

*CS 07351 –
Cybersecurity: Fundamentals, Principles, and Applications*

Week 6

Any questions from the previous week?

Chp 6



SID for Administrator

S-1-5-21-1559272821-92556266-
1055285598-500

As you can see, our SID starts with S-1-5- and ends with -500. If we can find a SID that fits that pattern, then we've found our local administrator account.

5 Government classifications

Classification	Description
Top Secret	Disclosure of top secret data would cause severe damage to national security.
Secret	Disclosure of secret data would cause serious damage to national security. This data is considered less sensitive than data classified as top secret.
Confidential	Confidential data is usually data that is exempt from disclosure under laws such as the Freedom of Information Act but is not classified as national security data.
Sensitive But Unclassified (SBU)	SBU data is data that is not considered vital to national security, but its disclosure would do some harm. Many agencies classify data they collect from citizens as SBU. In Canada, the SBU classification is referred to as protected (A, B, C).
Unclassified	Unclassified is data that has no classification or is not sensitive.



Government Access Control/Classification Models

Bell-LaPadula **addresses the confidentiality** of information.

Uses No Read Up & No Write Down

Biba **addresses integrity Uses No Read Down & No Write Up**

Clark-Wilson **addresses integrity**

Chinese Wall (aka Brewer and Nash) **addresses conflict of interest**

Safe Harbor

- European Union's Data Protection Directive creates a barrier for those countries, including the U.S., that do not meet the EU's "adequacy" requirements for data protection.
- U.S. Department of Commerce and European Commission negotiated the SAFE HARBOR to provide U.S. companies with a simple, streamlined means of complying with the adequacy requirement.

7 Safe Harbor Framework

Notice: purpose; how to contact organization; info. transferred to any 3rd parties

Choice: option to opt-out of 3rd party disclosures or purposes other than those originally collected; opt-in for other sensitive information.

Onward Transfers: to disclose info. to a 3rd party, organizations must apply NOTICE & CHOICE principles, unless its an agent & that agent either 1) complies with the SH principles or 2) is subject to the Directive or other adequacy finding or 3) enters into a written agreement with the organization. Review APEC's consent or accountability principles.

Security: reasonable precautions must be taken, but SH does not specify how.

Data Integrity: has to do w/the relevance of the purpose of use.

Access: individuals must have access except when expense of providing access is disproportionate to the individual's risk.

Enforcement: Basically the organization must have 1) verification, 2) dispute resolution & 3) remedies mechanism in place BEFORE certifying to the SH.

The top of the slide features a dark blue horizontal band. On the left side of this band, there are several lines of binary code (0s and 1s) in a lighter blue, semi-transparent font. To the right of the binary code, a faint, glowing image of a globe is visible, partially obscured by the text and the dark background.

Exploring Security Policies

Security Policies

- Written documents
- Created as an early step to mitigate risks
- Brief, high-level statements that identify goals
- Guidelines and Procedures are created later to support the policies
 - They provide details
- Security controls enforce the requirements of a security policy

Personnel Policies

- Acceptable use
- Mandatory vacations
- Separation of duties
- Job rotation
- Clean desk

Acceptable Use

- Defines proper system usage
- Includes definitions and examples of unacceptable use
 - Personal shopping on company computers
 - Web browsing
- Users must agree to the policy
 - Sometimes a written document they sign
 - Sometimes a logon banner or email

Mandatory Vacations

- Help detects fraud or embezzlement
- Often used for financial workers
- Good for administrators too
- Good examples in the Computer Fraud

Separation of Duties

- Prevents any one person from completing all the steps of a critical or sensitive process
- Prevents fraud, theft, and errors
- Accounting is designed this way
- IT systems need this protection too
 - The "all-powerful administrator" violates this principle
- Privilege Creep - is the gradual accumulation of access rights beyond what an individual needs to do their job

Job Rotation

- Employees rotate through different jobs
- They learn the processes and procedures for each job
- Helps expose dangerous shortcuts or fraudulent activity
- No one person can retain control of any process or data

Clean Desk Policy

- Keep desks organized and free of papers
- Prevents data theft or inadvertent disclosure of information
- Also presents a positive, professional image

Items Left on a Desk

- Keys
- Cell phones
- Access cards
- Sensitive papers
- Logged-in computer
- Printouts left in printer
- Passwords on sticky notes
- File cabinets left open or unlocked
- Personal items such as mail with PII

Require Administrators to Use Two Accounts

- One account for regular work, with limited privileges
- Elevated account only for administrative work

Never Use Shared Accounts

- If two users share an account, you lose these things:
 - Identification
 - Authentication
 - Authorization

Third-Party Issues

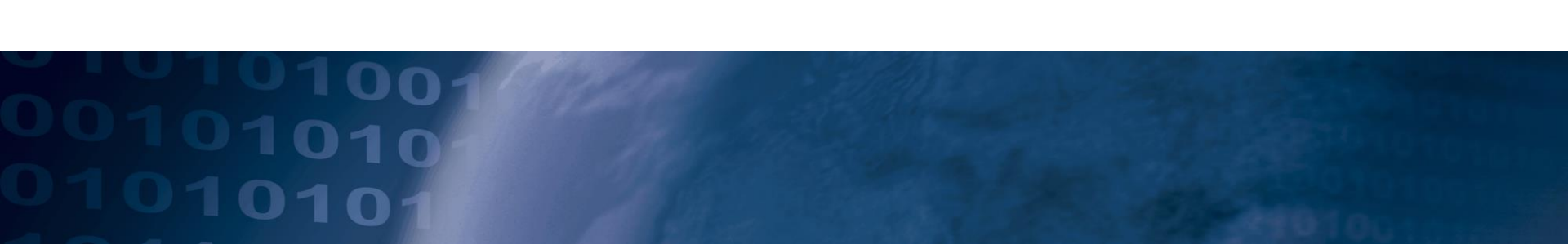
- Business partners like contractors have access to user data
- **Non-disclosure agreement**
 - Privacy considerations
 - Data ownership
 - Data backups
 - Unauthorized data sharing
 - Security policy and procedures
 - Reviews

Interoperability Agreements

- Interconnection Security Agreement (ISA)
 - Specifies technical and security requirements for a secure connection between entities
- Service Level Agreement (SLA)
 - Specifies minimum uptime and penalties
- Memorandum of Understanding (MOU)
 - Expresses an intention of working together towards a common goal
 - Defines responsibilities, but not penalties

Interoperability Agreements

- Business Partner Agreement (BPA)
 - Details each partner's obligations
 - Shares of profit or loss
 - Responsibilities
 - What to do if one partner leaves
 - Helps to settle conflicts if they arise



Understanding Cloud Computing

Cloud Computing

- Accessing computers elsewhere, usually over the Internet
- Example: Gmail
- Three specific services:
 - SaaS (Software as a Service)
 - IaaS (Infrastructure as a Service)
 - Also known as Hardware as a Service
 - PaaS (Platform as a Service)

Software as a Service

- Gmail
 - Customer can use any computer, OS, Browser
 - Service provides all the software required
- Google Docs
 - No need to have Microsoft Office yourself
- Security concern: data is now stored in the cloud

Infrastructure as a Service

- Outsource equipment requirements
- Servers, routers, switches

Platform as a Service

- Provides a computing platform with an easy-to-configure operating system
- Amazon E2C
- Customers rent virtual machines and configure them as needed

Public v. Private Cloud

- Public cloud
 - You don't own the servers
 - Ex: Amazon
 - You can't control the backups, data location, etc.
- Private cloud
 - On your own servers, in your own data center
 - More control, but more responsibility

Cloud Computing Risks

- Lose physical control of your data
- Cloud service could steal or lose your data
- Example: Dropbox failed to enforce passwords briefly in June 2011

Security Awareness

- View video
 - <https://www.youtube.com/watch?v=tmOGJVDvJaQ&index=6&list=PLNrl6cqVdDVgt7pWQenSgy7F2o6C6xrhI>
 - <https://training.knowbe4.com/login>

Change Management Policy

- Ensures that changes in IT systems don't cause unintended outages
- Provides an accounting structure to document changes
- Includes **patch management**

Change Management Process

- Change request
- Review of request
- Approval
- Technician implements change
- Every step is documented
- Plan for reversal of change if necessary

Data Policies

- Companies must protect private data
 - Research & Development
 - Customer databases
 - Proprietary information on products

Data Policies

- Types of Data Policies
 - Information classification
 - Data labeling and handling
 - Data wiping and disposing
 - Storage and retention
 - PII (Personally Identifiable Information)
 - Privacy policy for websites
 - Social media
 - P2P

Information Classification

- Identify, classify, and label data
- Gov't
 - Top Secret, Secret, Confidential, Sensitive but Unclassified, Unclassified
- Companies
 - Proprietary, Private, Classified, Public

Data Labeling and Handling

- Label media such as backup tapes
- File labels
 - Properties, headers, footers, watermarks
- Prevents accidental disclosure of confidential data during talks, etc.
- Backups need labeling and careful handling

Disclaimers

The information contained in this message may be privileged and confidential and protected from disclosure. If the reader of this message is not the intended recipient, or an employee or agent responsible for delivering this message to the intended recipient, you are hereby notified that any dissemination, distribution, or copying of this communication or use of the information contained herein is strictly prohibited. If you have received this communication in error, please notify the sender immediately by replying to the message and delete the message from your computer.

Data Wiping and Disposing

- Must clean computers before discarding or donating them
- Hard drives are the greatest risk
 - Bit-level overwrite
 - Degaussing
 - Physical destruction
- Copiers also have hard drives
- Paper must be shredded or burned

Wiping Files

- Securely erasing individual files
- File shredders are included in some antivirus products
- Must erase entire cluster to eliminate all possible fragments of a file
 - Tools
 - Darik's Boot and Nuke
 - Sites
 - <http://pcsupport.about.com/od/toolsofthetrade/tp/free-data-destruction-software.htm>

Storage and Retention Policies

- Defines what data is stored and for how long
- Reduces legal liability
 - Old data has little value, and can be required as evidence in a lawsuit

PII (Personally Identifiable Information)

- Two or more of
 - Full name
 - Birthday or birth place
 - Medical or health information
 - Address
 - Biometric data
 - SSN, Driver's License #, or any other ID #
- One item is not enough to count as PII
 - Passwords don't count as PII

PII Data Breach

- Many real data breaches each year
 - <https://www.privacyrights.org/data-breach/new>

Protecting PII

- If a company collects PII data, it must be protected
- California and many other states require notification of customers when a PII breach occurs
- Many breaches come from employees' sloppy handling of PII
 - USB sticks
 - Backup tapes
 - Files on public servers

Privacy Policy for Websites

- States how a website collects data
- Also how the data is used, and whom it is shared with
- California law requires a conspicuously posted privacy policy
 - On websites that collect information about CA residents
 - Even if the website is hosted outside CA

Social Networking

- Facebook, Twitter, etc.
- Users post personal information, including answers to security questions, such as birthday, home town, etc.
- Information can also be used in scams
- Employers search social networking sites when hiring

SSO and Social Media

- Facebook can be used to log into many other sites
- If someone gets your Facebook password, all those sites are compromised too
- Use two-factor authentication!

Banner Ads and Malvertisements

- Malware delivered through ads
- Have appeared on the New York Times and Yahoo!
- Either through hacking the servers, or simply purchasing ad space

P2P

- Peer-to-peer or file-sharing
- Used to share pirated MP3s, videos, and software
- Napster, MegaUpload, Bittorrent, Pirate Bay, etc.
- Can be blocked by content-aware firewalls
 - Also called Layer 7 Firewalls

P2P Risks

- Copyright infringement
- Bandwidth consumption
- Data leakage
 - President's helicopter plans found in Iran in 2009, shared accidentally on P2P
 - A schoolgirl found pornography on her computer that she didn't put there
 - P2P stores files for others on your system

Security Awareness and Training

- Minimizes risk posed by users
- Helps reinforce user compliance with policies
- Risks of USB drives
- Awareness and training plan needs support from senior management
- Refresher training required periodically

Role-Based Training

- Executive personnel
 - Need high-level briefings
 - Warning about whaling
- Incident response team
 - Detailed training on how to respond
 - Forensic procedures
- Administrators
- End users

Training Topics

- Security policy contents
- Keeping cipher codes private
- Acceptable use and user responsibilities
- Protection of PII
- Data labeling, handling, and disposal
- Information classification

Training Topics

- Laws, best practices, and standards
- Threat awareness
- Risky user habits like sharing passwords and tailgating
- Social networks and file-sharing

Training and Compliance Issues

- Many laws cover PII
- Other regulations may apply
 - Payment Card Industry Data Security Standard (PCI-DSS)
 - FERPA for colleges
 - FISMA for gov't entities
 - HIPAA for health-care companies
- Good site for training
 - <http://www.securingthehuman.org/>

Safe Computing Habits

- Don't click links in emails from unknown sources
- Don't open attachments in emails from unknown sources
- Be wary of free downloads
- Limit the information you post on social media
- Back up your data regularly
- Install updates and patches
- Keep antivirus software up-to-date

Why Social Engineering Works

- Scarcity
 - Convince target that this is their last chance to get something good, like an iPhone
- Urgency
 - Cryptolocker counts down your 72 hours to pay
- Familiarity/Liking
 - Social engineer builds rapport with target first, before asking for a favor

Why Social Engineering Works

- Trust
 - Social engineer builds a trusting relationship with the target
 - Finds "viruses" on your computer and offers to fix them