Home Depot breach bigger than Target at 56 million cards

BOSTON/CHICAGO (Reuters) - Home Depot Inc Thursday said some 56 million payment cards were likely compromised in a cyberattack at its stores, suggesting the hacking attack at the home improvement chain was larger than last year's unprecedented breach at Target Corp.

Home Depot, in providing the first clues to how much the breach would cost, said that so far it has estimated costs of $62 million. But it indicated that costs could reach much higher.

It will take months to determine the full scope of the fraud, which affected Home Depot stores in both the United States and Canada and ran from April to September.

Retailer Target incurred costs of $148 million in its second fiscal quarter related to its breach. Target hackers stole at least 40 million payment card numbers and 70 million other pieces of customer data.

Home Depot said that criminals used unique, custom-built software that had not been seen in previous attacks and was designed to evade detection in its most complete account of what had happened since it first disclosed the breach on Sept. 8.

REUTERS

The company said that the hackers' method of entry has been closed off, the malware eliminated from its network, and that it had rolled out "enhanced encryption of payment data" to all U.S. stores.

"We apologize to our customers for the inconvenience and anxiety this has caused and want to reassure them that they will not be liable for fraudulent charges," Chief Executive Frank Blake said in a statement.

Of the estimated cost so far of $62 million, which covers such items as credit monitoring, increased call center staffing, and legal and professional services, Home Depot said it believes that $27 million of the amount will be paid for by insurers.

REUTERS/Beck Diefenbach A closeup of an electronic payment station is shown at a Home Depot store in Daly City, California, in this February 21, 2012 file photo.

But the company said it has not yet estimated the impact of "probable losses" related to the possible need to reimburse banks for fraud and card replacement, as well as covering costs of lawsuits and government investigations.

"Those costs may have a material adverse effect on The Home Depot's financial results in the fourth quarter and/or future periods," the company said in its statement.

Wesley McGrew, an expert of retail breaches who is an assistant research professor at the department of computer science at Mississippi State University, said that Home Depot is going to be expected to bear the costs related to fraud and payment card replacement.

Banks typically seek to get retailers to cover those costs if there are any indications of shortcomings in their security.

Criminals have frequently used software that evades detection, but retailers are expected to closely monitor their networks using tools that are designed to uncover signs of a crime in progress, McGrew said.

"It's hard to feel sorry for them when there are things they could have done to improve the security of these transactions," McGrew said.

Hitesh Sheth, chief executive of Vectra Networks, a cybersecurity firm in San Jose, California, said Home Depot's breach exposes a weakness, noting that the company said hackers used unique, custom-built malware.

That "essentially means the technology they are using is only designed to detect malware that has already been used in a previous attack, and that is symptomatic of the retail industry," Sheth said.

"Retailers need to upgrade to technology that is available and detects behavior of malware that is new because these attacks are not going to stop anytime soon."

For its fiscal year ending in February, Home Depot revised its earnings estimate to $4.54 per share from $4.52. In addition to the cost related to the breach, it said the estimate includes a pre-tax gain of about $100 million on the sale of 3.6 million common shares of HD Supply stock.

The company left its outlook for sales growth for the year at 4.8 percent.

(Reporting by Jim Finkle in Boston and Nandita Bose in Chicago; Additional reporting by Shailaja Sharma in Bangalore; Editing by Leslie Adler and Jilian Mincer)

Secure Software Development Requirements

Objectives

- Differentiate between security goals and security functions
- Explain the concept of a security requirement
- List the three characteristics for secure software
- Explain the concept of a security profile
- Explain confidentiality requirements
- Explain integrity requirements
- Explain authentication requirements
- Compare and contract simple authentication, two factor authentication, and multifactor identification

How do you describe a system

Use cases / Requirements } Architecture diagrams

UML

How do you describe a system

Normative Behavior

⇒ Correct usage

⇒ Defect free SW

Assumption:

No one will abuse the system.

⇒ AKA "Bad Guys"

- What makes for good requirements?

Requirements

Detail

Complete

⇒ Stakeholder involvement

Unambiguous

:

:

- What is the key difference between software quality and software security?

Malicious Intent

Conceptualization

What security requirements are NOT

- Security goals

Goals are more abstract.

- Security functions

encryption
Logging
etc.

} Part of Solution

MSOE

Secure Software Characterization

- Reliability
  - The software functions as it is expected to
- Resiliency
  - The software does not violate any security policy and is able to withstand the actions of threat agents that are posed intentionally
- Recoverability
  - The software is able to restore operations to what the business expects by containing and limiting damage

What security is not

- Not a component that can be added to software
  - Cryptography
  - SSL
  - 128 bit encryption
- The tent example

Security Requirements

- Definition
  - Security requirements represent constraints placed upon functional requirements to achieve security goals
- Typically define what the system shall not do.
  - Example:
    - The system shall not provide Personnel Information except to members of the Human Resources Department.

Limits functionality

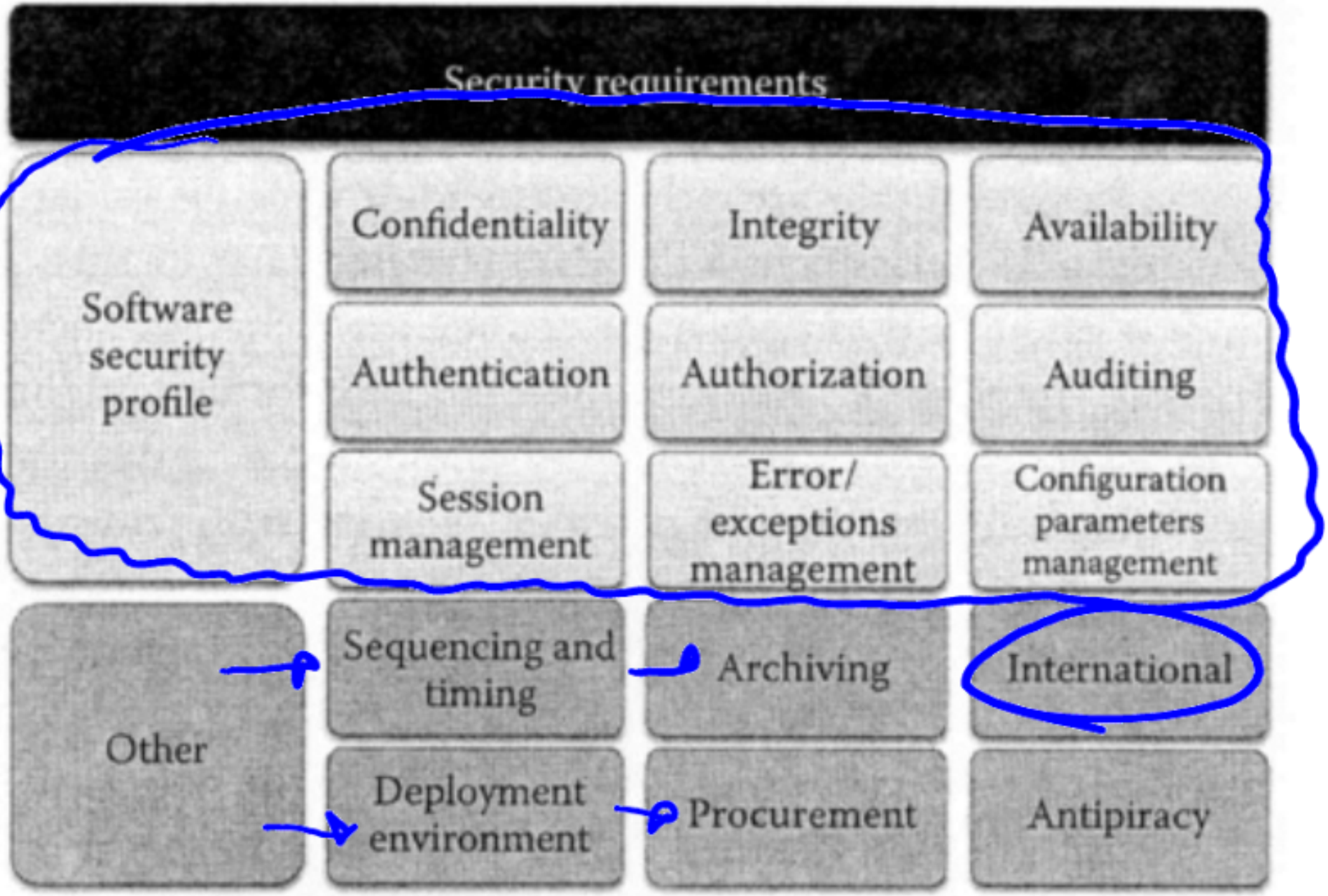
Question

- Which of the following policies is most likely to include the following requirement? "All software processing financial transactions needs to use more than one factor to verify the entity requesting access."

a. Authorization
b. Authentication
c. Auditing
d. Availability
e. Resiliency

Software Security Profile

Taxonomy of Security Requirements

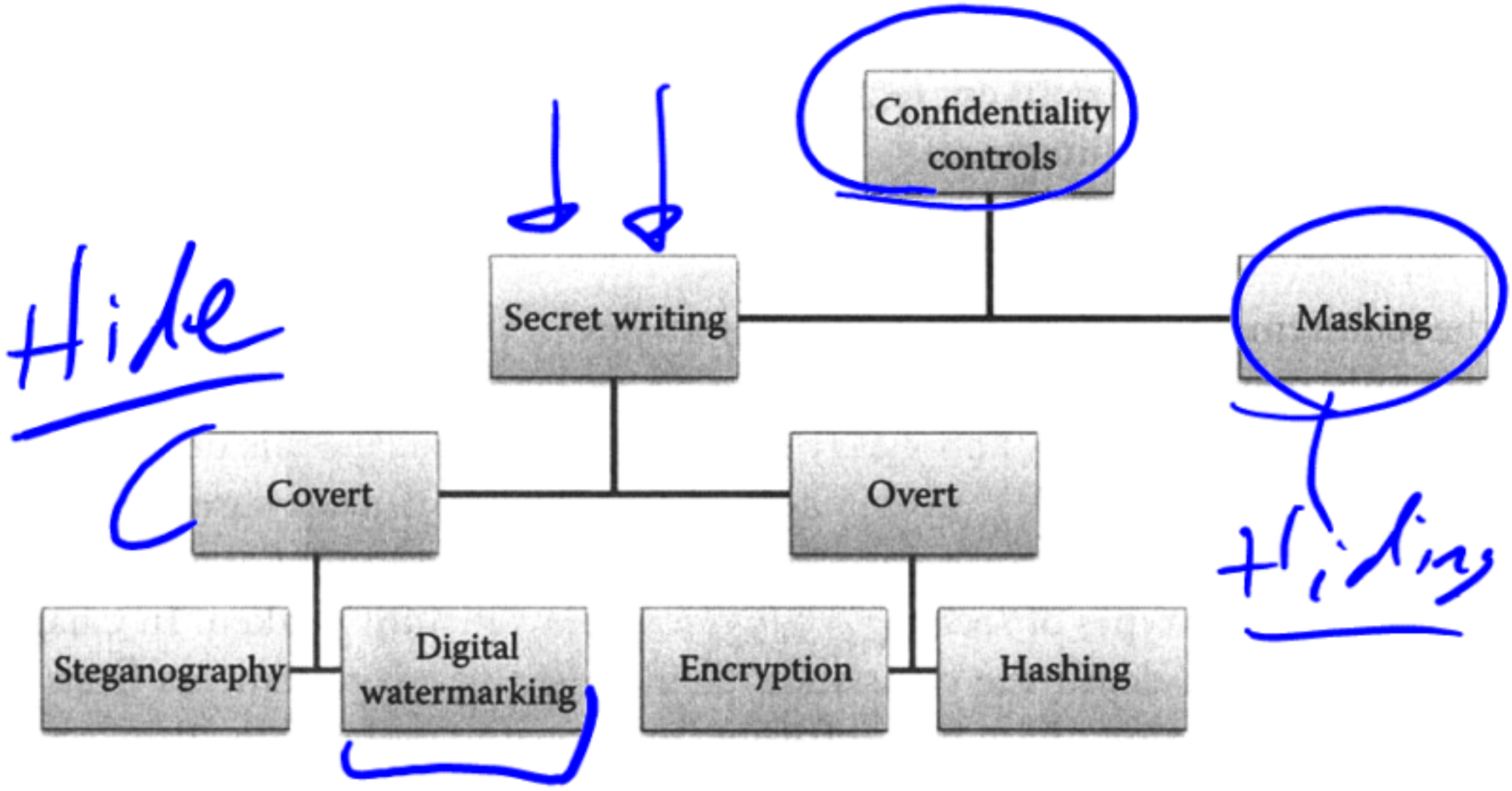


Confidentiality Requirements

- Requirements that address protection against the disclosure of data or information that is either personal or sensitive in nature
  - Uses data classification to define
  - Accomplished by one of many techniques
  - Need to be defined throughout the information lifecycle, from the origin of the data until retirement

Start to finish

Confidentiality Protection Mechanisms



Example confidentiality requirements

- Personal health information must be protected against disclosure using approved encryption mechanisms
- Passwords and other sensitive input fields need to be masked
- The use of nonsecure transport protocols such as File Transfer Protocol (FTP) to transmit account credentials in clear to third parties outside of your organization shall not be allowed.

Integrity Requirements

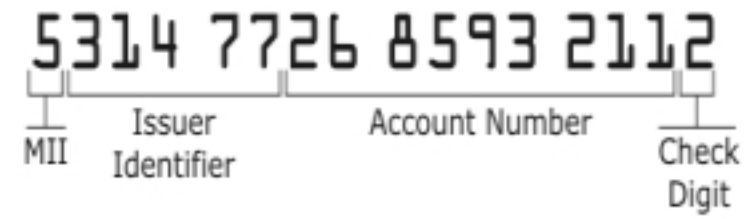
- Address reliability assurance and protection against unwanted modification
  - Needs to deal with both system and data integrity
- May use one or more of the following
  - Input validation
  - Parity bit checking
  - hashing

Example Requirements

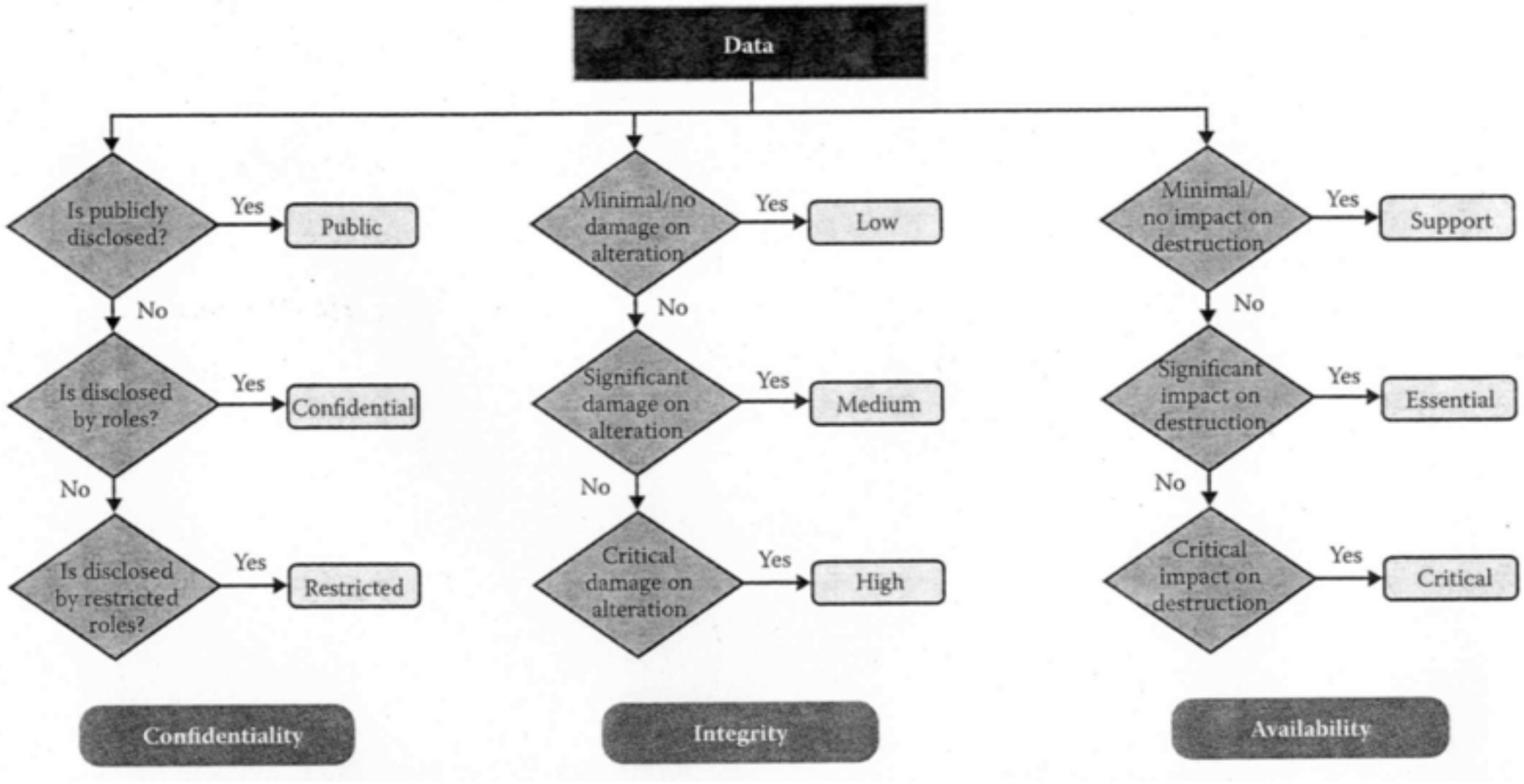
- All input forms and query strings shall be validated against a set of allowable inputs before the software accepts it for processing

- All messages transmitted over the internet shall be checked or corruption before being processed

Credit Card Validation



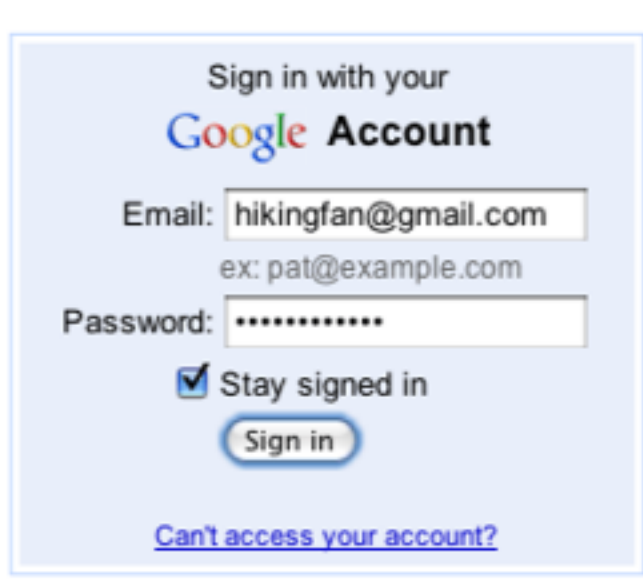
Categorization of data



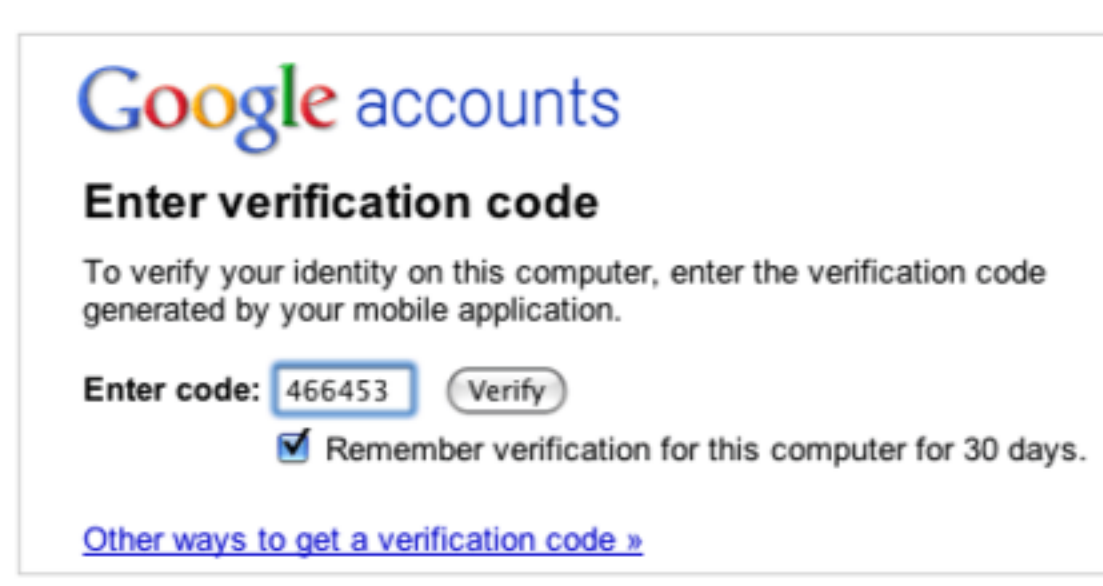
Authentication requirements

- The process of validating an entity's claim
  - Are you who you say you are
- Two factor identification
  - Uses two factors for identification
  - Something someone knows
  - Something someone has

1.



2.



- Multifactor authentication
  - Uses multiple factors for authentication