MIS 5206
Protection of Information Assets
- Unit #2 -

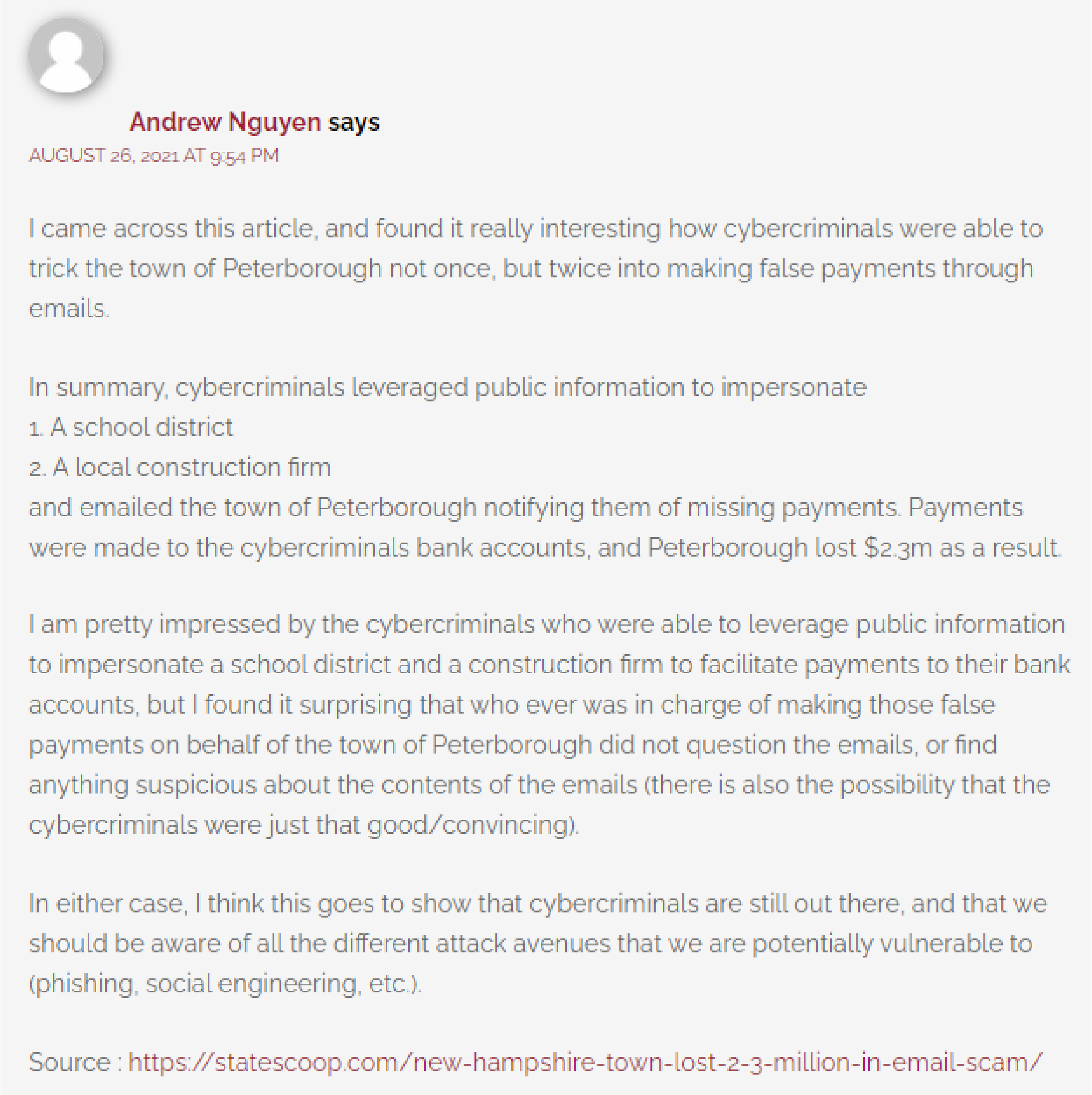
1. Case Study: Snowfall and a stolen laptop

2. Data Classification Processes and Models

Agenda

- In the News
- Case study analysis
- Data Classification Process and Models
- Test taking tip
- Quiz

In The News



Andrew Nguyen says

AUGUST 26, 2021 AT 9:54 PM

I came across this article, and found it really interesting how cybercriminals were able to trick the town of Peterborough not once, but twice into making false payments through emails.

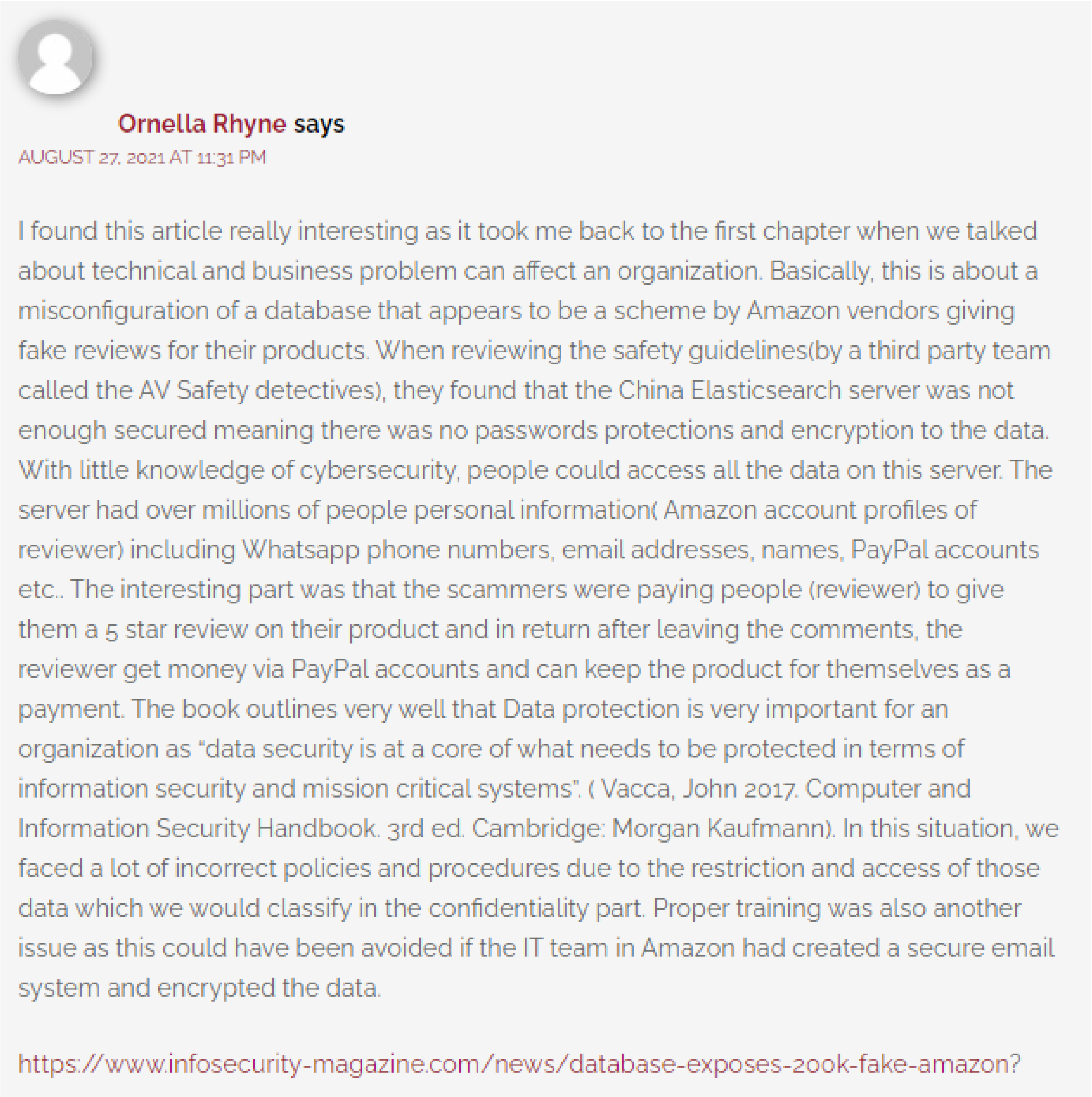
In summary, cybercriminals leveraged public information to impersonate
1. A school district
2. A local construction firm
and emailed the town of Peterborough notifying them of missing payments. Payments were made to the cybercriminals bank accounts, and Peterborough lost $2.3m as a result.

I am pretty impressed by the cybercriminals who were able to leverage public information to impersonate a school district and a construction firm to facilitate payments to their bank accounts, but I found it surprising that who ever was in charge of making those false payments on behalf of the town of Peterborough did not question the emails, or find anything suspicious about the contents of the emails (there is also the possibility that the cybercriminals were just that good/convincing).

In either case, I think this goes to show that cybercriminals are still out there, and that we should be aware of all the different attack avenues that we are potentially vulnerable to (phishing, social engineering, etc.).

Source : https://statescoop.com/new-hampshire-town-lost-2-3-million-in-email-scam/

In The News



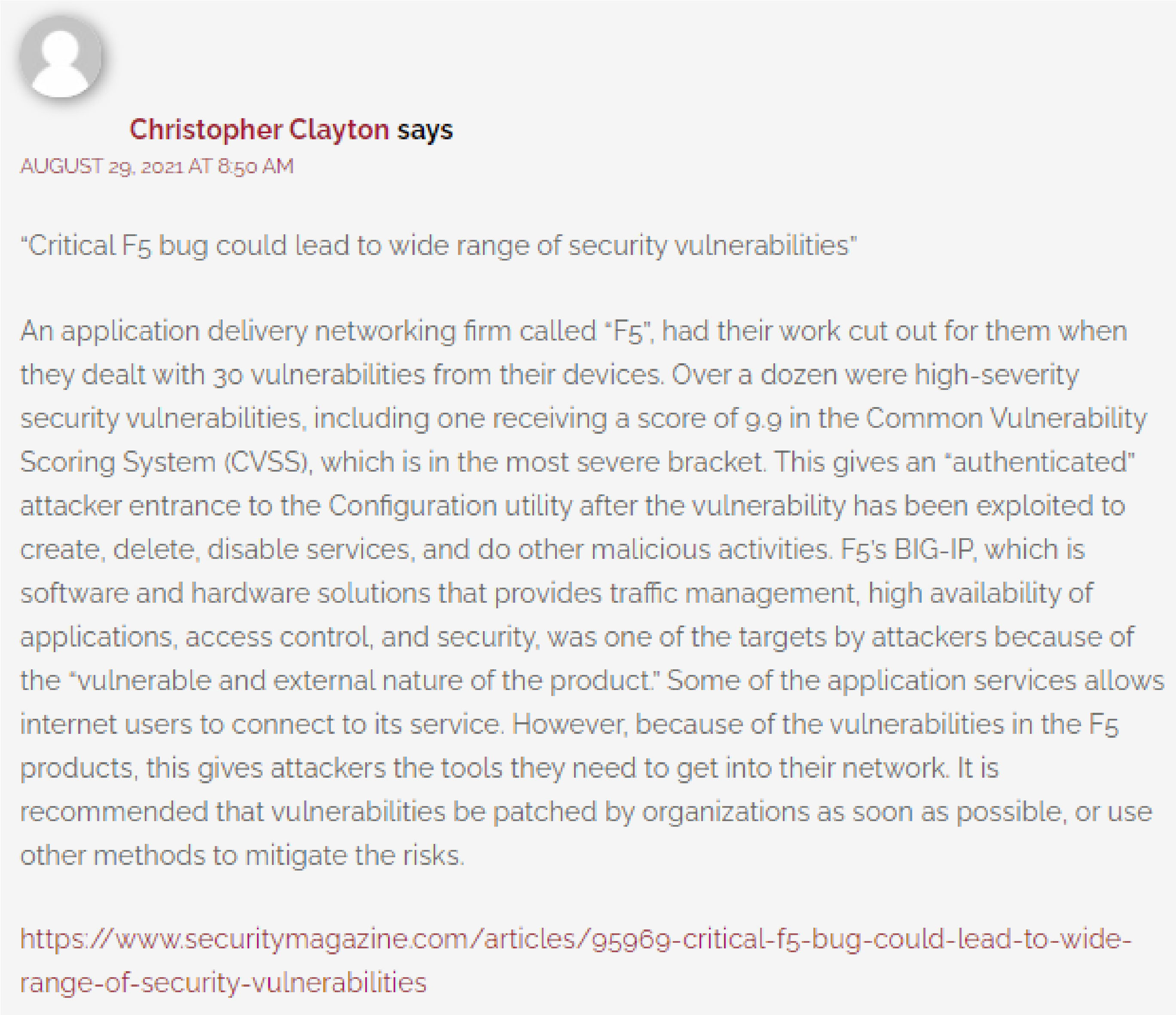
Ornella Rhyne says

AUGUST 27, 2021 AT 11:31 PM

I found this article really interesting as it took me back to the first chapter when we talked about technical and business problem can affect an organization. Basically, this is about a misconfiguration of a database that appears to be a scheme by Amazon vendors giving fake reviews for their products. When reviewing the safety guidelines(by a third party team called the AV Safety detectives), they found that the China Elasticsearch server was not enough secured meaning there was no passwords protections and encryption to the data. With little knowledge of cybersecurity, people could access all the data on this server. The server had over millions of people personal information(Amazon account profiles of reviewer) including Whatsapp phone numbers, email addresses, names, PayPal accounts etc.. The interesting part was that the scammers were paying people (reviewer) to give them a 5 star review on their product and in return after leaving the comments, the reviewer get money via PayPal accounts and can keep the product for themselves as a payment. The book outlines very well that Data protection is very important for an organization as "data security is at a core of what needs to be protected in terms of information security and mission critical systems". (Vacca, John 2017. Computer and Information Security Handbook. 3rd ed. Cambridge: Morgan Kaufmann). In this situation, we faced a lot of incorrect policies and procedures due to the restriction and access of those data which we would classify in the confidentiality part. Proper training was also another issue as this could have been avoided if the IT team in Amazon had created a secure email system and encrypted the data.

https://www.infosecurity-magazine.com/news/database-exposes-200k-fake-amazon?

In The News



Christopher Clayton says

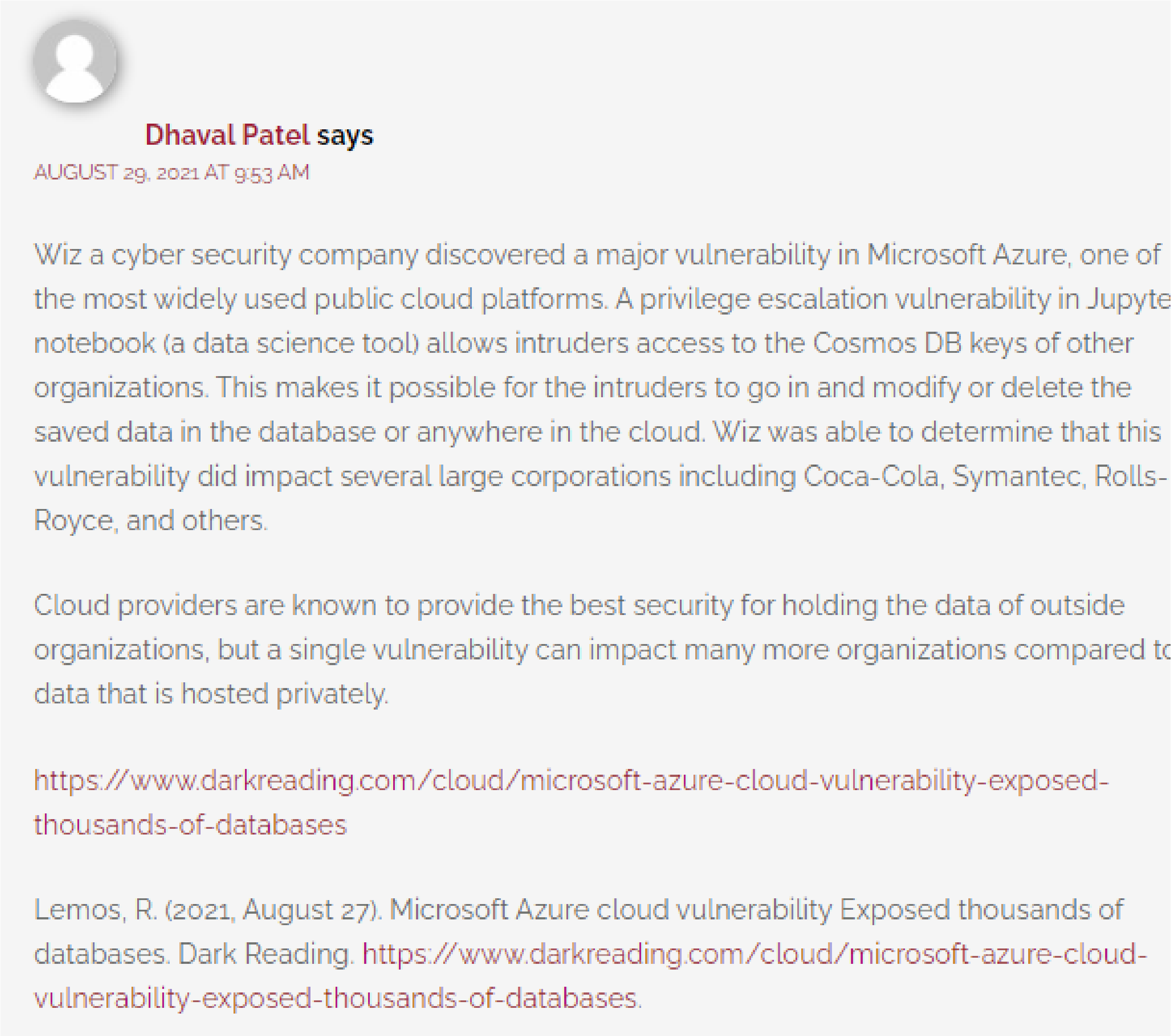
AUGUST 29, 2021 AT 8:50 AM

"Critical F5 bug could lead to wide range of security vulnerabilities"

An application delivery networking firm called "F5", had their work cut out for them when they dealt with 30 vulnerabilities from their devices. Over a dozen were high-severity security vulnerabilities, including one receiving a score of 9.9 in the Common Vulnerability Scoring System (CVSS), which is in the most severe bracket. This gives an "authenticated" attacker entrance to the Configuration utility after the vulnerability has been exploited to create, delete, disable services, and do other malicious activities. F5's BIG-IP, which is software and hardware solutions that provides traffic management, high availability of applications, access control, and security, was one of the targets by attackers because of the "vulnerable and external nature of the product." Some of the application services allows internet users to connect to its service. However, because of the vulnerabilities in the F5 products, this gives attackers the tools they need to get into their network. It is recommended that vulnerabilities be patched by organizations as soon as possible, or use other methods to mitigate the risks.

https://www.securitymagazine.com/articles/95969-critical-f5-bug-could-lead-to-wide-range-of-security-vulnerabilities

In The News



Dhaval Patel says

AUGUST 29, 2021 AT 9:53 AM

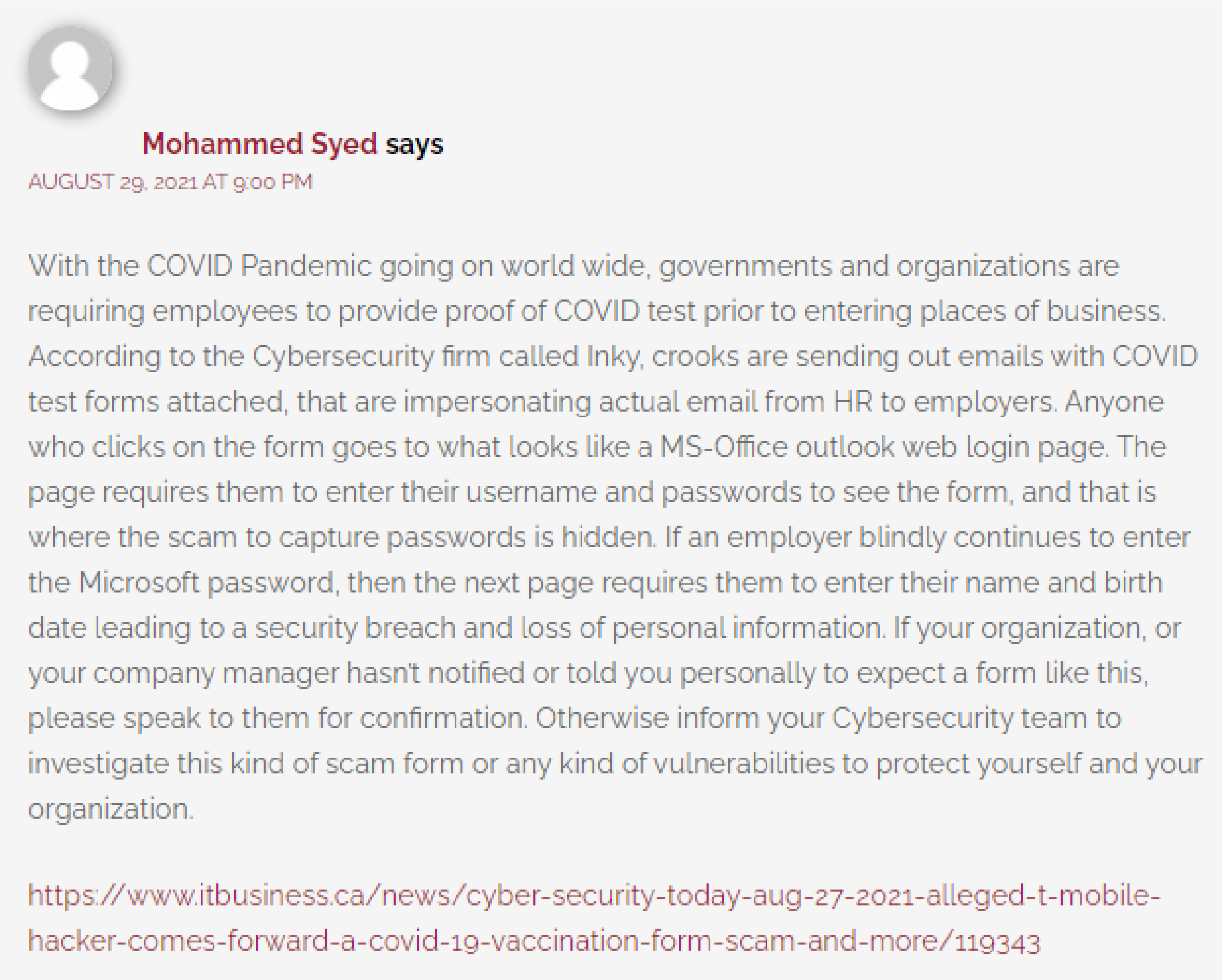
Wiz a cyber security company discovered a major vulnerability in Microsoft Azure, one of the most widely used public cloud platforms. A privilege escalation vulnerability in Jupyte notebook (a data science tool) allows intruders access to the Cosmos DB keys of other organizations. This makes it possible for the intruders to go in and modify or delete the saved data in the database or anywhere in the cloud. Wiz was able to determine that this vulnerability did impact several large corporations including Coca-Cola, Symantec, Rolls-Royce, and others.

Cloud providers are known to provide the best security for holding the data of outside organizations, but a single vulnerability can impact many more organizations compared t data that is hosted privately.

https://www.darkreading.com/cloud/microsoft-azure-cloud-vulnerability-exposed-thousands-of-databases

Lemos, R. (2021, August 27). Microsoft Azure cloud vulnerability Exposed thousands of databases. Dark Reading. https://www.darkreading.com/cloud/microsoft-azure-cloud-vulnerability-exposed-thousands-of-databases.

In The News



Mohammed Syed says

AUGUST 29, 2021 AT 9:00 PM

With the COVID Pandemic going on world wide, governments and organizations are requiring employees to provide proof of COVID test prior to entering places of business. According to the Cybersecurity firm called Inky, crooks are sending out emails with COVID test forms attached, that are impersonating actual email from HR to employers. Anyone who clicks on the form goes to what looks like a MS-Office outlook web login page. The page requires them to enter their username and passwords to see the form, and that is where the scam to capture passwords is hidden. If an employer blindly continues to enter the Microsoft password, then the next page requires them to enter their name and birth date leading to a security breach and loss of personal information. If your organization, or your company manager hasn't notified or told you personally to expect a form like this, please speak to them for confirmation. Otherwise inform your Cybersecurity team to investigate this kind of scam form or any kind of vulnerabilities to protect yourself and your organization.

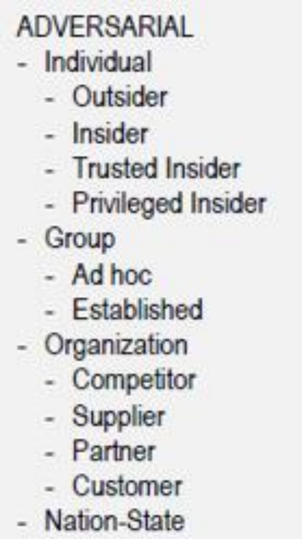
https://www.itbusiness.ca/news/cyber-security-today-aug-27-2021-alleged-t-mobile-hacker-comes-forward-a-covid-19-vaccination-form-scam-and-more/119343

Agenda

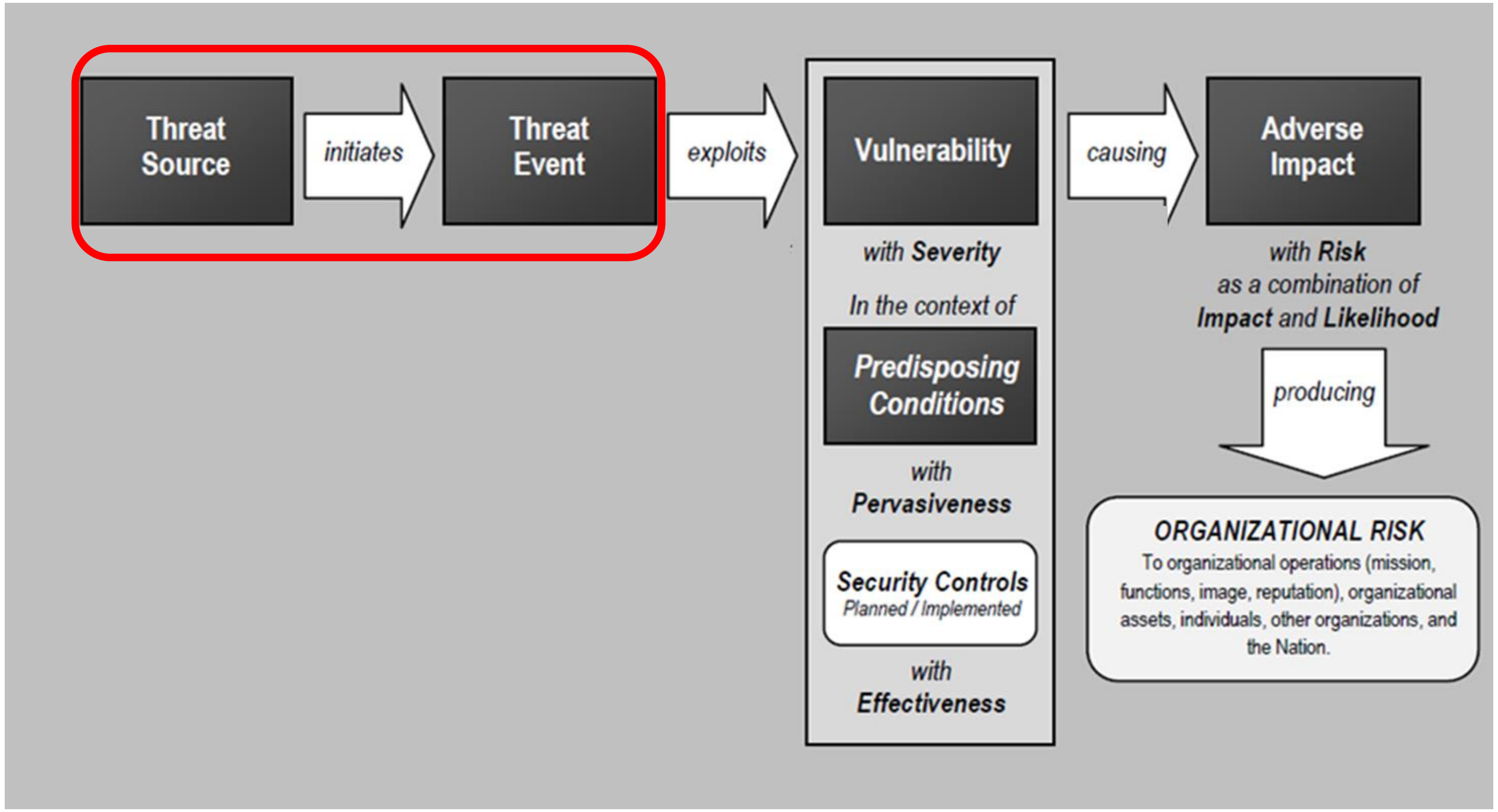
✓ In the News
- Case study analysis
- Data Classification Process and Models
- Test taking tip
- Quiz

What kind of threat was active in the case study?

- *Environmental ?*
- *Structural ?*
- *Accidental ?*
- *Adversarial ?*



ADVERSARIAL
- Individual
  - Outsider
  - Insider
  - Trusted Insider
  - Privileged Insider
- Group
  - Ad hoc
  - Established
- Organization
  - Competitor
  - Supplier
  - Partner
  - Customer
- Nation-State



NIST SP 800-30r1 “Guide for Conducting Risk Assessments”

Breakout Group Questions:

1. What information security reporting or organizational governance relationship exists between Information Security Office (ISO) and the organization(s) Ballard and Francesco report into?
2. How does RIT’s Information Classifications (Appendix F) relate to this case study scenario?
3. Was Francesco correct in his use of the term “proprietary” Saunders data” ?
4. Who else at RIT would be concerned with this stolen laptop incident?
5. Is the Information Security Office’s (ISO’s) conclusion valid that the Dean’s stolen laptop did not contain personally identifiable information on RIT students, faculty, or staff? Why or why not?

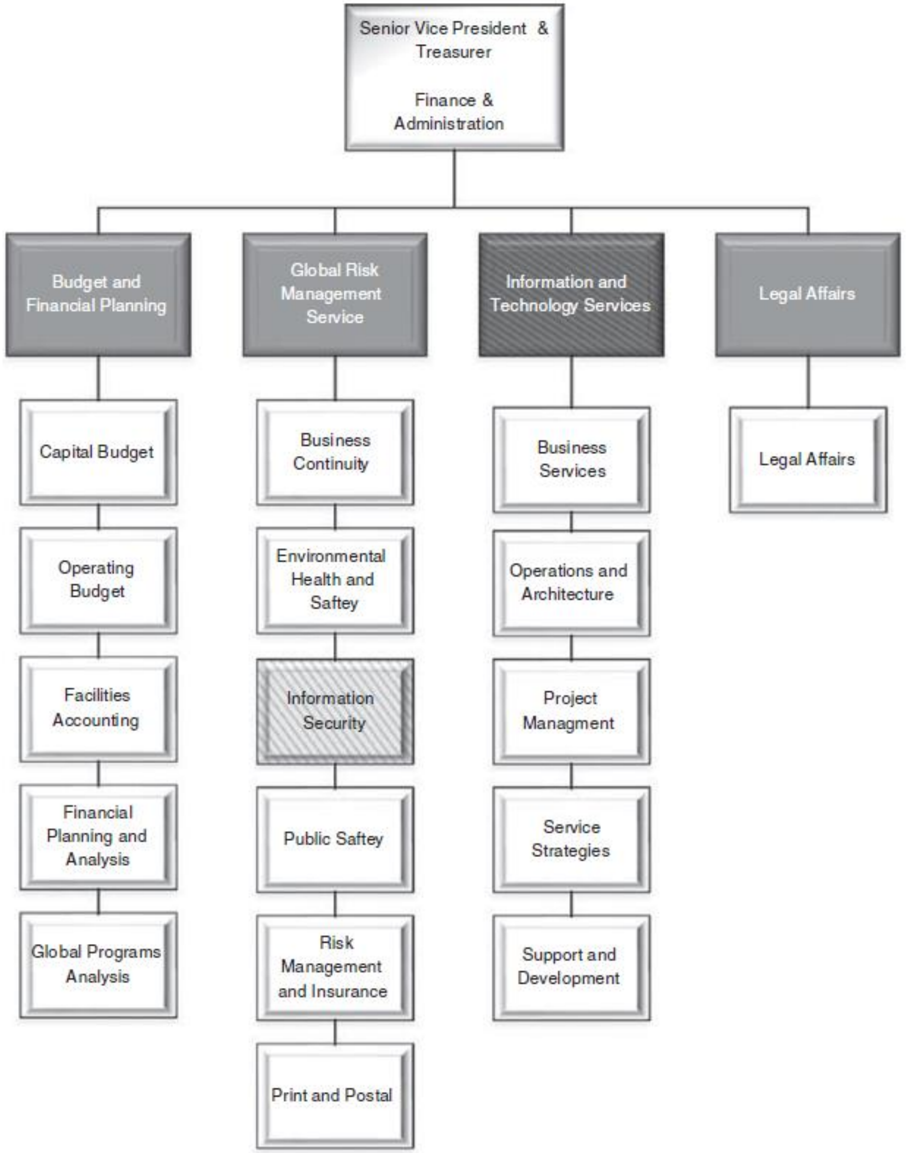
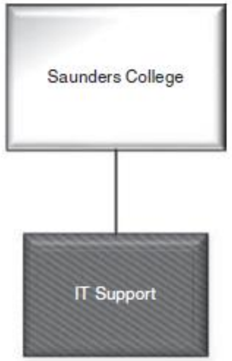


Figure C1 Partial RIT administrative organization chart.



Case Study Analysis: “Snowfall and a stolen laptop”

0. Which organization does:
    1. Dave Ballard report into?
        1. Network Administrator
    2. Nick Francesco report into?
        1. Manager of Technical Services
    3. Information Security Office (ISO) reside?

1. What information security reporting or organizational governance relationship exists between Information Security Office (ISO) and where in the organization(s) Ballard and Francesco report into?

RIT Information Classifications

A. **Private** – a classification for information that is confidential which could be used for identity theft and has additional requirements associated with its protection. Private information includes:

A. Social Security Numbers (SSNs), Taxpayer Identification Number (TIN), or other national identification number
B. Driver's license numbers
C. Financial account information (bank account numbers (including checks), credit or debit card numbers, account numbers)

B. **Confidential** – a classification for information that is restricted on a need to know basis, that, because of legal, contractual, ethical, or other constraints, may not be accessed or communicated without specific authorization. Confidential information includes:

A. Educational records governed by the Family Educational Rights & Privacy Act (FERPA) that are not defined as directory information
B. University Identification Numbers (UIDs)
C. Employee and student health information as defined by Health Insurance Portability and Accountability Act (HIPAA)
D. Alumni and donor information
E. Employee personnel records
F. Employee personal information including: home address and telephone number; personal e-mail addresses, usernames, or passwords; and parent's surname before marriage
G. Management information, including communications or records of the Board of Trustees and senior administrators, designated as confidential
H. Faculty research or writing before publication or during the intellectual property protection process.
I. Third party information that RIT has agreed to hold confidential under a contract

C. **Internal** – a classification for information restricted to RIT faculty, staff, students, alumni, contractors, volunteers, and business associates for the conduct of University business. Examples include online building floor plans, specific library collections, etc.

D. **Public** – a classification for information that may be accessed or communicated by anyone without restriction.

Francesco continued: 'Think about this carefully, because it has implications much bigger than you and me. ***What proprietary Saunders data did you have on that laptop?'***

The Dean replied, 'I really didn't have anything too important. It was committee notes, faculty salary information, stuff like that. It may have been confidential, but not really proprietary.'

2. Specifically, how does RIT's Information Classifications (Appendix F) relate to this case study scenario?

3. Was Francesco correct in his use of the term "proprietary" Saunders data" ?

4. Who else at RIT would be concerned with this stolen laptop incident?

5. Is the Information Security Office’s (ISO’s) conclusion valid that the Dean’s stolen laptop did not contain personally identifiable information on RIT students, faculty, or staff? Why or why not?

Recovering deleted data files

“On your computer, accessing "deleted" data can easily be done with one of many file undelete and data recovery programs widely available on the Internet. These programs are touted as conveniences, which in some cases, they are

  - But when it comes to security, the way your computer deletes (or doesn't delete) your data is a liability
  - Someone accessing your computer remotely (i.e. a hacker) could very easily "recover" your deleted data
  - The same goes for someone who buys your used computer on eBay or digs your discarded, failed hard drive out of the dumpster

- This has been an issue for decades. Yet still, there are no built-in system operations designed for securely deleting your data. On the contrary, Windows tends to do everything it can to keep all historical data, in case you want to perform a system restore or recover a lost file.”

https://www.r-studio.com/file-recovery-basics.html

Francesco asked ‘What student records did you have on your laptop?’
The Dean quickly replied ‘None.’

Francesco clarified: “Until recently we used Social Security numbers to identify our students. Are you sure you didn’t have any old class rosters, exams or other records on there?”

The Dean took a few seconds to deeply consider what he was asked. ‘No. I am not teaching this semester, and ***I deleted everything from previous semesters****.’*

Case Study epilogue

I. **Social security numbers were eliminated as identifiers at the University**
   - This change required modifications to every IT system used at RIT

II. **RIT implemented 2-layered approach to protecting data**
   1. New software purchased to identify (and report) potential personally identifiable information on laptops
      - *In the case of a theft, RIT was able to identify what personal information may have been at risk*
   2. RIT implemented enterprise full disk encryption technologies on laptops to limit financial risks resulting from lost Personally Identifiable Information (PII)
      - Solution included ability to report on the state of the data (i.e. report when data is decrypted)

Case Study epilogue and wrap-up

Rochester Institute of Technology (RIT)

Saunders College of Business

ROCHESTER INSTITUTE OF TECHNOLOGY · FOUNDED 1829 · ART SCIENCE INDUSTRY

RIT TIGERS

Ashok Rao

Janis Gogan • 3rd

Professor at Bentley U and President at Cases for Action

Bentley University • Harvard University

Greater Boston Area • 274

Agenda

✓ In the News

✓ Case study analysis

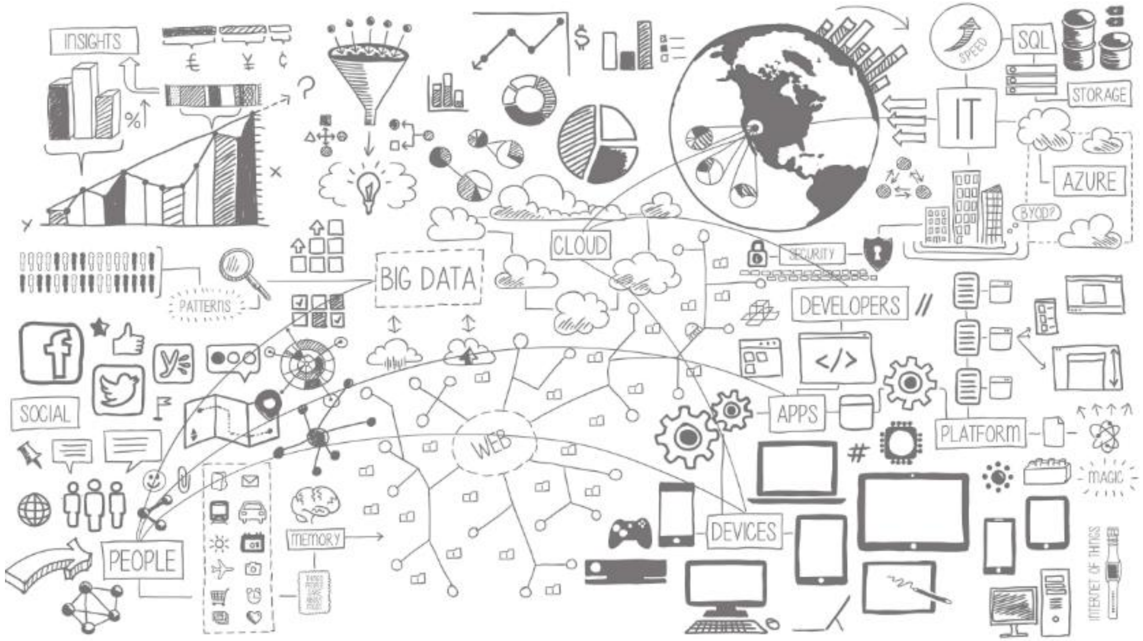
- Data Classification Process and Models
- Test taking tip
- Quiz

What is data ?

http://researchdata.ox.ac.uk/

1. Known facts or things used as a basis for inference or reckoning
2. Quantities or characters operated on by a computer etc.

The Concise Oxford Dictionary



https://blogs.microsoft.com/blog/2014/04/15/a-data-culture-for-everyone/

What is the nature of data stored in the attributes comprising the entities within the information system's databases

What is information?

An Entity's attribute values can be understood in terms of ***"measurement levels"***

Stevens, S.S. 1946. On the theory of scales of measurement. Science 103:677-680.

Measurements levels describe the inherent nature of information in the attribute data that make up entities

- **Qualitative information** tells what things exist
- **Quantitative information** orders and measures the magnitude of these things

Steven's 4 measurement levels

1. Nominal
2. Ordinal
3. Interval
4. Ratio

Scale

Increasing information content

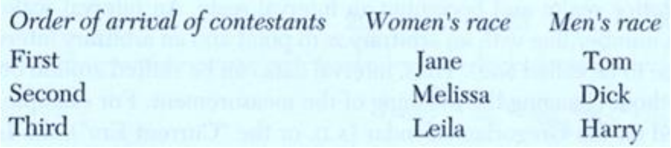
Nominal

- Defining relations
    - Equivalence
        - Class A = Class A
        - Class A <> Class B

Polka dot
Solid Color

Ordinal

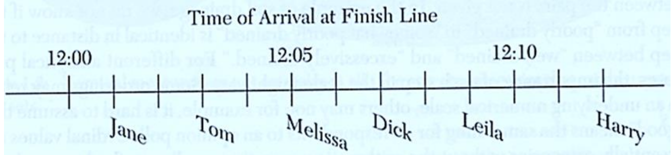
- Defining relations
    - Equivalence
    - Greater-less than
        - A > B
        - B < A



Order of arrival of contestants	*Women's race*	*Men's race*
First	Jane	Tom
Second	Melissa	Dick
Third	Leila	Harry

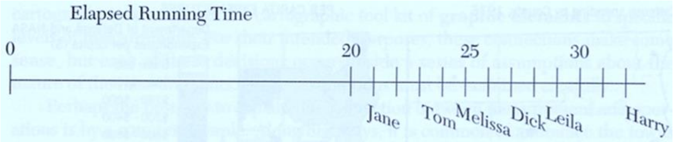
Interval

- Equivalence
- Greater-less than
- Addition and subtraction



Ratio

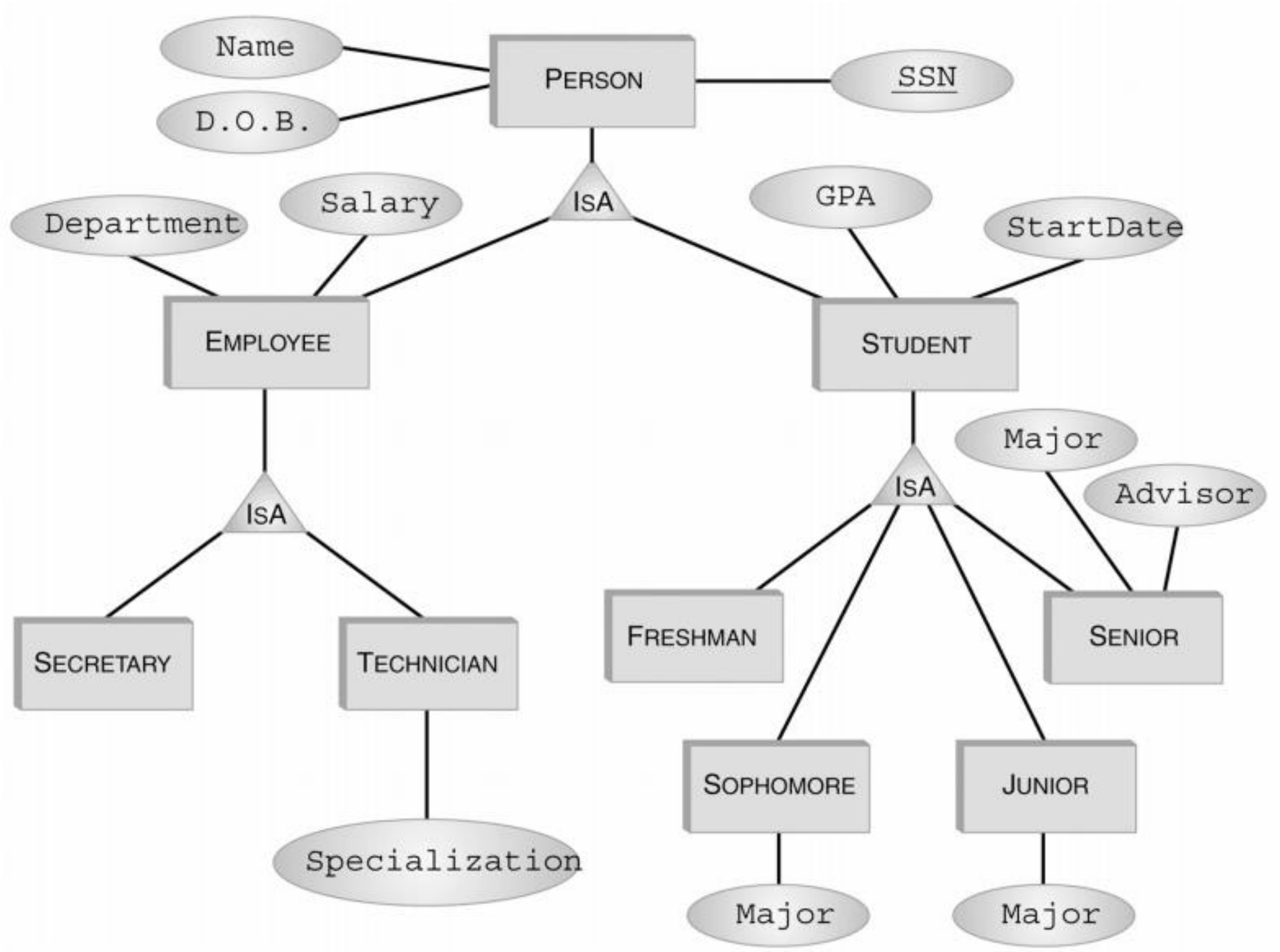
- Equivalence
- Greater-less than
- Addition and subtraction
- Multiplication and division
- Ratio of any two scale values (assumed true 0 value)



Entity Attribute Value Measurement Types

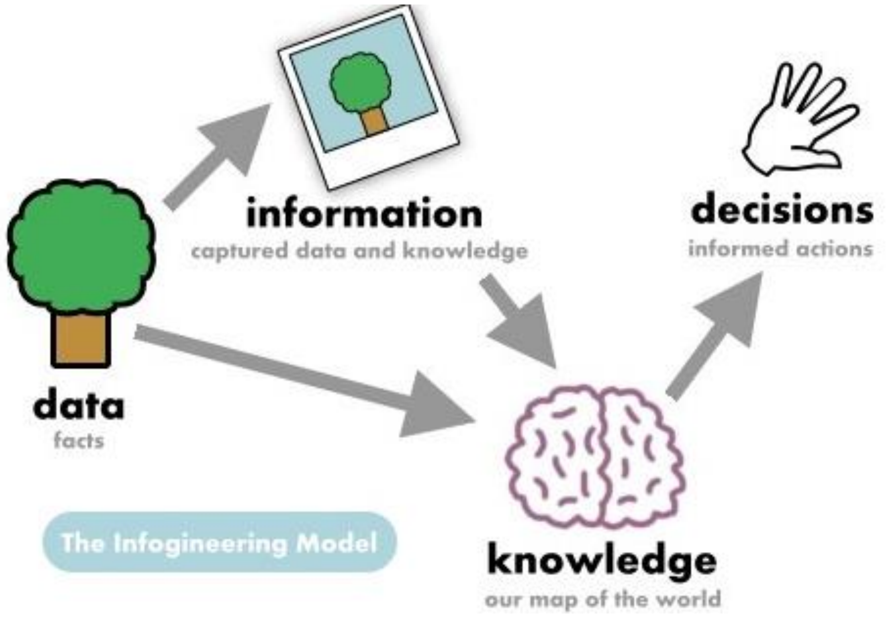
	Qualitative	**Quantitative**
Nominal	X	
Ordinal	X	
Interval		X
Ratio		X

How would you use Steven’s measurements levels to categorize this information ?



How do data and information relate to each other ?

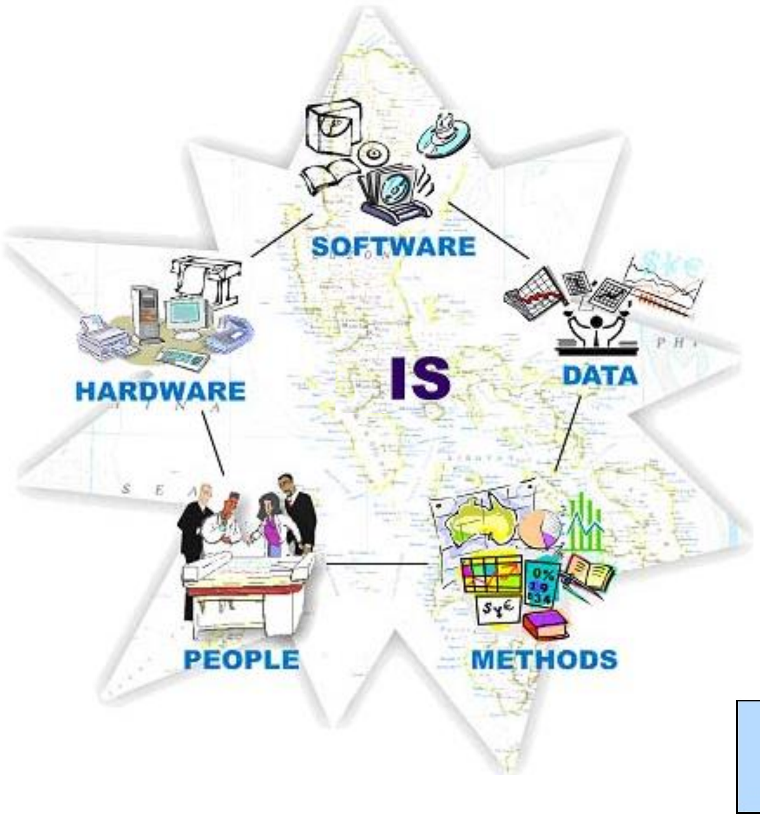
Information is data "put to work" in a decision-making context!

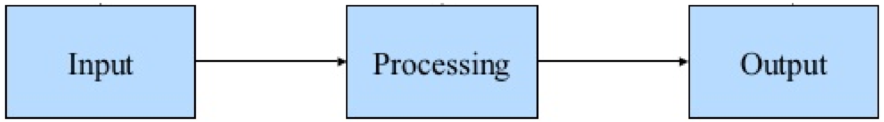


http://www.infogineering.net/data-information-knowledge.htm

What is an information system ?

"An **information system** (**IS**) is an organized system for the collection, organization, storage and communication of information. … Further, an information system (IS) is a group of components that interact to produce information." Wikepedia

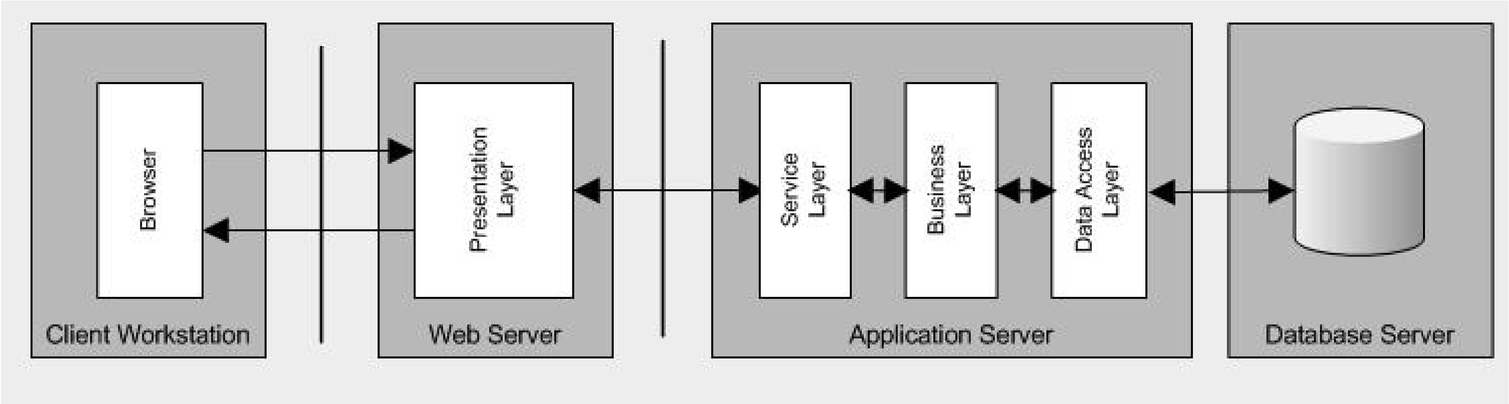



Input

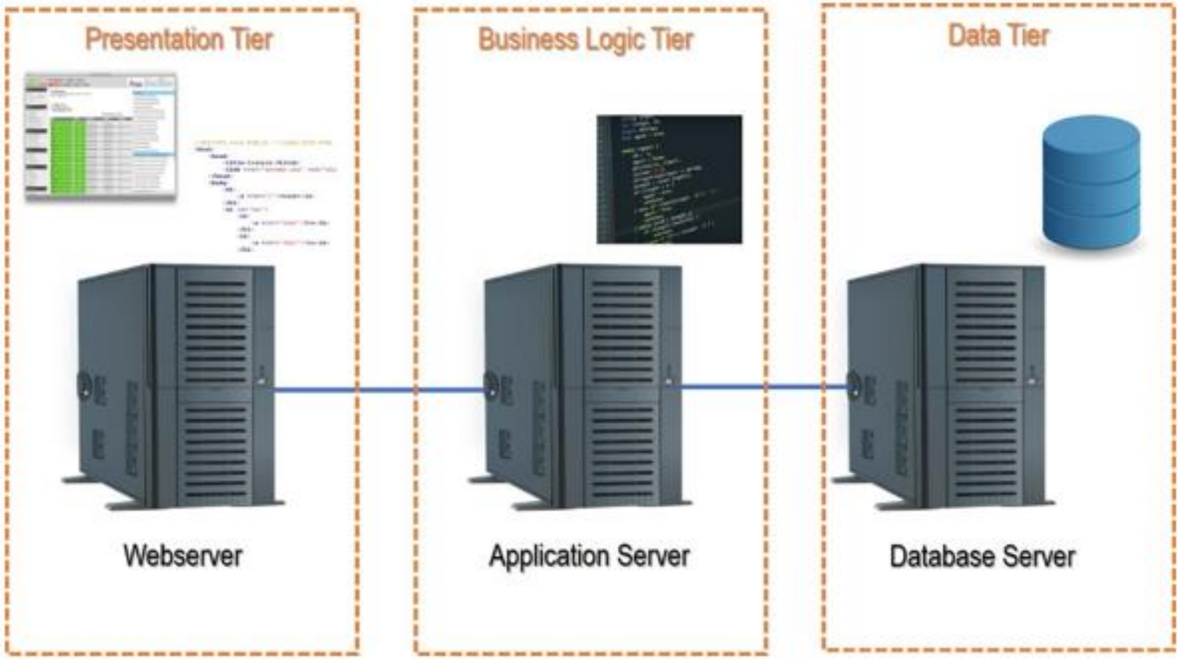
Processing

Output

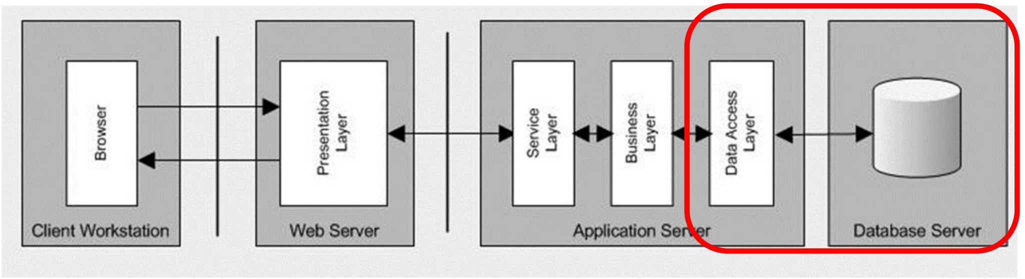
Information system (IS) architecture example

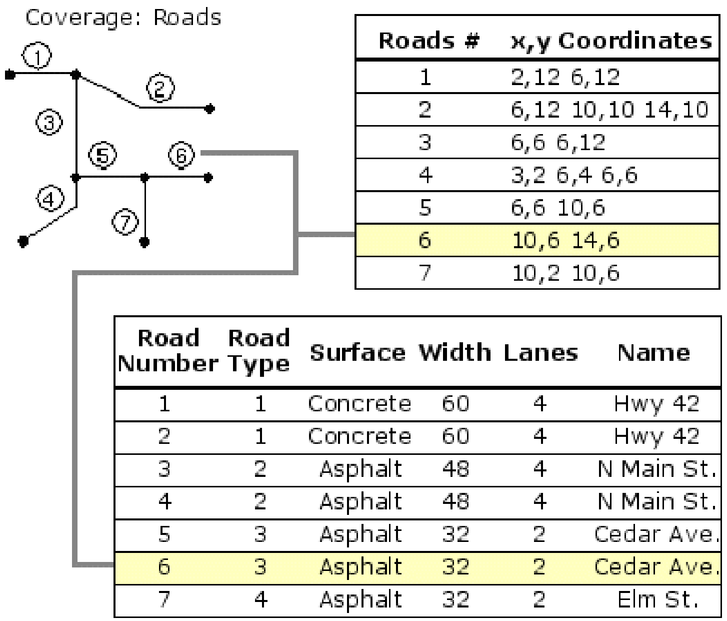


N-Tier Architecture examples



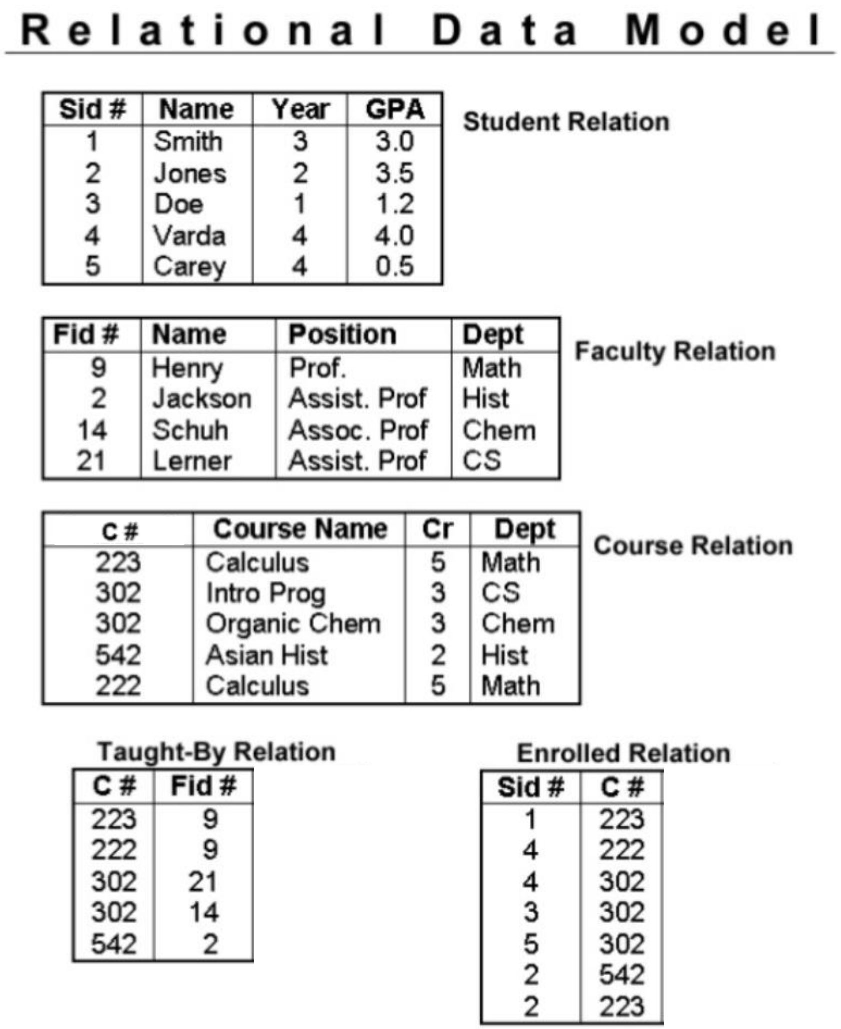
Information System Data example





Roads #	x,y Coordinates
1	2,12 6,12
2	6,12 10,10 14,10
3	6,6 6,12
4	3,2 6,4 6,6
5	6,6 10,6
6	10,6 14,6
7	10,2 10,6

Road Number	Road Type	Surface	Width	Lanes	Name
1	1	Concrete	60	4	Hwy 42
2	1	Concrete	60	4	Hwy 42
3	2	Asphalt	48	4	N Main St.
4	2	Asphalt	48	4	N Main St.
5	3	Asphalt	32	2	Cedar Ave.
6	3	Asphalt	32	2	Cedar Ave.
7	4	Asphalt	32	2	Elm St.



Relational Data Model

Student Relation

Sid #	Name	Year	GPA
1	Smith	3	3.0
2	Jones	2	3.5
3	Doe	1	1.2
4	Varda	4	4.0
5	Carey	4	0.5

Faculty Relation

Fid #	Name	Position	Dept
9	Henry	Prof.	Math
2	Jackson	Assist. Prof	Hist
14	Schuh	Assoc. Prof	Chem
21	Lerner	Assist. Prof	CS

Course Relation

C #	Course Name	Cr	Dept
223	Calculus	5	Math
302	Intro Prog	3	CS
302	Organic Chem	3	Chem
542	Asian Hist	2	Hist
222	Calculus	5	Math

Taught-By Relation

C #	Fid #
223	9
222	9
302	21
302	14
542	2

Enrolled Relation

Sid #	C #
1	223
4	222
4	302
3	302
5	302
2	542
2	223

Concept

Classification Grouping of data according to pre-determined types

Why classify data ?

Data Classification Processes and Models

Data classification (“categorization”) is essential to ensuring that data is appropriately protected, and done so in the most cost-effective manner

The goal is to classify data according to risk associated with a breach to their confidentiality, integrity, and availability

Enables determining the appropriate cost expenditure of security control mitigations required to protect the IT assets

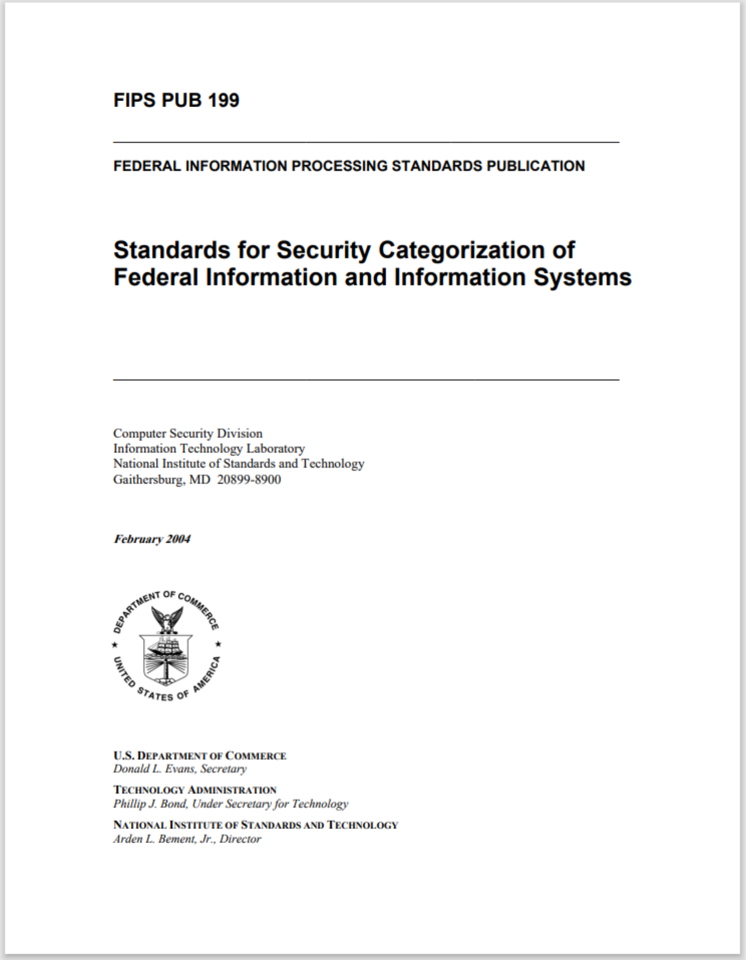
Key Concepts

Classification	Grouping of data according to pre-determined types
Cost-Effectiveness	Appropriateness of the level of risk mitigation expenditure
Confidentiality	Restriction who may know about and/or have access to information
Integrity	Confidence that information is complete and unaltered
Availability	Access to information

Question:

How should we determine the information security categorization of an IT asset?

FIPS 199 Standards



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

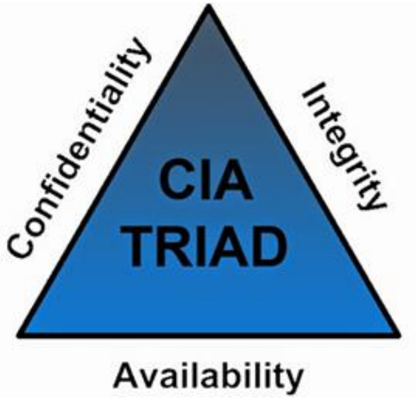
February 2004

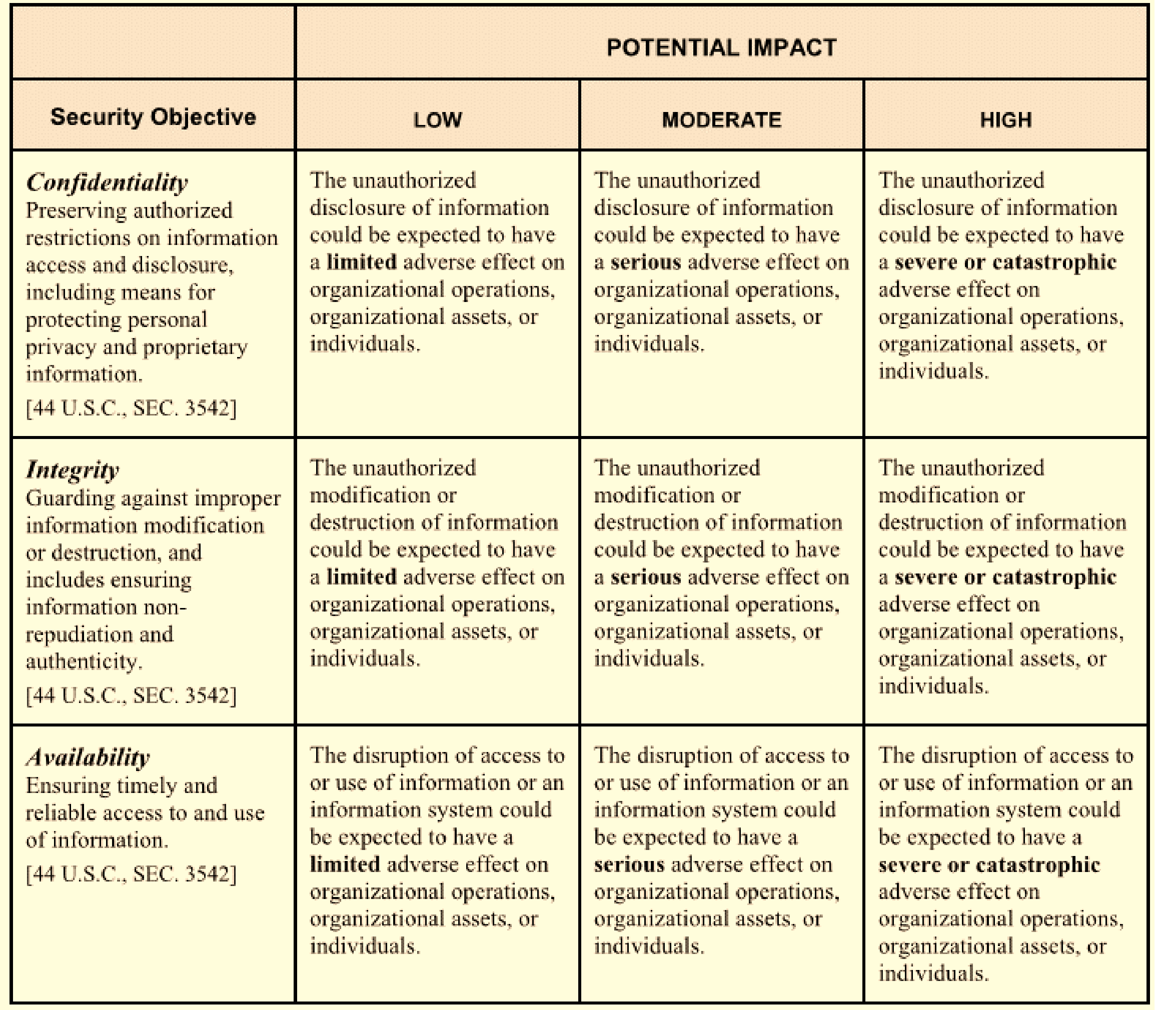
DEPARTMENT OF COMMERCE ★ UNITED STATES OF AMERICA ★

U.S. DEPARTMENT OF COMMERCE
Donald L. Evans, Secretary

TECHNOLOGY ADMINISTRATION
Phillip J. Bond, Under Secretary for Technology

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Arden L. Bement, Jr., Director



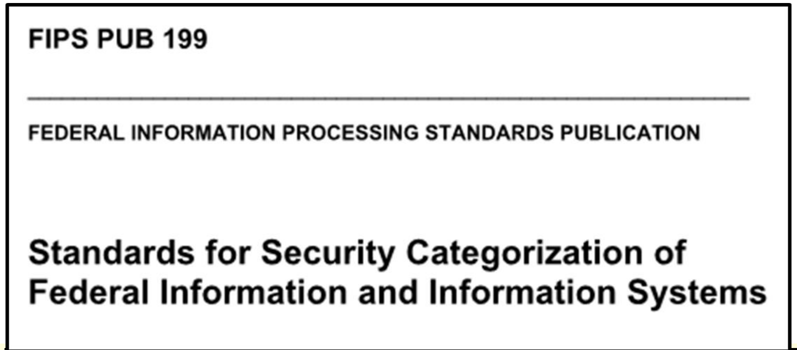


	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Low: *Limited adverse effect*

Moderate: *Serious adverse effect*

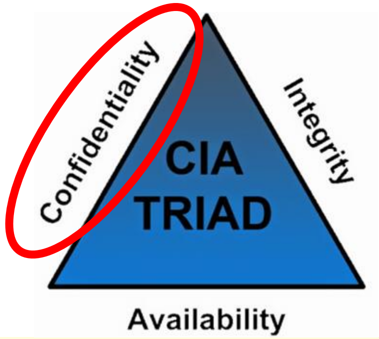
High: *Severe or catastrophic adverse effect*

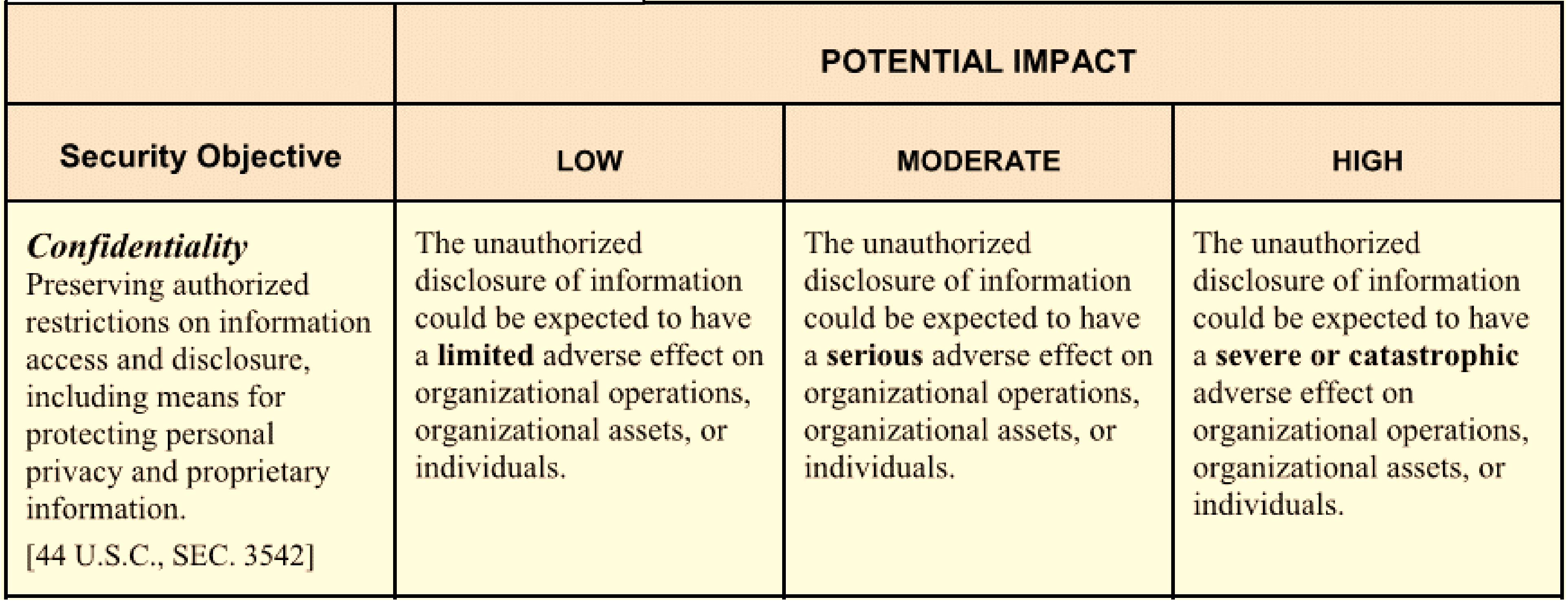


FIPS PUB 199

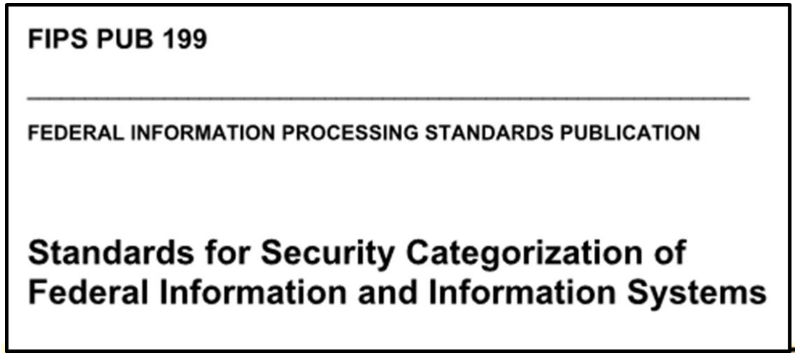
FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Standards for Security Categorization of Federal Information and Information Systems





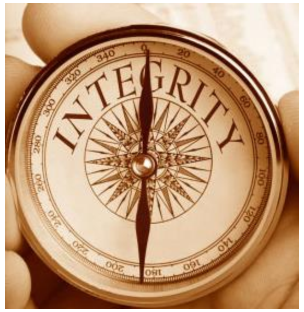
	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

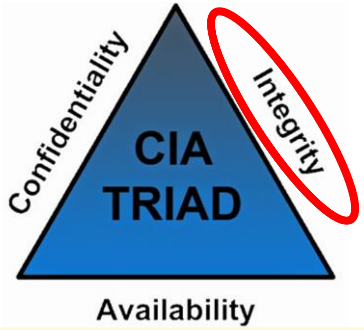


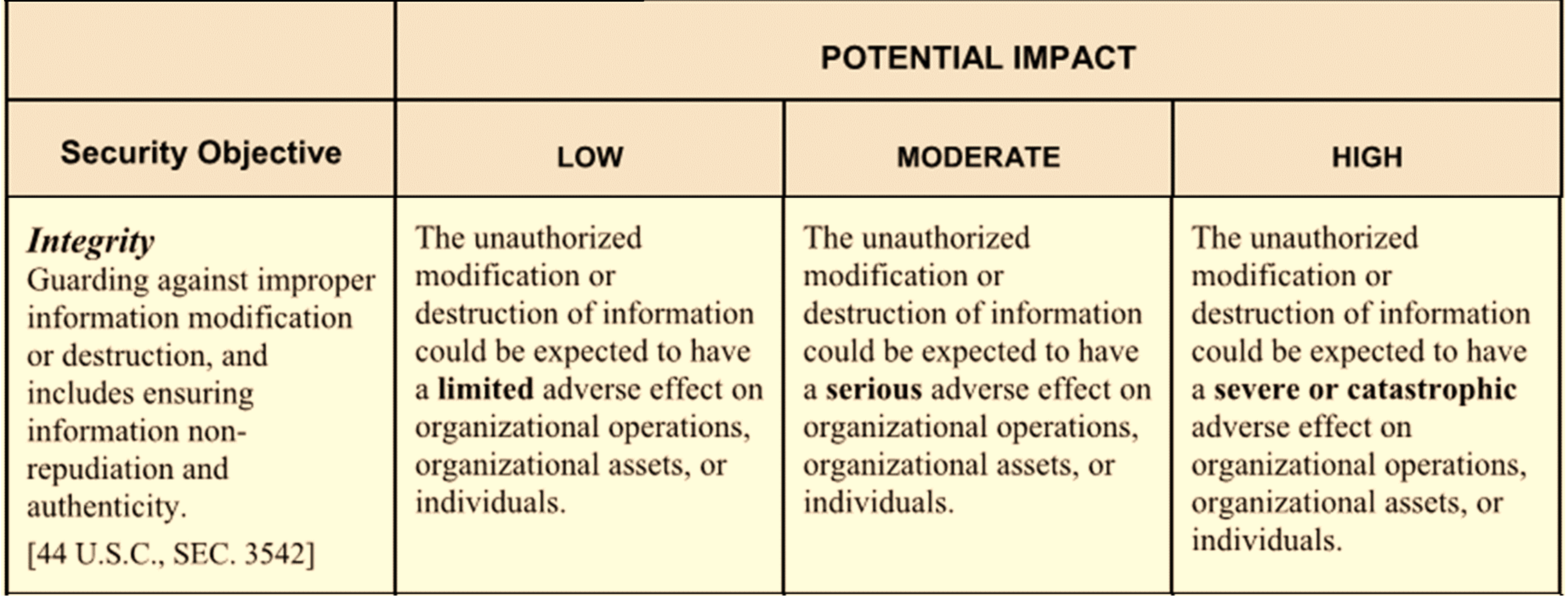
FIPS PUB 199

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

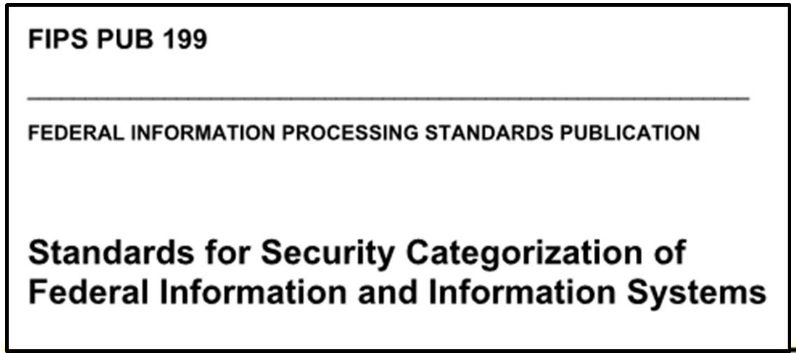
Standards for Security Categorization of Federal Information and Information Systems







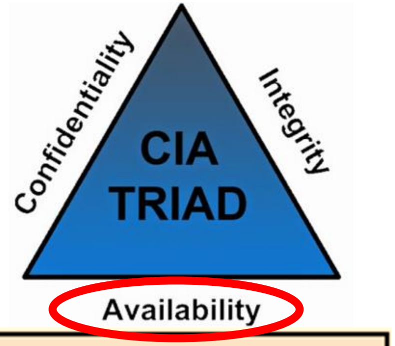
	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

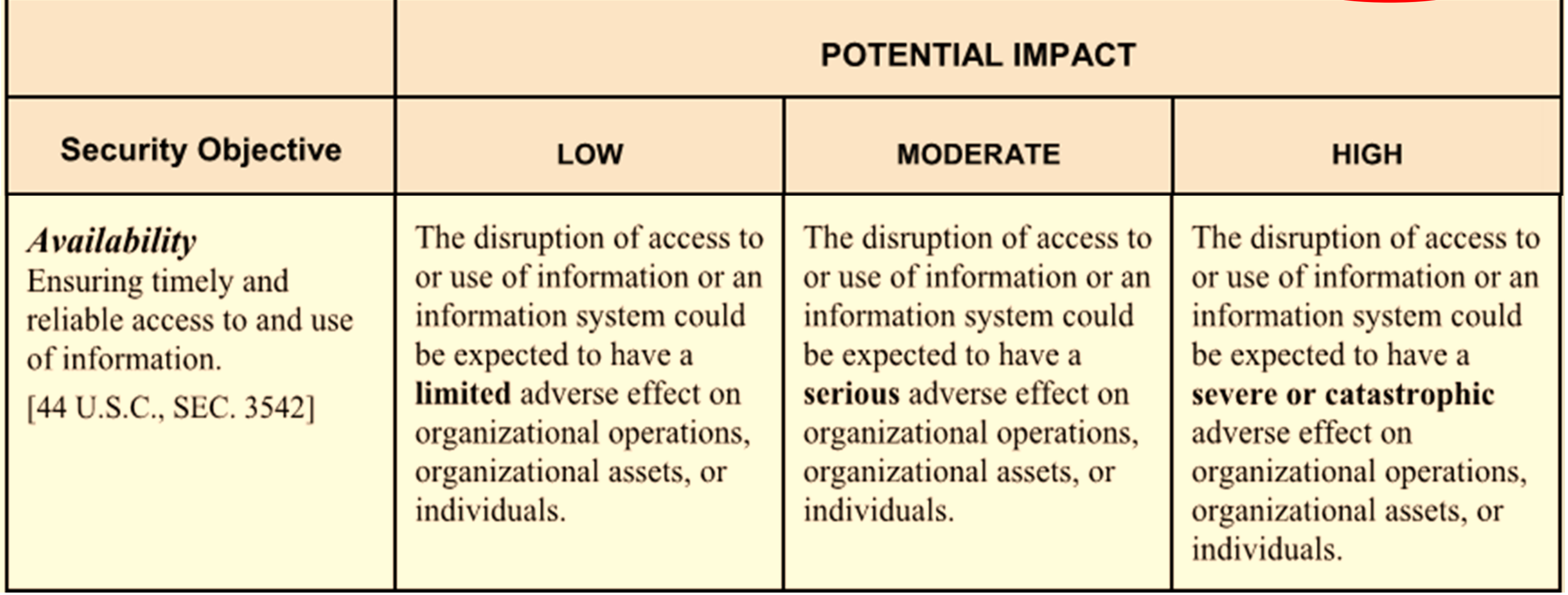


FIPS PUB 199

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Standards for Security Categorization of Federal Information and Information Systems





	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

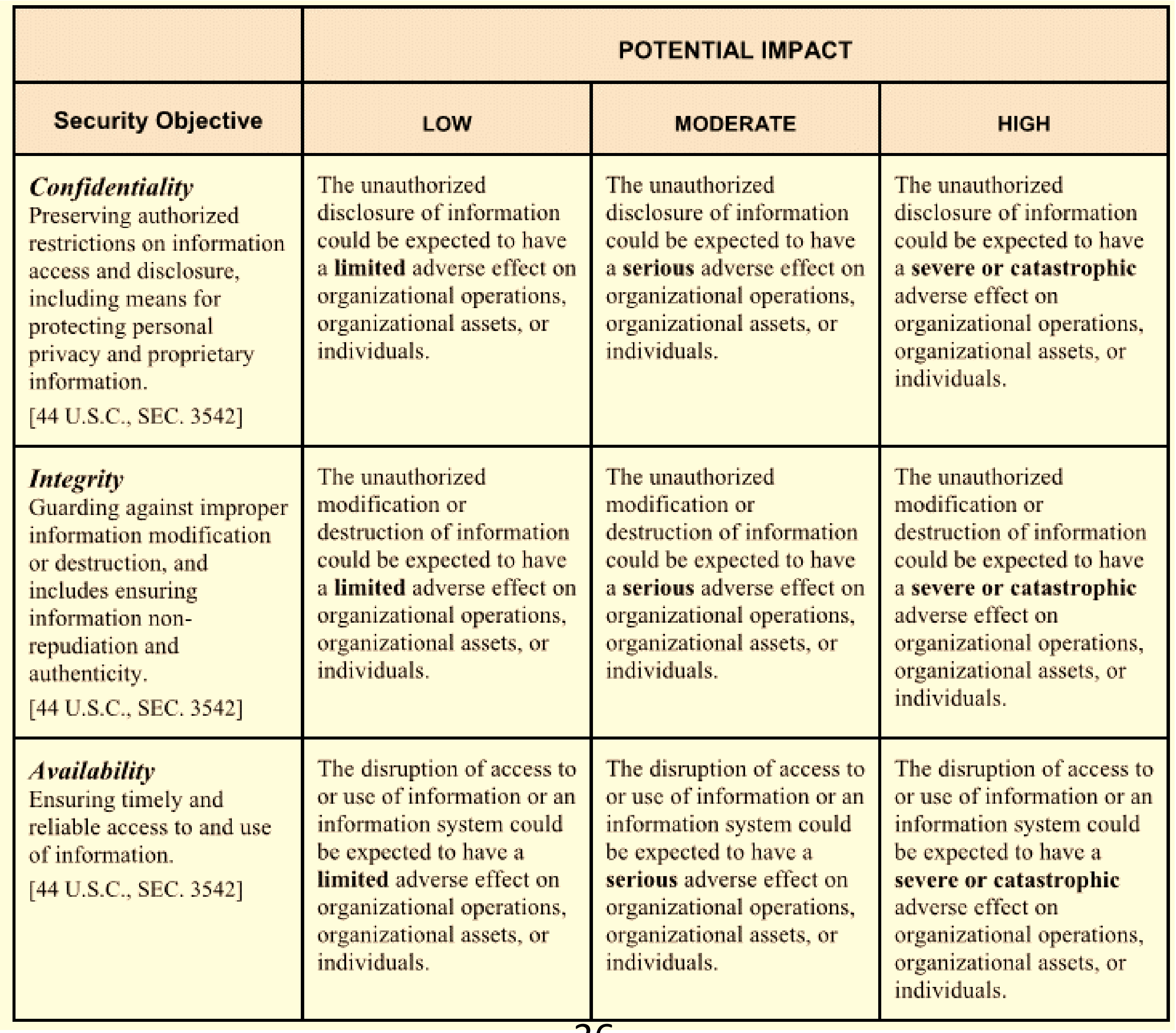
FIPS 199 standard: Security objectives and impact ratings

Low: *Limited adverse effect*

Moderate: *Serious adverse effect*

High: *Severe or catastrophic adverse effect*

What kind of Steven's measurement level is used by the FIPS 199 Information Security categorization standard?



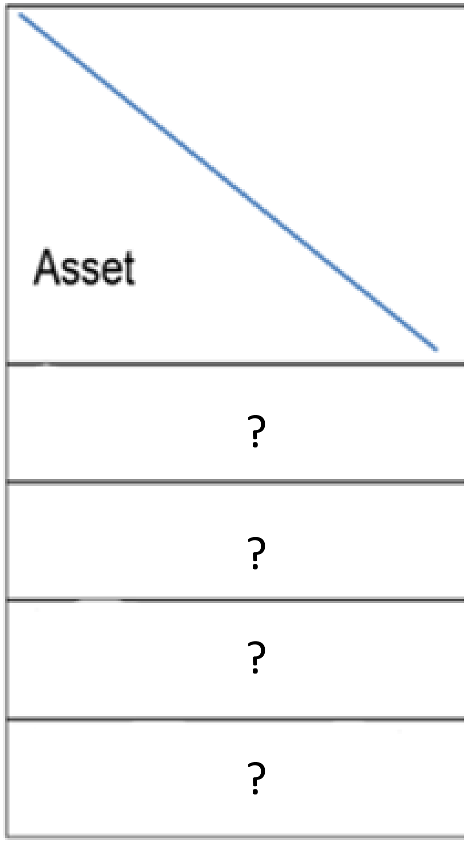
	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

How would you determine the information security categorization of each dataset <u>on the Dean's computer?</u>

Steps:

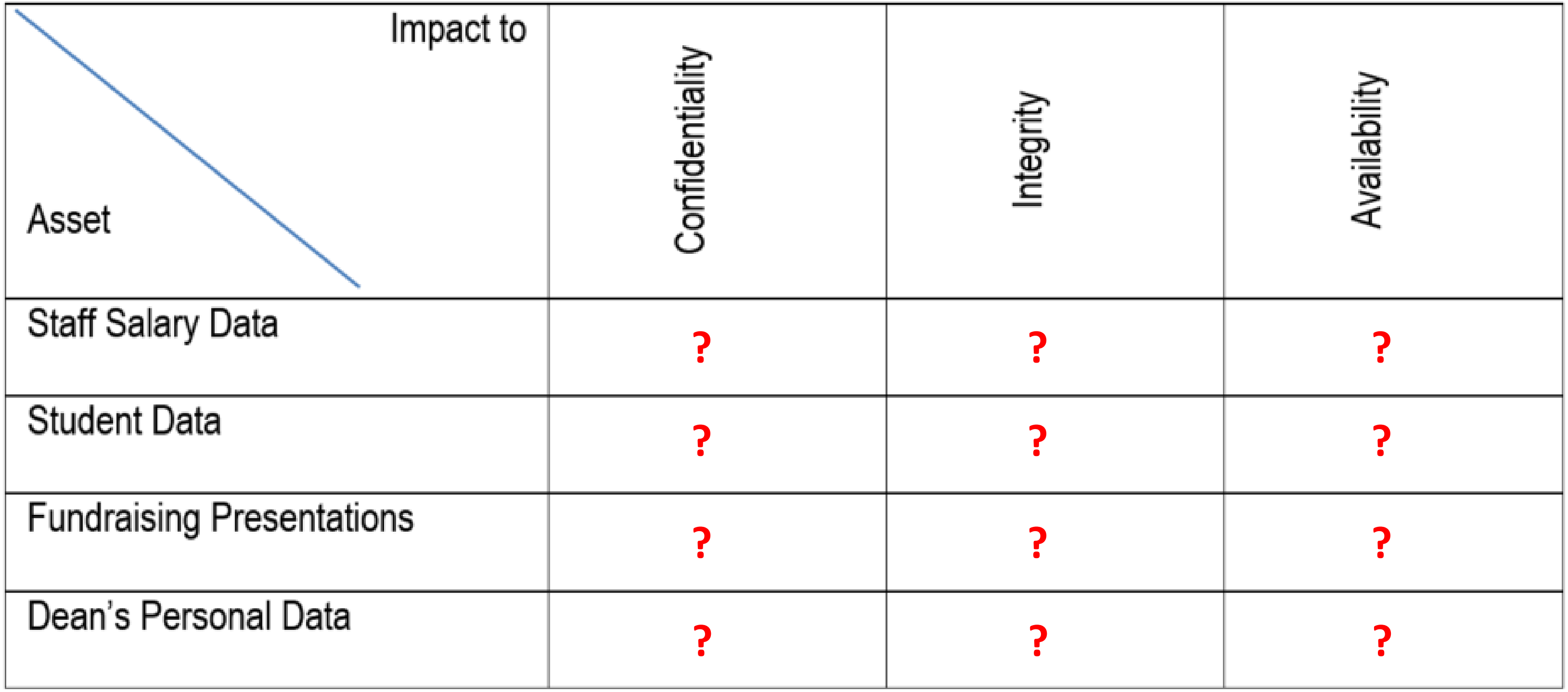
1. *Inventory the (possible) types of information that might be on the Dean's laptop*
2. *Assign information security categorizations to the information contained on the Dean's laptop*
3. *Provide an overall security categorization for the laptop*

1. Create an inventory of types of datasets possibly stored on the Dean’s laptop



Asset
?
?
?
?

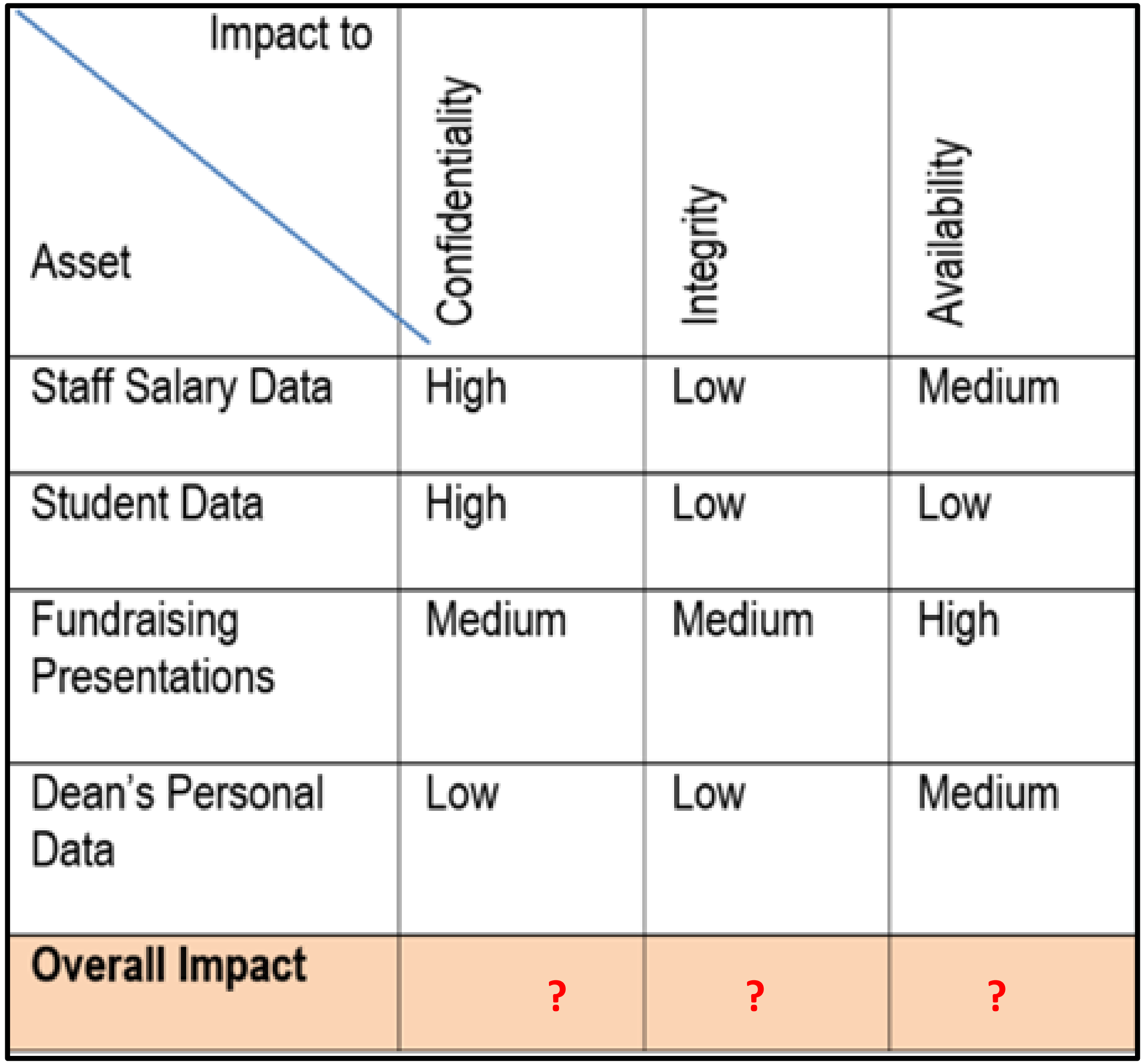
2. Assign information security categorization impact ratings to the datasets on the Dean’s laptop…



Impact to Asset	Confidentiality	Integrity	Availability
Staff Salary Data	?	?	?
Student Data	?	?	?
Fundraising Presentations	?	?	?
Dean’s Personal Data	?	?	?

How do you determine the overall information security categorization of the Dean’s laptop?

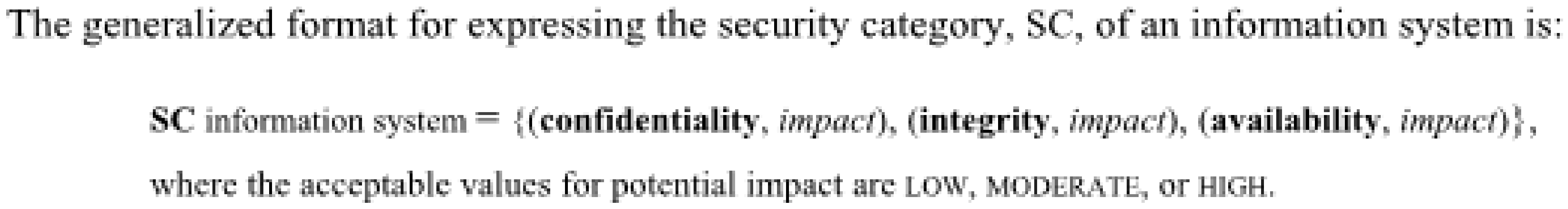
For this example, “Medium” = FIPS 199 “Moderate”



Impact to Asset	Confidentiality	Integrity	Availability
Staff Salary Data	High	Low	Medium
Student Data	High	Low	Low
Fundraising Presentations	Medium	Medium	High
Dean's Personal Data	Low	Low	Medium
Overall Impact	?	?	?

FIPS Pub 199 Standards for Security Categorization

Low: Limited adverse effect
Medium: Serious adverse effect
High: Severe or catastrophic adverse effect

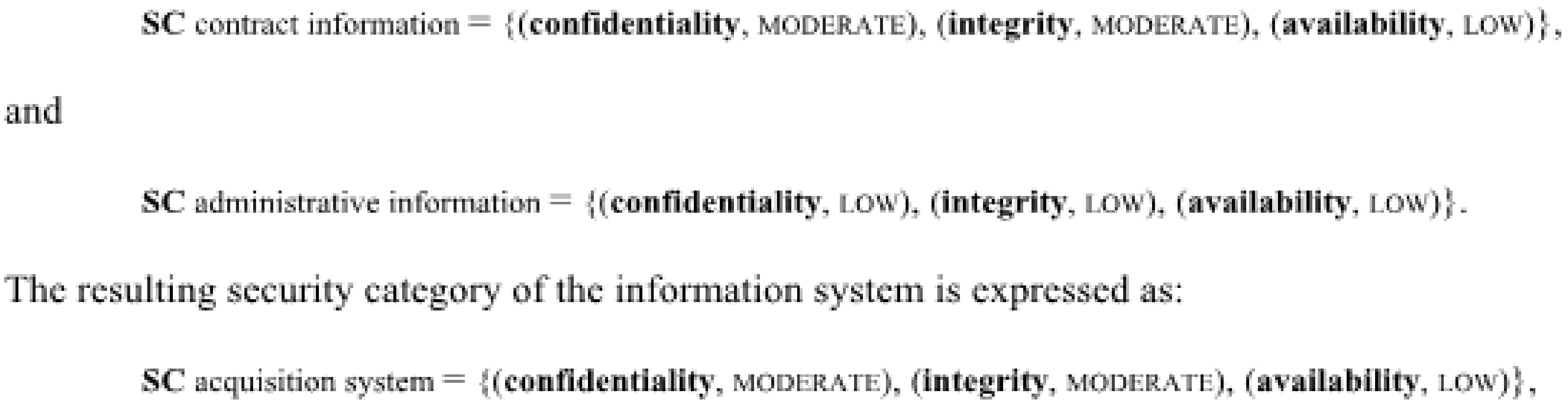


The generalized format for expressing the security category, SC, of an information system is:

SC information system = {(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *impact*)},

where the acceptable values for potential impact are LOW, MODERATE, or HIGH.

Example with multiple information types:



SC contract information = {(**confidentiality**, MODERATE), (**integrity**, MODERATE), (**availability**, LOW)},

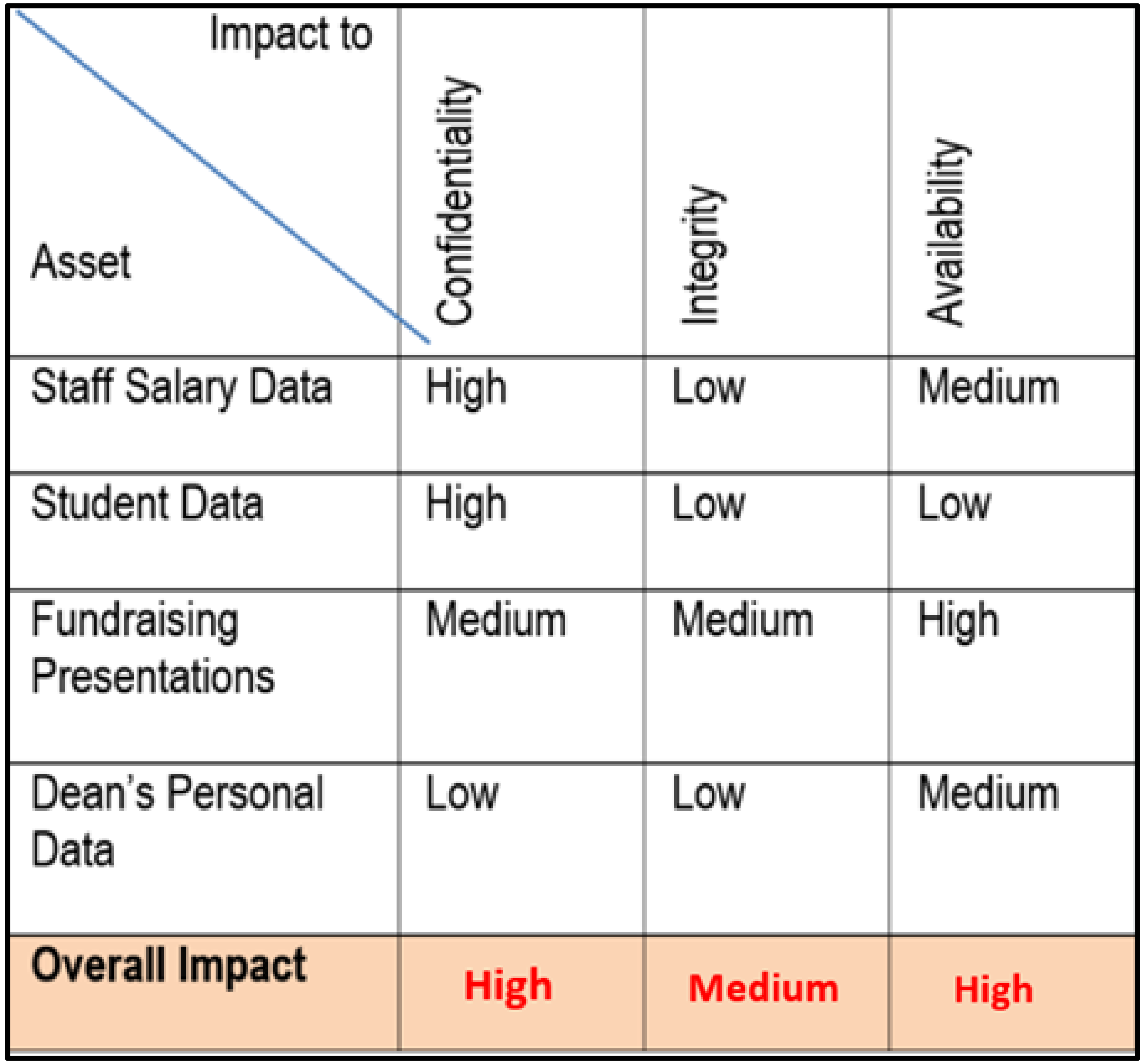
and

SC administrative information = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}.

The resulting security category of the information system is expressed as:

SC acquisition system = {(**confidentiality**, MODERATE), (**integrity**, MODERATE), (**availability**, LOW)},

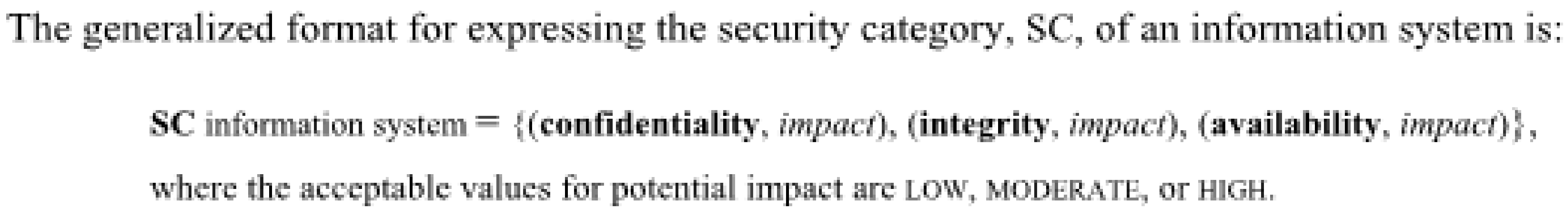
Overall impact in each of the CIA dimensions is based on the <u>highest</u> impact dataset in each of the dimensions



Impact to Asset	Confidentiality	Integrity	Availability
Staff Salary Data	High	Low	Medium
Student Data	High	Low	Low
Fundraising Presentations	Medium	Medium	High
Dean's Personal Data	Low	Low	Medium
Overall Impact	**High**	**Medium**	**High**

FIPS Pub 199 Standards for Security Categorization

Low: Limited adverse effect
Medium: Serious adverse effect
High: Severe or catastrophic adverse effect

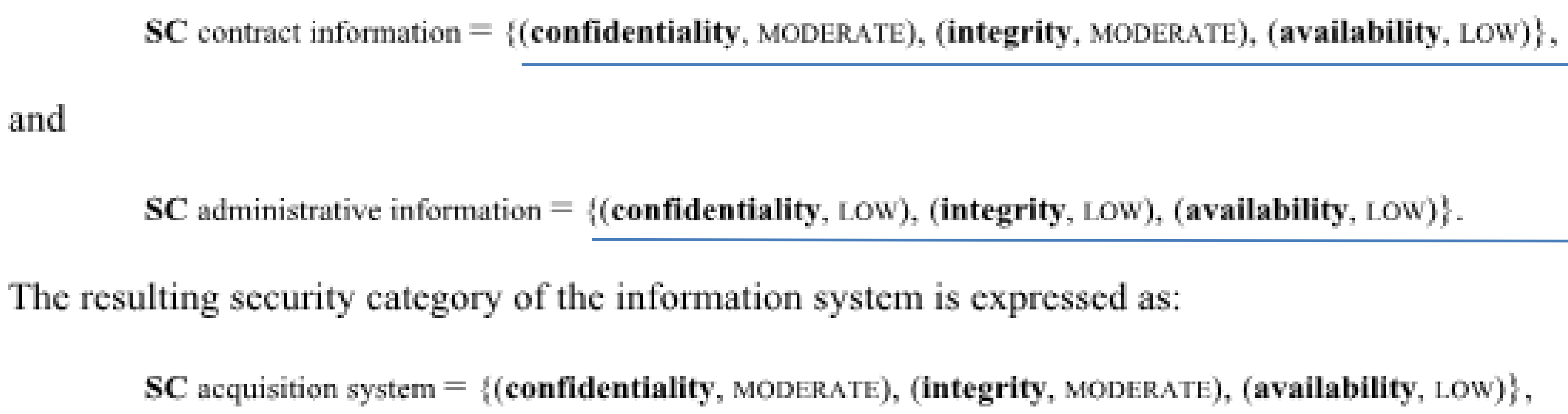


The generalized format for expressing the security category, SC, of an information system is:

SC information system = {(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *impact*)},

where the acceptable values for potential impact are LOW, MODERATE, or HIGH.

Example with multiple information types:



SC contract information = {(**confidentiality**, MODERATE), (**integrity**, MODERATE), (**availability**, LOW)}, = MODERATE rating

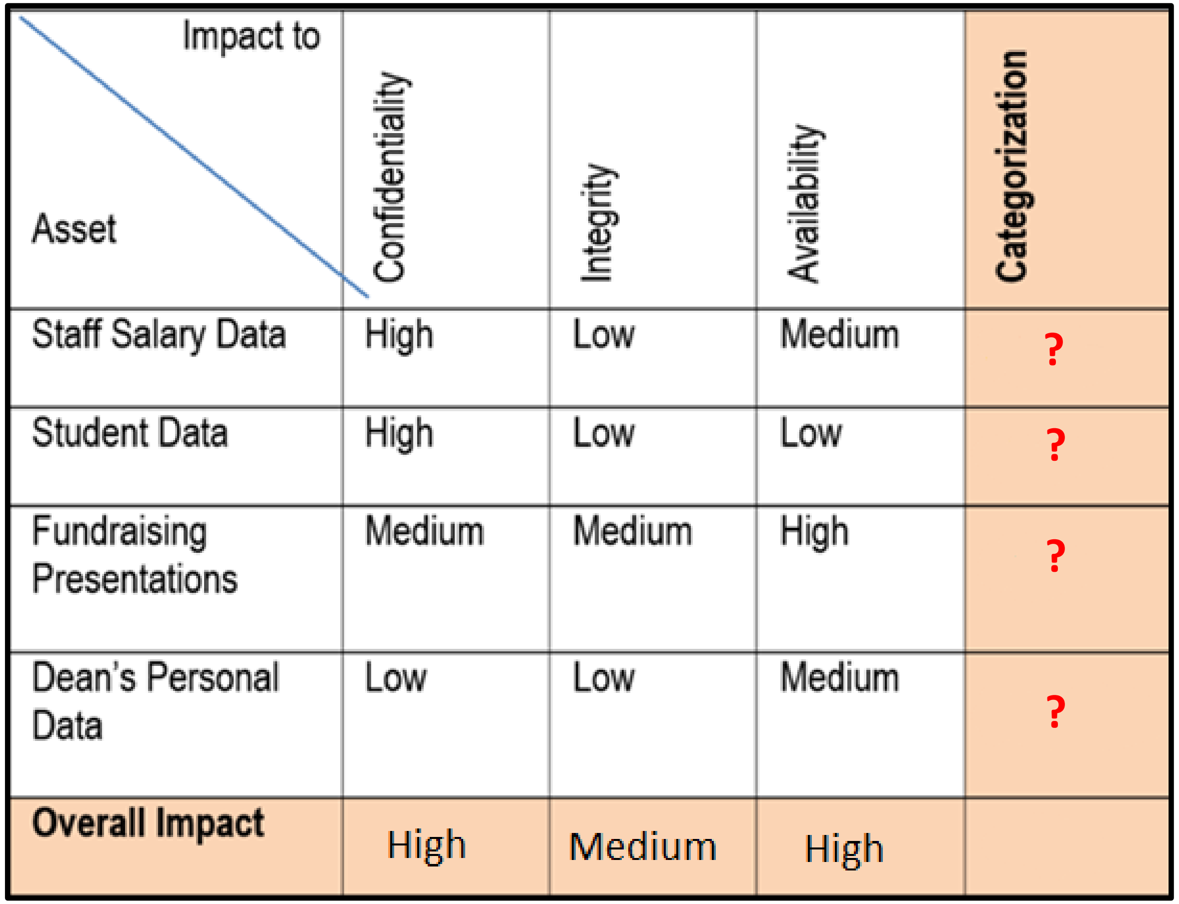
and

SC administrative information = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}. = LOW rating

The resulting security category of the information system is expressed as:

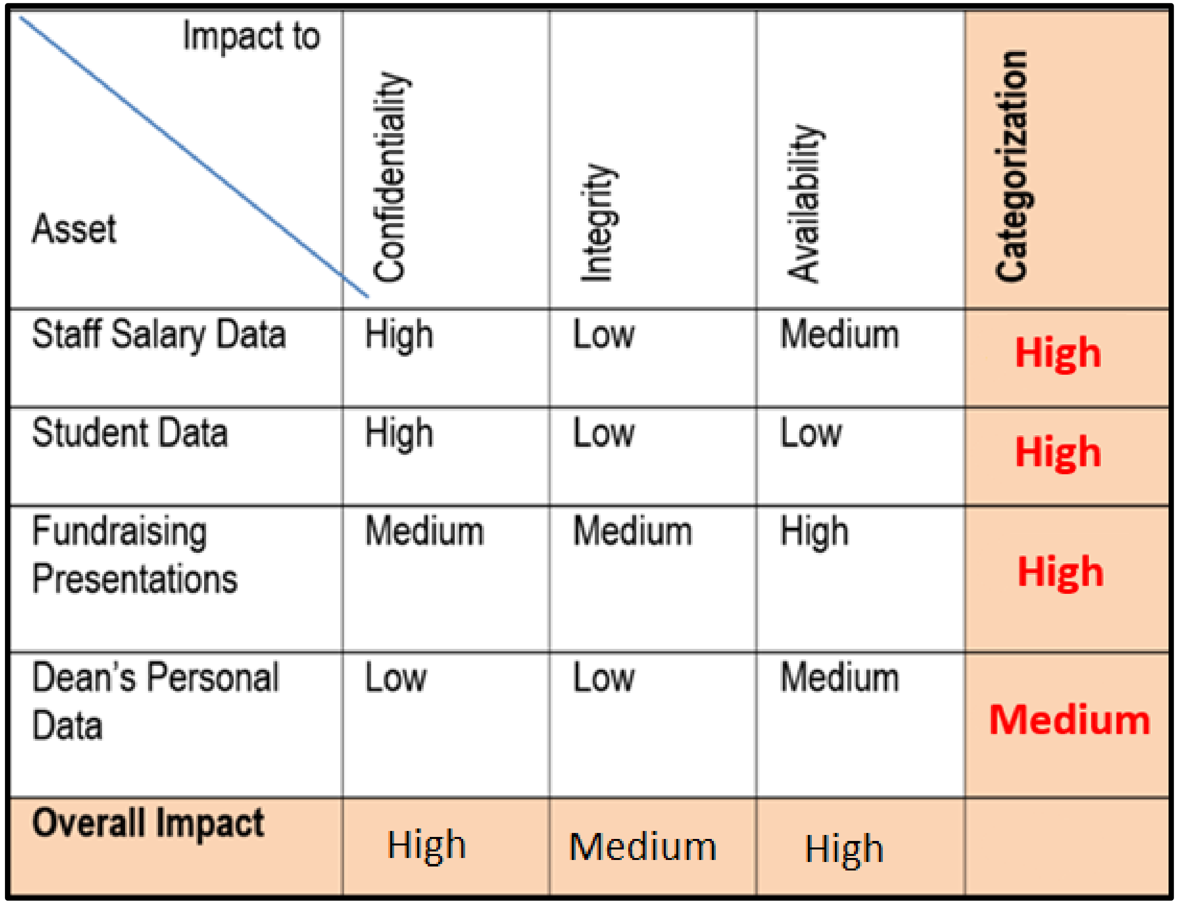
SC acquisition system = {(**confidentiality**, MODERATE), (**integrity**, MODERATE), (**availability**, LOW)}, = MODERATE rating

What single overall information security categorization would you give each dataset on the Dean’s laptop?



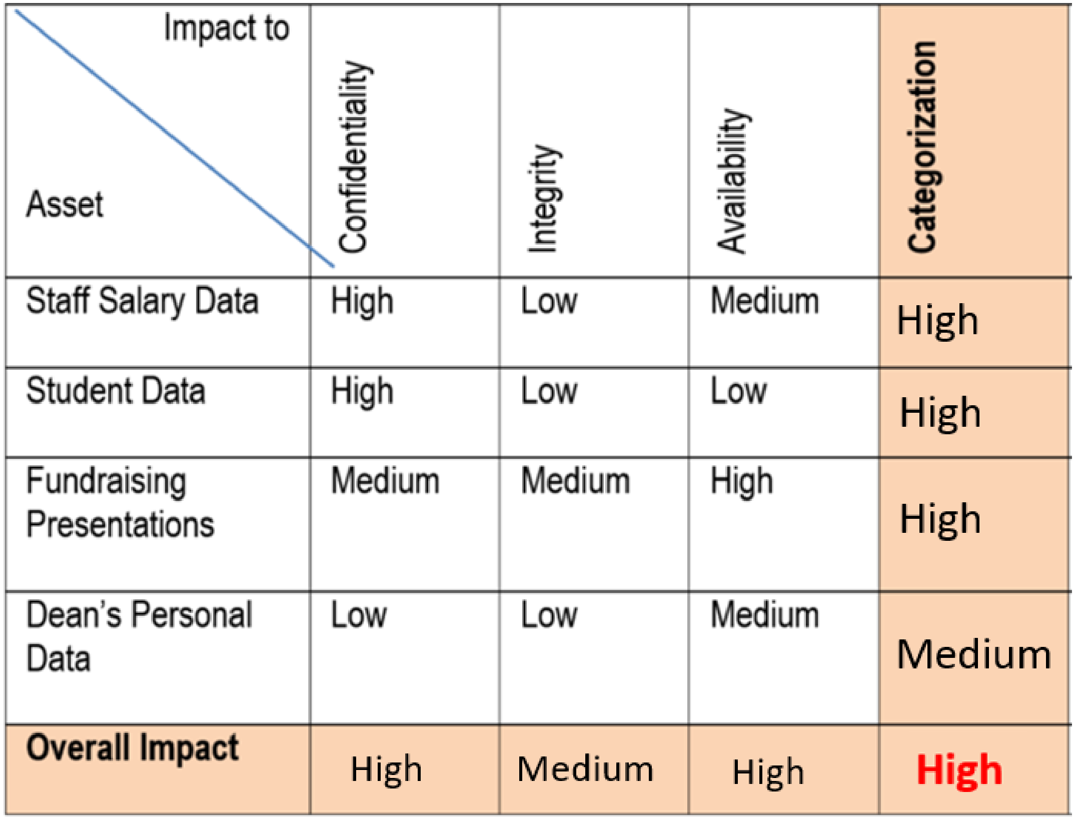
Impact to Asset	Confidentiality	Integrity	Availability	**Categorization**
Staff Salary Data	High	Low	Medium	?
Student Data	High	Low	Low	?
Fundraising Presentations	Medium	Medium	High	?
Dean’s Personal Data	Low	Low	Medium	?
Overall Impact	High	Medium	High	

What single overall information security categorization would you give each dataset on the Dean's laptop?



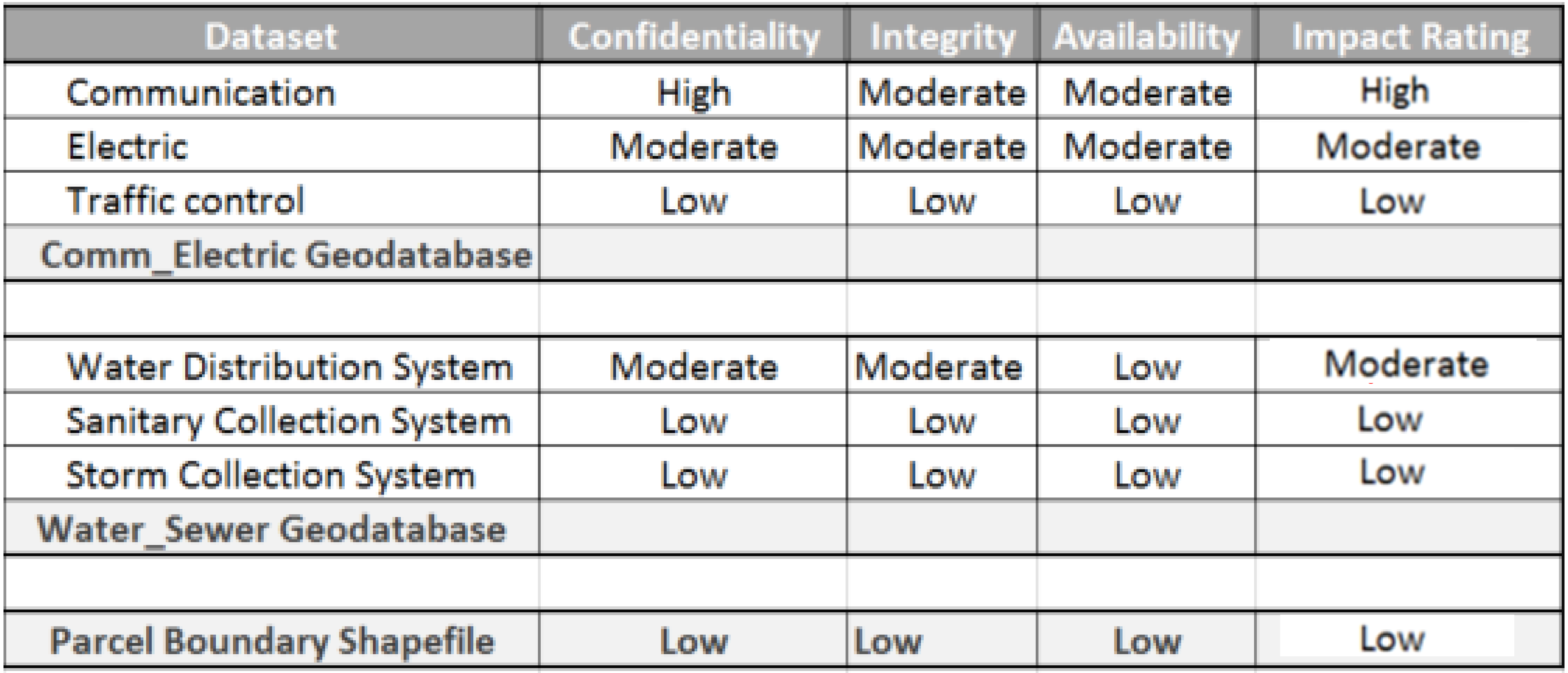
Impact to Asset	Confidentiality	Integrity	Availability	Categorization
Staff Salary Data	High	Low	Medium	High
Student Data	High	Low	Low	High
Fundraising Presentations	Medium	Medium	High	High
Dean's Personal Data	Low	Low	Medium	Medium
Overall Impact	High	Medium	High	

What single information security categorization value would you give the Dean’s laptop?



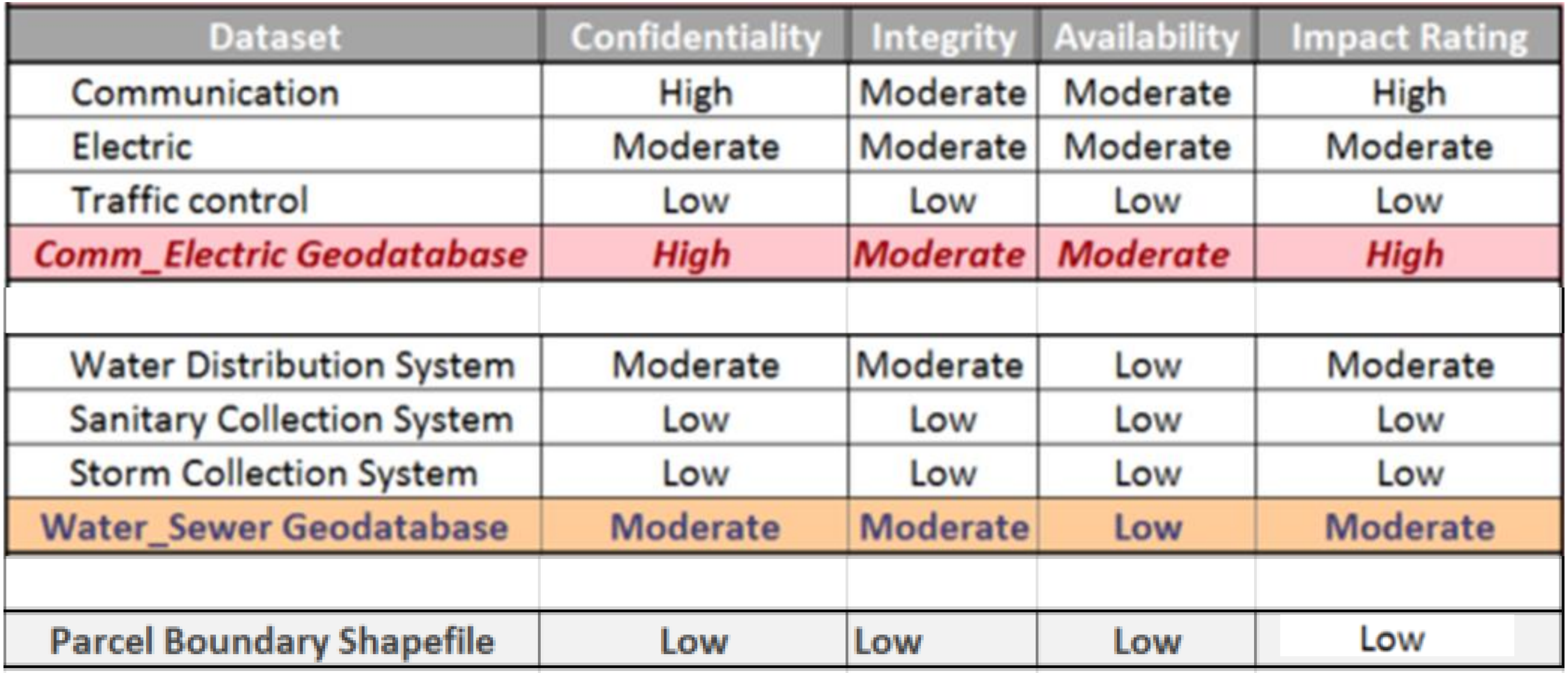
Impact to Asset	Confidentiality	Integrity	Availability	**Categorization**
Staff Salary Data	High	Low	Medium	High
Student Data	High	Low	Low	High
Fundraising Presentations	Medium	Medium	High	High
Dean’s Personal Data	Low	Low	Medium	Medium
Overall Impact	High	Medium	High	**High**

What are the security categorizations of these datasets?



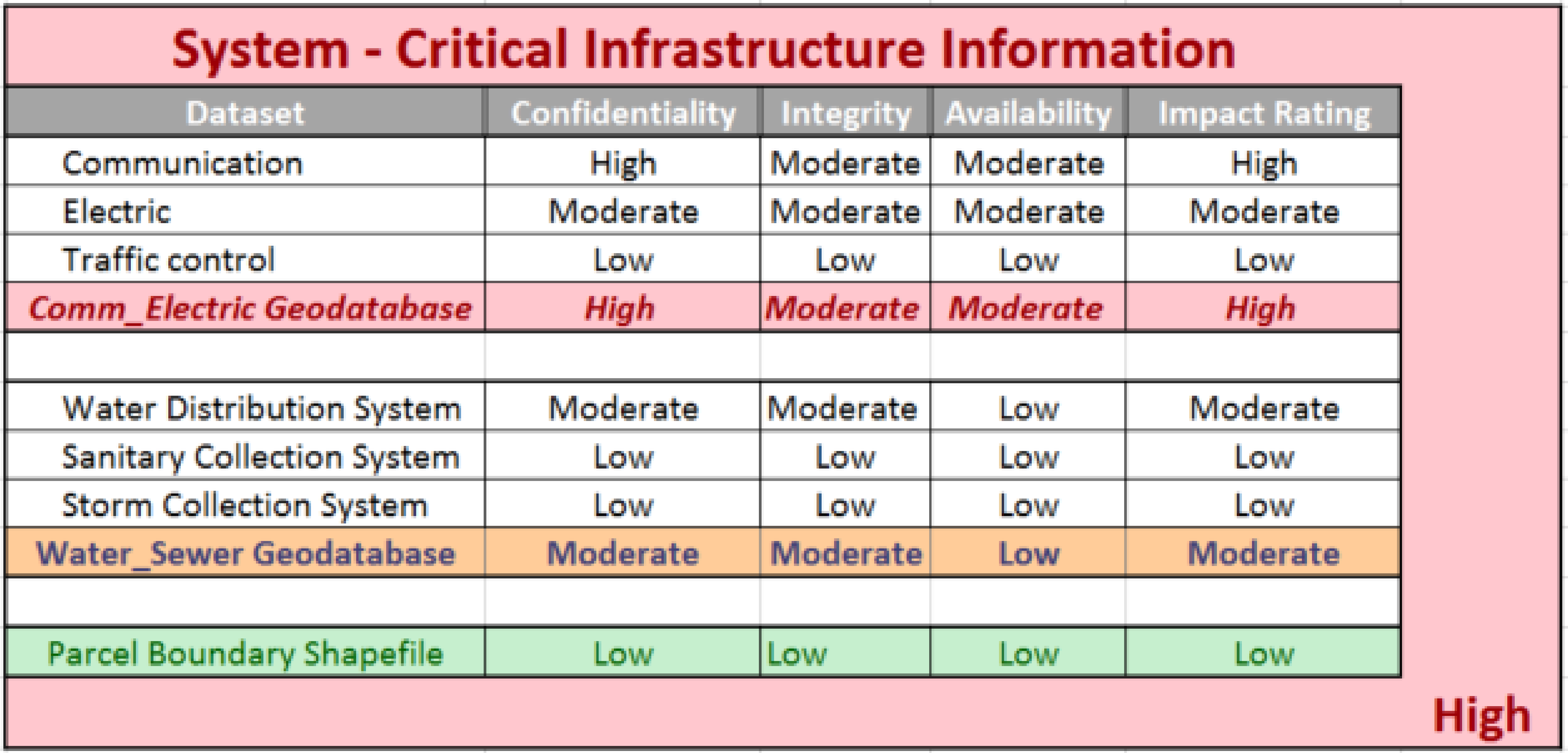
Dataset	Confidentiality	Integrity	Availability	Impact Rating
Communication	High	Moderate	Moderate	High
Electric	Moderate	Moderate	Moderate	Moderate
Traffic control	Low	Low	Low	Low
Comm_Electric Geodatabase				
Water Distribution System	Moderate	Moderate	Low	Moderate
Sanitary Collection System	Low	Low	Low	Low
Storm Collection System	Low	Low	Low	Low
Water_Sewer Geodatabase				
Parcel Boundary Shapefile	Low	Low	Low	Low

What are the security categorizations of the geodatabases?



Dataset	Confidentiality	Integrity	Availability	Impact Rating
Communication	High	Moderate	Moderate	High
Electric	Moderate	Moderate	Moderate	Moderate
Traffic control	Low	Low	Low	Low
Comm_Electric Geodatabase	***High***	***Moderate***	***Moderate***	***High***
Water Distribution System	Moderate	Moderate	Low	Moderate
Sanitary Collection System	Low	Low	Low	Low
Storm Collection System	Low	Low	Low	Low
Water_Sewer Geodatabase	**Moderate**	**Moderate**	**Low**	**Moderate**
Parcel Boundary Shapefile	**Low**	**Low**	**Low**	**Low**

What is the overall security categorization of the information system containing these datasets?



System - Critical Infrastructure Information

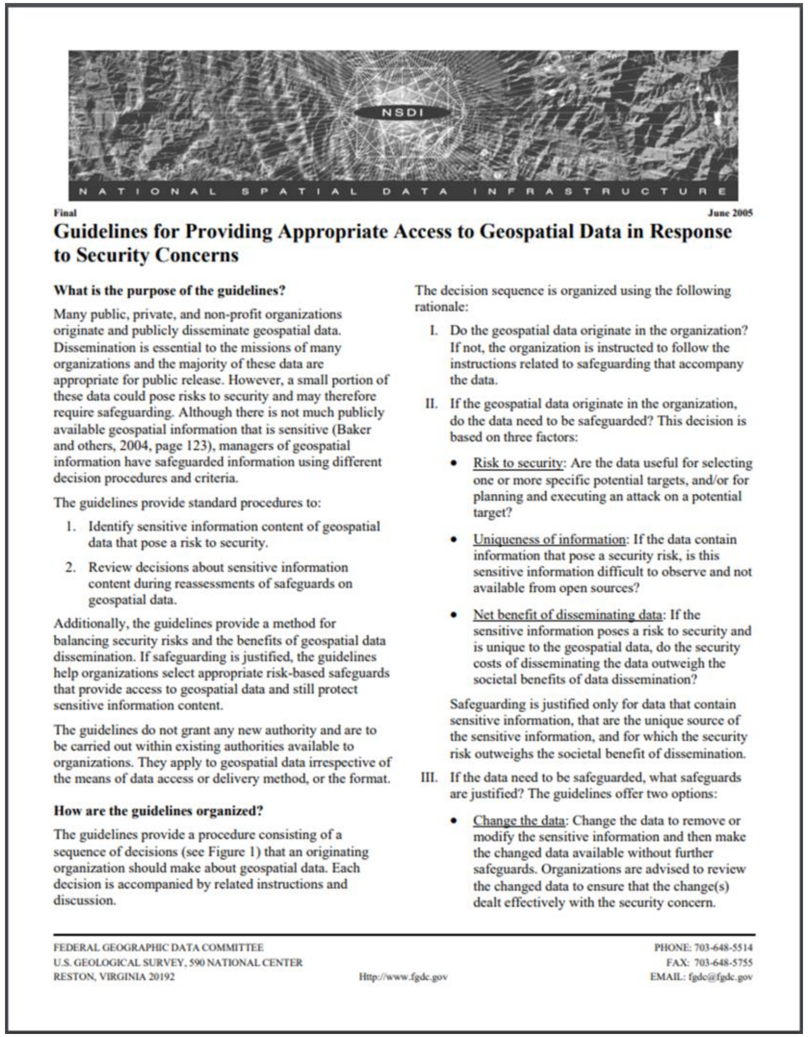
Dataset	Confidentiality	Integrity	Availability	Impact Rating
Communication	High	Moderate	Moderate	High
Electric	Moderate	Moderate	Moderate	Moderate
Traffic control	Low	Low	Low	Low
Comm_Electric Geodatabase	*High*	*Moderate*	*Moderate*	*High*
Water Distribution System	Moderate	Moderate	Low	Moderate
Sanitary Collection System	Low	Low	Low	Low
Storm Collection System	Low	Low	Low	Low
Water_Sewer Geodatabase	Moderate	Moderate	Low	Moderate
Parcel Boundary Shapefile	Low	Low	Low	Low

High

Protecting Publicly Shared GIS datasets

Federal Geographic Data Committee’s Risk Assessment and Control Guidelines for Sharing Geospatial Data are based on the RAND framework we covered earlier, which helps:

- Identify sensitive information contents of geospatial datasets that may pose a risk to security objectives
- Make information security decisions
- Apply safeguards to sensitive geospatial data contents



NSDI

NATIONAL SPATIAL DATA INFRASTRUCTURE

Final **June 2005**

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

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 guidelines provide standard procedures to:

1. Identify sensitive information content of geospatial data that pose a risk to security.
2. Review decisions about sensitive information content during reassessments of safeguards on geospatial data.

Additionally, the guidelines provide a method for balancing security risks and the benefits of geospatial data dissemination. If safeguarding is justified, the guidelines help organizations select appropriate risk-based safeguards that provide access to geospatial data and still protect sensitive information content.

The guidelines do not grant any new authority and are to be carried out within existing authorities available to organizations. They apply to geospatial data irrespective of the means of data access or delivery method, or the format.

How are the guidelines organized?

The guidelines provide a procedure consisting of a sequence of decisions (see Figure 1) that an originating organization should make about geospatial data. Each decision is accompanied by related instructions and discussion.

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 planning and executing an attack on a potential target?
- Uniqueness of information: If the data contain information that pose a security risk, is this sensitive information difficult to observe and not available from open sources?
- Net benefit of disseminating data: If the sensitive information poses a risk to security and is unique to the geospatial data, do the security costs of disseminating the data outweigh the societal benefits of data dissemination?

Safeguarding is justified only for data that contain sensitive information, that are the unique source of the sensitive information, and for which the security risk outweighs the societal benefit of dissemination.

III. If the data need to be safeguarded, what safeguards are justified? The guidelines offer two options:

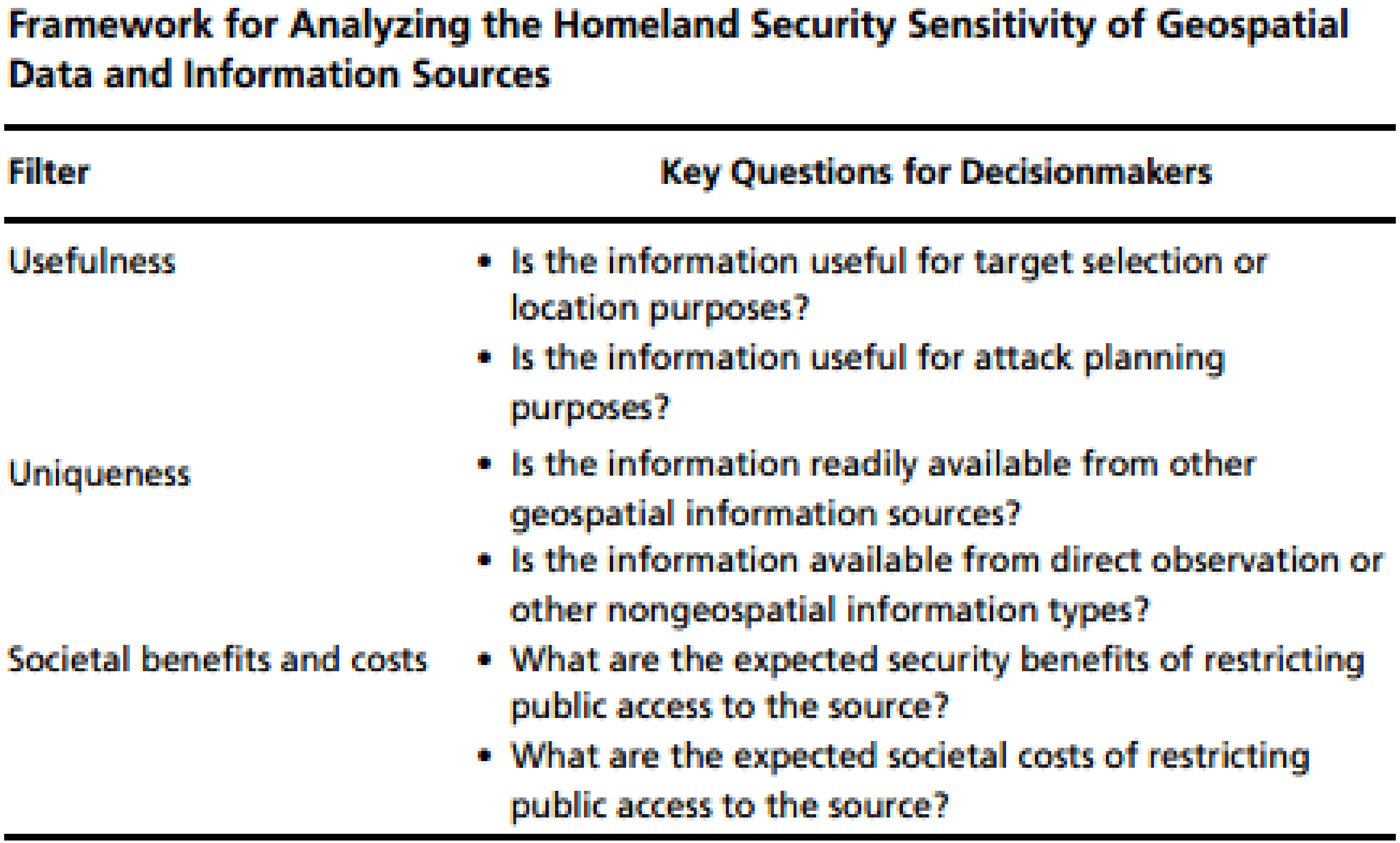
- Change the data: Change the data to remove or modify the sensitive information and then make the changed data available without further safeguards. Organizations are advised to review the changed data to ensure that the change(s) dealt effectively with the security concern.

FEDERAL GEOGRAPHIC DATA COMMITTEE
U.S. GEOLOGICAL SURVEY, 590 NATIONAL CENTER
RESTON, VIRGINIA 20192

Http://www.fgdc.gov

PHONE: 703-648-5514
FAX: 703-648-5755
EMAIL: fgdc@fgdc.gov

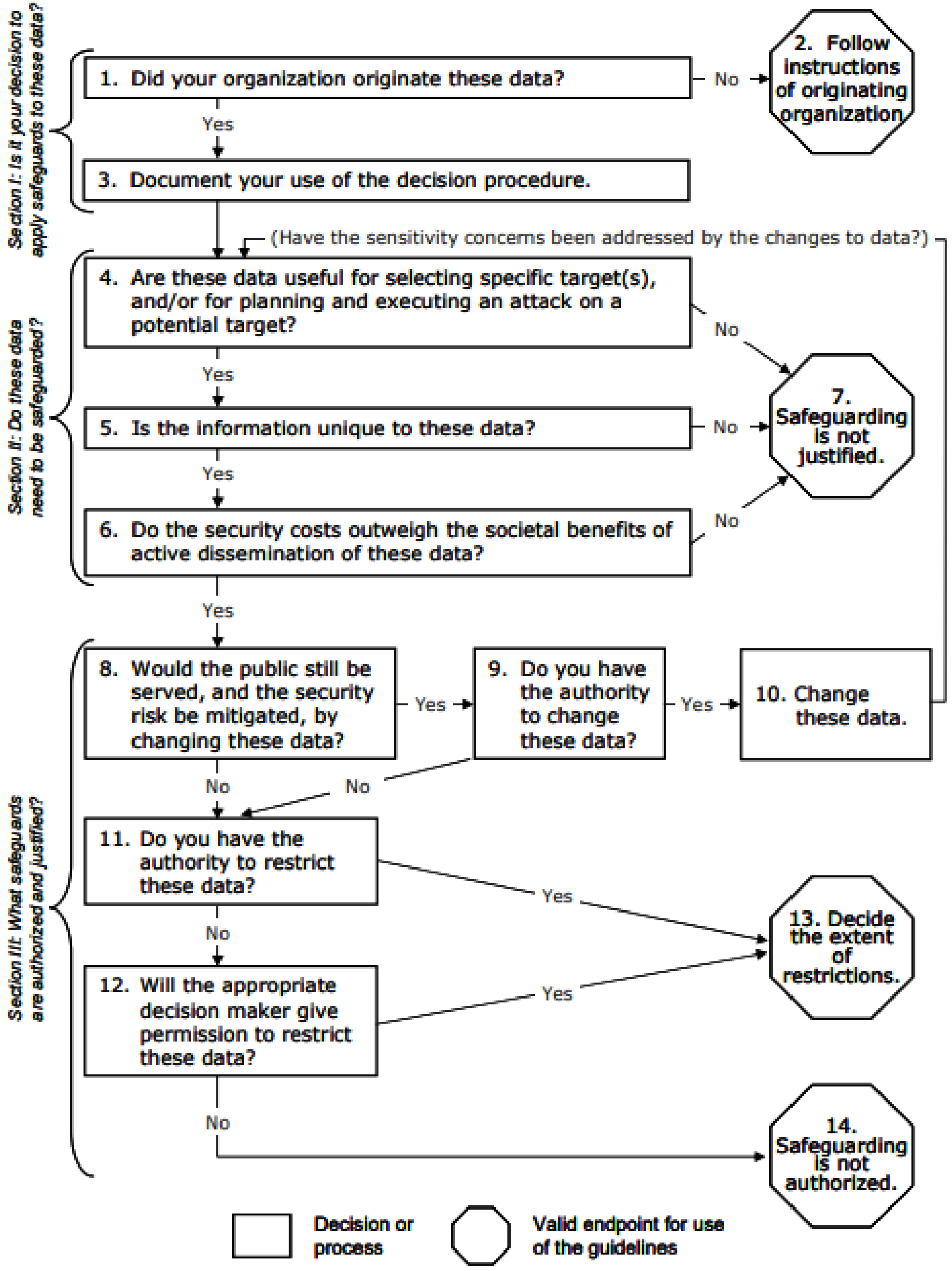
Recall RAND’s risk assessment framework focused by 3 “filters”



Framework for Analyzing the Homeland Security Sensitivity of Geospatial Data and Information Sources

Filter	Key Questions for Decisionmakers
Usefulness	• Is the information useful for target selection or location purposes? • Is the information useful for attack planning purposes?
Uniqueness	• Is the information readily available from other geospatial information sources? • Is the information available from direct observation or other nongeospatial information types?
Societal benefits and costs	• What are the expected security benefits of restricting public access to the source? • What are the expected societal costs of restricting public access to the source?

Figure 1. Decision Tree for Providing Appropriate Access to Geospatial Data in Response to Security Concerns



Section I: Is it your decision to apply safeguards to these data?

1. Did your organization originate these data?

No → 2. Follow instructions of originating organization

Yes ↓

3. Document your use of the decision procedure.

(Have the sensitivity concerns been addressed by the changes to data?)

Section II: Do these data need to be safeguarded?

4. Are these data useful for selecting specific target(s), and/or for planning and executing an attack on a potential target?

No → 7. Safeguarding is not justified.

Yes ↓

5. Is the information unique to these data?

No → 7. Safeguarding is not justified.

Yes ↓

6. Do the security costs outweigh the societal benefits of active dissemination of these data?

No → 7. Safeguarding is not justified.

Yes ↓

Section III: What safeguards are authorized and justified?

8. Would the public still be served, and the security risk be mitigated, by changing these data?

Yes → 9. Do you have the authority to change these data?

Yes → 10. Change these data.

No ↓

11. Do you have the authority to restrict these data?

Yes → 13. Decide the extent of restrictions.

No ↓

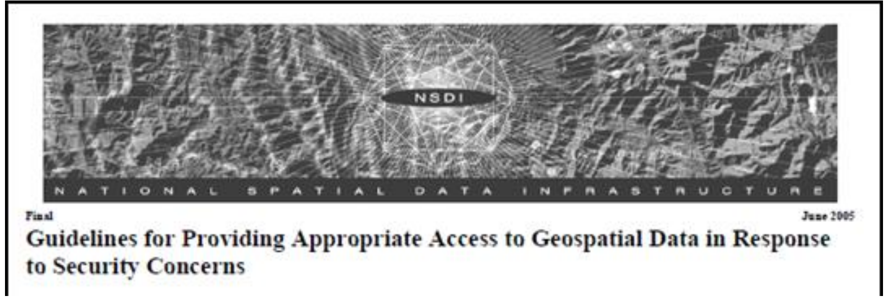
12. Will the appropriate decision maker give permission to restrict these data?

Yes → 13. Decide the extent of restrictions.

No → 14. Safeguarding is not authorized.

□ Decision or process

○ Valid endpoint for use of the guidelines



NATIONAL SPATIAL DATA INFRASTRUCTURE

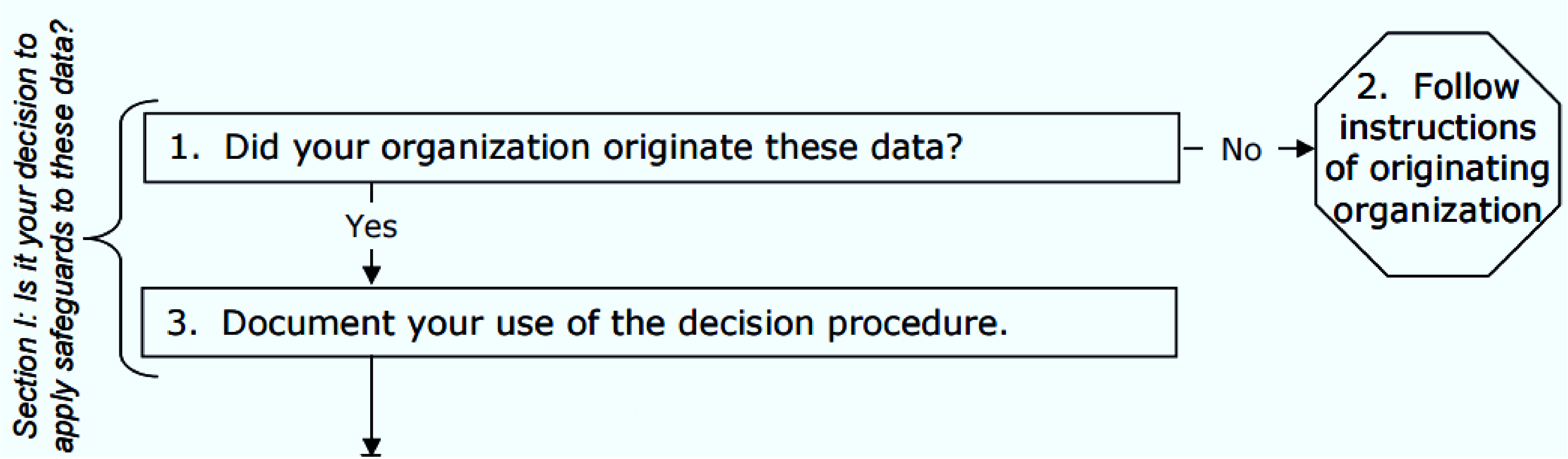
Final

June 2005

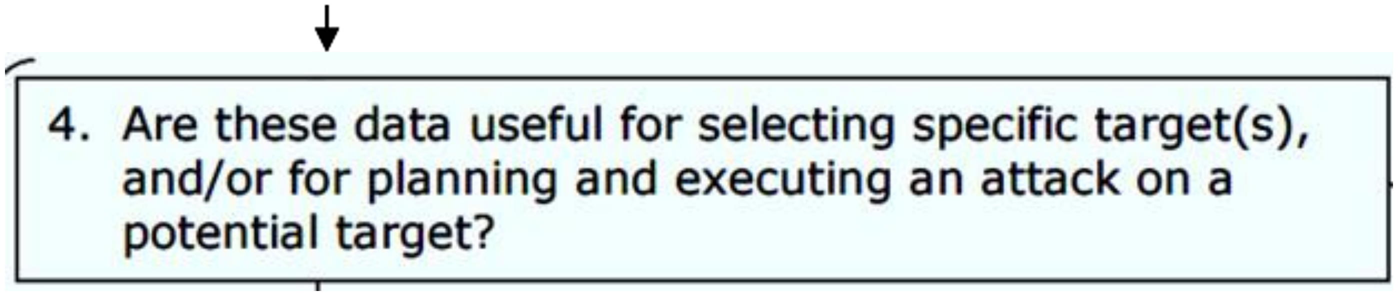
Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns

https://fas.org/sgp/othergov/fgdc0605.pdf

Decision Tree: Is it your decision… ?


Section I: Is it your decision to apply safeguards to these data?
1. Did your organization originate these data?
No
2. Follow instructions of originating organization
Yes
3. Document your use of the decision procedure.

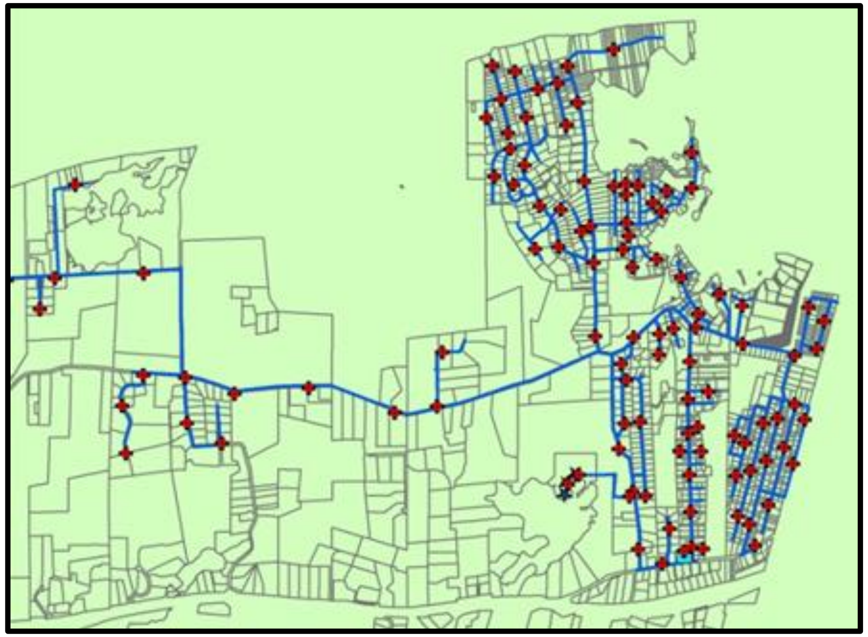
Decision Tree: *…risk assessment…*



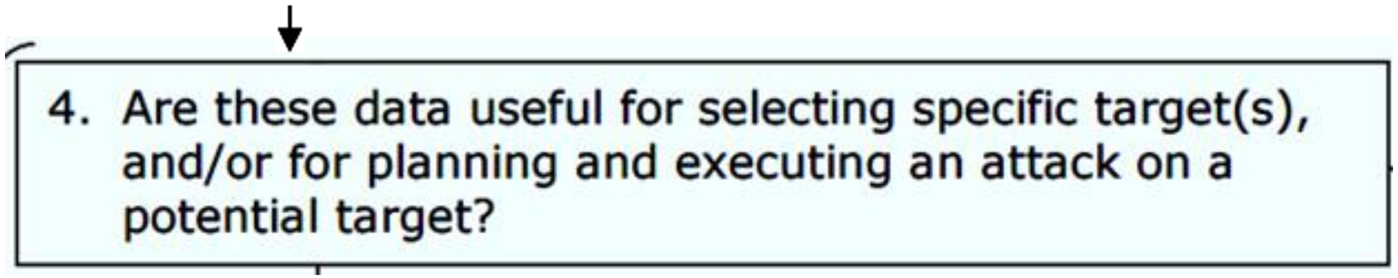
4. Are these data useful for selecting specific target(s), and/or for planning and executing an attack on a potential target?

“Sensitivity” of geospatial data is based on usefulness to terrorists

Do the data show “<u>choke points </u>to increase effectiveness of an attack ?”



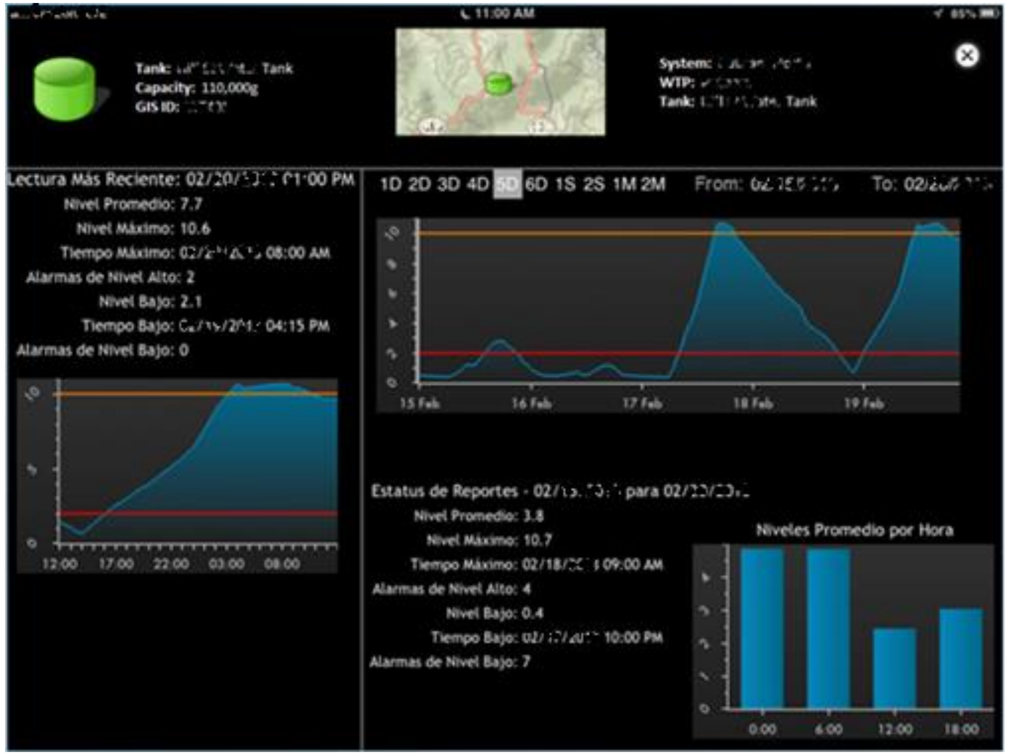
Decision Tree: *…risk assessment…*



4. Are these data useful for selecting specific target(s), and/or for planning and executing an attack on a potential target?

“Sensitivity” of geospatial data is based on usefulness to terrorists

Do the data “provide relevant current security-related data” that can help an attacker “find the best way to cause catastrophic failure ?”



Tank: [redacted] Tank
Capacity: 110,000g
GIS ID: [redacted]

System: [redacted]
WTP: [redacted]
Tank: [redacted] Tank

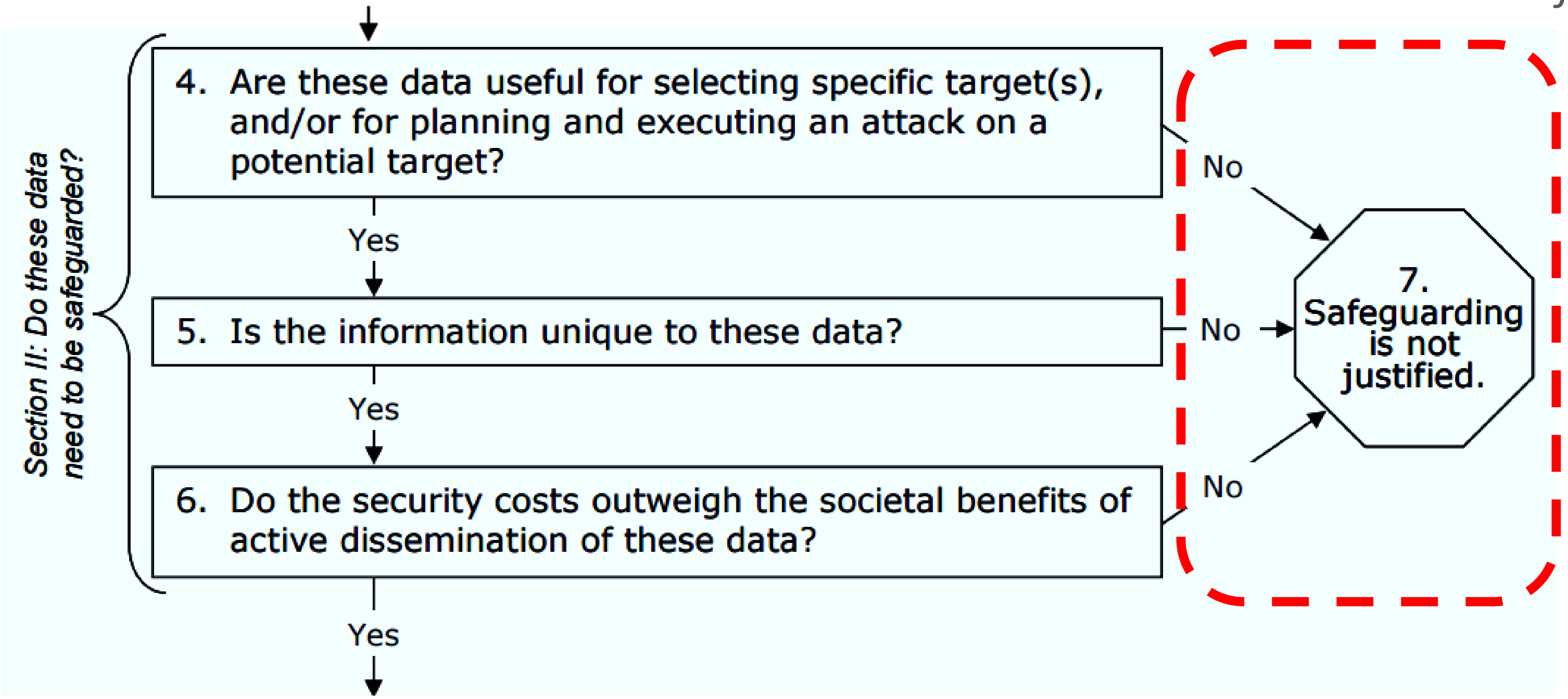
Lectura Más Reciente: 02/20/[redacted] 01:00 PM
Nivel Promedio: 7.7
Nivel Máximo: 10.6
Tiempo Máximo: 02/[redacted] 08:00 AM
Alarmas de Nivel Alto: 2
Nivel Bajo: 2.1
Tiempo Bajo: [redacted] 04:15 PM
Alarmas de Nivel Bajo: 0

From: [redacted] To: [redacted]

Estatus de Reportes - 02/[redacted] para 02/[redacted]
Nivel Promedio: 3.8
Nivel Máximo: 10.7
Tiempo Máximo: 02/18/[redacted] 09:00 AM
Alarmas de Nivel Alto: 4
Nivel Bajo: 0.4
Tiempo Bajo: 02/[redacted] 10:00 PM
Alarmas de Nivel Bajo: 7

Decision Tree: *…assess the risk…*

Do these data need to be safeguarded?



Section II: Do these data need to be safeguarded?

4. Are these data useful for selecting specific target(s), and/or for planning and executing an attack on a potential target?

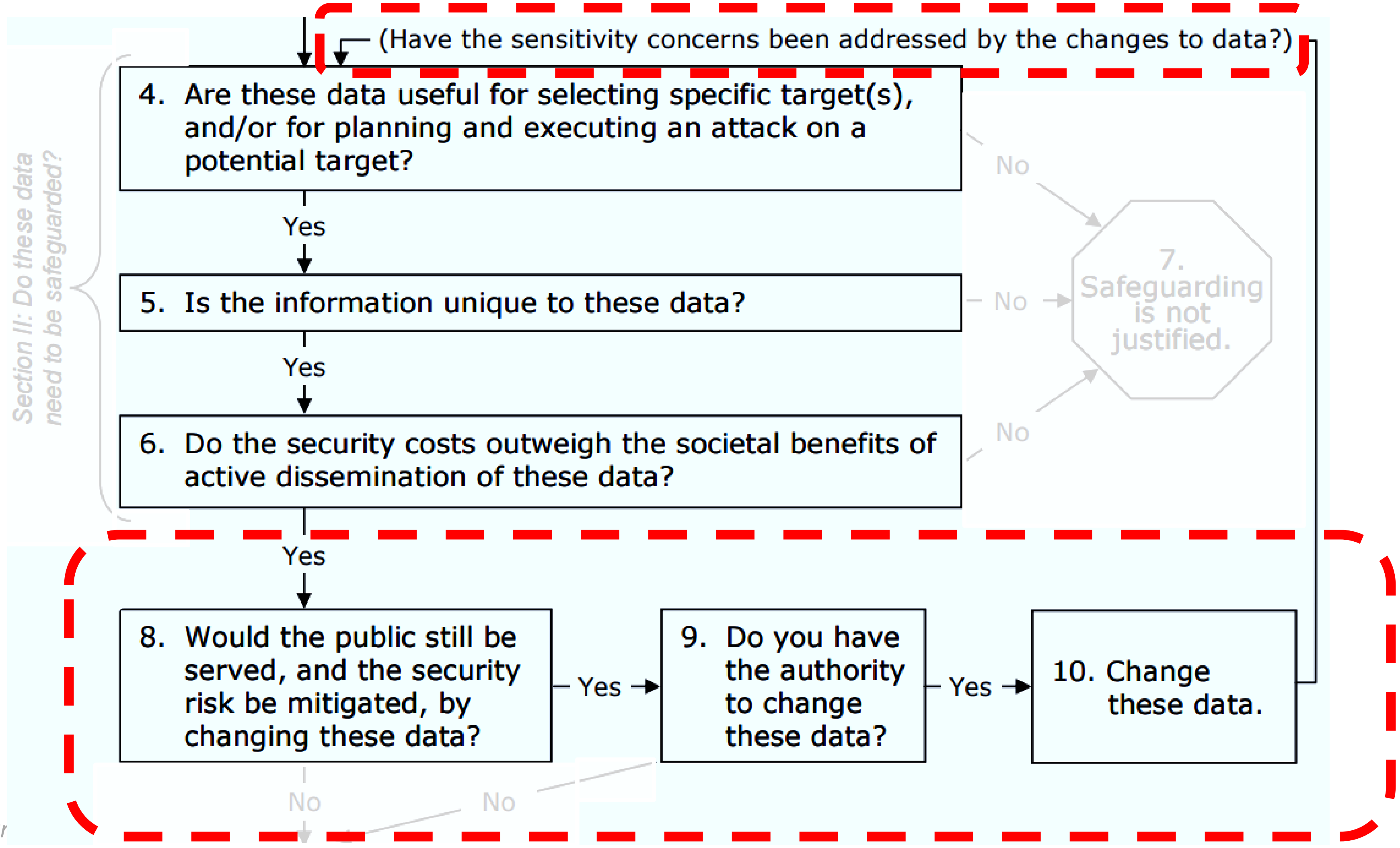
5. Is the information unique to these data?

6. Do the security costs outweigh the societal benefits of active dissemination of these data?

7. Safeguarding is not justified.

Decision Tree: *…control/mitigate the risk…*

Do these data need to be safeguarded?



(Have the sensitivity concerns been addressed by the changes to data?)

4. Are these data useful for selecting specific target(s), and/or for planning and executing an attack on a potential target?

5. Is the information unique to these data?

6. Do the security costs outweigh the societal benefits of active dissemination of these data?

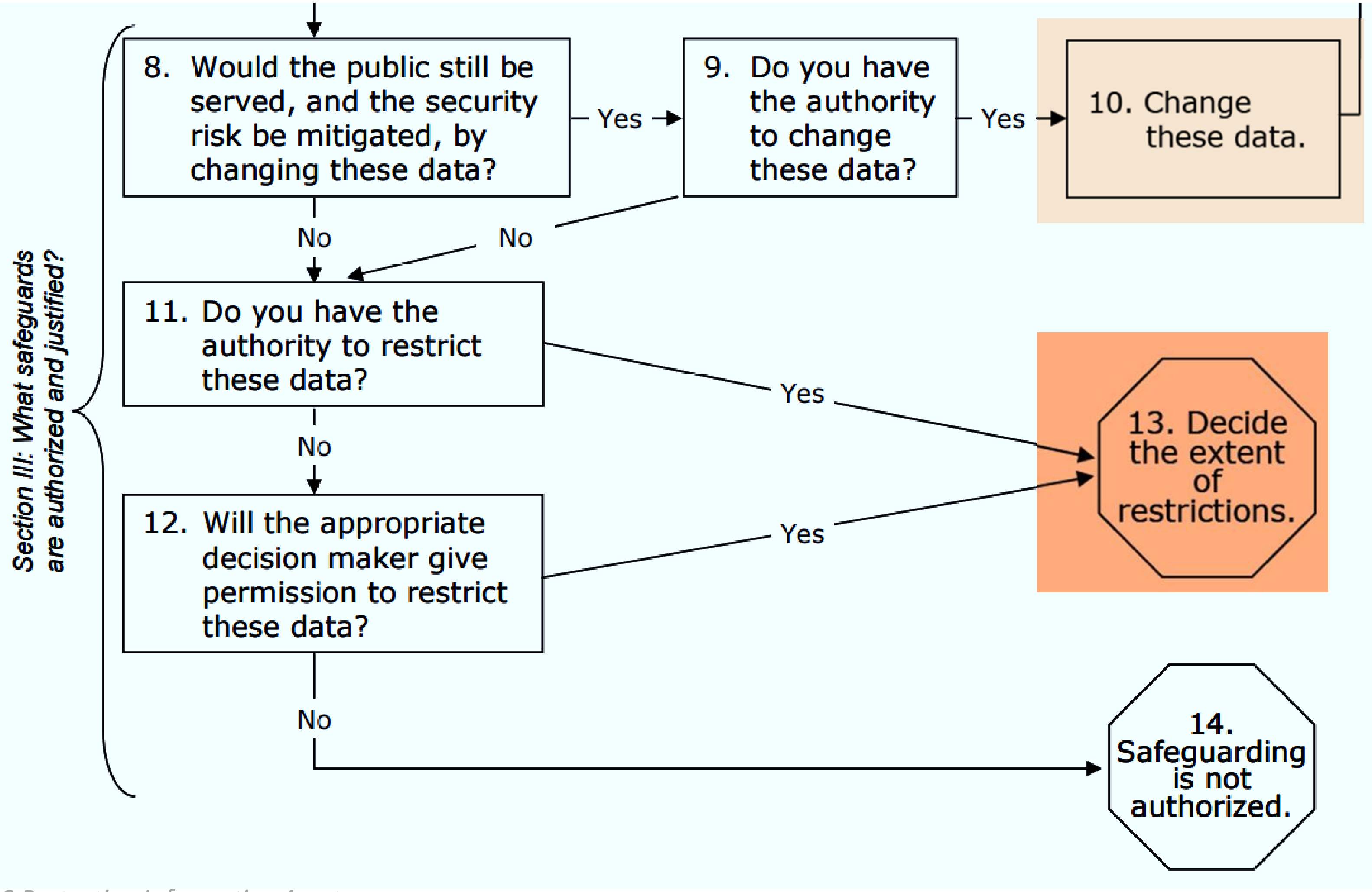
7. Safeguarding is not justified.

8. Would the public still be served, and the security risk be mitigated, by changing these data?

9. Do you have the authority to change these data?

10. Change these data.

Decision Tree: *…control/mitigate the risk…*


Section III: What safeguards are authorized and justified?
8. Would the public still be served, and the security risk be mitigated, by changing these data?
Yes
9. Do you have the authority to change these data?
Yes
10. Change these data.
No
No
11. Do you have the authority to restrict these data?
Yes
13. Decide the extent of restrictions.
No
12. Will the appropriate decision maker give permission to restrict these data?
Yes
No
14. Safeguarding is not authorized.

Decision Tree: *…control/mitigate the risk…*

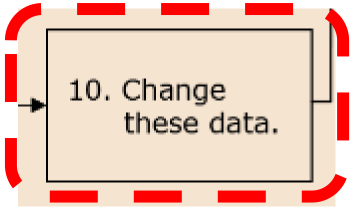
If security risks outweigh benefits of releasing the data to the public, and

if you have authority to change or restrict the data

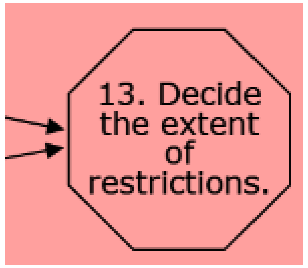
or if the appropriate decision maker gives permission to restrict the data

you can choose to safeguard data by:

- **Modifying data**
  - Remove or reduce detail in offending data elements
    - either in the attributes, spatial representations, or both

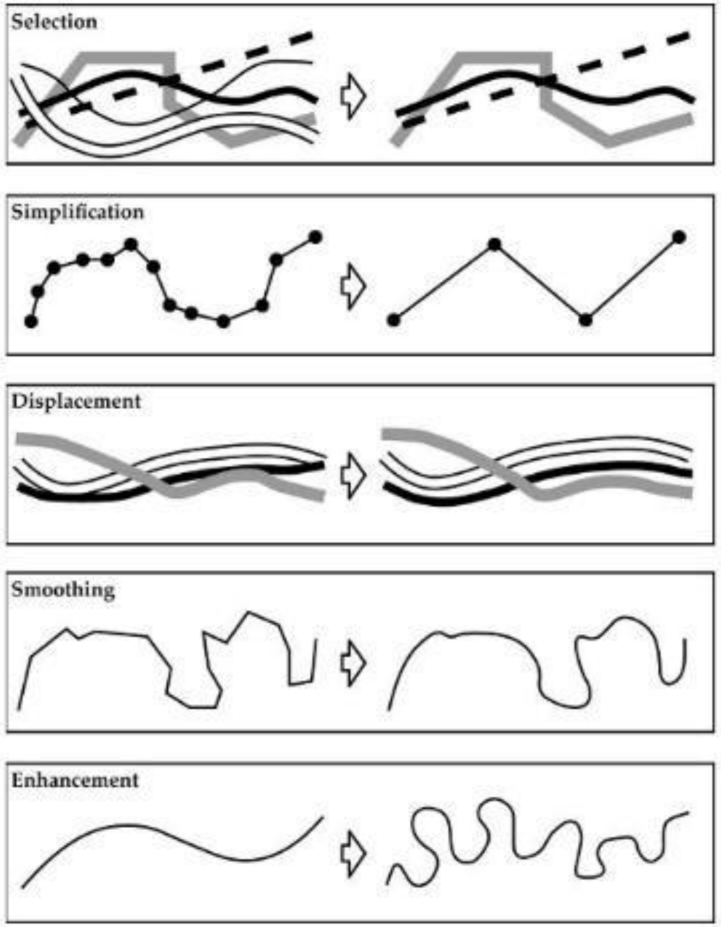


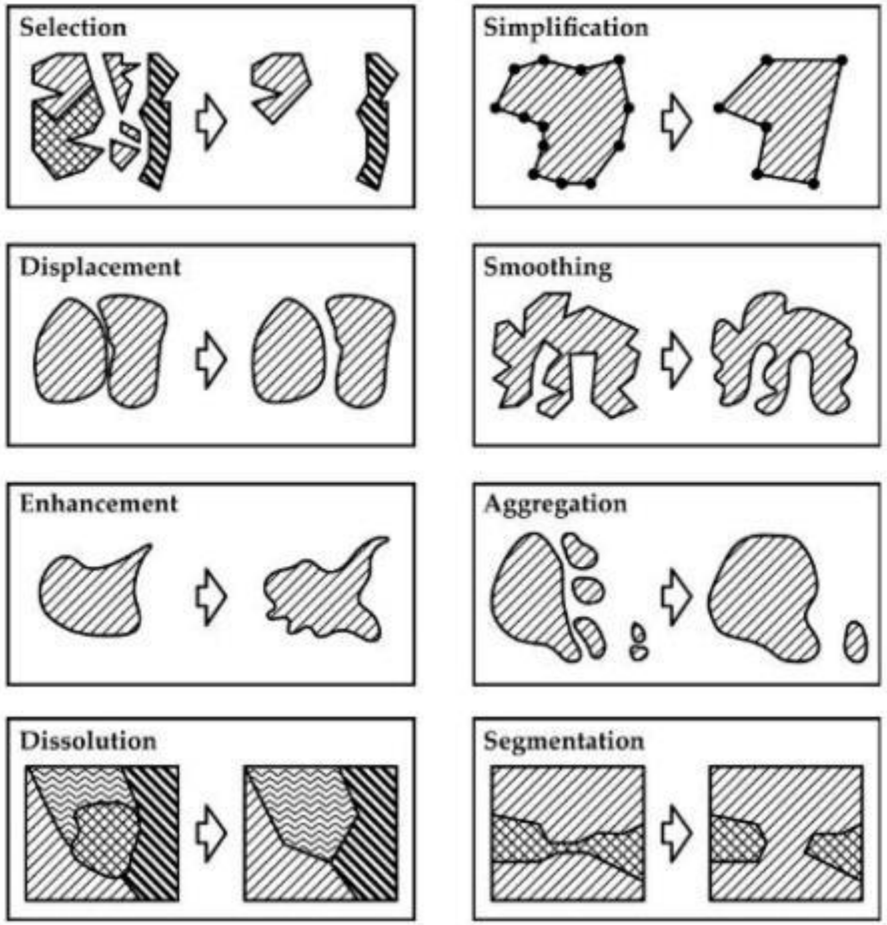
- **Restricting access to data**
  - If agency lacks authority to change data, or believes modifying data will undermine its value to the public, then agency can restrict access

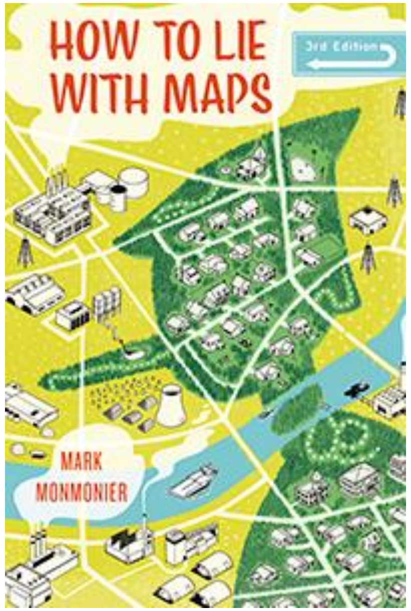


Change the Data to Control or Mitigate Risk

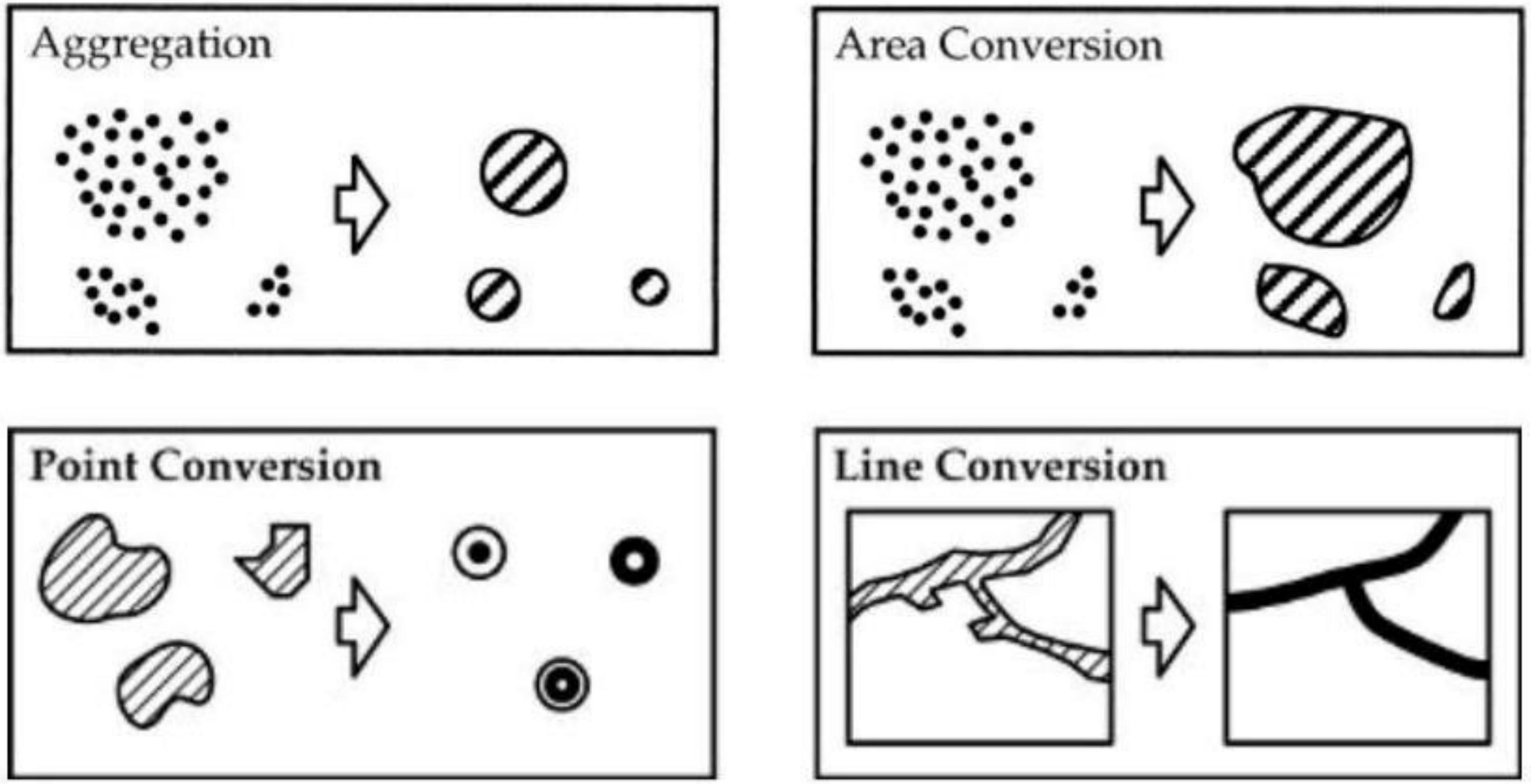
through "cartographic generalization"

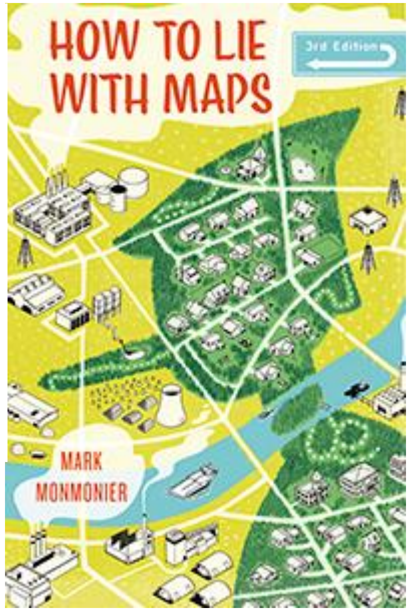




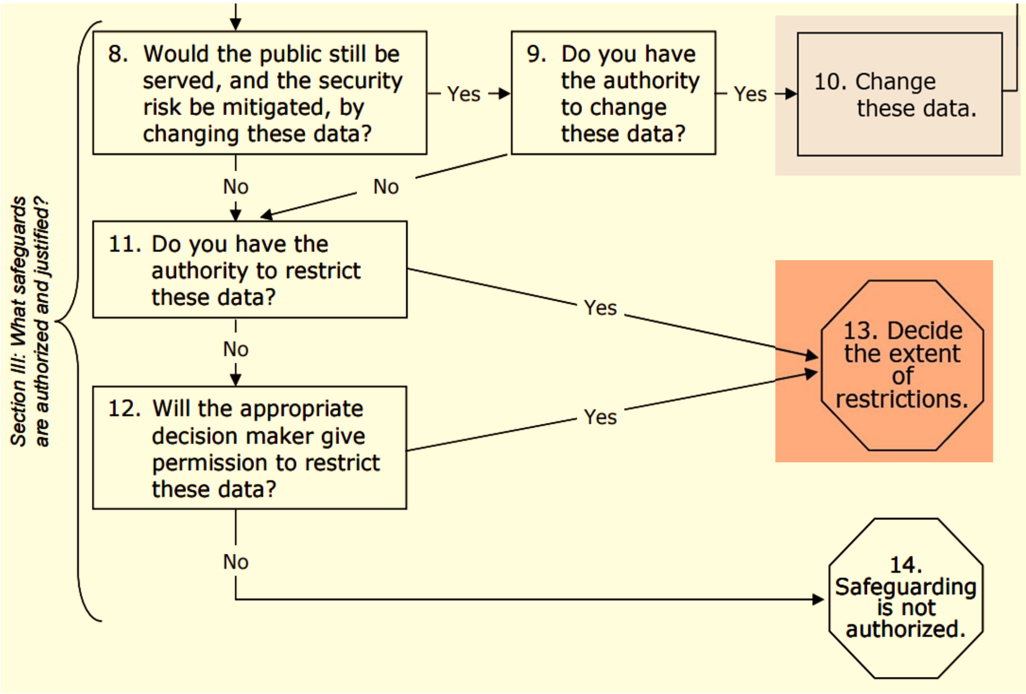


Change the Data to Control or Mitigate Risk





FGDC Guidelines' and FIPS 199 share which security objectives ?



Section III: What safeguards are authorized and justified?

8. Would the public still be served, and the security risk be mitigated, by changing these data?

Yes

9. Do you have the authority to change these data?

Yes

10. Change these data.

No

No

11. Do you have the authority to restrict these data?

Yes

No

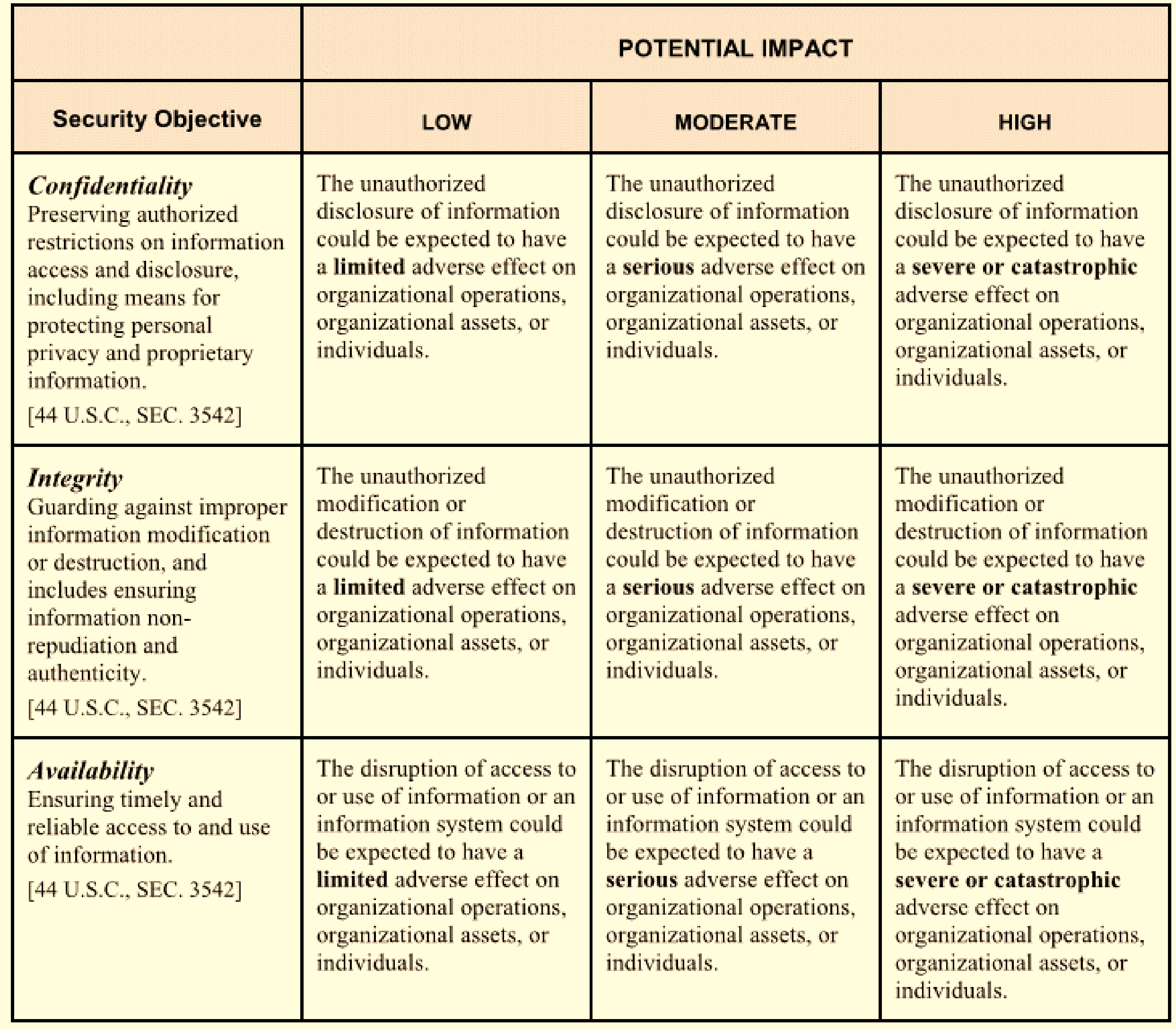
12. Will the appropriate decision maker give permission to restrict these data?

Yes

13. Decide the extent of restrictions.

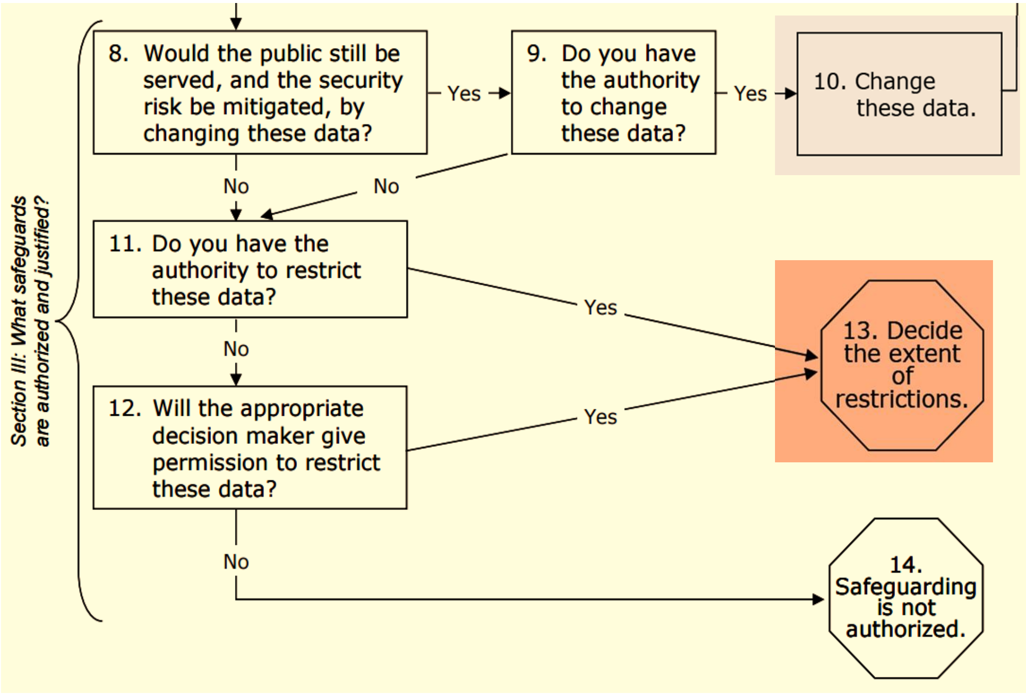
No

14. Safeguarding is not authorized.



	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

The FGDC guidelines potentially affect which FIPS 199 security objectives?



Section III: What safeguards are authorized and justified?

8. Would the public still be served, and the security risk be mitigated, by changing these data?

Yes →

9. Do you have the authority to change these data?

Yes →

10. Change these data.

No

No

11. Do you have the authority to restrict these data?

Yes

No

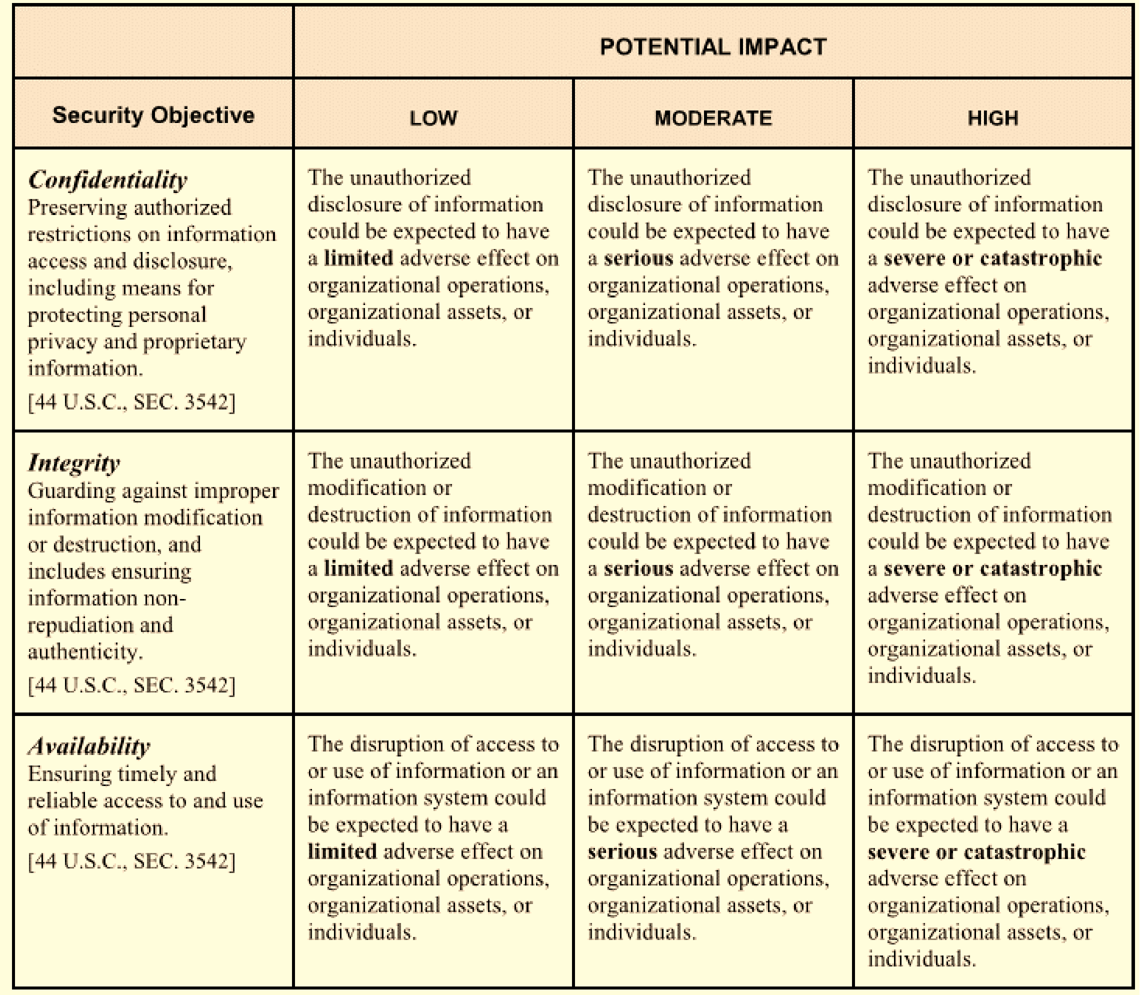
12. Will the appropriate decision maker give permission to restrict these data?

Yes

13. Decide the extent of restrictions.

No

14. Safeguarding is not authorized.



	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Agenda

- ✓ In the News
- ✓ Case study analysis
- ✓ Data Classification Process and Models
- Test taking tip
- Quiz

Test Taking Tip

- Read the answers first -

This contradicts many people's test taking recommendations…

…but, it works. Here's why:

- Quickly alerts you to the type of question to expect
- Focuses your attention in reading the question for meaningful information
- Gives you advanced warning that there may be more than one significant concepts (option to answer in the form "Both A & B")
- Gives you an opportunity to get a sense of the sort of answer the test maker is looking for
- There may be more than one valid answer, but the test maker may be looking for "best mitigation for the situation" or "least risk in the situation"

Test Taking Tip

Example:

A. Transaction authorization
B. Loss or duplication of EDI transmissions
C. Transmission delay
D. Deletion or manipulation of transactions prior to or after establishment of application controls

Test Taking Tip

Example:

Which of the following represents the GREATEST potential risk in an Electronic Data Interchange (EDI) environment?

A. Transaction authorization
B. Loss or duplication of EDI transmissions
C. Transmission delay
D. Deletion or manipulation of transactions prior to or after establishment of application controls

Test Taking Tip

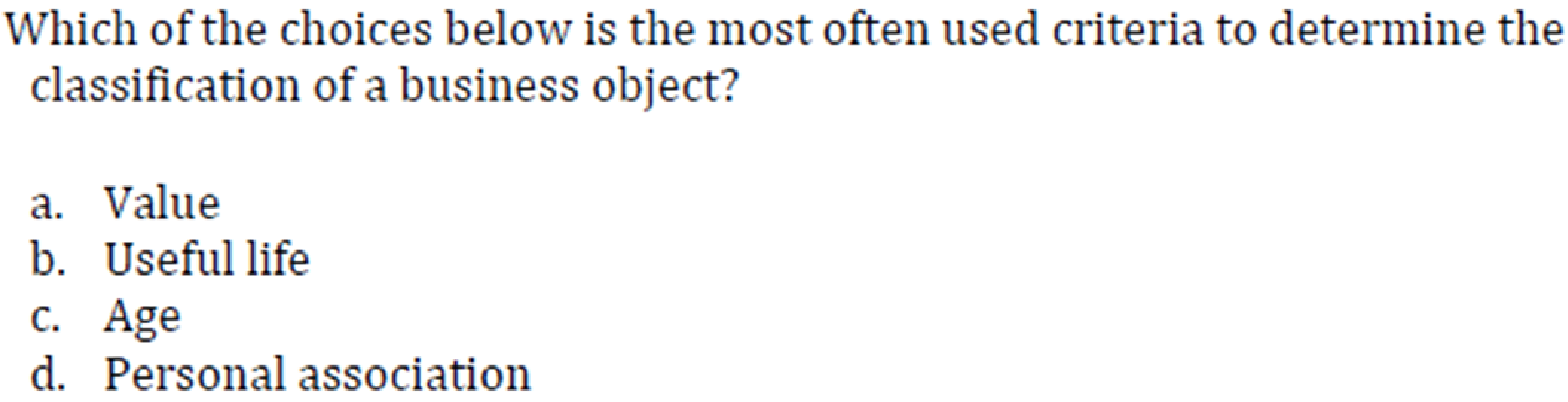
Example:

Which of the following represents the GREATEST potential risk in an Electronic Data Interchange (EDI) environment?

A. Transaction authorization
B. Loss or duplication of EDI transmissions
C. Transmission delay
D. Deletion or manipulation of transactions prior to or after establishment of application controls

Answer: A

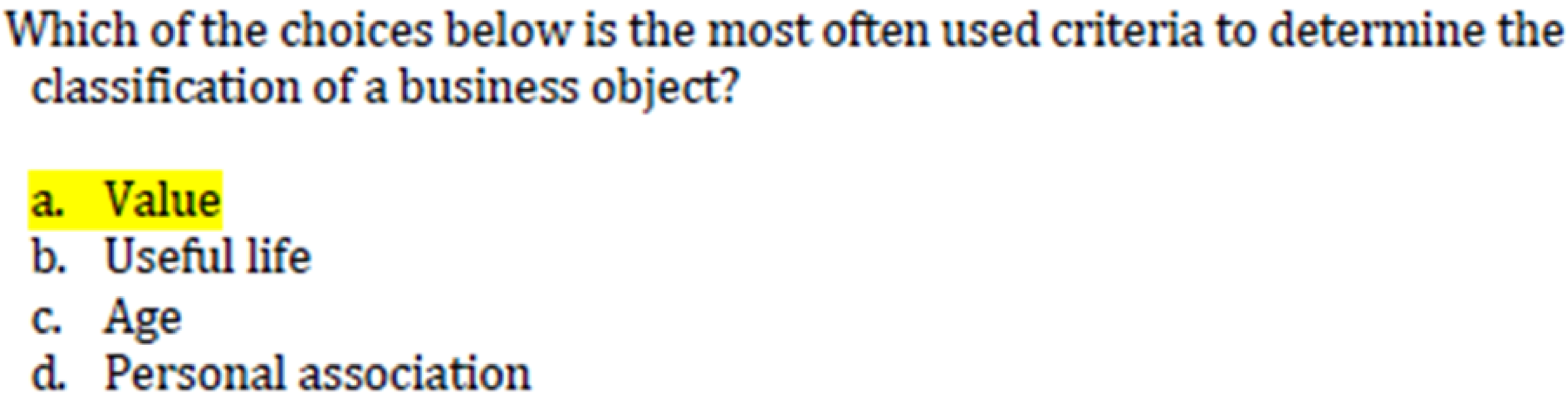
Quiz



Which of the choices below is the most often used criteria to determine the classification of a business object?

a. Value
b. Useful life
c. Age
d. Personal association

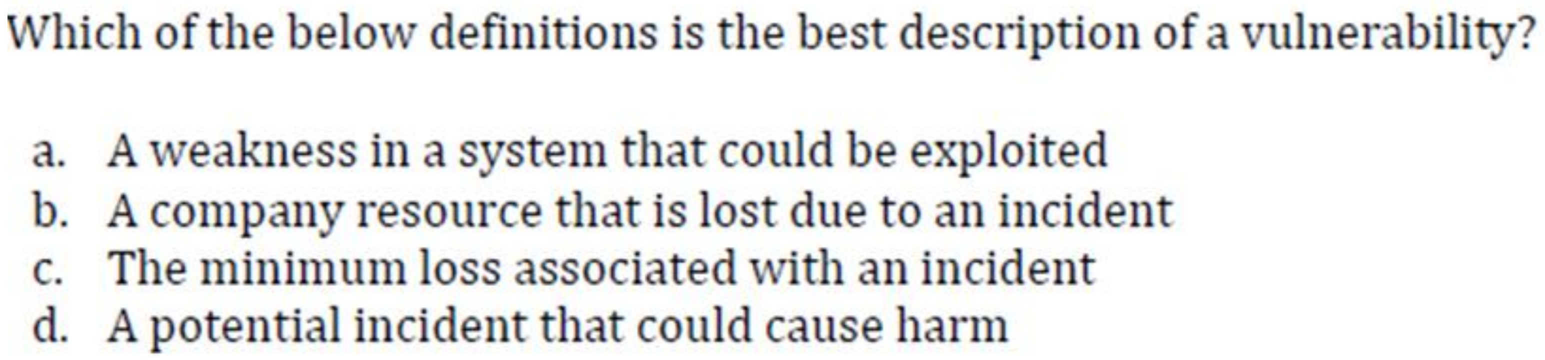
Quiz



Which of the choices below is the most often used criteria to determine the classification of a business object?

a. Value
b. Useful life
c. Age
d. Personal association

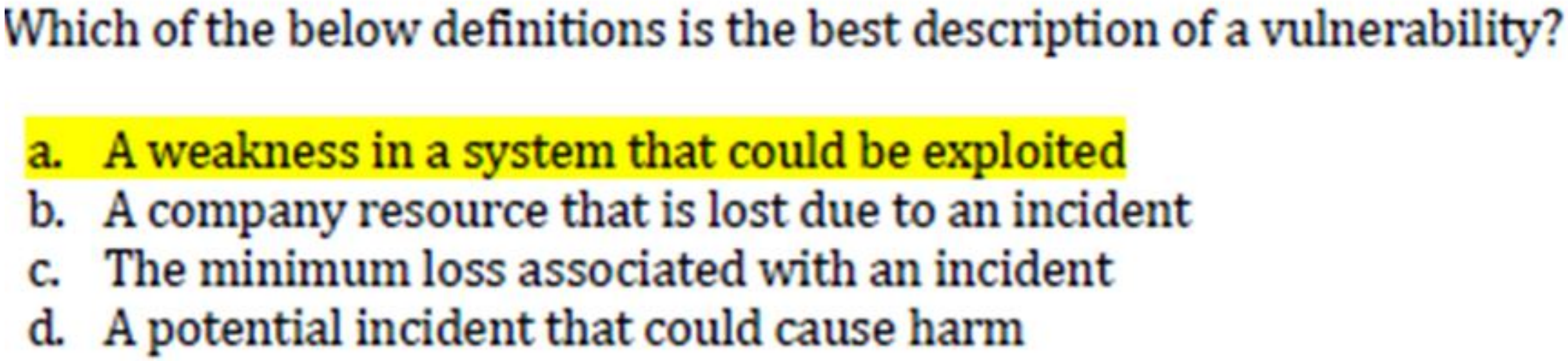
Quiz



Which of the below definitions is the best description of a vulnerability?

a. A weakness in a system that could be exploited
b. A company resource that is lost due to an incident
c. The minimum loss associated with an incident
d. A potential incident that could cause harm

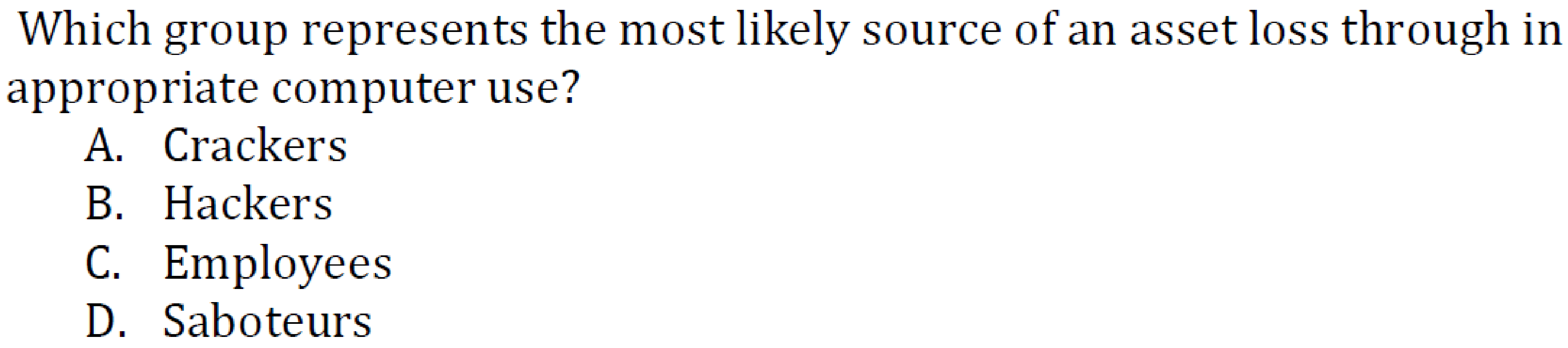
Quiz



Which of the below definitions is the best description of a vulnerability?

a. A weakness in a system that could be exploited
b. A company resource that is lost due to an incident
c. The minimum loss associated with an incident
d. A potential incident that could cause harm

Quiz



Which group represents the most likely source of an asset loss through in appropriate computer use?

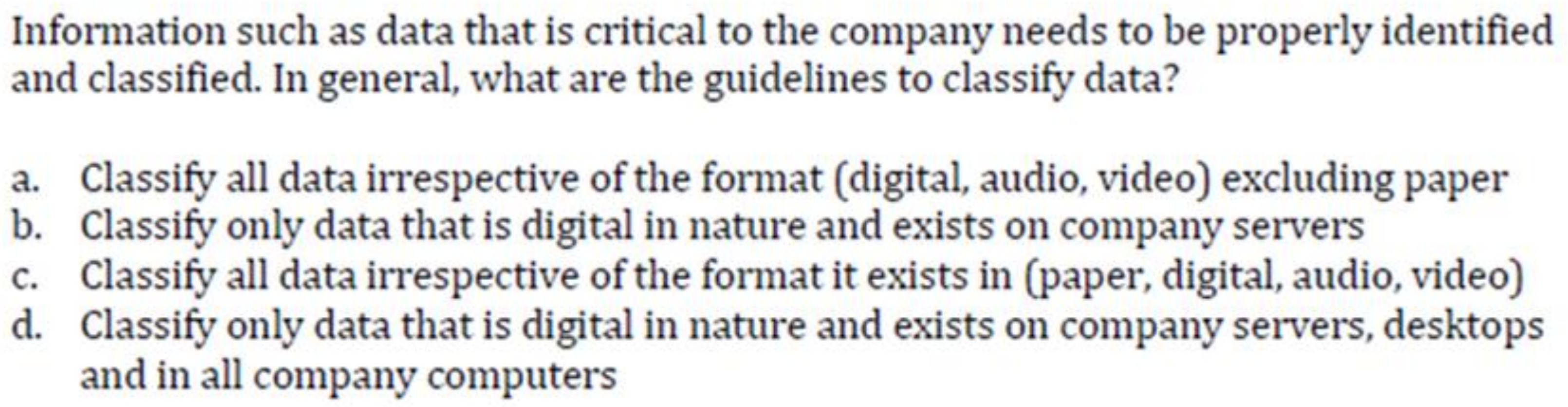
A. Crackers
B. Hackers
C. Employees
D. Saboteurs

Quiz

Which group represents the most likely source of an asset loss through in appropriate computer use?

A. Crackers
B. Hackers
C. Employees
D. Saboteurs

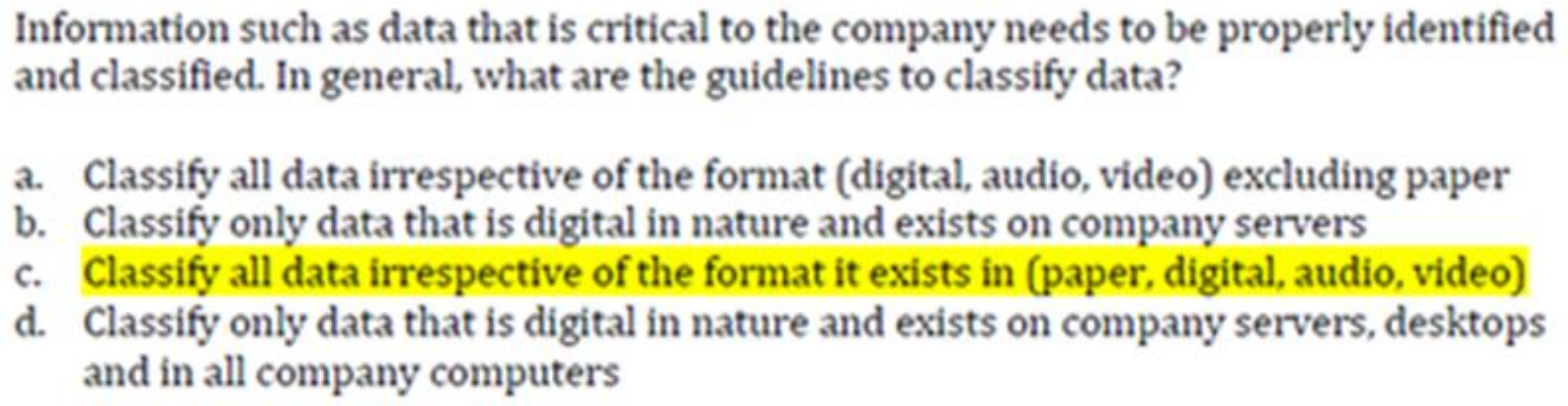
Quiz



Information such as data that is critical to the company needs to be properly identified and classified. In general, what are the guidelines to classify data?

a. Classify all data irrespective of the format (digital, audio, video) excluding paper
b. Classify only data that is digital in nature and exists on company servers
c. Classify all data irrespective of the format it exists in (paper, digital, audio, video)
d. Classify only data that is digital in nature and exists on company servers, desktops and in all company computers

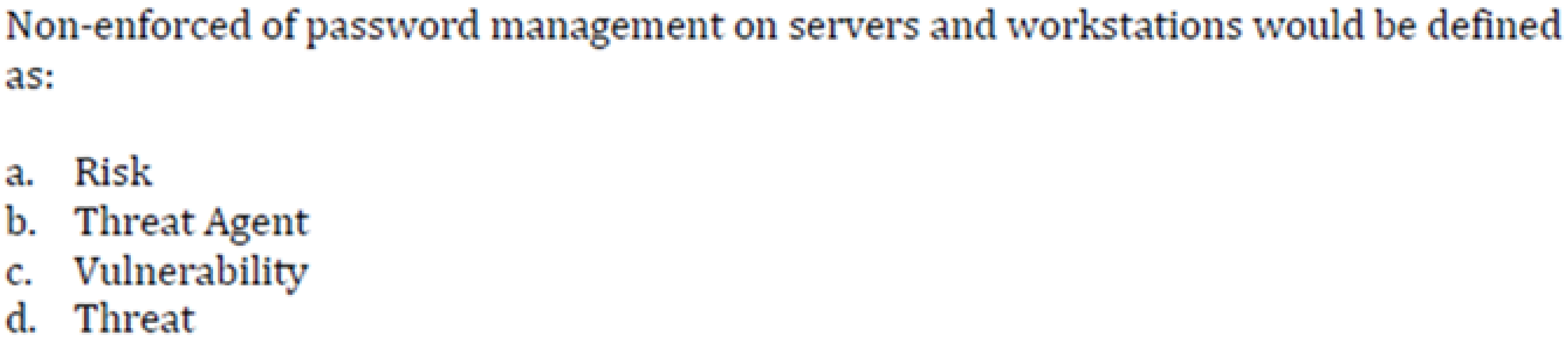
Quiz



Information such as data that is critical to the company needs to be properly identified and classified. In general, what are the guidelines to classify data?

a. Classify all data irrespective of the format (digital, audio, video) excluding paper
b. Classify only data that is digital in nature and exists on company servers
c. Classify all data irrespective of the format it exists in (paper, digital, audio, video)
d. Classify only data that is digital in nature and exists on company servers, desktops and in all company computers

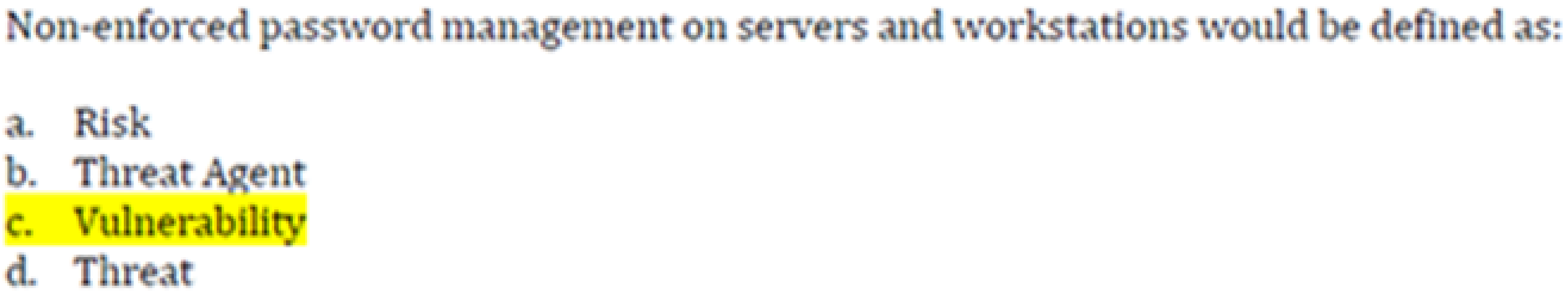
Quiz



Non-enforced of password management on servers and workstations would be defined as:

a. Risk
b. Threat Agent
c. Vulnerability
d. Threat

Quiz



Non-enforced password management on servers and workstations would be defined as:

a. Risk
b. Threat Agent
[✓ c. Vulnerability]
d. Threat

Agenda

- ✓In the News
- ✓Case study analysis
- ✓Data Classification Process and Models
- ✓Test taking tip
- ✓Quiz