Notes

Day 1 - Introduction

Syllabus overview and expectation of class

Nothing special

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

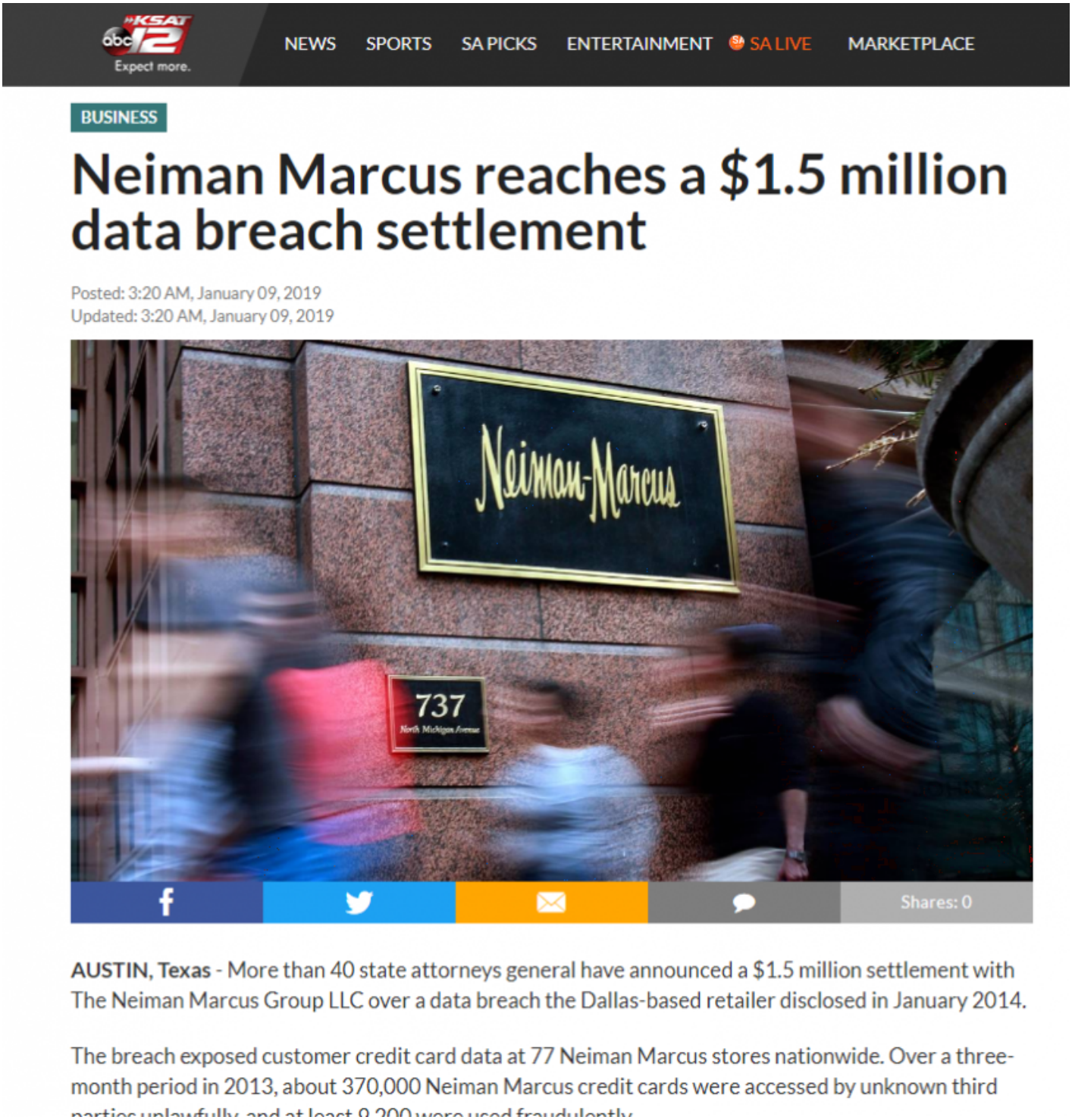
The protected resource

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

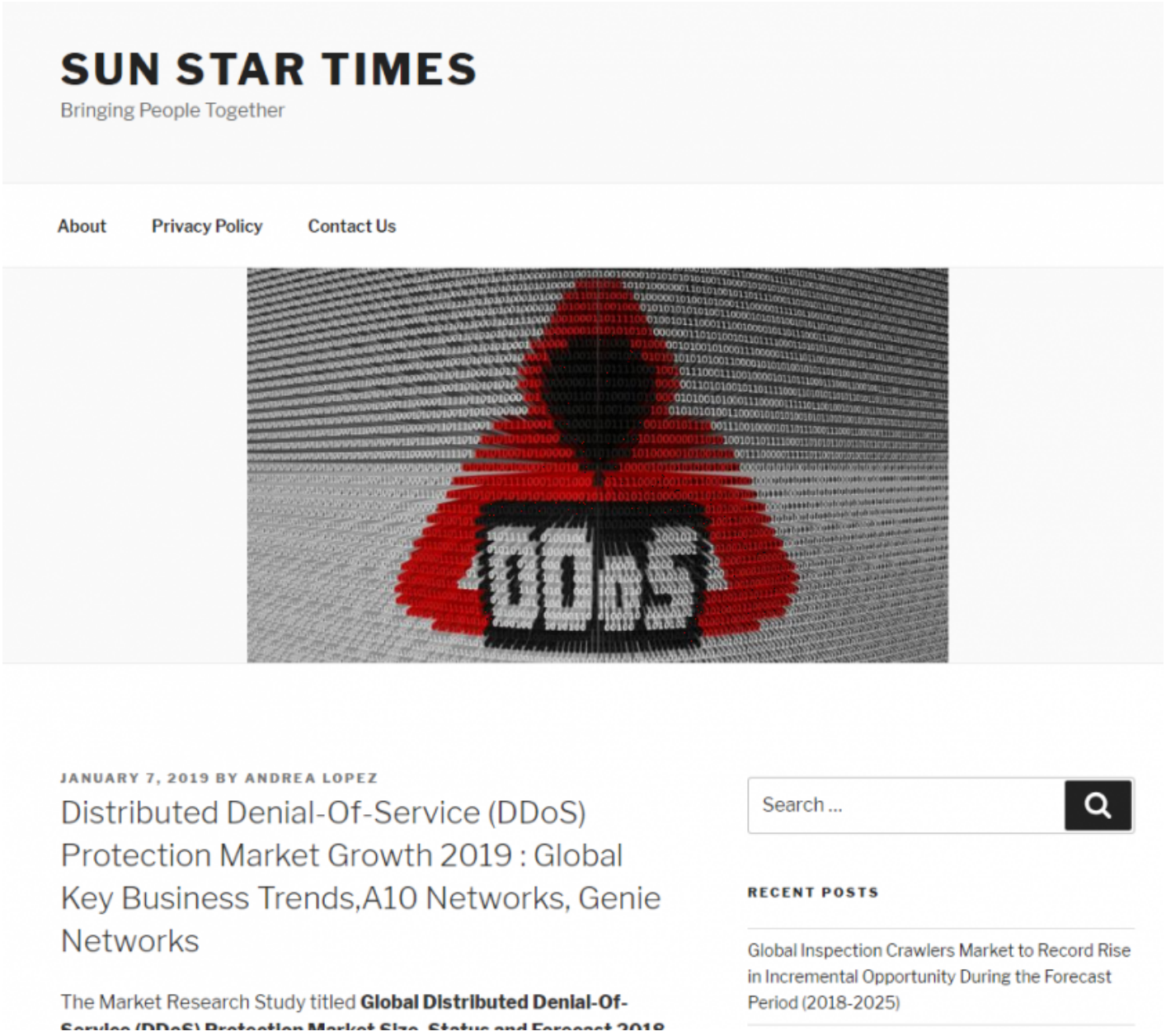
Violation of Integrity

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



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”

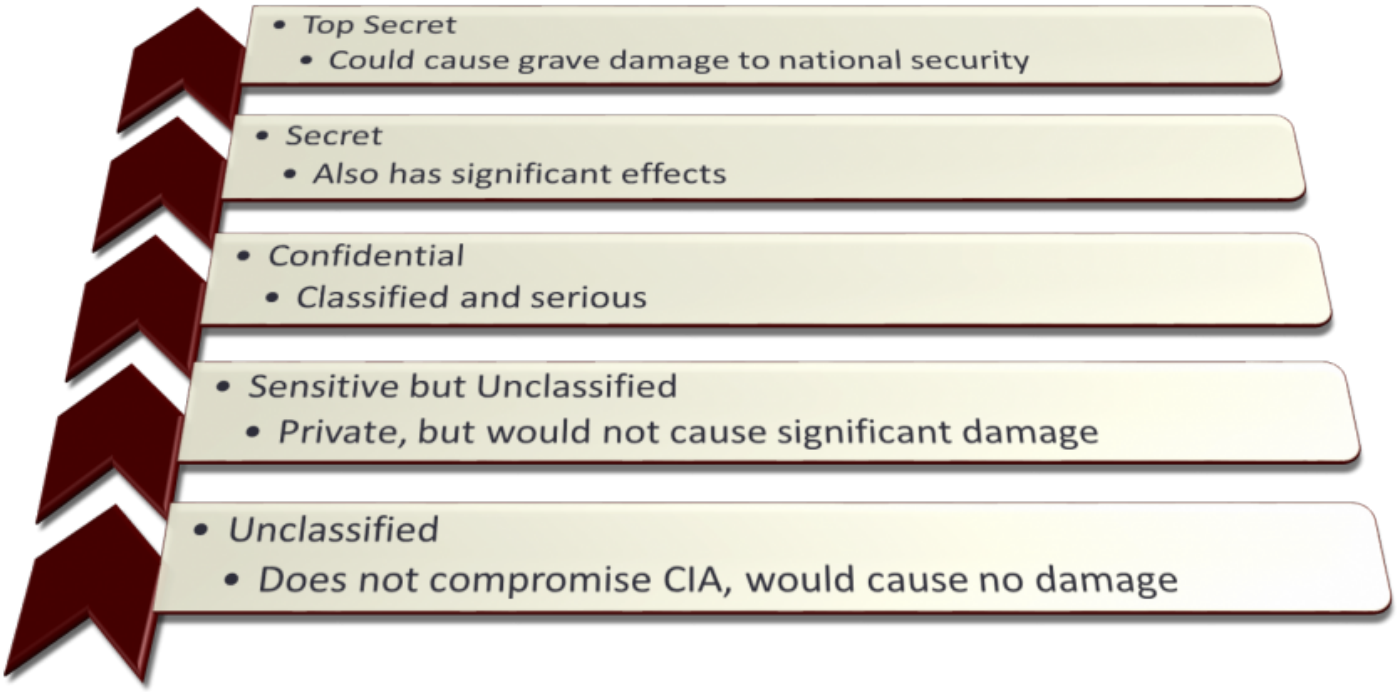
Useful for:

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

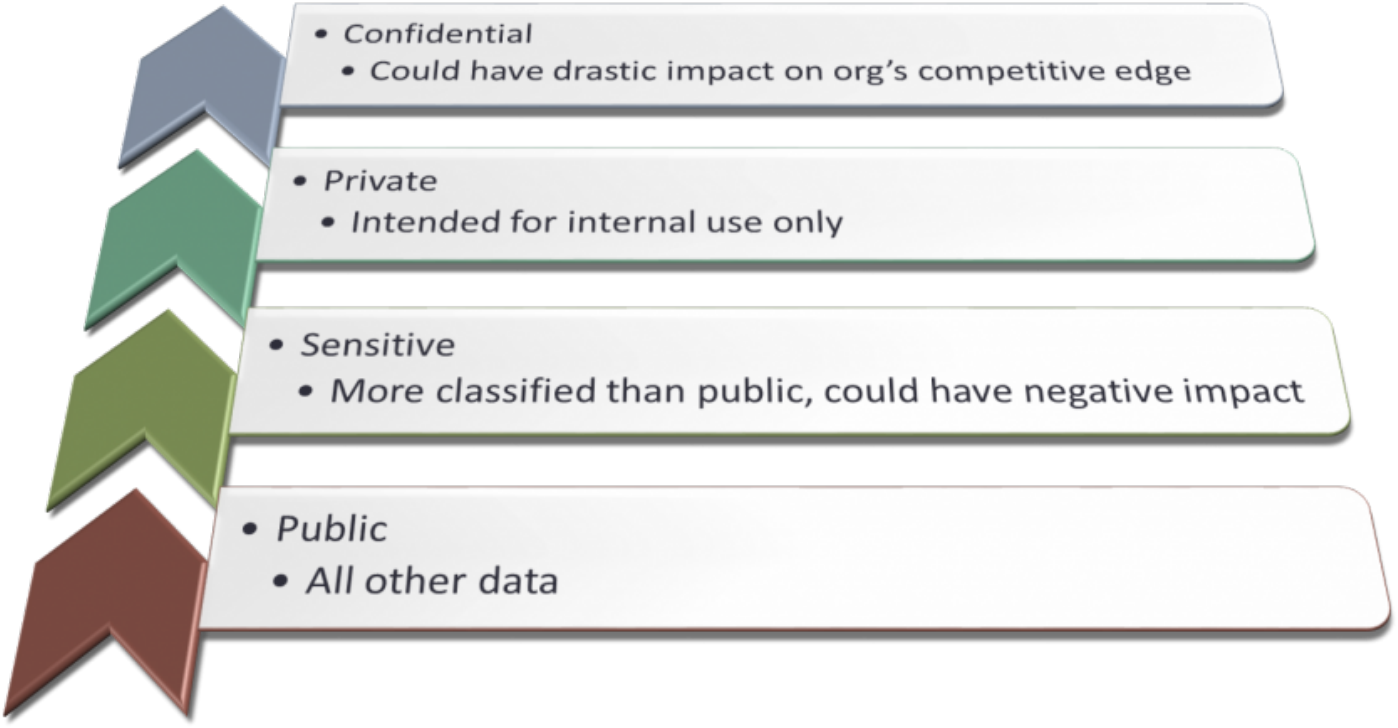
Hierarchical View of Data

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

Day 4 - Ch13 cont. & Ch 11

Exam Hints:

Stack Layer model layers

Exam 2 notes

Four main functions of applications:

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

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