BIS Security Management

- Syllabus
- Schedule
- Course Intro
- Assignments
  - Wardriving
  - Network Address Translation
  - Shodan
- Project
  - Overview
  - Deliverable 1
  - Deliverable 2
- Notes
  - Day 1 - Introduction
  - Day 2 - Chapter 1
  - Day 3 - Chapter 13
  - Day 4 - Ch13 cont. & Ch 11
  - Exam 2 notes

Syllabus

MW 2:00-3:15pm McCool 202

Instructor: Dr. Kent Marett **E-Mail:** kmarett@business.msstate.edu I check my email several times daily. Will reply within 24 hours.	**Office:** McCool 302P **Virtual Office Hours:** MW 1:00-2:00 PM (or by appointment)

Course Description

Prerequisite: BIS 3233 or consent of instructor). Three hours lecture. Concepts, skills, tools and techniques involved in management of computer security as it applies to today's business environment.

Textbooks (required)

CISSP $(ISC)^2$ Certified Information Systems Security Professional Official Study Guide, 8th Edition by Chapple, Stewart, & Gibson.

ISBN: 978-1-119-47593-4

course textbook

Image not found or type unknown

You are strongly encouraged to read the suggested portions of the books before coming to class. See schedule below for details.

Software

e will complete several hands-on assignments this semester that will require the use of outside software. Where possible, we will use freeware suitable for the purpose we will need it. I will provide links to download on the course website.

Grade Appeals

I am willing to review grades. If you wish to appeal a grade, you should submit a written explanation to the instructor summarizing why you believe your grade should be modified. Appeals must be made within one week of the score being made available to you.

Exam and Assignment Policy

If, for some reason*, you must miss class, or one of the exams or quizzes, you are obligated to **contact me beforehand** so we can arrange an alternative. The same goes for dates assignments are due. There will be no makeup exams after the fact, and late assignments will likely not be accepted.

* - a university-approved reason, such as severe illness, death, job interview, participating in an athletic event, etc. See student handbook.

Assignments

There will be a few homework exercises assigned to you throughout the semester. These assignments will typically be hands-on exercises that reinforce classroom material, and depending on the assignment and should be completed individually. These details will be thoroughly described by the instructor.

Business Security Review

The semester-long project in this class will require you to work with 3 or 4 of your classmates on an Information Security Review of a business or organization. This will consist of both a written report and a class presentation detailing the various policies and procedures your chosen business has instituted with regard to safeguarding its information, information systems, and computer networks. There will be two deliverables due over the course of the semester.

Extra Credit

There may be an opportunity to earn extra points through your participation in various research projects throughout the semester. These projects may or may not come about, so I cannot guarantee this will happen. You will need to be in class to take part.

Academic Dishonesty

I will enforce university regulations regarding the MSU student honor code to their fullest. The code states “As a Mississippi State University student I will conduct myself with honor and integrity at all times. I will not lie, cheat, or steal, nor will I accept the actions of those who do.” Information is also available at this link: http://students.msstate.edu/honorcode

You will have to sign a copy of the honor code before accessing the first course assignment, and you will sign the honor code again before every exam.

Students with Disabilities

I am committed to providing assistance to help you be successful in this course. Reasonable accommodations are available for students with a documented disability. Please visit the Disability Support Services (DSS) during the first two weeks of every semester to seek information or to qualify for accommodations. All accommodations **MUST** be approved through the DSS office (01 Montgomery Hall). Call (662) 325-3335 to make an appointment with a disability counselor.

Title IX

MSU is committed to complying with Title IX, a federal law that prohibits discrimination, including violence and harassment, based on sex. This means that MSU’s educational programs and activities must be free from sex discrimination, sexual harassment, and other forms of sexual misconduct. If you or someone you know has experienced sex discrimination, sexual violence and/or harassment by any member of the University community, you are encouraged to report the conduct to MSU’s Director of Title IX/EEO Programs at 325-8124 or by e-mail to titleix@msstate.edu. Additional resources are available at http://www.msstate.edu/web/security , or at http://students.msstate.edu/sexualmisconduct .

Classroom Technology Policy

This is a BIS course, and it is understood that many students will want to use personal technology devices (laptops, tablets, phones, etc.) to access materials during class. I am fine with that as long as you are not distracting others and that you are actually using a device for class purposes.

Recordings of lectures and other class videos are property of the instructor. They will be made available to all students signed up for the course.

For more on the university's technology policies, please see the ITS website.

Changes to the Syllabus

Any changes will be announced during class and posted on the course website. Please contact me for any clarifications.

Schedule

Date	Details		
Mon Jan 7, 2019		Course Intro	2pm to 3:15pm
Wed Jan 9, 2019		Security Governance Principles (Chap 1)	2pm to 3:15pm
Mon Jan 14, 2019		Managing Identity and Authentication (Chap 13)	2pm to 3:15pm
Wed Jan 16, 2019		Managing Identity and Authentication (Chap 13) ***NOTE: Late Start Time***	2:30pm to 3:15pm
Mon Jan 21, 2019		*** ML KING DAY ***	2pm to 3:15pm
Wed Jan 23, 2019		Securing Network Architecture (Chapter 11)	2pm to 3:15pm
		Wardriving	due by 11:59pm
Mon Jan 28, 2019		Securing Network Architecture (Chapter 11)	2pm to 3:15pm
Wed Jan 30, 2019		Securing Communications (Chap 12)	2pm to 3:15pm
		Deliverable 1	due by 11:59pm

Date	Details		
Mon Feb 4, 2019		Securing Communications (Chap 12)	2pm to 3:15pm
Wed Feb 6, 2019		Physical Security (Chap 10)	2pm to 3:15pm
		Network Address Translation	due by 11:59pm
Mon Feb 11, 2019		Security Management Decisions (Chap 16)	2pm to 3:15pm
Wed Feb 13, 2019		Midterm Exam #1	due by 3:15pm
Mon Feb 18, 2019		Malicious Code and Application Attacks (Chap 21)	2pm to 3:15pm
Wed Feb 20, 2019		Malicious Code and Application Attacks (Chap 21)	2pm to 3:15pm
Mon Feb 25, 2019		Data and Application Security (Chap 7)	2pm to 3:15pm
Wed Feb 27, 2019		Data and Application Security (Chap 20)	2pm to 3:15pm
		Deliverable 2	due by 11:59pm
Mon Mar 4, 2019		Cryptography (Chap 6)	2pm to 3:15pm
Wed Mar 6, 2019		Private Key Encryption (Chap 7)	2pm to 3:15pm

Date	Details		
Mon Mar 11, 2019		*** SPRING BREAK ***	2pm to 3:15pm
Wed Mar 13, 2019		*** SPRING BREAK ***	2pm to 3:15pm
Mon Mar 18, 2019		Review	2pm to 3:15pm
Wed Mar 20, 2019		Midterm Exam #2	due by 3:15pm
Mon Mar 25, 2019		Personnel Security (Chap 2)	2pm to 3:15pm
Wed Mar 27, 2019		Risk Assessment (Chap 2) ***NOTE: Late Start Time***	2:30pm to 3:15pm
Mon Apr 1, 2019		Business Continuity Planning (Chap 3)	2pm to 3:15pm
Wed Apr 3, 2019		Disaster Recovery Planning (Chap 18)	2pm to 3:15pm
Mon Apr 8, 2019		Security Assessment and Testing (Chap 15)	2pm to 3:15pm
Wed Apr 10, 2019		Law, Regulations, and Compliance (Chap 4)	2pm to 3:15pm
Mon Apr 15, 2019		Social Engineering (Chap 14)	2pm to 3:15pm
Wed Apr 17, 2019		*** Group Presentations ***	2pm to 3:15pm

Date	Details		
Mon Apr 22, 2019		*** Group Presentations ***	2pm to 3:15pm
Wed Apr 24, 2019		*** Group Presentations ***	2pm to 3:15pm
Tue Apr 30, 2019		Final Exam	due by 6pm

Course Intro

A university course in information security would normally be thought to reside in a computer science department, or in a college of engineering. But this particular course is housed in the College of Business for good reason. As you will see this semester, the strength of a firm's information security program often comes down to a business decision. "Is there enough bang for the buck?" as the cool kids say.

Take the world's largest hotel chain Marriott (Links to an external site.)Links to an external site., for instance. At least five million unencrypted passport numbers (very useful for identity theft) and over eight million credit card numbers (very useful for regular theft) were taken in a breach of one of its acquisition's (Starwood Hotels) guest databases. Marriott is phasing all of the legacy data into its better protected systems, but we will be left wondering why the data had not been protected all along. I hate to pass judgement until all of the facts are in, but if I had to guess, it will likely come down to a monetary decision made years ago. Many firms, large and small, have been victimized as a result of trying to fly under the radar to save a little money.	Marriott Image not found or type unknown

Atlanta.jpg Image not found or type unknown	Sometimes a little investment can save a lot of heartache down the road. Ask the city of Atlanta (Links to an external site.)Links to an external site.. The people behind its ransomware infection of municipal information systems asked for $50,000, but the city was unable (or unwilling) to decrypt its data, and it is now costing well over $2 million to recover everything. They will be less vulnerable once the city implements reliable backup operations, but a lot of time, effort, and profanity has been poured into restoring normal order.

I assure you, many of the businesses you transact with are also facing the same decisions. You trust them with valuable personal and financial information. What have they decided to do?

We will find out this semester! Enjoy!

Assignments

Assignments

Wardriving

- Due Jan 23 by 11:59pm
- Points 100
- Submitting a text entry box
- Available Jan 7 at 12am - Apr 30 at 11:59pm 4 months

Note: This lab should be conducted on a machine with a working wireless network card.

Also note: I have used some of these applications for years and have never had a problem (virus, spyware, etc.) with them. Still, assessing them with an anti-malware scan is always the safest idea. Beware any homebrew applications that are available online.

Final Note: Avoid using Kismet or any similar packet capturing software. We want to detect, not collect.

One of the most popular free applications that can be used with wireless networks is network locating software. To complete this assignment, you will need to use software of this nature. Using the software will give you information about the networks around you, including whether or not certain networks are utilizing security features. If you do utilize this software, **do not try accessing any of the open networks** you will likely find. That could well be illegal in your area.

- If you use Windows XP, you can download and install the “NetStumbler 0.4.0” software at netstumbler.com (Links to an external site.)Links to an external site.. It is located under the Downloads link at the top of the page.
- If you use Windows 10 (and 7, 8, and Vista), try “Vistumbler v10.6.4” at vistumbler.net (Links to an external site.)Links to an external site. . The download link is at the very top of page. I have been unable to test this with Windows 8.
- For Mac users, Apple offers AirRadar 3.1.9 at https://itunes.apple.com/us/app/airradar/id414758651?mt=12 (Links to an external site.) Links to an external site.. This used to be free, but now Apple appears to be charging $9.99 for it. Try to avoid doing this if you can (unless you think it would be fun to own).

There may be free options available for your mobile devices. Consult iTunes, Google Play, or whatever app market may apply. I cannot personally vouch for anything other than the three above though.

Windows XP: NetStumbler The screencap shows the blank slate that you begin with. Once your wireless NIC has been detected, NetStumbler should automatically begin locating wireless APs within range. If it doesn't start automatically, click the green "Play" button.	NetStumbler Image not found or type unknown
Vistumbler The Scan APs button in the top left corner will begin the search for wireless networks.	Vistumbler Image not found or type unknown
AirRadar (for Mac) The Start Scan/Stop Scan button is in the upper right corner. Pretty straight forward.	AirRadar Image not found or type unknown

As you'll see, there will be a number of rows and columns that will soon populate. Some of the columns include:

MAC Address: The unique identifier for the AP network interface card.

SSID: Service Set Identifier, also known as the "network name."

Encryption: The type of security implemented on this particular wireless network. This may include WEP, WPA, EAP, or something similar.

To submit the assignment, please report the following information below:

- Date of the wardrive
- Location of the wardrive
- Software and device used
- In percentages:
  - How many of the detected networks have the default SSID (i.e. it has not been changed by the owner)?
  - How many of the detected networks had some type of encryption enabled?
- What different channels are the detected networks broadcasting on?
- Judging from info you gathered, how many 802.11 a, b, g, n, and ac networks did you detect?
- Any other observations or strange occurrences to report?

Assignments

Network Address Translation

Instructions: Run a test of your network address translation using the instructions on page 549 of our textbook. You will need to be connected to a network.

Please report your results for the assignment. There are no right or wrong answers, so report your results faithfully, whatever they may be.

1. Define Network Address Translation.
2. What is the IP address of the computer you are currently working on?

- Use the cmd program, *ipconfig* on Windows computers.
- Use the Terminal program, *ifconfig* on Mac OS

3. Is this IP address within the range of private addresses on page 550?
4. Go to IPChicken.com (Links to an external site.)Links to an external site.. What IP address do they report for your computer?
5. Do the two IP addresses match?
6. So, are you running under NAT on your current computer?
7. Any interesting/surprising observations?

More info for Mac iOS users (thanks to Mia Woods and Brooke McKee for bringing this up)

Depending on the age of your Mac, your IP address info may be displayed in different places (see image below). I have an elderly (> 8 years old) MacBook at home that displays info in the opposite location in ifconfig than where your newer Mac (< 5 years old) does. I both enabled WiFi and plugged it directly into my router with a patch cable so you can see the multiple entries below.

NAT_iOS_ports.png
Image not found or type unknown

For newer Macs, your WiFi information should be listed under the en0 entry. The IPv4 address is listed next to "inet". The entries are flipflopped on my dinosaur MacBook, but since both entries display internal IP addresses, it doesn't really matter... NAT is enabled either way. You will likely see two internal IP addresses or two "real" IP addresses if you have two connection entries, so use either one for your homework. (If you only have one connection entry, that probably means that only your wireless card is currently being used.)

Assignments

Shodan

Shodan Vulnerability Assessment & IoT

The Shodan website is a “search engine for Internet-connected devices.” There are a ton of connected devices out there that are constantly broadcasting data, video, audio, etc. This probably does not come as a huge surprise in general, but maybe it hits a little harder when the devices are close to home. This assignment will attempt to look at some IoT devices that you are personally aware of.

Instructions

1) Go to the search engine at shodan.io (Links to an external site.)Links to an external site.

2) You don’t have to log in to run an assessment, but it helps provide more comprehensive search returns, like the maps. I logged in with my Google account, but Facebook, Twitter, etc. logins are also available. The Login button is at the top right.

Device are located and identified by the content of its "banner" object. This is metadata that is publicly transmitted and includes things like SSIDs, IP addresses, etc. You should use filters when you perform a search, otherwise your search returns will be limited by the contents of a device's banner. Filters include "country:", "org:", "city:"

3) **Freestyle Search:** Search your hometown or something “close to home.” Example: city:Starkville

4) Report what you find. Can you identify any businesses, individuals, etc? What type of data seems to be broadcasting?

5) **Third Floor Search:** Run a second search, this time the IP address 130.18.86.48. What device is this? Can you tell when the SSL certificate expires on this device?

6) Now search 130.18.86.47. What about its SSL certificate?

Like most search engines, you sometimes find results that are relevant to what you are attempting to find and sometimes you don’t, but that is the spice of life, isn’t it?

Project

Project

Overview

An information security review of an existing business or organization will be performed by you and the rest of the group. My hope is that you and your group will be able to identify a business of convenience to you fairly quickly. You will also need to receive approval from the business, of course.

Obviously, this assignment will not be on the order of a full-fledged technology audit that can take months to complete and usually requires technology for testing and full access to the network infrastructure. This will be more along the lines of a general control review, and information will be gathered using less technical means, such as observation, inquiry, and possible inspection (if allowed). We are also not in a position to make security recommendations.

In addition to a couple of midterm deliverables, you will prepare a white paper and a presentation detailing policies, procedures, risk assessment, preventative hardware/software, etc. that will be given at a yet-to-be-determined time around the final week of the course. Links to the deliverable details can be found below and also under the Assignments menu option.

First Deliverable (due January 30)

Second Deliverable (due February 27)

Project

Deliverable 1

Identify the organization being reviewed. A brief description should be included. This should include information about the following

- Name of the organization (to be withheld later)
- Location
- Size and scope
- Industry type, main products and services offered
- Number of employees
- Anything relevant about the types of facilities
- If you have a point of contact already (or a probable contact), describe that

You should also include discussion about why this is an organization worthy of reviewing. Although it may be speculation at this point, what types of information assets would the organization need to protect? Do you consider them a prime target for security breaches? Any apparent vulnerabilities, either man-made or natural? *Generally speaking, if someone were to ask you, "Why review this organization?", how would you respond?* That should help produce the discussion here.

NOTE: All you have to do is describe the organization in the manner described above. There is no need to thoroughly interview anyone at this point. If you would like to provide your point of contact (or the person who would grant your group permission to perform the review) some idea of what you might be asking about, please see the 2nd deliverable description on the website. Again, for the first deliverable, merely describe the organization and justify your selection.

Reasonable expectation: around 2-3 pages

Project

Deliverable 2

In this deliverable, you should prepare an initial draft of questions that you will use in your interview(s) with your point(s) of contact. This list should include both questions that will meet the generic guidelines of the review (see below) and questions that are specific for the organization of interest. You should treat these as sort of icebreaker questions; you are by no means limited to these questions during the interview.

Section 1 of your milestone report should include a series of generic questions that could be used within pretty much every organizational setting. Questions should involve the following:

1. General information about the organization's IS infrastructure
    1. Number & type of network users (customers, suppliers, etc.)
    2. Key information assets
    3. In-house IT support, or outsourced?
    4. Type of networks (LAN, WAN, etc.)
    5. Types of communicative media and devices accommodated (wireless, Bluetooth, RFID, etc.)
2. Security Policies and Procedures (Key policies and programs already in place)
    1. Pay particular attention to how security policies are implemented. Is management involved, as in identifying key assets, best practices, etc?
    2. How often are security audits performed?
    3. Reviewing and purging unnecessary applications from the network
    4. Handling new employees entering the company
    5. Handling employees leaving the company
    6. Policies for disclosing sensitive information to persons outside the company
3. Access control systems
    1. Authentication methods
    2. Special access policies (e.g. password policies)
    3. Identifying which individuals have access to which systems and/or data
4. Risk assessment procedures
    1. Preventative measures and systems
        1. IDS, firewalls, proxy servers, data encryption, etc.
    2. VPN availability
    3. Business continuity planning (including testing)
    4. Physical security
    5. Electronic monitoring
    6. Policies for removing laptops and/or computer equipment from the premises

Section 2 should include any other questions that are specific for your particular organization. In other words, this section should be highly unique, to the extent that it would be impossible to

provide a list of concepts here. Despite the list of concepts for Section 1 above, you should spend quite a bit more time planning for Section 2.

NOTE: This deliverable is a list of questions only… **a “wish list**,” if you will. Do not provide answers to the questions in this deliverable.

Reasonable expectation: around 2-3 pages

Notes

Notes

Day 1 - Introduction

Syllabus overview and expectation of class

Nothing special

Notes

Day 2 - Chapter 1

Project

The company under review must not be associated with Mississippi State University.
Groups will be decided on Monday.

Slide Notes

This is not hacking 101.
We are trying to wrap our head around how we protect information and what business decisions are made in this process

Outline

- CIA Triad
- Other Security Concepts
- Data Classification

Security in a nutshell

Subjects are allowed or denied access to an object.

Subjects

The user/process/system requesting access to a protected resource

Objects

The protected resource

CIA Triad

Confidentiality

- Keeping information protected from unauthorized access
- Violation
  - Capturing network traffic / Eavesdropping
  - Social engineering
  - Port scanning
  - Shoulder surfing
- Relies on Integrity
  - Necessary, but not sufficient
- Previous versions of Study Guide: Most important goal for government agencies

Violation of Confidentiality

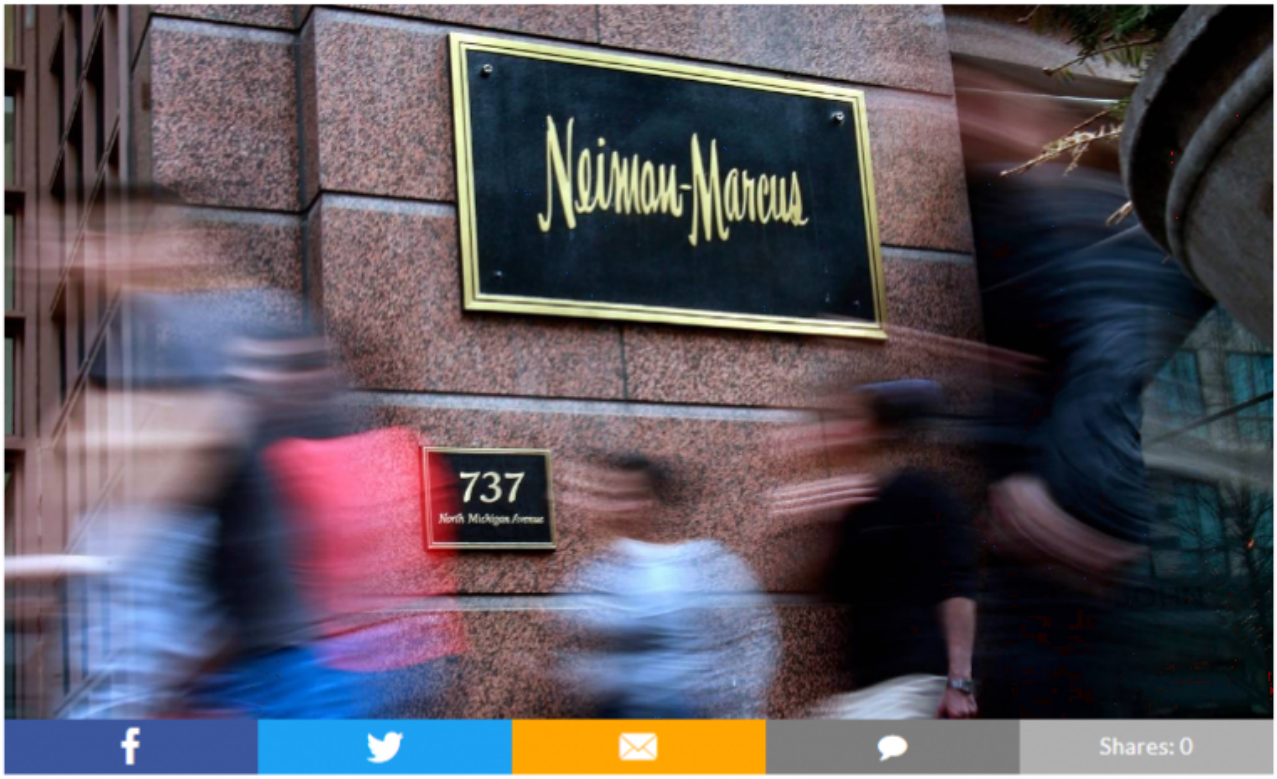
KSAT 12 Expect more.

NEWS SPORTS SA PICKS ENTERTAINMENT SA LIVE MARKETPLACE

BUSINESS

Neiman Marcus reaches a $1.5 million data breach settlement

Posted: 3:20 AM, January 09, 2019
Updated: 3:20 AM, January 09, 2019



Shares: 0

AUSTIN, Texas - More than 40 state attorneys general have announced a $1.5 million settlement with The Neiman Marcus Group LLC over a data breach the Dallas-based retailer disclosed in January 2014.

The breach exposed customer credit card data at 77 Neiman Marcus stores nationwide. Over a three-month period in 2013, about 370,000 Neiman Marcus credit cards were accessed by unknown third parties unlawfully, and at least 9,200 were used fraudulently.

Integrity

- Information can only be modified by authorized subjects
  - Information is protected from “honest mistakes”
  - Information is valid, consistent, and verifiable
- Violations
  - Viruses
  - “Logic Bombs”
  - Sabotage
- Dependent on confidentiality

Violation of Integrity

Availability

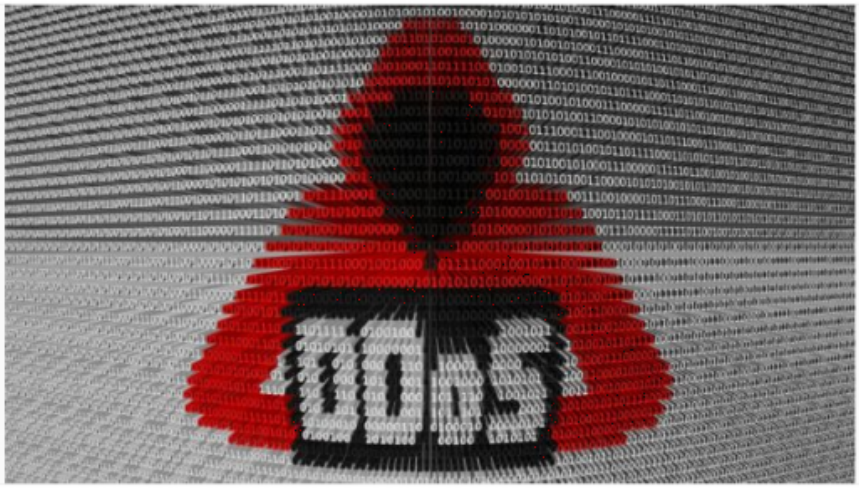
- Information is timely and accessible to subjects
  - Handles interruptions and outages
- Violations
  - Attacks (denial of service)
  - Device failure
  - Environmental issues
- Dependent on both confidentiality & integrity
- Most important goal for business organizations (p.7)

Violation of Availability

SUN STAR TIMES

Bringing People Together

About Privacy Policy Contact Us



JANUARY 7, 2019 BY ANDREA LOPEZ

Distributed Denial-Of-Service (DDoS) Protection Market Growth 2019 : Global Key Business Trends,A10 Networks, Genie Networks

The Market Research Study titled **Global Distributed Denial-Of-**

Search ...

RECENT POSTS

Global Inspection Crawlers Market to Record Rise in Incremental Opportunity During the Forecast Period (2018-2025)

CIA Triad + 1

Agility (Harvard Business School)

- “The capability to change with managed cost and speed”- Westerman and Hester
- Could affect:
  - Developing countermeasures
  - Availability
- Trade-off between agility and security?

Other Security Concepts

Privacy

- Multiple definitions
  - Freedom from being observed, monitored, or examined without consent or knowledge
- Company Monitoring
  - 4th amendment rights
- “If you gather any type of information about any person or company, you must address privacy”

Accountability

- The capability to prove a subject’s identity and track their activities

Nonrepudiation

- Ensures that the subject of an activity or event cannot deny that the event occurred
- “A suspect cannot be held accountable if they can repudiate the claim against them” (p.32)

Data Classification

A realistic means of securing data based on its “value”

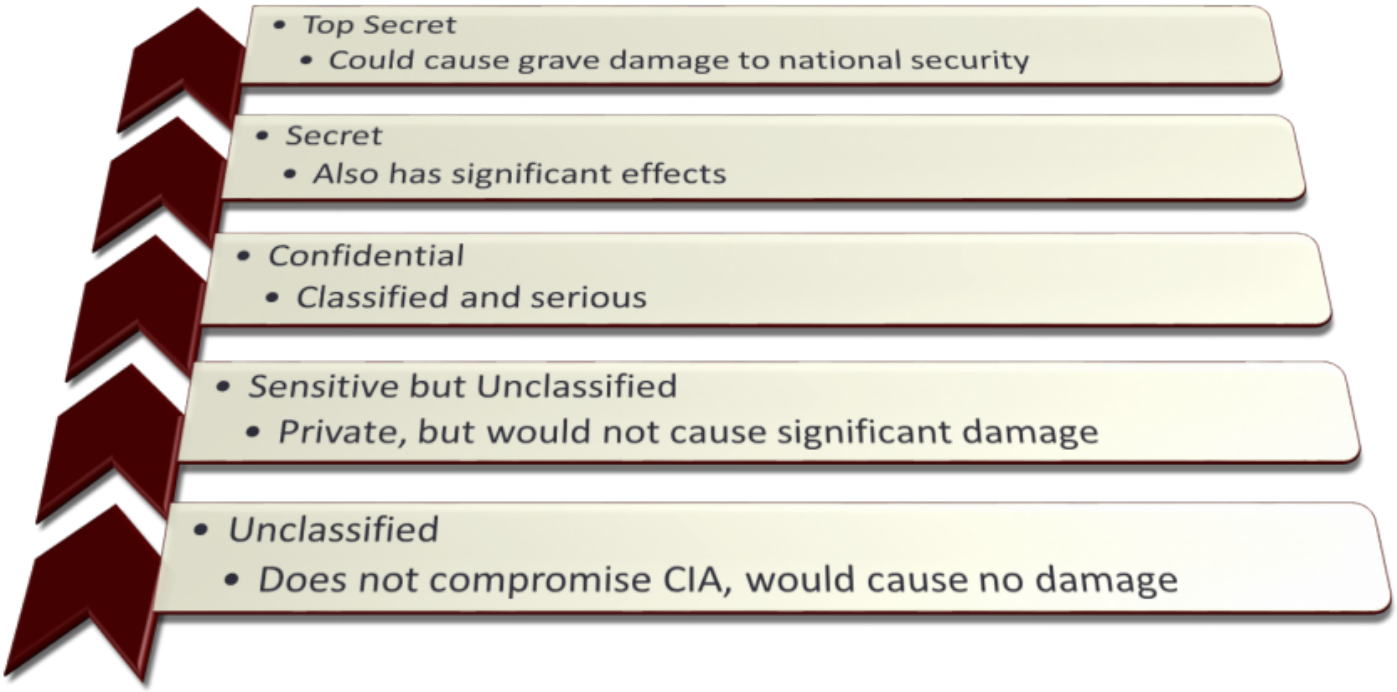
Useful for:

- Determining where best to deploy security resources
- Establishing access control and rights
- Implementing procedures for data dissemination, maturation, storage, and disposal

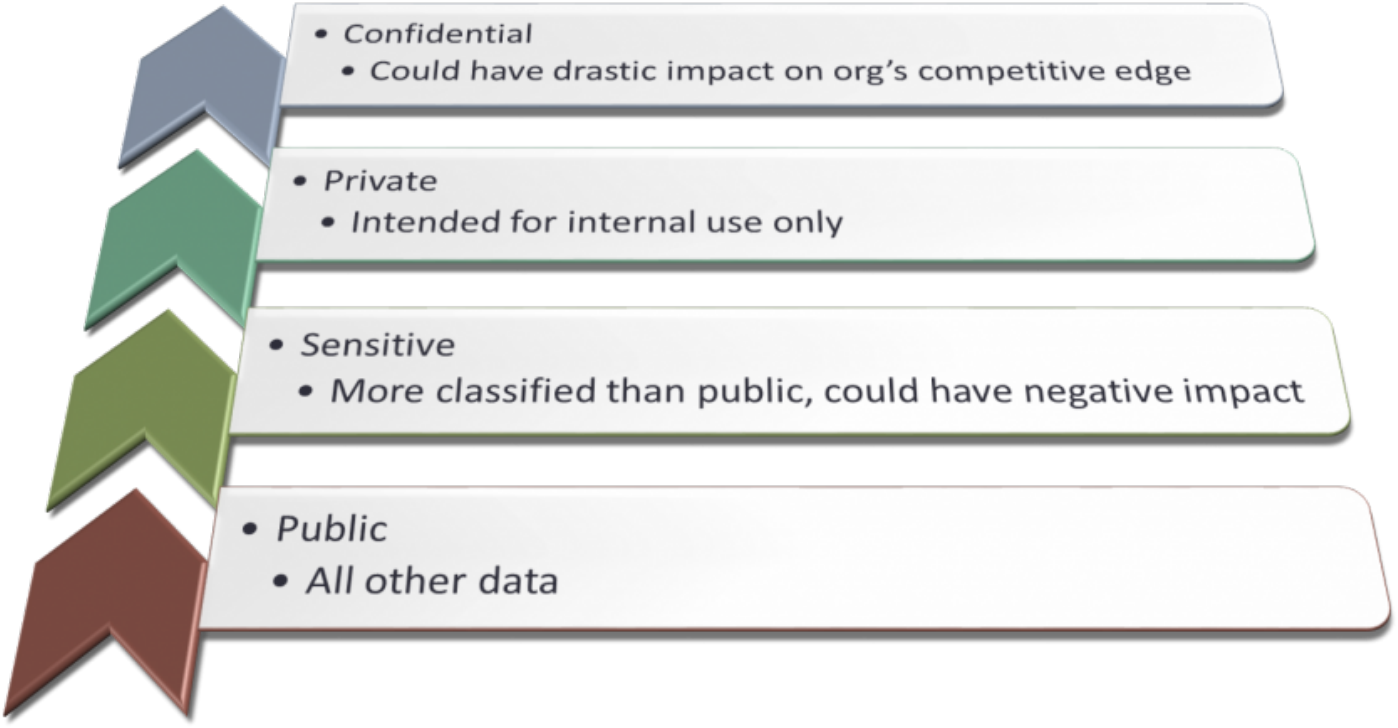
Hierarchical View of Data

Data Classification

Government/Military



Business/Corporate



Security Standards

National Institute of Standards and Technology (NIST)
International Organization for Standardization (ISO)
International Society for Automation (ISA)

Federal & State Laws

- HIPAA
- Sarbanes-Oxley / COBIT
- Banking (Gramm-Leach-Bliley Act)

Day 3 - Chapter 13

Assignments

First assignment will be discussed in next class

Notes

Notes

Day 4 - Ch13 cont. & Ch 11

Exam Hints:

Stack Layer model layers

Notes

Exam 2 notes

Four main functions of applications:

1. Input
2. Output
3. Processing
4. Storage

Chapter 21, 20,7,6
Sets 007-011