACA students represent information security vulnerabilities to Temple University, each other or both.
- Students are encouraged to use the course materials to enhance their understanding.

#### Textbook and Readings

<table>
<thead>
<tr>
<th>Class #</th>
<th>Readings</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
</tr>
</tbody>
</table>

#### ISO

- ISO 27001:2005
- ISO 27002:2013
- ISO 27015:2013

#### Harvard Business Publishing (HBP)

- Harvard Business Review (HBR)
- Harvard Business School Press (HBS)
- Harvard Business Essentials (HBE)

#### MIS 5206 Protecting Information Assets
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 four (4) substantive posts that include your thoughtful comments as you participate in the discussion of the questions.

The posting of these additional four comments is due by **Tuesday @ 11:59am**.
2. “In the News” articles

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.

The deadline for posting is by Tuesday by 11:59am.
Participation

3. During class

We will typically start each session with “opening” questions about the assigned readings and their online discussion, and the next case study.

We will also discuss “in the news” articles that you have discovered and posted to the class blog. I may ask for volunteers, or I may call on you.

Students called on to answer should be able to summarize the key issues, opportunities, and challenges in the case study. All students should be prepared to answer these questions.

Another important aspect of in-class participation is completion of in-class assignments and contribution to any break out activities.
Participation

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

2. Find and summarize on blog and present “In the News” article in class

3. Participate in discussions during class
Team presentation

During the Class #3, the students will be organized into a series of presentation development and delivery teams. Each team will have ~3 members and be assigned a topic.

The team will develop a presentation covering the assigned topic, and the presentation will be designed/planned so that it is completed in no less than 15 minutes and no more than 30 minutes.

Each member of the team will present for no less than 5 minutes and no more than 10 minutes.

For example, the team may cover all three of the following areas in its presentation. Each presenter on the team will focus on one of the assigned areas:
1) Business/organizational context
2) Technical environment
3) Risk management/mitigation focus
Exams

There will be two (2) exams during the semester. Together these exams are weighted 30% of your final grade.

<table>
<thead>
<tr>
<th>Class #</th>
<th>Exam</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Exam 1</td>
<td>10/5</td>
</tr>
<tr>
<td>14</td>
<td>Exam 2</td>
<td>12/7</td>
</tr>
</tbody>
</table>

Exams will consist of multiple-choice, fill in the blank and possible short answer questions.

You will have a fixed time (e.g. 40 minutes) to complete the exam.

In general, the exams will not be cumulative but focused on the course materials since the beginning of last exam. However, some concepts highlighted in class as a ‘Core Principle’ or ‘Important’ may appear on any of the exams.

A missed exam can only be made up in the case of documented and verifiable extreme emergency situations. No make-up is possible for the final exam.
Protecting IT Assets

August 11, 2016 by David Lantin

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 test taking skills

Welcome (1)
Class Web Site – “INSTRUCTOR”

http://community.mis.temple.edu/itacs5206fall16/
Class Web Site – “SYLLABUS”

http://community.mis.temple.edu/itacs5206fall16/
Class Web Site – “SCHEDULE”

http://community.mis.temple.edu/itacs5206fall16/

Week 1: Course Introduction and the Risk IT Framework

Readings:
- Start the reading assignment for Week 2...

Assignments For Class 2:
- Readings
- Answer Reading/Discussion Question Due by 9/4 11:59 pm (evening)
- Comment on your fellow students' question answers by Wednesday 9/7 am (morning)
- In the News Topic by 9/7 11:59 am (morning)
Class Web Site – “DELIVERABLES”

http://community.mis.temple.edu/itacs5206fall16/
Weekly Quiz

– Practice exam questions
– Grades for quiz do not count
– Taking the quiz counts toward participation score
### Semester Schedule

<table>
<thead>
<tr>
<th>Class</th>
<th>Topic</th>
<th>Readings</th>
<th>Exams</th>
<th>Case Studies</th>
<th>Team Presentations</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Course Introduction and the Risk IT Framework</td>
<td>Vacca Chapter 1</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>Understanding an Organization’s Risk Environment</td>
<td>ISACA Risk IT Framework pp. 1 - 42, NIST Reading 1</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>3</td>
<td>Data Classification Process and Models</td>
<td>Vacca (2013) Chapter 21, or Vacca (2009) Chapter 14, FIPS Reading 1, FGDC Reading 1, ISO 27001 Reading 1</td>
<td>-</td>
<td>Read and be prepared to discuss: Case 1: HDFC Bank - Securing Online Banking</td>
<td>-</td>
</tr>
<tr>
<td>5</td>
<td>Creating a Security Aware Organization</td>
<td>Vacca Chapter (2013) Chapter 24 or Vacca (2009) Chapter 16, SANS Readings 1 &amp; 2, NIST Reading 2, Chapter 4 – “Awareness and Training”; pp. 16-34</td>
<td>-</td>
<td>Case Analysis 1 Due</td>
<td>-</td>
</tr>
<tr>
<td>6</td>
<td>Review Managing IT Security Risk</td>
<td>HBR Reading 1</td>
<td>Mid-Term Exam</td>
<td>-</td>
<td>Teams and Topics Assigned</td>
</tr>
<tr>
<td>9</td>
<td>Network Security</td>
<td>Vacca (2013) Chapters 5, 9-15, 17-18; or Vacca (2009) Chapters 4-13</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

**FALL BREAK**

<table>
<thead>
<tr>
<th>Class</th>
<th>Topic</th>
<th>Readings</th>
<th>Exams</th>
<th>Case Studies</th>
<th>Team Presentations</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>Review Security Threats and Mitigations</td>
<td>-</td>
<td>-</td>
<td>Case Analysis 2 Due</td>
<td>-</td>
</tr>
<tr>
<td>14</td>
<td>Final Exam</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
### Semester Schedule – 1st Half

<table>
<thead>
<tr>
<th>Class</th>
<th>Topic</th>
<th>Readings</th>
<th>Exams</th>
<th>Case Studies</th>
<th>Team Presentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Course Introduction and the Risk IT Framework</td>
<td>Vacca Chapter 1, ISACA RiskIT Framework pp. 1 - 42, NIST Reading 1</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>Understanding an Organization’s Risk Environment</td>
<td>Vacca (2013) Chapter 21, or Vacca (2009) Chapter 14, FIPS Reading 1, FGDC Reading 1, ISO 27001 Reading 1</td>
<td>-</td>
<td>-</td>
<td>Read and be prepared to discuss: Case 1: HDFC Bank - Securing Online Banking</td>
</tr>
<tr>
<td>4</td>
<td>Risk Evaluation</td>
<td>Vacca Chapter (2013) Chapter 24 or Vacca (2009) Chapter 16, SANS Readings 1 &amp; 2, NIST Reading 2, Chapter 4 – “Awareness and Training”, pp. 26-34</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>5</td>
<td>Creating a Security Aware Organization</td>
<td></td>
<td>-</td>
<td>Case Analysis 1 Due</td>
<td>-</td>
</tr>
<tr>
<td>6</td>
<td>Review Managing IT Security Risk</td>
<td>HBR Reading 1</td>
<td>Mid-Term Exam</td>
<td>-</td>
<td>Teams and Topics Assigned</td>
</tr>
</tbody>
</table>

MIS 5206 Protecting Information Assets
## Semester Schedule – 2nd Half

<table>
<thead>
<tr>
<th>Class</th>
<th>Topic</th>
<th>Readings</th>
<th>Exams</th>
<th>Case Studies</th>
<th>Team Presentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Physical and Environmental Security</td>
<td>Vacca (2013) Chapter 54, or Vacca (2009) Chapter 36; SANS Reading 3</td>
<td>-</td>
<td>-</td>
<td>Draft Outline Due</td>
</tr>
<tr>
<td>8</td>
<td>Business Continuity and Disaster Recovery Planning</td>
<td>Vacca (2013) Chapter 57, or Vacca (2009) Chapter 38; ISACA Readings 1 &amp; 2</td>
<td>-</td>
<td>-</td>
<td>Draft Presentation Due</td>
</tr>
<tr>
<td>9</td>
<td>Network Security</td>
<td>Vacca (2013) Chapters 5, 9-15, 17-18; or Vacca (2009) Chapters 4-13</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>FALL BREAK</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Review</td>
<td></td>
<td>-</td>
<td>-</td>
<td>Case Analysis 2 Due 12/5</td>
</tr>
<tr>
<td></td>
<td>Security Threats and Mitigations</td>
<td></td>
<td></td>
<td>Final Exam</td>
<td></td>
</tr>
</tbody>
</table>

**MIS 5206 Protecting Information Assets**
## Weekly Rhythm

### Section 001

<table>
<thead>
<tr>
<th>When</th>
<th>Actor</th>
<th>Task</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Friday</td>
<td>Instructor (me)</td>
<td>Post reading questions (Friday am)</td>
<td></td>
</tr>
<tr>
<td>Sunday 11:59pm</td>
<td>Student</td>
<td>Post answers to reading questions</td>
<td>Assignment</td>
</tr>
<tr>
<td>Monday 9:00am</td>
<td>Student</td>
<td>Post case study analysis (when due)</td>
<td>Assignment</td>
</tr>
<tr>
<td>Tuesday 11:59am</td>
<td>Student</td>
<td>Post 4 comments to others’ answers</td>
<td>Participation</td>
</tr>
<tr>
<td>Tuesday 11:59am</td>
<td>Student</td>
<td>Post “In The News” article</td>
<td>Participation</td>
</tr>
<tr>
<td>Wednesday 9am-12:30pm</td>
<td>Both of Us</td>
<td>Class meeting</td>
<td>Participation</td>
</tr>
<tr>
<td>Thursday</td>
<td>Instructor</td>
<td>Post summary notes</td>
<td></td>
</tr>
</tbody>
</table>

### Section 701

<table>
<thead>
<tr>
<th>When</th>
<th>Actor</th>
<th>Task</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Friday</td>
<td>Instructor (me)</td>
<td>Post reading questions (Friday am)</td>
<td></td>
</tr>
<tr>
<td>Monday 11:59pm</td>
<td>Student</td>
<td>Post answers to reading questions</td>
<td>Assignment</td>
</tr>
<tr>
<td>Tuesday 9:00am</td>
<td>Student</td>
<td>Post case study analysis (when due)</td>
<td>Assignment</td>
</tr>
<tr>
<td>Wednesday 11:59am</td>
<td>Student</td>
<td>Post 4 comments to others’ answers</td>
<td>Participation</td>
</tr>
<tr>
<td>Wednesday 11:59am</td>
<td>Student</td>
<td>Post “In The News” article</td>
<td>Participation</td>
</tr>
<tr>
<td>Thursday 5:30pm-8pm</td>
<td>Both of Us</td>
<td>Class meeting</td>
<td>Participation</td>
</tr>
<tr>
<td>Friday</td>
<td>Instructor</td>
<td>Post summary notes</td>
<td></td>
</tr>
</tbody>
</table>
Typical in-class session

1. In the News
2. Lecture/discussion
3. Presentations (later in the semester)
4. Quiz
Agenda

✓ Welcome - introductions
✓ Course Objectives
✓ Textbook and Readings
✓ Grading
  ✓ Assignments
  ✓ Participation in class and online
  ✓ Team Presentation
  ✓ Exams
✓ Class Web Site “Blog”
✓ Quizzes
✓ Semester Schedule
✓ Weekly Rhythm
✓ Typical Class Session
  • Week 1: Risk Management
In the News

• Coalition of spammers pooled resources and launched the largest distributed denial of service (DDoS) attack on the Internet

What information needs protection?

• Personally Identifiable Information (PII)
What Personally Identifiable Information have you already provided Temple University to use and protect?

What new PII will the university create and compile about you that also needs to be used and protected?
Personally Identifiable Information (PII)

Data able to uniquely identify, contact or locate a person, or can be combined with other sources to uniquely identify an individual

Commonly used in identity theft, financial crimes and various criminal activities

**Typical PII Components:**
- Full name
- National identification number
- Vehicle registration plate number
- Driver’s license number
- Face, finger prints or handwriting
- Credit card numbers
- Digital identity
- Birthday
- Birthplace
- IP address (sometimes)
- Genetic information

**Often shared, but can be considered PII:**
- First or last name
- Country, state or city of residence
- Geolocation
- Age
- Gender
- Race
- Name of the school attended
- Workplace,
- Grades, salary, or job position
- Criminal record
- ...?
Protected Health Information (PHI)

PHI is defined by the Health Insurance Portability and Accountability Act (HIPAA)

PHI is individually identifiable health information that relates to the

– Past, present, or future physical or mental health or condition of an individual
– Provision of health care to the individual by a covered entity (for example, hospital or doctor)
– Past, present, or future payment for the provision of health care to the individual
When combined with health information about a person, the following becomes considered protected health information:

- Names
- Telephone numbers
- Fax numbers
- Email addresses
- Social Security numbers
- Medical record numbers
- Health plan beneficiary numbers
- License plate numbers
- URLs
- Full-face photographic images
- Any other unique identifying number, characteristic, code, or combination that allows identification of an individual
What information needs protection?

- Personally Identifiable Information (PII)
- Protected Health Information
- Business information
  - What business information needs protecting?
    - Customer data
    - Proprietary information / trade secrets
What is ISACA?

Previously known as “Information Systems Audit and Control Association”, now goes by ISACA acronym only

• Founded in 1969, is leading global provider of knowledge, certifications, community, advocacy and education on
  – Information systems assurance and security, enterprise governance of IT, and IT-related risk and compliance

More than 86,000 members in more than 160 countries

• ISACA sponsors international conferences
• Publishes the ISACA® Journal
• Develops international information systems auditing and control standards
• Administers the globally respected designations
  – Certified Information Systems Auditor ® (CISA®)
  – Certified Information Security Manager® (CISM®)
  – Certified in the Governance of Enterprise IT® (CGEIT®)

www.isaca.org
ISACA’s Risk IT Framework

- ISACA’s Risk IT Framework is useful to guide an organization’s approach to risk management and governance
- Used to help implement IT governance in enterprises that have adopted (or are planning to adopt) COBIT as their IT governance framework
- COBIT
  - Stands for Control Objectives for Information and Related Technologies
  - Is an IT governance framework and supporting toolset that allows managers to bridge the gap between business risks, risk control requirements, and technical issues
The Risk IT framework is about trading off IT value with IT risk—in other words... business risk related to the use of IT

- The connection to business is founded in the principles on which the framework is built, i.e., effective enterprise governance and management of IT risk
IT risk is business risk

- Associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise

- Consists of IT-related events and conditions that could potentially impact the business
  - *Can occur with both uncertain frequency and magnitude*
  - *Create challenges in meeting strategic goals and objectives*
The RiskIT Framework

ISACA’s risk management process and governance model groups key activities into a number of processes, grouped into three domains

Substantial guidance is provided on:
• Key activities within each process,
• Responsibilities for the process, information flows between processes
• Performance management of the process
U.S. laws and regulations require protection of data and computer (IT) systems that process them.

What information needs protection?

- Personally Identifiable Information (PII)
- Protected Health Information (PHI)
- Business information
  - Critical Infrastructure Information (CII)
Critical National Infrastructure

In 1996, President Clinton signed an Executive Order 13010 identifying infrastructure vulnerable to attack

“Certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States”

- Telecommunications
- Electrical power systems
- Gas and oil storage and transport
- Banking and finance
- Transportation
- Water supply systems
- Emergency services
- Continuity of government

Executive Order 13010 of July 15, 1996

Title 3—
The President

Critical Infrastructure Protection

Certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States. These critical infrastructures include telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government. Threats to these critical infrastructures fall into two categories: physical threats to tangible property (“physical threats”), and threats of electronic, radio-frequency, or computer-based attacks on the information or communications components that control critical infrastructures (“cyber threats”). Because many of these critical infrastructures are owned and operated by the private sector, it is essential that the government and private sector work together to develop a strategy for protecting them and assuring their continued operation.

NOW, THEREFORE, by the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:
Federal Homeland Security Act of 2002 defined...

**Critical Infrastructure Information** – as data that can be used in either physical or computer-based attack that directly or indirectly

- Affects viability of a facility or critical infrastructure
- Threatens public health or safety
- Harms interstate commerce or the United States
- Violates Federal, State, or local law

**Protected System** – any physical or computer-based system, information or data, process or procedure that directly or indirectly affects the viability of a facility or critical infrastructure
16 U.S. Critical Infrastructure Sectors

Transportation

Water and Wastewater Systems

Dams

Emergency Services

Commercial Facilities

Nuclear Reactors, Materials, and Waste

Defence Industrial Base

Communications

Energy

Chemical

Government Facilities

Critical Manufacturing

Healthcare and Public Health

Information Technology

Food and Agriculture

Financial Services
Cyber Security is One of the Most Serious Potential Risks in Transportation

- Increasing dependence on information systems and networks
- Risks are significant and growing
- Need a comprehensive approach
- Need a culture/ecosystem of cyber security (like fire safety)
- Cyber security is necessary for transportation mobility and safety!
Transportation sector - example

Cyber Security is One of the Most Serious Potential Risks in Transportation

- Increasing dependence on information systems and networks
- Risks are significant and growing
- Need a comprehensive approach
- Need a culture/ecosystem of cyber security (like fire safety)
- Cyber security is necessary for transportation mobility and safety!

Even "Isolated" Legacy Systems Are Vulnerable
14 Year Old Boy Derails Polish Trams, January 2008

- 4 light rail trains derailed, 12 people hurt
- Used modified television remote controller
- Locks disabling switch when vehicle present not installed
16 U.S. Critical Infrastructure Sectors

Transportation

Water and Wastewater Systems

Dams

Emergency Services

Commercial Facilities

Nuclear Reactors, Materials, and Waste

Defense Industrial Base

Communication

Energy

Chemical

Government Facilities

Critical Manufacturing

Healthcare and Public Health

Information Technology

Food and Agriculture

Financial Services
Technical drivers for protection

- Public and private sector enterprises are **highly dependent** on information systems to carry out their missions and business functions.
- Industrial Control System (ICS) evolution has transformed traditionally closed systems into open and internet-connected ones, putting critical national **infrastructure at risk**
  - It is difficult to differentiate attacks from malfunctions
- Enterprise systems including: Customer Information Systems, Asset Management Systems, GIS, and Back Office Analytics, are interfacing through networks and accessing and drawing data from ICSs.
- To achieve mission and business success, enterprise information systems must be **dependable** in the face of serious cyber threats.
- To achieve information system dependability, the systems must be appropriately **protected**.
Water/Wastewater sector – Attack example

Vitek Boden worked for Hunter Watertech, an Australian firm that installed SCADA radio-controlled sewage equipment for the Maroochy Shire Council in Queensland, Australia (a rural area of great natural beauty and a tourist destination)

– Applied for a job with the Maroochy Shire Council
– Walked away from a “strained relationship” with Hunter Watertech
– The Council decided not to hire him
– Boden decided to get even with both the Council and his former employer

• Maroochy Shire Council had no existing information security policies, procedures, nor cyber security defenses
• On at least 46 occasions Boden issued radio commands to the sewage equipment
  – Caused 800,000 liters of raw sewage to spill out into local parks, rivers and even the grounds of a Hyatt Regency hotel
  – Marine life died, the creek water turned black and the stench was unbearable for residents
The Water and Wastewater Systems Sector is vulnerable to:
- Natural disasters
- A variety of attacks, including:
  - Contamination with deadly agents
  - Physical attacks (such as the release of toxic gaseous chemicals)
  - Cyberattacks

Denial of service in Water and Wastewater System Sector would impact:
- Critical services: firefighting and healthcare (hospitals),
- Other sectors: Energy, Food and Agriculture, and Transportation Systems

**Attack impacts:**
- Large numbers of illnesses or casualties

**Denial of service impacts:**
- Public health
- Economic vitality

Needs for InfoSec driven by:
- Regulatory
- Financial (save or earn $)
- Political
- Environmental/Social benefit
- Reputation
- Technological need
- Other

~153,000 public drinking water systems
- >80% of U.S. population receives their potable water from these drinking water systems

>16,000 publicly owned wastewater treatment systems
- ~75 percent of the U.S. population has its sanitary sewerage treated by these wastewater systems

Federal Information Security Management Act of 2002
Federal Information Security Modernization Act of 2014

Recognize importance of information security to U.S. economy and national security

• Require each federal agency to provide information security
  – For information and information systems supporting their operations and assets
    – Including those provided or managed by another agency, contractors, or other source

https://www.dhs.gov/fisma
FISMA - Federal Information Security Management Act defines “Information security” as protection of...

- Confidentiality, integrity, and availability (“CIA”) of data and information
- Data, information and information systems from unauthorized...

- Access, use, disclosure = Confidentiality
- Modification = Integrity
- Disruption or destruction = Availability
What is NIST?

– Non-regulatory agency of the United States Department of Commerce
– Measurement standards laboratory

Mission: *Promote innovation and industrial competitiveness*

• NIST's activities organized as laboratory programs:
  – Nanoscale Science and Technology, Engineering, Neutron Research, Material Measurement, Physical Measurement...
  – Information Technology

*NIST is responsible for developing standards, guidelines, and associated methods and techniques for providing adequate information security for all agency operations and assets (excluding national security systems)*
The selection and specification of security controls for an information system is accomplished as part of an organization-wide information security program that involves the management of organizational risk—that is, the risk to the organization or to individuals associated with the operation of an information system. The management of organizational risk is a key element in the organization's information security program and provides an effective framework for selecting the appropriate security controls for an information system—the security controls necessary to protect individuals and the operations and assets of the organization.
MIS 5206 Protecting Information Assets

Diagram:

- **Risk Governance**: Ensure that IT risk management practices are embedded in the enterprise, enabling it to secure optimal risk-adjusted return.
  - Integrate With ERM
  - Establish and Maintain a Common Risk View
  - Make Risk-aware Business Decisions

- **Business Objectives**: Communication
  - Manage Risk
  - Articulate Risk
  - React to Events

- **Risk Response**: Ensure that IT-related risk issues, opportunities, and events are addressed in a cost-effective manner and in line with business priorities.

- **Risk Evaluation**: Ensure that IT-related risks and opportunities are identified, analyzed, and presented in business terms.
Holistic Approach to Information Security Risk Management

ISACA RiskIT

NIST Risk Management Framework
No Class 1 QUIZ
Next time (001)...

<table>
<thead>
<tr>
<th>Class #</th>
<th>Readings</th>
<th>Class Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>• Vacca Ch.1 “Building a Secure Organization”</td>
<td>9/7</td>
</tr>
<tr>
<td></td>
<td>• ISACA Risk IT Framework, pp. 1-42</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• NIST Reading 1: “Framework for Improving Critical Infrastructure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cybersecurity”</td>
<td></td>
</tr>
</tbody>
</table>
Reading questions for next time...

1. Do ITACS students represent information security vulnerabilities to Temple 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 the nature of the problem in the context(s) you chose

3. What is quantitative information security risk analysis? Provide an example of a measurement used in quantitative information security risk analysis. What challenges are involved in calculating such a measurement?
Next time (001)...

<table>
<thead>
<tr>
<th>When</th>
<th>Actor</th>
<th>Task</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Friday</td>
<td>Instructor (me)</td>
<td>Post reading questions (Friday am)</td>
<td></td>
</tr>
<tr>
<td>Sunday 11:59pm</td>
<td>Student</td>
<td>Post answers to reading questions</td>
<td>Assignment</td>
</tr>
<tr>
<td>Tuesday 11:59am</td>
<td>Student</td>
<td>Post 4 comments to others’ answers</td>
<td>Participation</td>
</tr>
<tr>
<td>Tuesday 11:59am</td>
<td>Student</td>
<td>Post “In The News” article</td>
<td>Participation</td>
</tr>
<tr>
<td>Wednesday 9am-12:30pm</td>
<td>Both of Us</td>
<td>Class meeting</td>
<td>Participation</td>
</tr>
<tr>
<td>Thursday</td>
<td>Instructor</td>
<td>Post summary notes</td>
<td></td>
</tr>
</tbody>
</table>
Agenda

• Welcome - introductions
• Course Objectives
• Textbook and Readings
• Grading
  – Assignments
  – Participation in class and online
  – Team Presentation
  – Exams
• Class Web Site “Blog”
• Quizzes
• Semester Schedule
• Weekly Rhythm
• Typical Class Session
• Week 1: Risk Management
• Next time...
Protecting Information Assets
Week 1