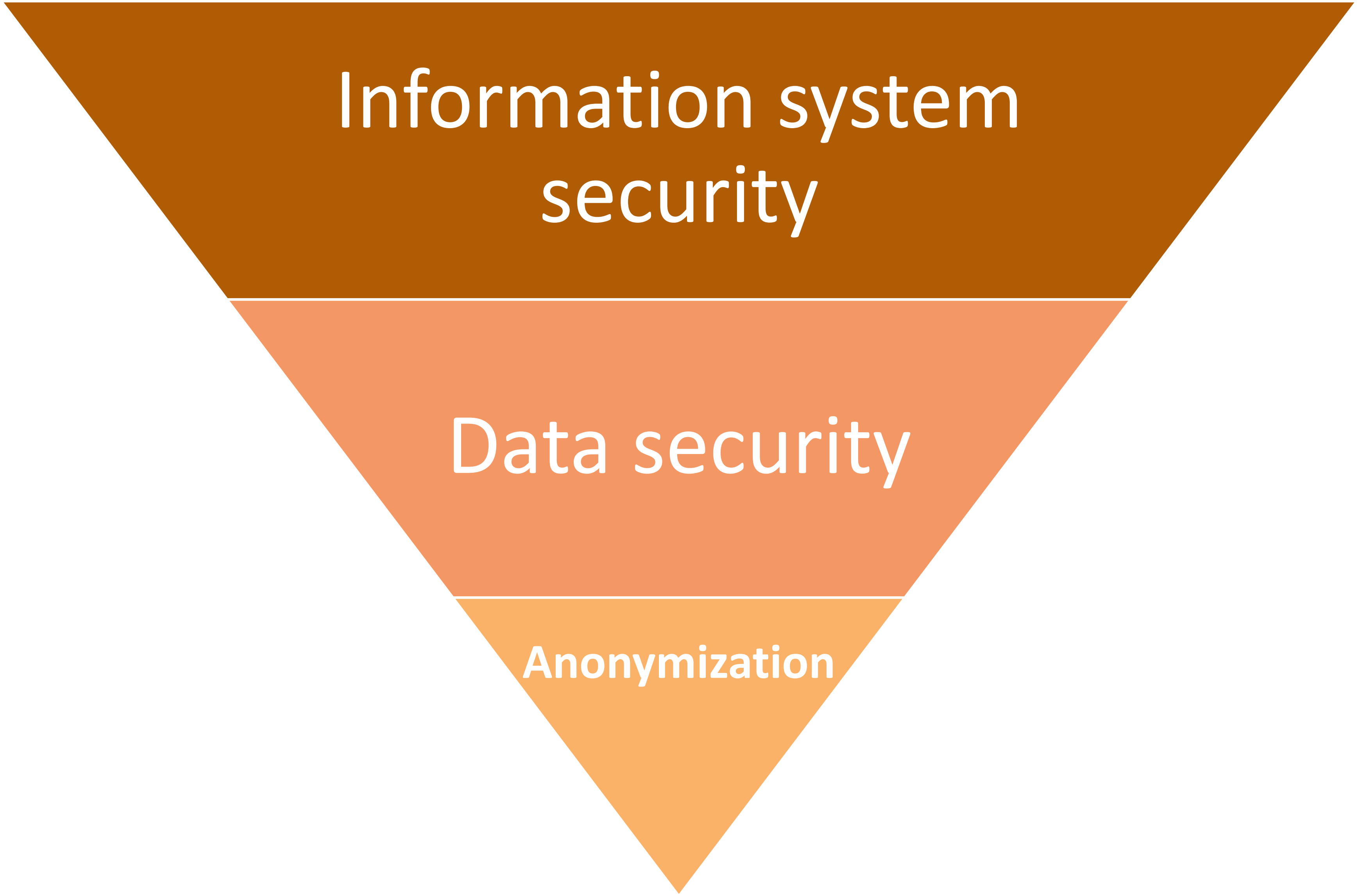
DATA SECURITY – PART 1

I. WATTIAU

IDSI32403 – MASTER DATA SCIENCE

Learning objectives

- ❑ Describe the key concepts of **information system security**
- ❑ Explain the fundamental **data security** principles
- ❑ Understand the **anonymization** techniques



Information system security

Data security

Anonymization

Figures [Source: CSO]

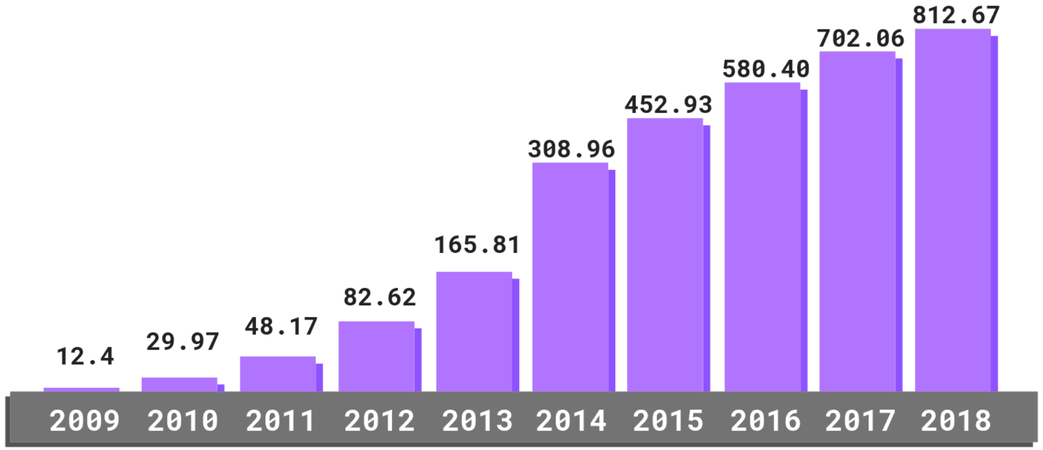
1. Cyber crime damage costs to hit $6 trillion annually by 2021 (up from $3 trillion in 2015)

2. Cybersecurity spending to exceed $1 trillion from 2017 to 2021

3. Cyber crime will more than triple the number of unfilled cybersecurity jobs, which is predicted to reach 3.5 million by 2021

4. Human attack surface to reach 6 billion people by 2022 (75% of the projected world population of 8 billion)

5. **Global Ransomware Damage Costs** Predicted To Reach $20 Billion (USD) By 2021 **(vs. $5 billion in 2017)**



Total Malware Infection Growth Rate (In Millions)

Figures from other sources

- Cybercrime now accounts for more than 50% of all crimes in the UK. (*Source:* National Crime Agency)
- Hackers are attacking computers and networks at a **“near-constant rate”**, with an average of one attack every 39 seconds. (*Source*: University of Maryland)
- Most network intrusions (**63%) are the result of compromised user passwords** and usernames. (*Source:* Microsoft)
- Cisco found that globally, 8% of malicious email attachments were **docm files** (*Source:* Cisco)
- **18 million new malware samples** were captured in Q3 2016. (*Source:* Panda Security)
- **IoT devices suffer an average of 5,200 cyber attacks every month (**Source: network of security bloggers)
- At 91.6% **“Theft of Data” continues to be the chief cause of data breaches** in 2016 counting total by identities stolen. “Phishing, Spoofing, and Social Engineering” were a distant second at 6.4% (*Source:* Symantec)
- The number of ransomware families increased from 30 in 2015 to 98 in 2016, revealing the distinct focus by cyber criminals on **using ransomware to extort money from businesses and individuals.** (*Source:* Symantec)

Frequently Reported Computer Crimes

Credit-card fraud

- Numbers captured and used fraudulently

Data communications fraud

- Piggyback on someone else's network
- Office network for personal purposes
- Computer-directed diversion of funds

Unauthorized access to computer files

- Accessing confidential employee records
- Theft of trade secrets and product pricing

Unlawful copying of copyrighted software

Information System Security: A definition

❑ **Protecting** information and information systems [NIST definition]

from unauthorized access, use, disclosure, disruption, modification, or destruction

in order to provide:

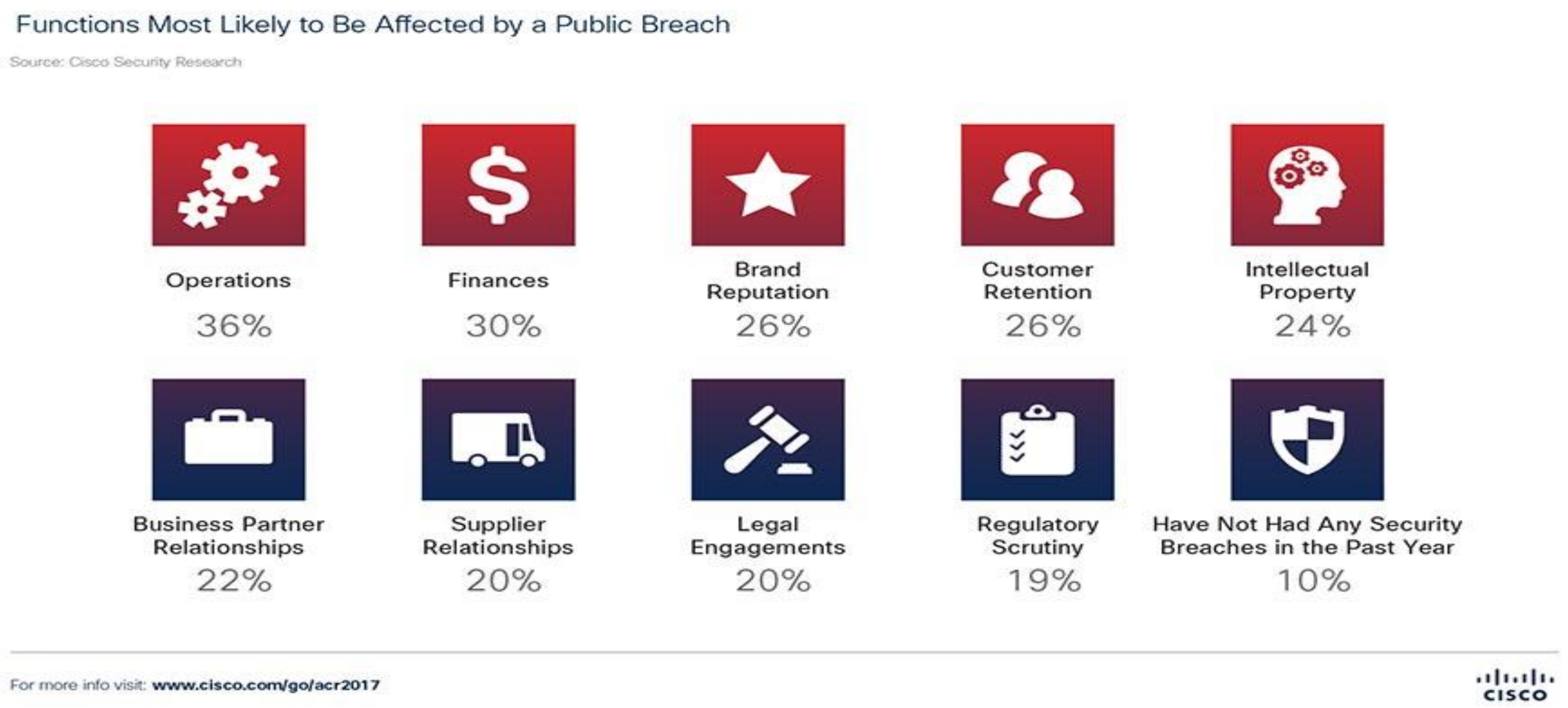
- ❑ **integrity**
- ❑ **confidentiality**
- ❑ **availability**

Information System Security (cont’d)

- ❑ **integrity**: guarding against improper information modification or destruction
  - ❑ includes ensuring information non-repudiation and authenticity
- ❑ **confidentiality**: preserving authorized restrictions on access and disclosure
  - ❑ includes means for protecting personal **privacy** and proprietary information
- ❑ **availability:** ensuring timely and reliable access to and use of information [NIST definition]

EXERCISE 1

Protect assets and reputation



Functions Most Likely to Be Affected by a Public Breach

Source: Cisco Security Research

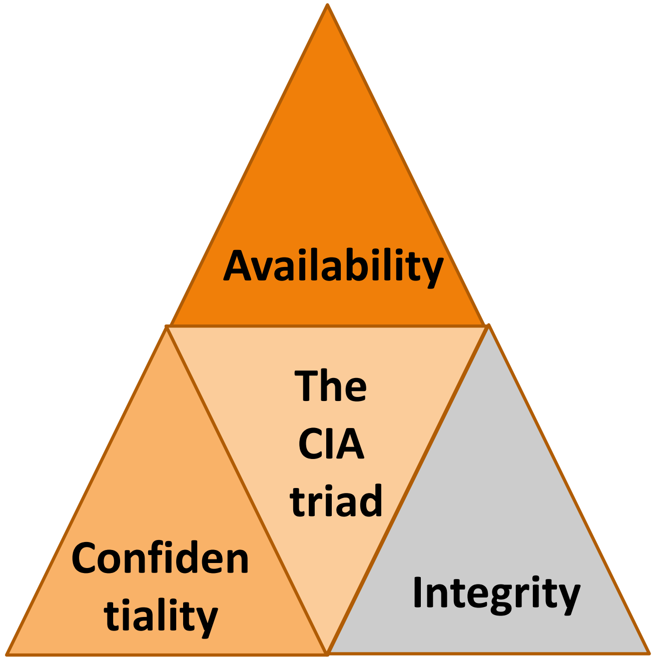
Operations	36%
Finances	30%
Brand Reputation	26%
Customer Retention	26%
Intellectual Property	24%
Business Partner Relationships	22%
Supplier Relationships	20%
Legal Engagements	20%
Regulatory Scrutiny	19%
Have Not Had Any Security Breaches in the Past Year	10%

For more info visit: **www.cisco.com/go/acr2017**

Challenges of information system security

- Many evolving concepts
- You must consider potential (unexpected) attacks
- Procedures used are often counter-intuitive
- It is not perceived on benefit until fails
- Requires constant monitoring
- Contradiction between protection and availability

Three security objectives



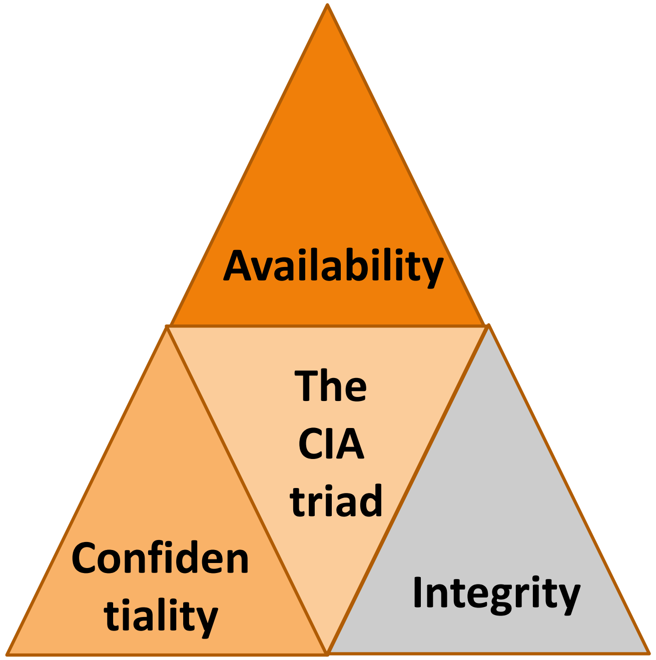
Keep data secure

- Destruction
- Accidental damage
- Theft
- Espionage

Keep data private

- Salaries
- Medical information
- Social security numbers
- Bank balances

Three security objectives (and more?)



Authenticity: the property of being genuine and being able to be verified and trusted; confident in the validity of a transmission, or a message, or its originator

Accountability: generates the requirement for actions of an entity to be traced uniquely to that individual to support nonrepudiation, deference, fault isolation, etc

Security Implementation Principles

- **Confidentiality**
- **Integrity**
- **Availability**
- **Need-to-know**
  - Users should only have access to information (or systems) that enable them to perform their assigned job functions.
- **Least privilege**
  - Users should only have sufficient access privilege that allow them to perform their assigned work.
- **Separation of duties**
  - No person should be responsible for completing a task involving sensitive, valuable or critical information from the beginning to end.
  - No single person should be responsible for approving his/her own work.
- **Job rotation**
  - To reduce risk of collusion
  - To ensure no single point of failure
- **Mandatory vacation**
  - To allow auditors to review records

A security model

Threat Agent Entity that may act on a vulnerability

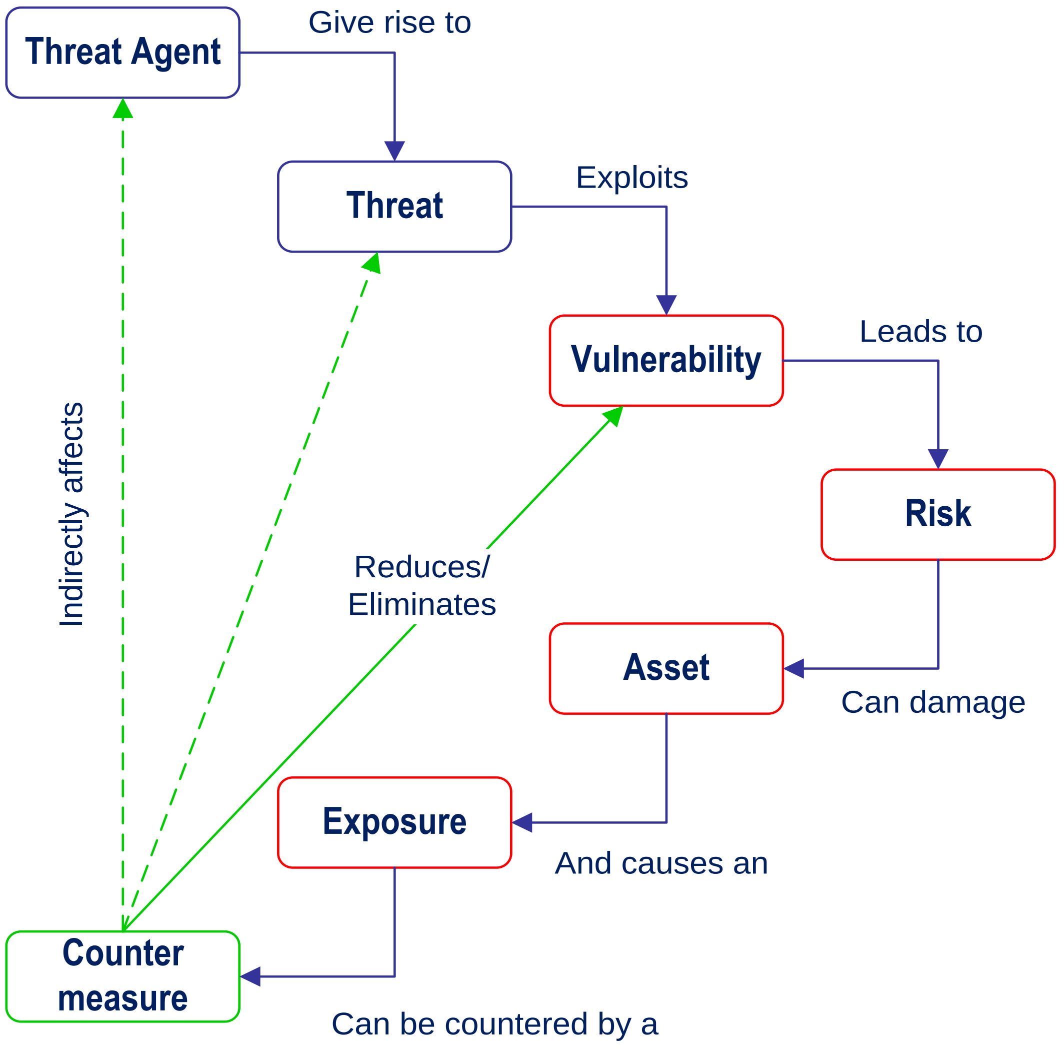
Threat Potential danger to information life cycle

Vulnerability Weakness that may provide an opportunity for a threat agent

Risk Likelihood of a threat agent exploits the discovered vulnerability

Exposure Instance of being compromised by a threat agent.

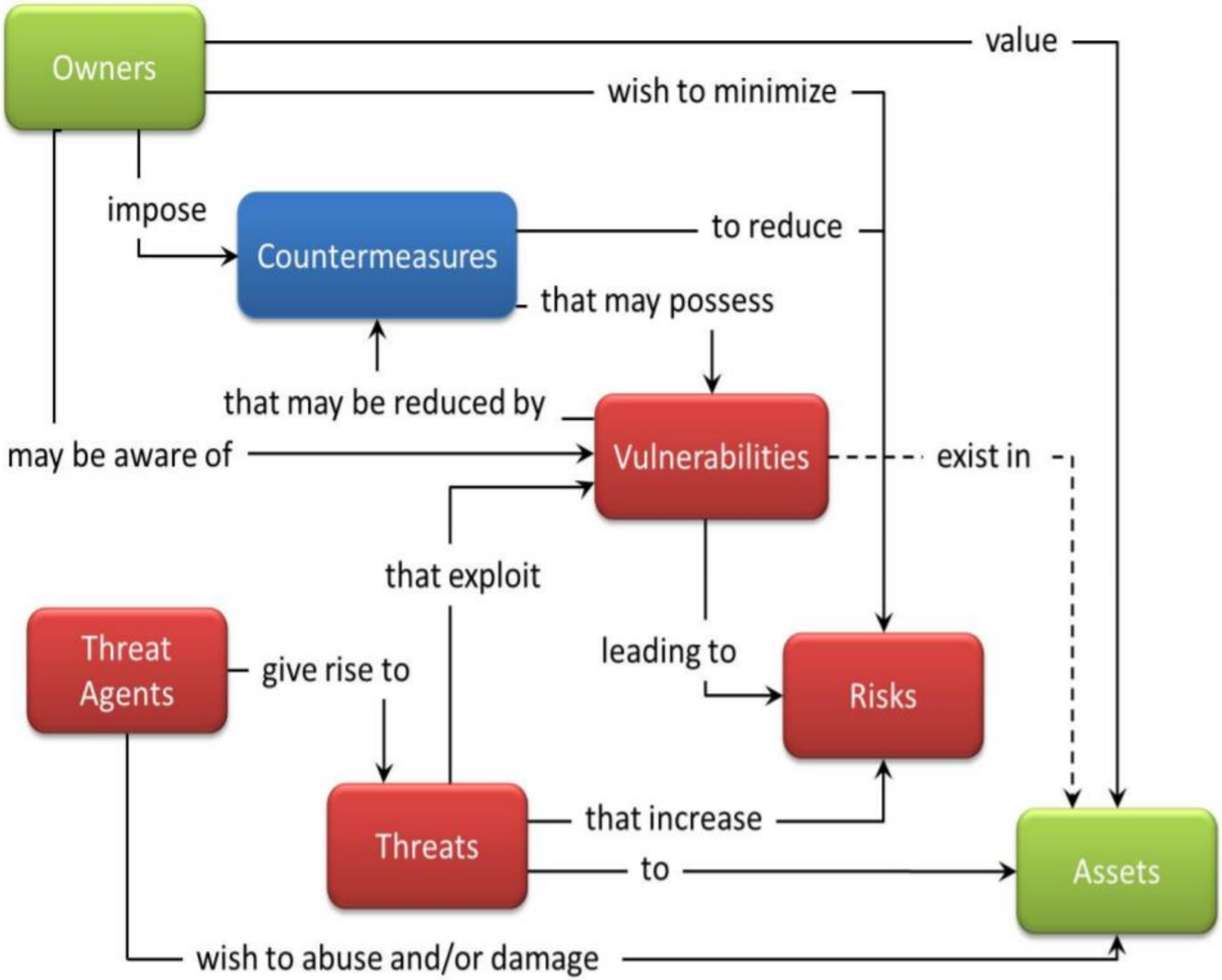
Countermeasure / safeguard/control Administrative, operational, or logical mitigation against potential risk(s)



Reference: *Information Assurance Technical Framework (IATF)*, Release 2.3

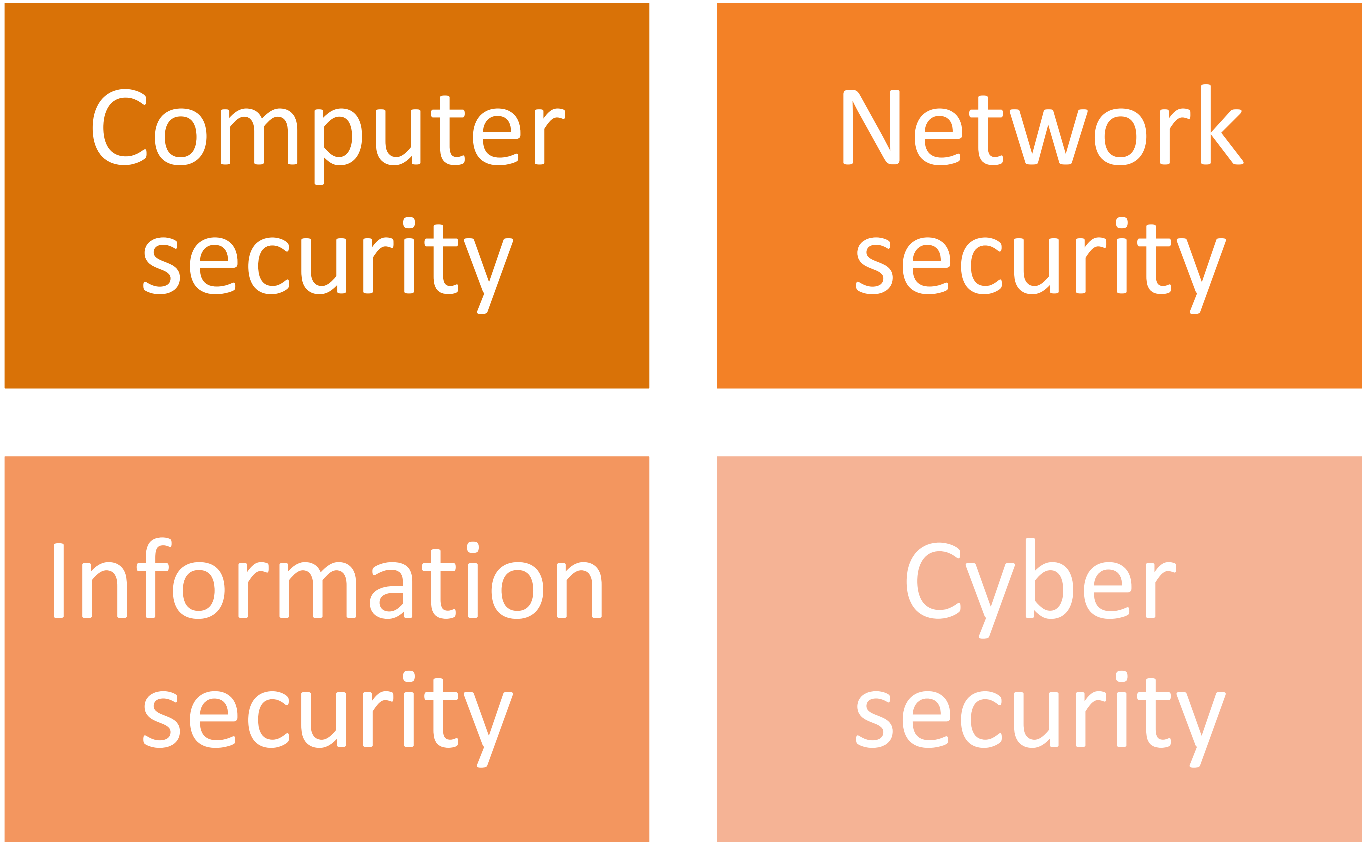
Another Security Model

http://blog.patriot-tech.com/



EXERCISE 2

Many terms – no strong consensus



Computer security

Protect Hardware and Software in Computers

Network security

Protect Hardware and Software in Networks

Information security

Protect Informational Asset: digitally stored, printed, written on papers, in human memory information

Cyber security

Protect against Cyber Threats (malicious attempts to damage or disrupt computers)

Physical security vs. Logical security

- **Physical Security**
  - preventative measures used to halt intruders from physically accessing the location.
- **Logical Security**
  - safeguards in place to protect access to the data and information storage system itself.

Risks

- General definition
  - Relationship between the likelihood of a loss and the potential impact to the business (/ mission)

- For information security
  - The likelihood of a threat agent (a threat) exploiting vulnerabilities in a “system” (where “system” = people + process + technology); and
  - The potential impact of a successful attack to an organization’s information operations

Exercice 3

Risk Control – Risk Management Actions

Risk Acceptance

- Establish risk acceptance criteria to determine what is acceptable

Risk Mitigation

- Establish plan of action for implementing safeguards and countermeasures

Risk Transfer

- Transfer the potential liability to another entity (e.g., insurance company)

Total Risk = ∑ (Threats x Vulnerability x Asset value)

Residual Risk = (Total Risk) – (Countermeasures and Safeguards)

Policies – Roles & Responsibilities

- **Information owner**: responsible for the protection of information assets
- **Information custodian**: provides security services that support the execution of business processes
  - Security managers / officers
  - Security administrators (network, systems, databases, etc.)
  - Security analysts
  - Network, system, database administrators
  - Application owner
- **Information user**: responsible for safeguarding & handling of information
  - Line managers
  - Analysts
- **Information (systems) auditor**: provides independent assessment of the security of information and/or information systems

Categories of Security Controls

Management (Administrative) Controls

- Policies, Standards, Processes, Procedures, & Guidelines

Operational (and Physical) Controls

- Operational Security (Execution of Policies, Standards & Process, Education & Awareness)
- Physical Security (Facility or Infrastructure Protection)
  - Locks, Doors, Walls, Fence, Curtain, etc.
  - Service Providers: FSO, Guards, Dogs

Technical (Logical) Controls

- Access Controls, Identification & Authorization, Confidentiality, Integrity, Availability, Non-Repudiation
  - Service Providers: Enterprise Architect, Security Engineer, etc.

CLASS	FAMILY	IDENTIFIER
Management	Risk Assessment	RA
	Planning	PL
	System and Services Acquisition	SA
	Security Assessment and Authorization	CA
	Program Management	**PM**
Operational	Personnel Security	PS
	Physical and Environmental Protection	PE
	Contingency Planning	CP
	Configuration Management	CM
	Maintenance	MA
	System and Information Integrity	SI
	Media Protection	MP
	Incident Response	IR
	Awareness and Training	AT
Technical	Identification and Authentication	IA
	Access Control	AC
	Audit and Accountability	AU
	System and Communications Protection	SC

NIST

Example of threat: Forces of Nature

- Include fire, flood, earthquake, and lightning as well as volcanic eruption and insect infestation
- Are unexpected and can occur with very little warning
- Can disrupt not only the lives of individuals, but also the storage, transmission, and use of information
- It is not possible to avoid many of these threats
- Management must implement controls to limit damage and also prepare contingency plans for continued operations

Example of threat: Technical Hardware or Software Failures

- Equipment containing flaws can cause the system to perform outside of expected parameters, resulting in unreliable service or lack of availability
- Software with unrevealed faults
- Obsolescence: When the infrastructure becomes antiquated or outdated, it leads to unreliable and untrustworthy systems

ATTACKS

- An attack is the deliberate act that exploits vulnerability
- It is accomplished by a threat-agent to damage or steal an organization’s information or physical asset
  - An exploit is a technique to compromise a system
  - A vulnerability is an identified weakness of a controlled system whose controls are not present or are no longer effective
  - An attack is then the use of an exploit to achieve the compromise of a controlled system

Malicious Code

- Attack that includes the execution of viruses, worms, Trojan horses, and active web scripts with the intent to destroy or steal information
- Self-replicating software that is viral in nature; is disseminated by attaching to or mimicking authorized computer system files

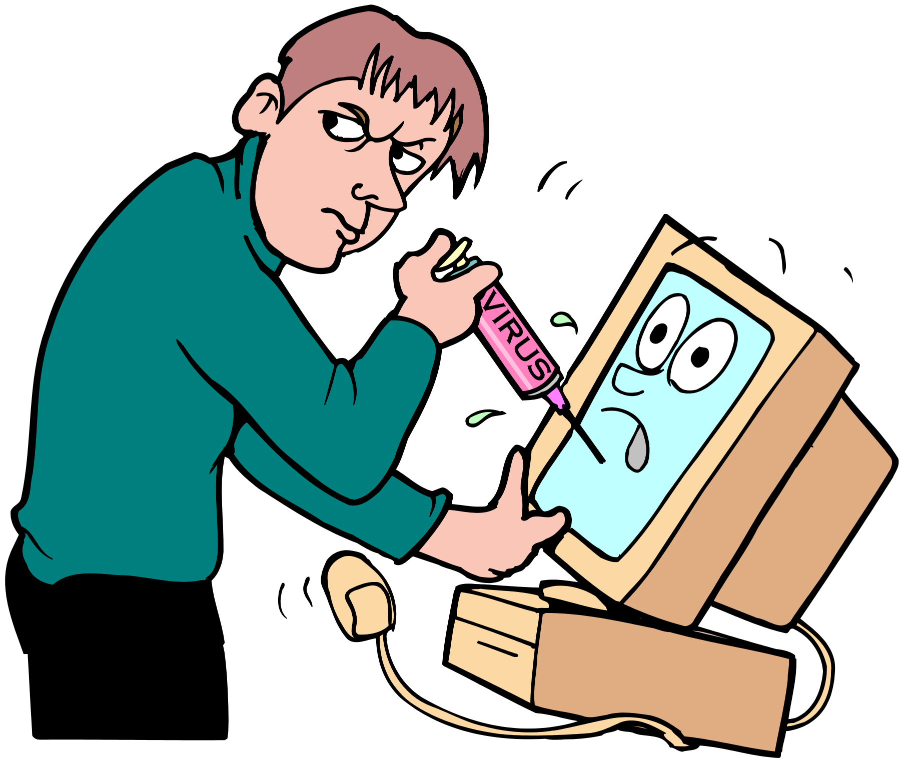
Information Extortion

Information extortion is an attacker stealing information from a computer system and demanding compensation for its return or non-use

Extortion found in credit card number theft

Sabotage or Vandalism

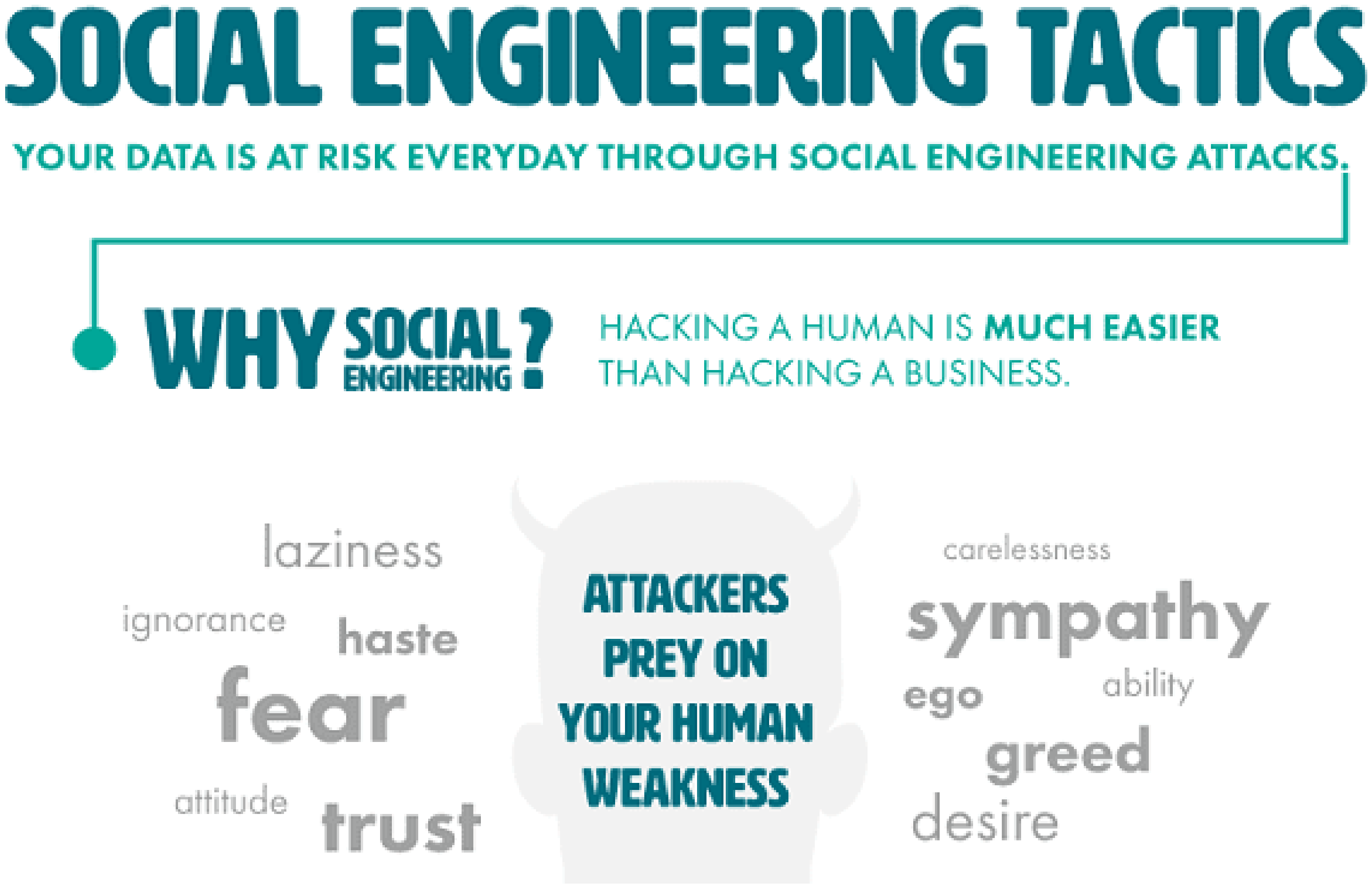
- Individual or group who want to deliberately disturb the operations of a computer system or business, or perform acts of vandalism to either destroy an asset or damage the image of the organization
- These threats can range from petty vandalism to organized sabotage
- Organizations rely on image so Web defacing can lead to dropping consumer confidence and sales
- Rising threat of hacktivist or cyber-activist operations – the most extreme version is cyber-terrorism



Deliberate Acts of Theft

- ❑ Illegal taking of another’s property - physical, electronic, or intellectual
- ❑ The value of information suffers when it is copied and taken away without the owner’s knowledge
- ❑ Physical theft can be controlled - a wide variety of measures used from locked doors to guards or alarm systems
- ❑ Electronic theft is a more complex problem to manage and control - organizations may not even know it has occurred

Social engineering



SOCIAL ENGINEERING TACTICS

YOUR DATA IS AT RISK EVERYDAY THROUGH SOCIAL ENGINEERING ATTACKS.

WHY SOCIAL ENGINEERING?

HACKING A HUMAN IS **MUCH EASIER** THAN HACKING A BUSINESS.

ATTACKERS PREY ON YOUR HUMAN WEAKNESS

White-hat hackers vs attackers

- Computer professionals hired to illicitly gain entry into a system
  - Reveal weak points
  - Protect the points
  - May not alert its own employees of the testing
- Intrusion tester

Counter-measure
Identification and Authentication

- Provide access to authorized individuals only
- Uses one of more of the following systems
  - What you have
  - What you know
  - What you are

- Strong authentication: two-factor authentication

Authentication

What You Have

Key

Badge

Token

Plastic card – magnetized strip

Active badge – signals wearer’s location using infrared signals

Authentication

What You Know

Password

Identification number

Combination

Authentication

What You Are

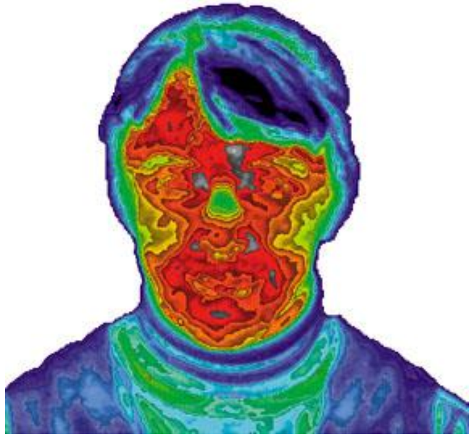
Biometrics – science of measuring individual body characteristics

Fingerprints

Voice pattern

Retina of the eye

Entire face



Other counter-measures: examples

Secured waste

- Shredders
- Locked trash barrels

Applicant screening

- Verify the facts on a resume
- Background checks

Built-in software protection

- Record unauthorized access attempts
- User profile

Disaster Recovery Plan

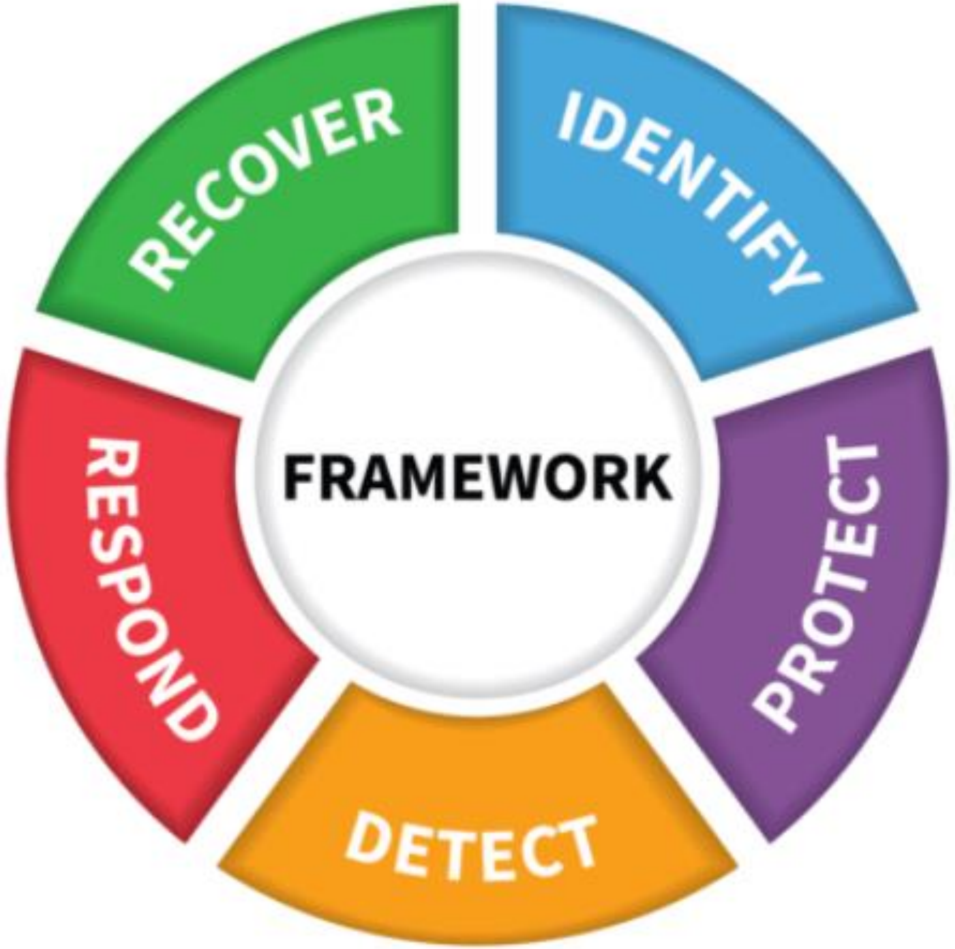
- Definition: Restoring computer processing operations and data files if operations are halted or files are damaged by major destruction

- Approaches
  - Manual services temporarily
  - Purchase time from a service bureau
  - Mutual aid pack
    - Two or more companies will lend each other computer power
    - Problem if regional disaster
  - Sites
    - Hot site – fully equipped and environmentally controlled computer center
    - Cold site – environmentally suitable empty shell

  - EXERCISE 4 & Exercise 5

The Five Functions of a security framework [NIST]

- Highest level of abstraction in the core
- Represent five key pillars of a successful cybersecurity program
- Aid organizations in expressing their management of cybersecurity risk at a high level

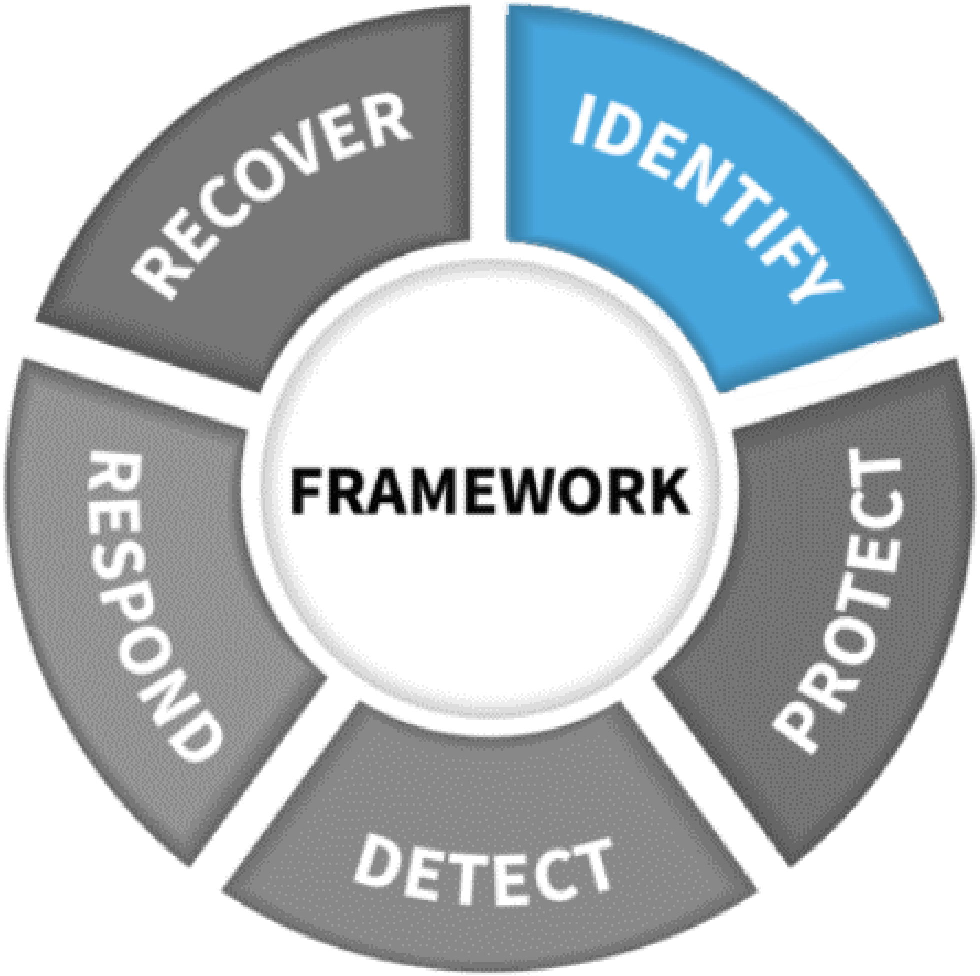


The Identify Function

- assists in developing an organizational understanding of managing cybersecurity risk to systems, people, assets, data, and capabilities

Example Outcomes:

- Identifying physical and software assets to establish an Asset Management program
- Identifying cybersecurity policies to define a Governance program
- Identifying a Risk Management Strategy for the organization

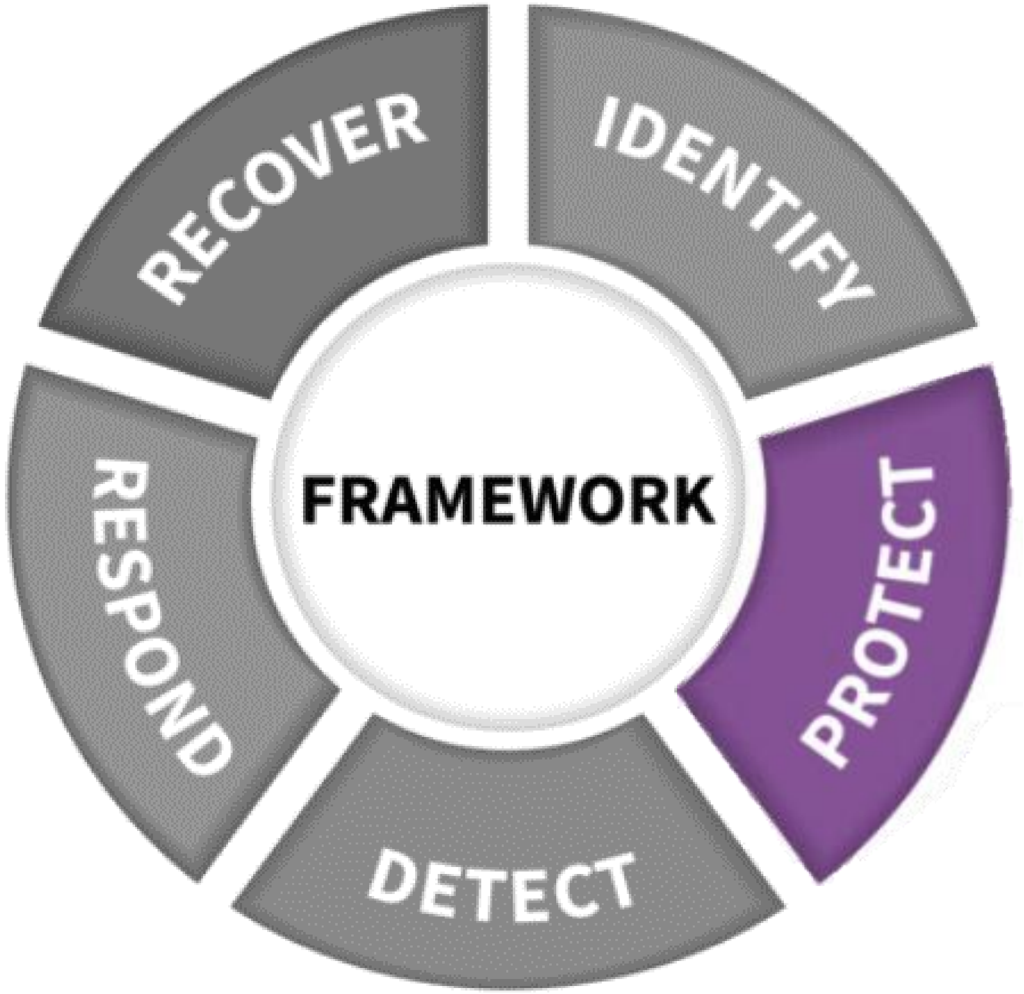


The Protect Function

- supports the ability to limit or contain the impact of potential cybersecurity events and outlines safeguards for delivery of critical services

Example Outcomes:

- Establishing Data Security protection to protect the confidentiality, integrity, and availability
- Managing Protective Technology to ensure the security and resilience of systems
- Empowering staff within the organization through Awareness and Training

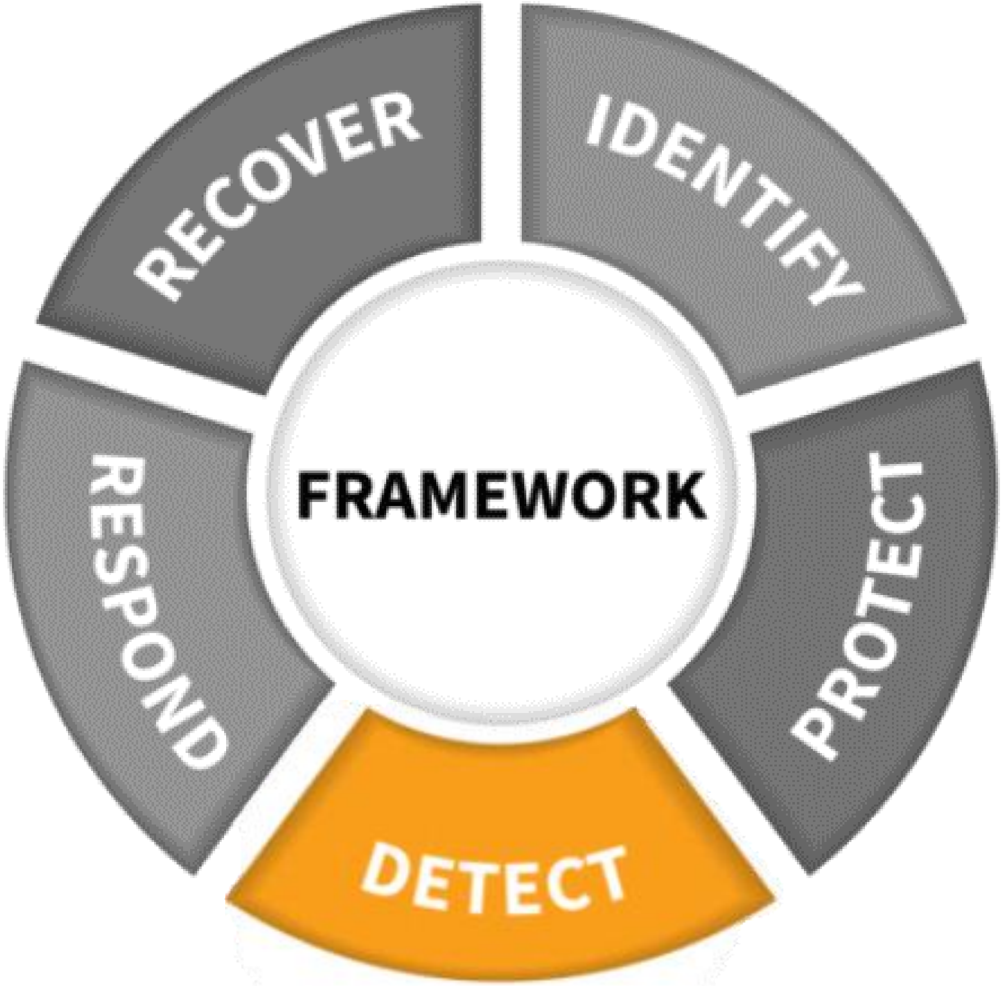


The Detect Function

- defines the appropriate activities to identify the occurrence of a cybersecurity event in a timely manner

Example Outcomes:

- Implementing Security Continuous Monitoring capabilities to monitor cybersecurity events
- Ensuring Anomalies and Events are detected, and their potential impact is understood
- Verifying the effectiveness of protective measures

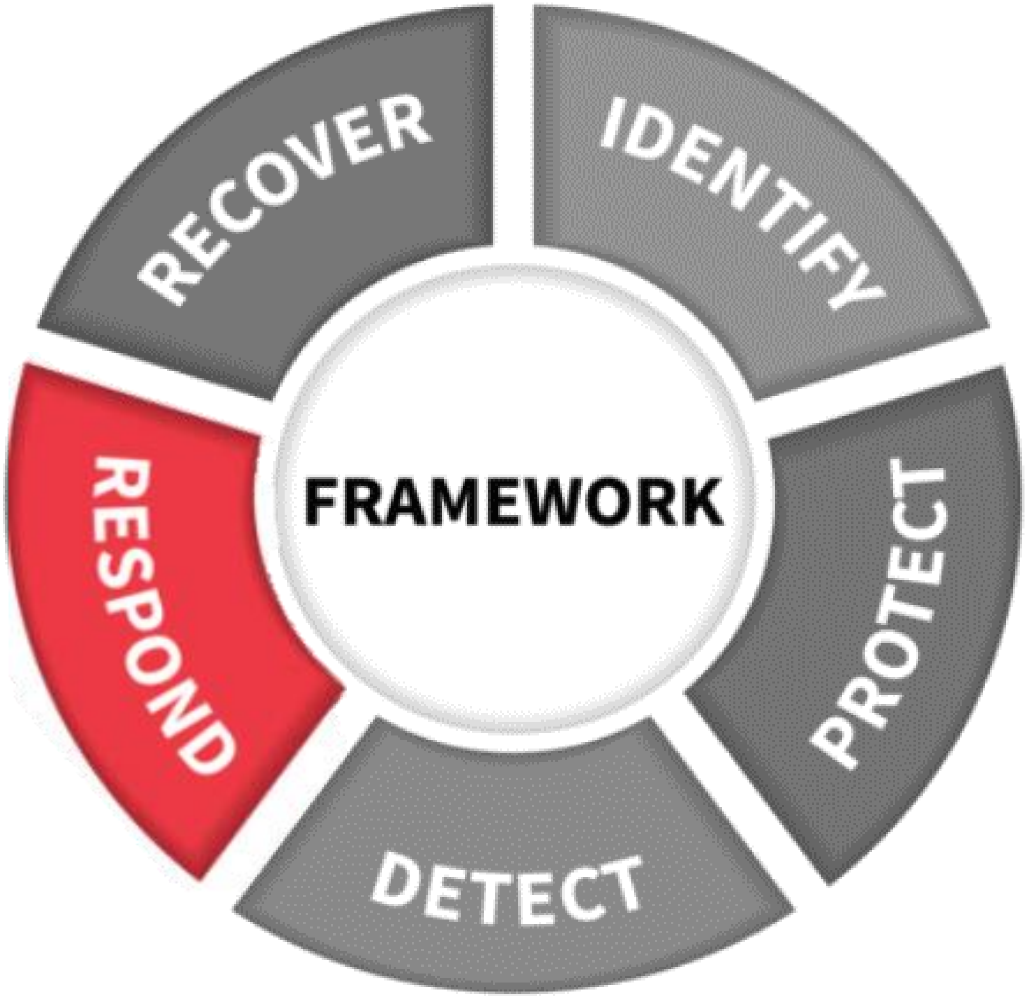


The Respond Function

- includes appropriate activities to take action regarding a detected cybersecurity incident to minimize impact

Example Outcomes:

- Ensuring Response Planning processes are executed during and after an incident
- Managing Communications during and after an event
- Analyzing effectiveness of response activities



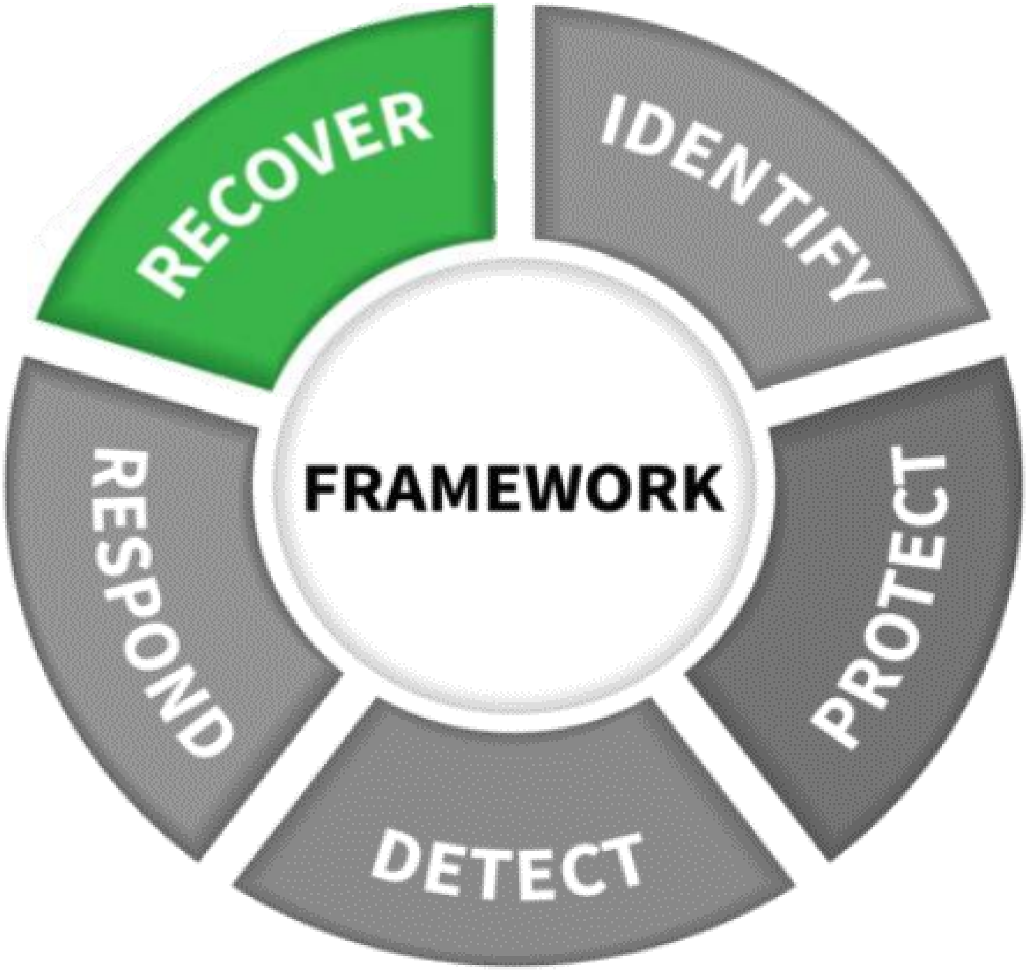
The Recover Function

- identifies appropriate activities to maintain plans for resilience and to restore services impaired during cybersecurity incidents

Example Outcomes:

- Ensuring the organization implements Recovery Planning processes and procedures
- Implementing improvements based on lessons learned
- Coordinating communications during recovery activities

Exercise 6



Industry standards

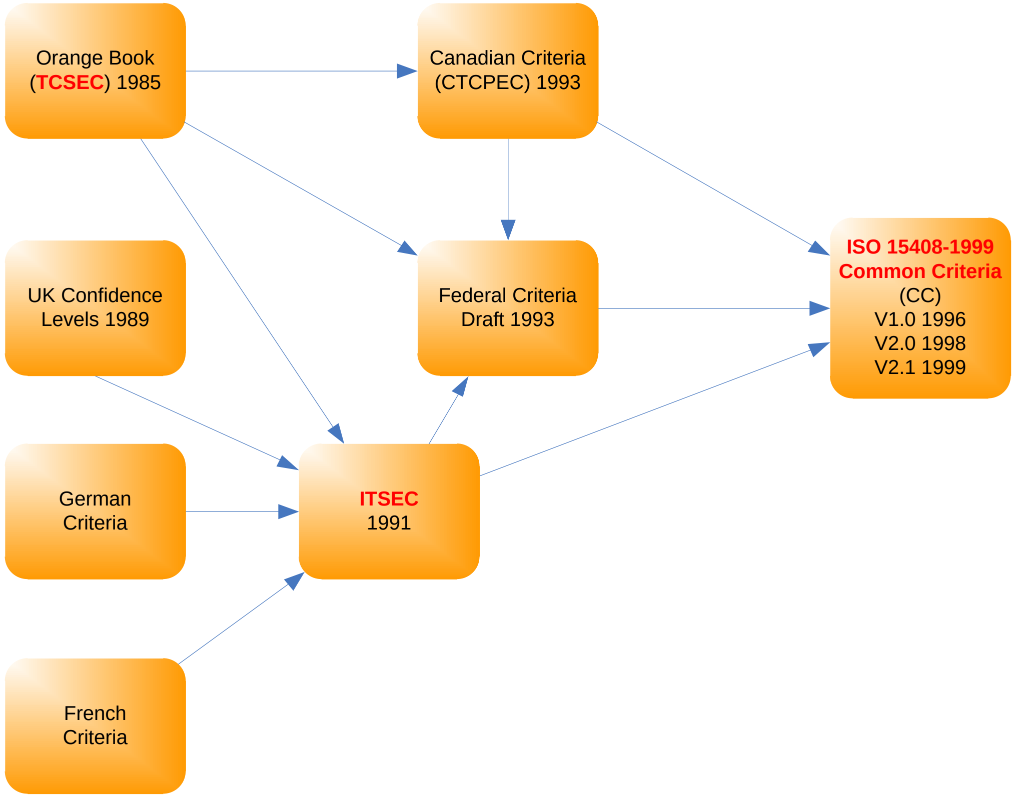
ISO/IEC 27001:2005, *Information Technology*

– Security Techniques

– Security Management System – Requirements

CONTROL CATEGORY	SUB-CATEGORY OF CONTROLS
Security Policy	Information security policy
Organization of Information Security	Internal organization; External parties
Asset Management	Responsibility for assets; Information classification
Human Resource Security	Prior to employment; During employment; Termination or change of employment
Physical and Environmental Security	Secure areas; Equipment security
Communications and Operations Management	Operational procedures and responsibilities; Third party service delivery management; System planning and acceptance; Protection against malicious and mobile code; Back-up; Network security management; Media handling; Exchange of information; Electronic commerce services; Monitoring
Access Control	Business requirement for access control; User access management; User responsibilities; Network access control; Operating system access control; Application and information access control; Mobile computing and teleworking
Information Systems Acquisition, Development, and Maintenance	Security requirements of information systems; Correct processing in applications; Cryptographic controls; Security of system files; Security in development and support processes; Technical vulnerability management
Information Security Incident Management	Reporting information security events and weaknesses; Management of information security incidents and improvements
Business Continuity Management	Information security aspects of business continuity management
Compliance	Compliance with legal requirements; Compliance with security policies and standards, and technical compliance; Information system audit considerations

Standards

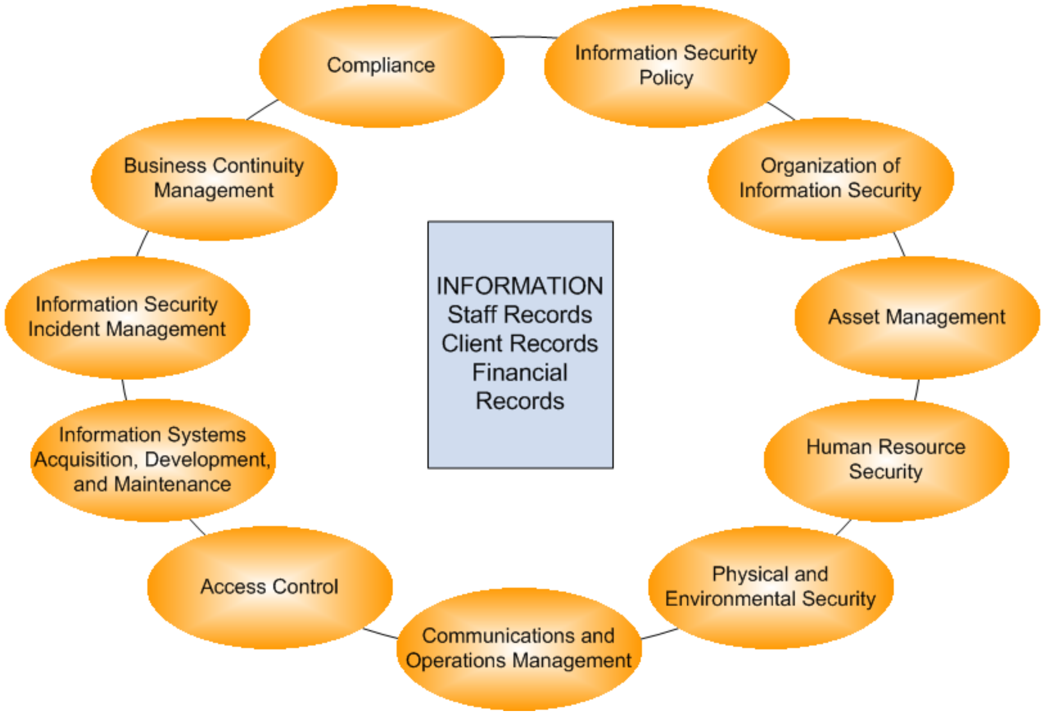

Orange Book (TCSEC) 1985
Canadian Criteria (CTCPEC) 1993
UK Confidence Levels 1989
Federal Criteria Draft 1993
ISO 15408-1999 Common Criteria (CC) V1.0 1996 V2.0 1998 V2.1 1999
German Criteria
ITSEC 1991
French Criteria

- DoD 5200.28-STD *Trusted Computer System Evaluation Criteria* (TCSEC)
  - Evaluates Confidentiality

- Information Technology Security Evaluation Criteria (ITSEC)
  - Evaluates Confidentiality, Integrity and Availability

- Common Criteria (CC)
  - Provided a common structure and language.
  - It’s an International standard (ISO 15408)

Standards – ISO/IEC 27001:2005


Compliance
Information Security Policy
Organization of Information Security
Asset Management
Human Resource Security
Physical and Environmental Security
Communications and Operations Management
Access Control
Information Systems Acquisition, Development, and Maintenance
Information Security Incident Management
Business Continuity Management
INFORMATION
Staff Records
Client Records
Financial Records

- ISO/IEC 27001 is an Information Security Management System Standard
- Commercially, the systems are certified based on meeting ISO/IEC 27001
- ISO/IEC 27002:2005 is a “Code of practice” for information security management

HIPAA Privacy and Confidentiality Standards

- Limit the non-consensual use and release of personal health information
- Give patients new rights to access their medical records and to know who else has accessed them
- Restrict most disclosure of health information to the minimum needed for the intended purpose
- Establish new criminal and civil sanctions for improper use or disclosure
- Establish new requirements for access to records by researchers and others

Data Security

Information

- knowledge acquired in any manner; facts; **data**; learning; lore
- in information theory and computer science, a precise measure of the information content of a message, measured in bits and ranging from zero when the entire message is known in advance to some maximum when nothing is known of its content
- any **data** that can be stored in and retrieved from a computer

Source: Webster's New World College Dictionary, Fifth Edition

Data

- **information** collected for use
- **information**, especially facts or numbers, collected to be examined and considered and used to help with making decisions
- **information** in an electronic form that can be stored and processed by a computer

Source: Cambridge University Press

Data, Information, Knowledge

Data

- What is given
- Describes objects or events of interest
- **Example: The quantity purchased of product A in invoice Number 6 is 20 units**

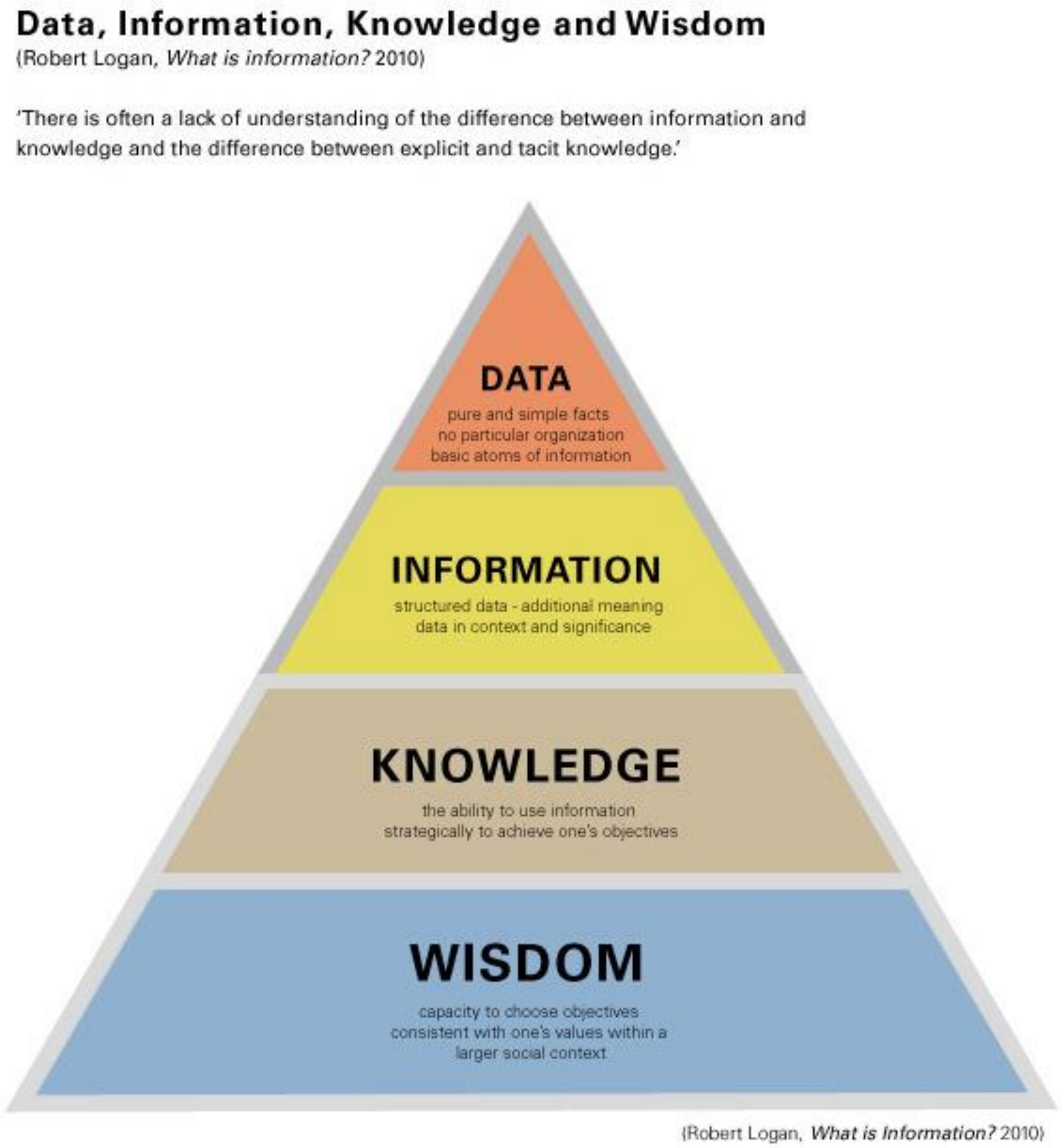
Information

- What informs
- Alters our worldview and reduces uncertainty
- Data becomes information through an interpretation process that involves the knowledge of the individual
- Data in a context becomes information
  - **Example: data = yes, yes, no, no, yes, yes, yes**
    - Context: survey responses = would you buy this product at this price?
  - **Example: Sales of product A in the North region increased by 10% in 2012**

Knowledge

- Set of schemas which increases our understanding (M.J. Earl)
- Formalized or explicit knowledge. Is transmitted by speech. Example: the accounting model
- Tacit knowledge. Acquired by practice. Example: water skiing
- **Example: Generally, a customer who bought product A then buys product B**

DIKW pyramid



Data, Information, Knowledge and Wisdom

(Robert Logan, *What is information?* 2010)

'There is often a lack of understanding of the difference between information and knowledge and the difference between explicit and tacit knowledge.'

DATA

pure and simple facts
no particular organization
basic atoms of information

INFORMATION

structured data - additional meaning
data in context and significance

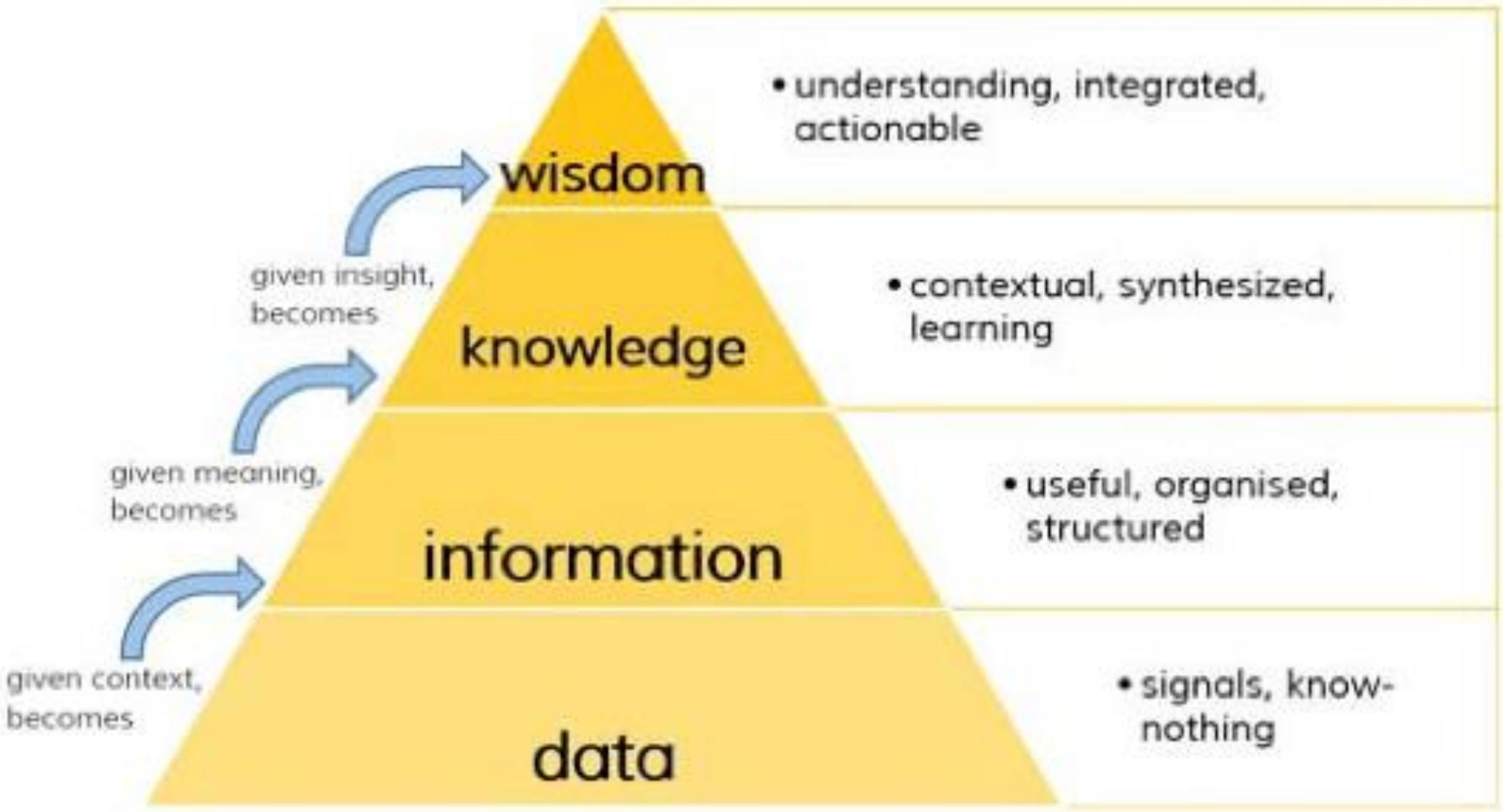
KNOWLEDGE

the ability to use information
strategically to achieve one's objectives

WISDOM

capacity to choose objectives
consistent with one's values within a
larger social context

(Robert Logan, *What is Information?* 2010)



Source: BP trends.com

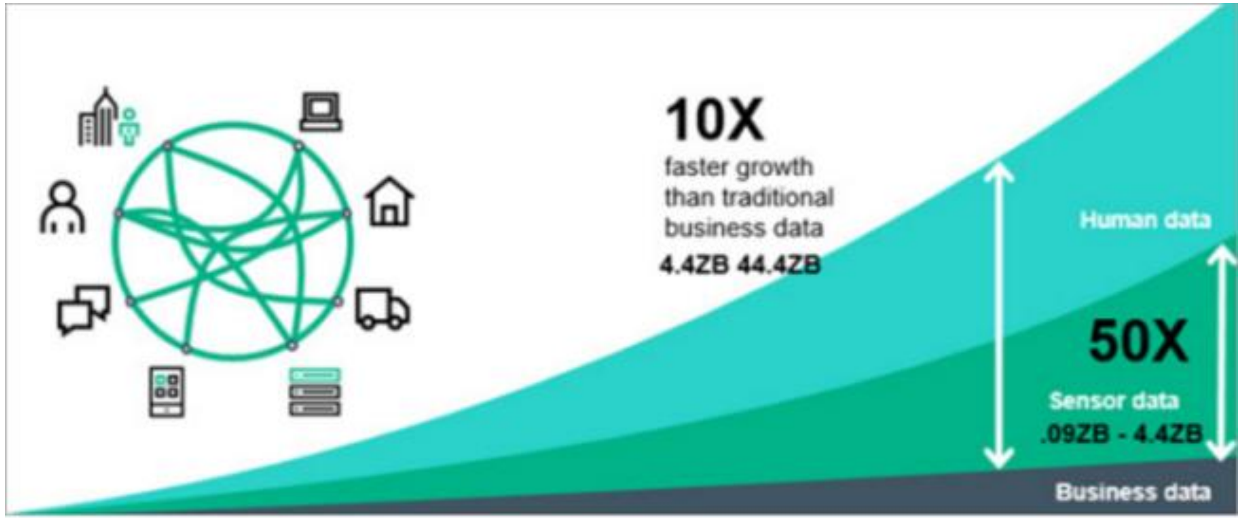
Data Everywhere

Source: simplicable

Abstract Data	Atomic Data
Big Data	Dark Data
Empirical Evidence	Event Data
Hard Data	Machine Data
Master Data	Metadata
Primary Data	Qualitative Data
Quantitative Data	Raw Data
Reference Data	Small Data
Soft Data	Source Data
Transactional Data	Unstructured Data
More ...	

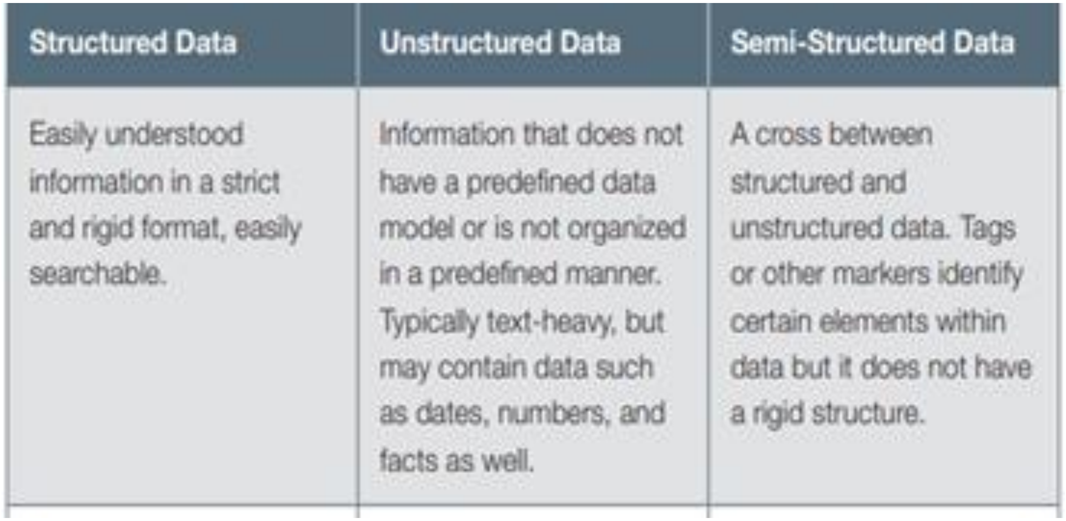
Exponential growth of data and information

- The size of the digital universe will double every two years at least
- Human- and machine-generated data is experiencing an overall 10x faster growth rate than traditional business data
- Machine data is increasing even more rapidly at 50x the growth rate

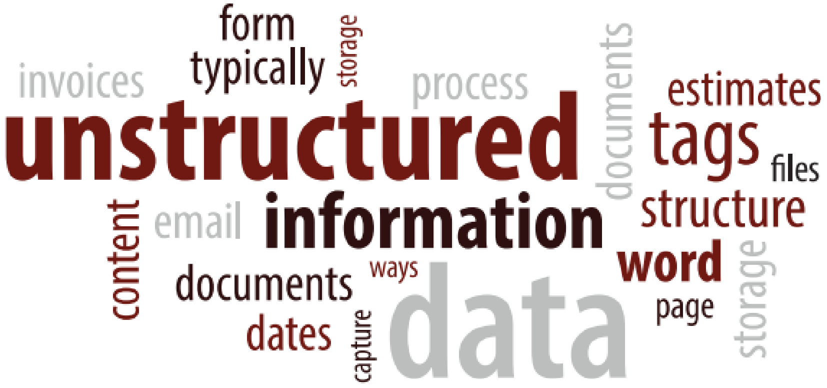


Source: insidebigdata.com

Data Types

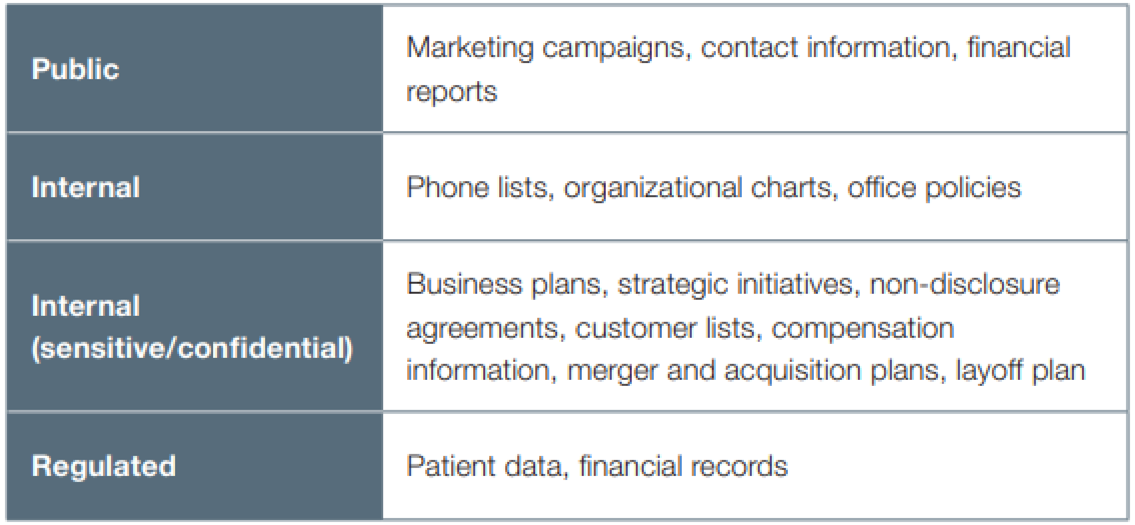


Structured Data	Unstructured Data	Semi-Structured Data
Easily understood information in a strict and rigid format, easily searchable.	Information that does not have a predefined data model or is not organized in a predefined manner. Typically text-heavy, but may contain data such as dates, numbers, and facts as well.	A cross between structured and unstructured data. Tags or other markers identify certain elements within data but it does not have a rigid structure.



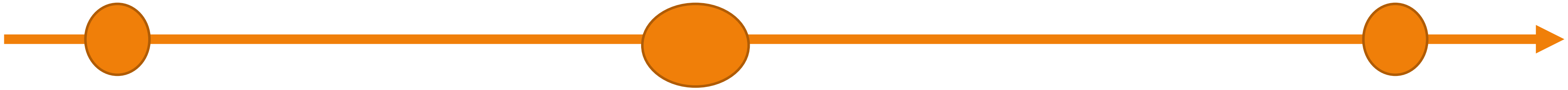
Data Classification

- The process of organizing data by relevant categories so that it may be used and protected more efficiently
- Example of classification schema:



Public	Marketing campaigns, contact information, financial reports
Internal	Phone lists, organizational charts, office policies
Internal (sensitive/confidential)	Business plans, strategic initiatives, non-disclosure agreements, customer lists, compensation information, merger and acquisition plans, layoff plan
Regulated	Patient data, financial records

Typology of Data (1)



Redundant, Obsolete, Trivial (ROT) Data (33%):

Has little or no business value

Dark Data (52%):

- Hidden and unstructured, expensive to secure and store, operational data that is left unanalyzed or underused, and often lost altogether
- Can be an opportunity for organizations if they can take advantage of it to drive new revenues or reduce internal costs
- Costs of dark data: loading, updating, storing, and managing unused data (consumes personnel time and storage space)
- Examples: server log files that can give clues to website visitor behavior and customer call detail records that can indicate consumer sentiment

Business Critical Data (15%):

Data strategically important to an organization's daily operations and success (product road maps, business plans, customer lists, etc.)

Risks with dark data

- **Regulatory**: Leaking or losing sensitive, dormant data
- **Reputational** damage: may be leaked by a security attack
- **Intellectual Property** (IP): Failing to protect IP
- Operation **Cost**: manage useless information
- **Opportunity**: Missing out on chances to improve
- **Environment**: wasteful practice

Sensitive vs. Critical Information

- **Sensitive:** requires protection, include:
  - Private information about individuals (e.g., employees, contractors, vendors, business partners, and customers) including marital status, age, birth date, race, and buying habits.
  - Confidential business information including trade secrets, proprietary information, financial information, contractor bid or proposal information, and source selection information.
  - Data susceptible to fraud including accounts payable, accounts receivable, payroll, and travel reimbursement.

- **Critical:** its unavailability would have a catastrophic adverse impact on the following:
  - Customer or employee life, safety, or health.
  - Payment to suppliers or employees.
  - Revenue collection.
  - Movement of mail.
  - Communications.
  - Legal or regulatory.

Information Classification

Identifies and characterizes the critical information assets (i.e. sensitivity)

Explains the level of safeguard (protection level) or how the information assets should be handled (sensitivity and confidentiality)

Commercial

- Public
- Private / Sensitive
- Confidential / Proprietary

Military and Civil Gov.

Unclassified

Sensitive But Unclassified (SBU)

Confidential

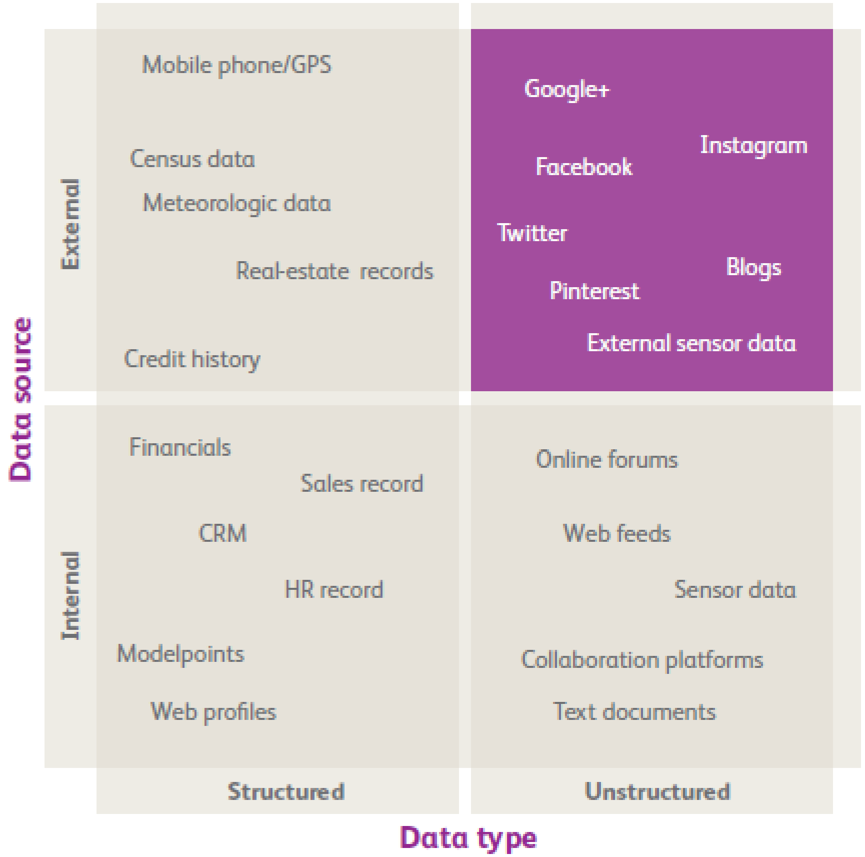
Secret

Top Secret

In health and care settings, you might see:

Confidential information.
Sensitive information.
Personal information.
Pseudonymised information
Anonymised information.

Types of Information



Data source

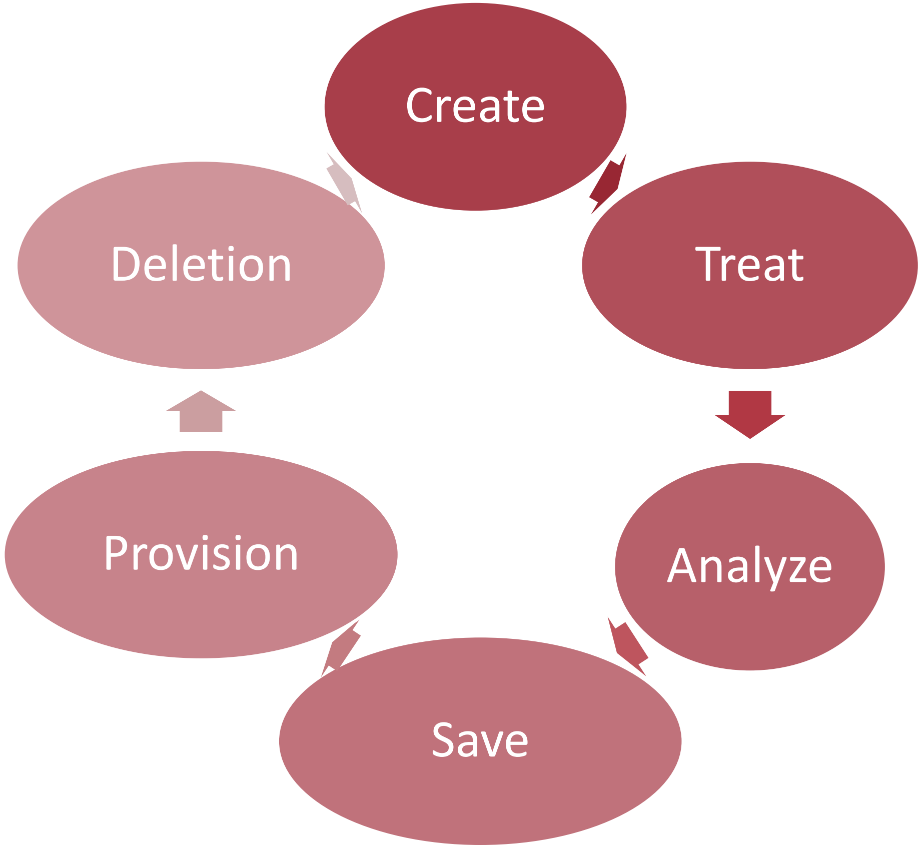
	Structured	Unstructured
External	Mobile phone/GPS Census data Meteorologic data Real-estate records Credit history	Google+ Instagram Facebook Twitter Blogs Pinterest External sensor data
Internal	Financials Sales record CRM HR record Modelpoints Web profiles	Online forums Web feeds Sensor data Collaboration platforms Text documents

Data type

Source: BearingPoint Institute

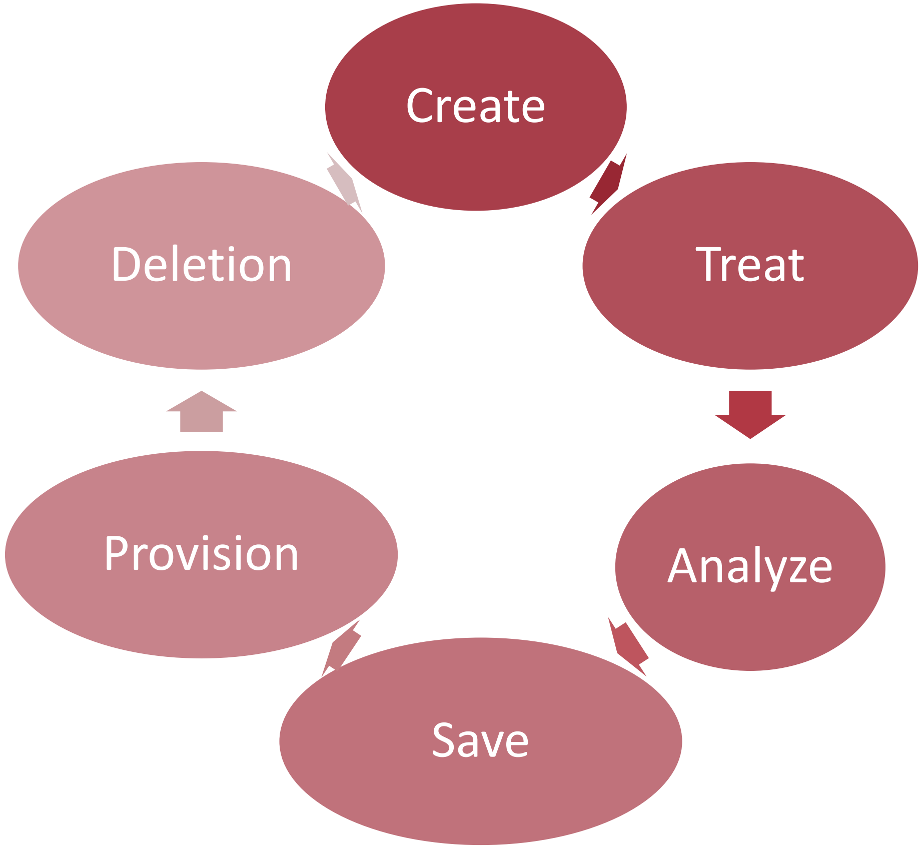
Data Life Cycle

- The sequence of stages that a particular unit of data goes through from its initial generation or capture to its eventual archival and/or deletion at the end of its useful life



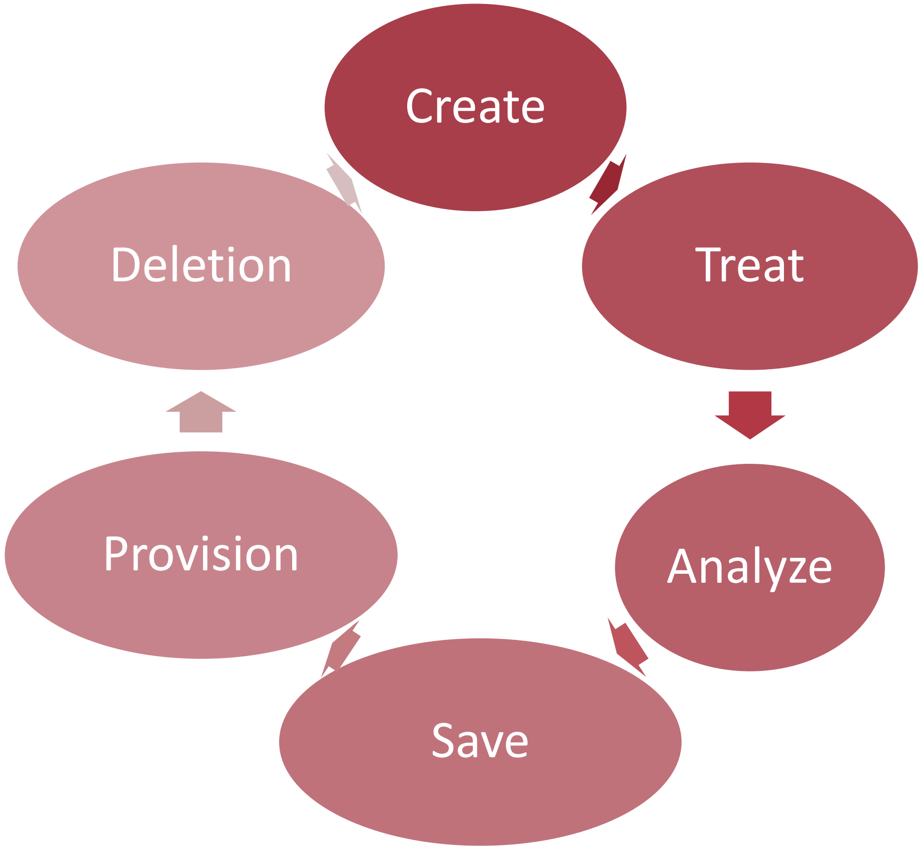
Data Creation

- Capture and create metadata -> data design / modeling
- Collect data (buy, measure, simulate, interrogate, simulate, etc.)
- Locate existing data ("sourcing", map)



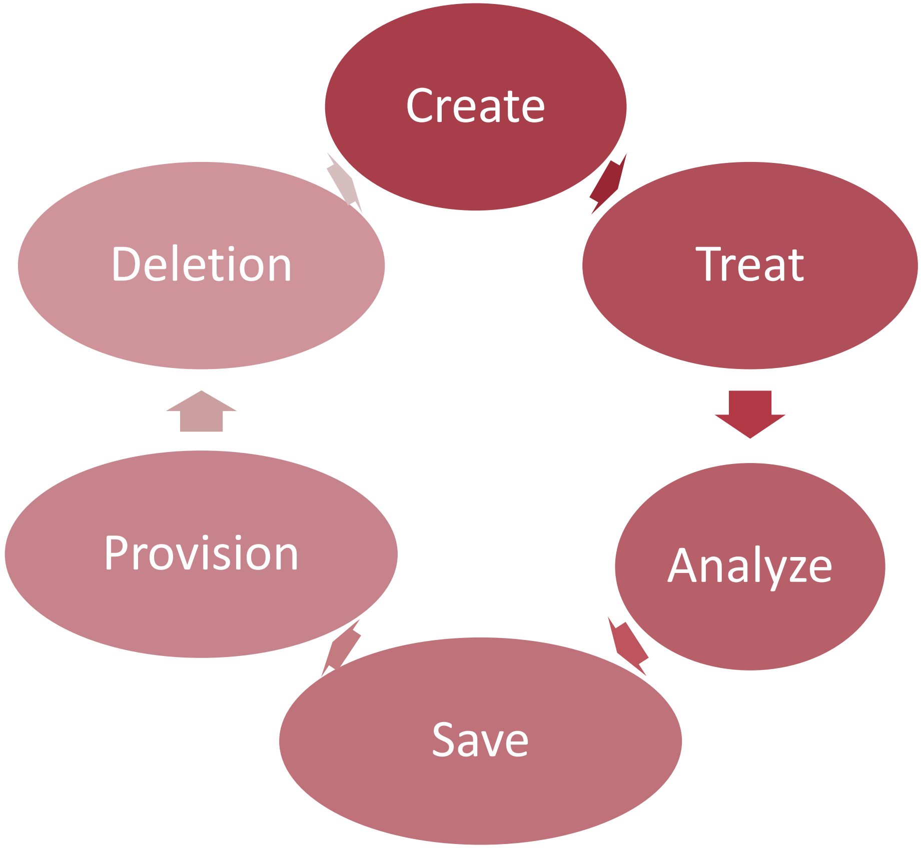
Data Processing

- Capture data, code, digitize, translate, transform
- Check, validate, clean data
- Anonymize sensitive data
- Describe the data
- Manage and store data



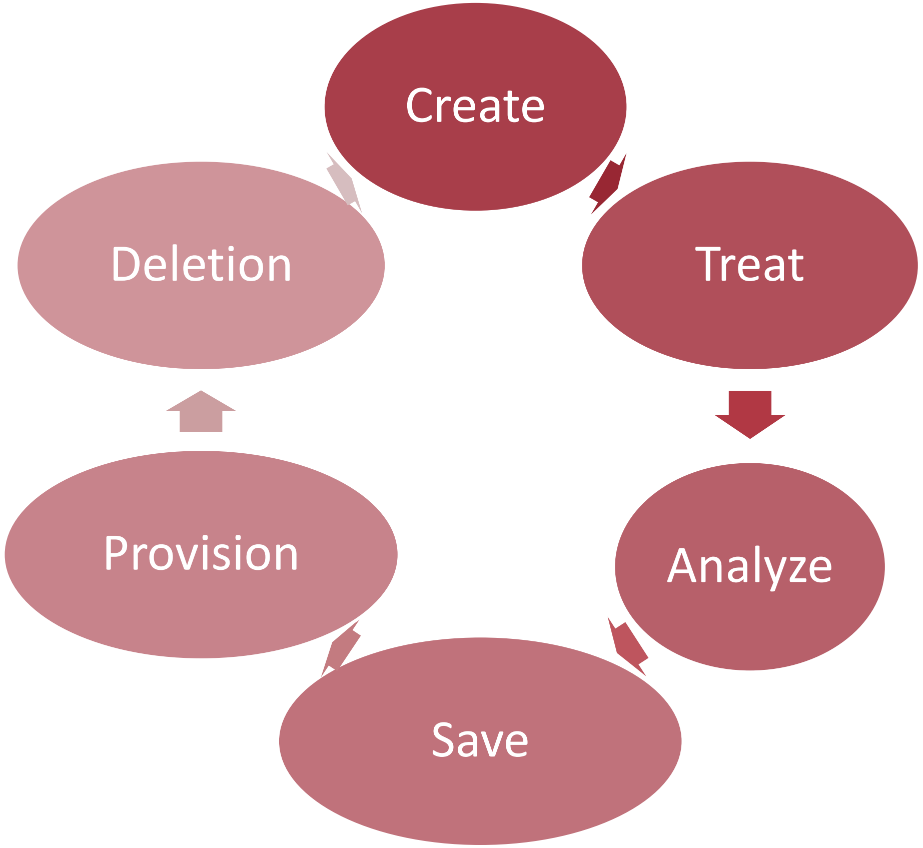
Data Analysis

- Interpret information
- Infer information and knowledge
- Generate knowledge



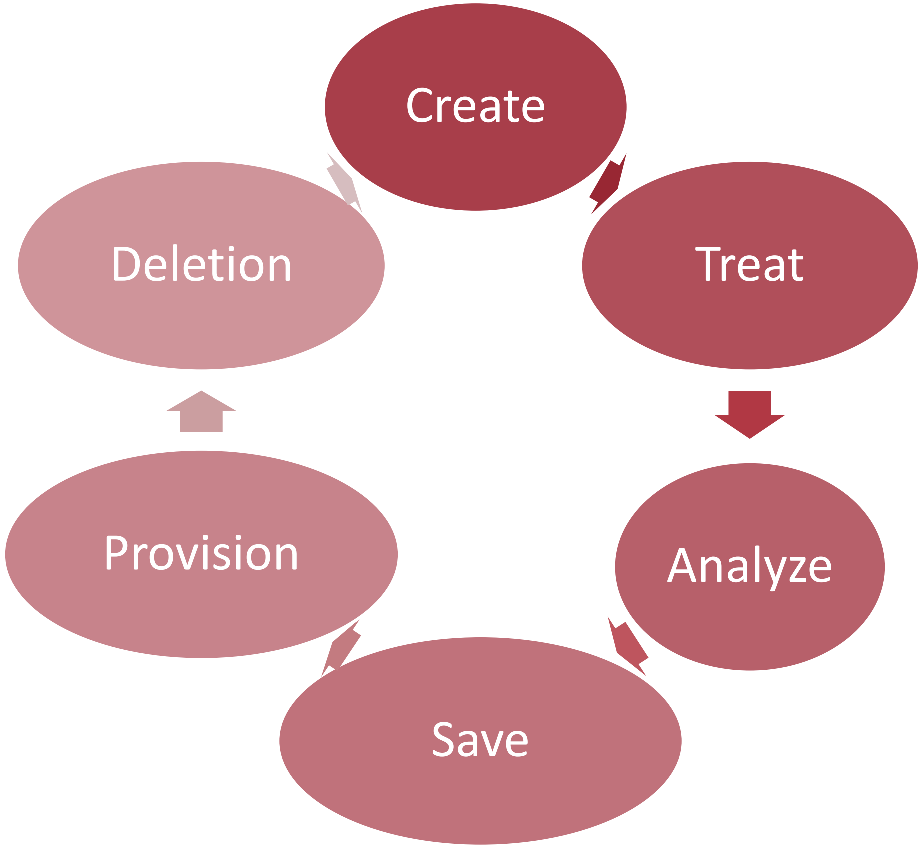
Data Saving

- Migrate data in the right format
- Migrate data to the right medium
- Create metadata and documentation
- Archive information



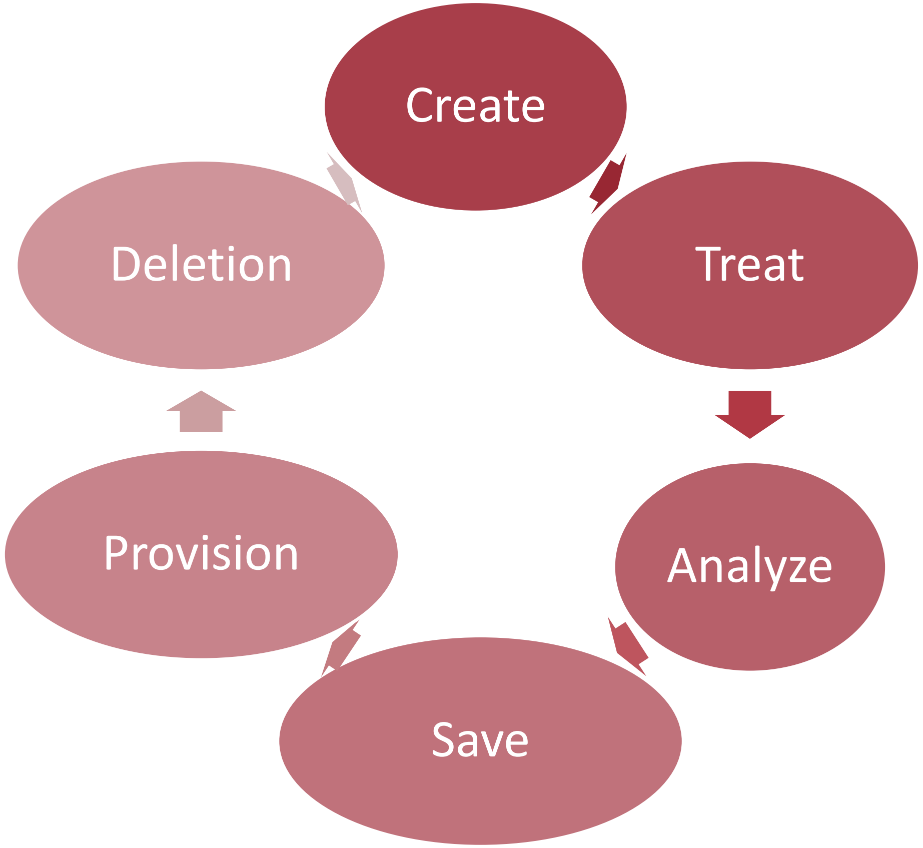
Make Data Accessible

- Distribute data
- Share data
- Control access
- Promote information

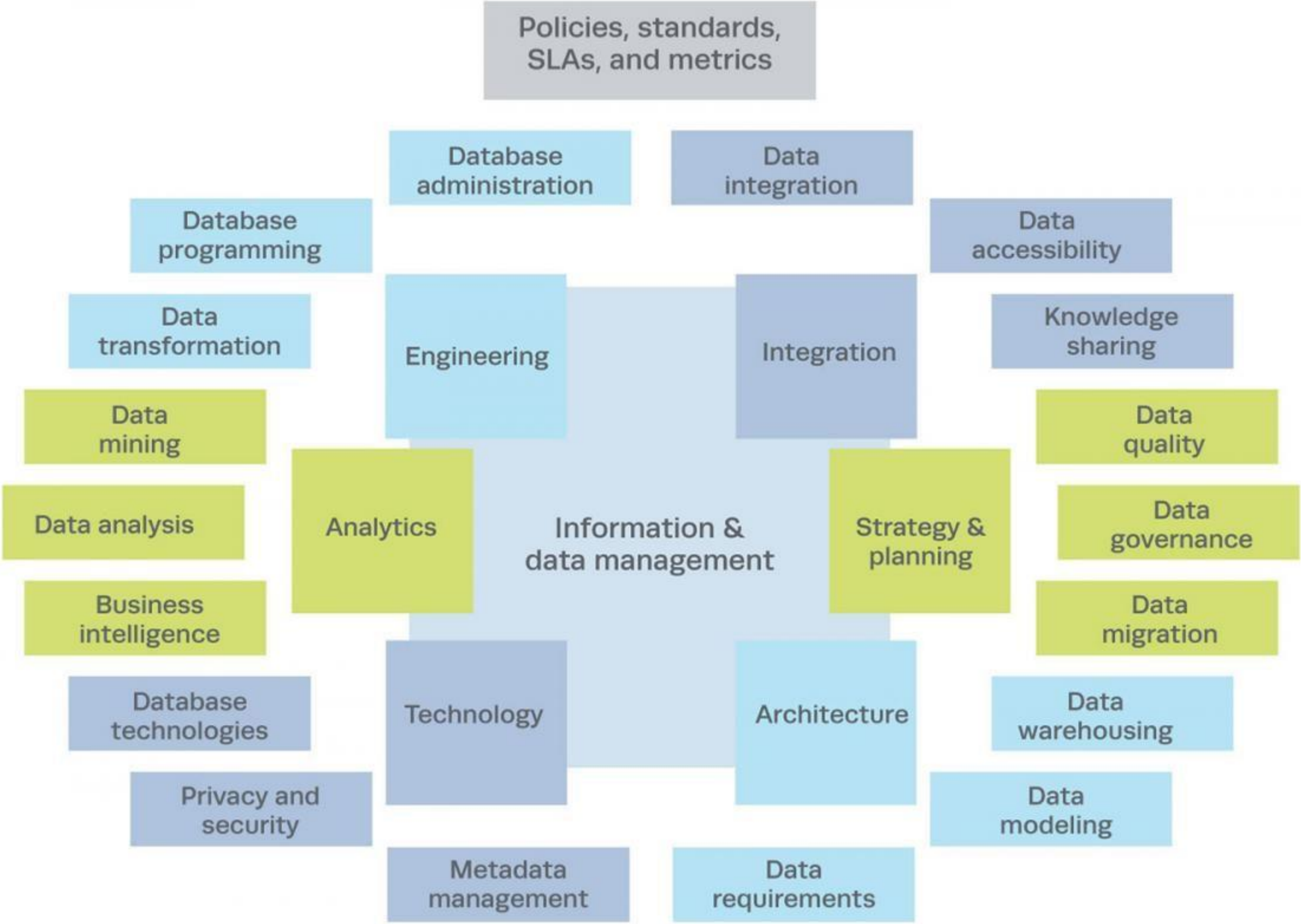


Data Destruction

- An important process: who is responsible for it?
- Legal aspects: rules for keeping information, documents, processes, etc.
- Usefulness of historical data
- Sustainable development issue: storage cost
- Choice of destruction method: overwriting, degaussing, physical destruction



Data Management Discipline



Source: mitre.org

Data Security Overview

There are four key issues in data security, just as with all security systems

- Availability
- Authenticity
- Integrity
- Confidentiality

Availability

- Data needs to be available at all necessary times
- But: data needs to be available to only the appropriate users
- And: Need to be able to track who has access to and who has accessed what data

Authenticity

- ❑ Need to ensure that the data has been edited by an authorized source
- ❑ Need to confirm that users accessing the system are who they say they are
- ❑ Need to verify that all report requests are from authorized users
- ❑ Need to verify that any outbound data is going to the expected receiver

Integrity

- ❑ Need to verify that any data has the correct formatting
- ❑ Need to verify that all input data is accurate and verifiable
- ❑ Need to ensure that data is following the correct work flow rules in the organization
- ❑ Need to be able to report on all data changes and who authored them to ensure compliance with corporate rules and privacy laws.

Confidentiality

- ❑ Need to ensure that confidential data is only available to correct people
- ❑ Need to ensure that entire database is secured from external and internal system breaches
- ❑ Need to provide for reporting on who has accessed what data and what they have done with it
- ❑ One objective of confidentiality is privacy

What is Privacy?

- The concept of privacy varies widely among (and sometimes within) countries, cultures, and jurisdictions.
- It is shaped by public expectations and legal interpretations
  - as such, a concise definition is elusive if not impossible.
- Privacy rights or obligations are related to the collection, use, disclosure, storage, and destruction of personal data
- Privacy is about the accountability of organizations to data subjects, as well as the transparency to an organization's practice around personal information.

From [6] Cloud Security and Privacy by Mather and Kumaraswamy

Privacy: *How Did They Get My Data?*

Loans

Charge accounts

Orders via mail

Magazine subscriptions

Tax forms

Applications for schools, jobs, clubs

Insurance claim

Hospital stay

Sending checks

Fund-raisers

Advertisers

Warranties

Court petition

Everything about you is in at least one computer file

Privacy: Monitoring software

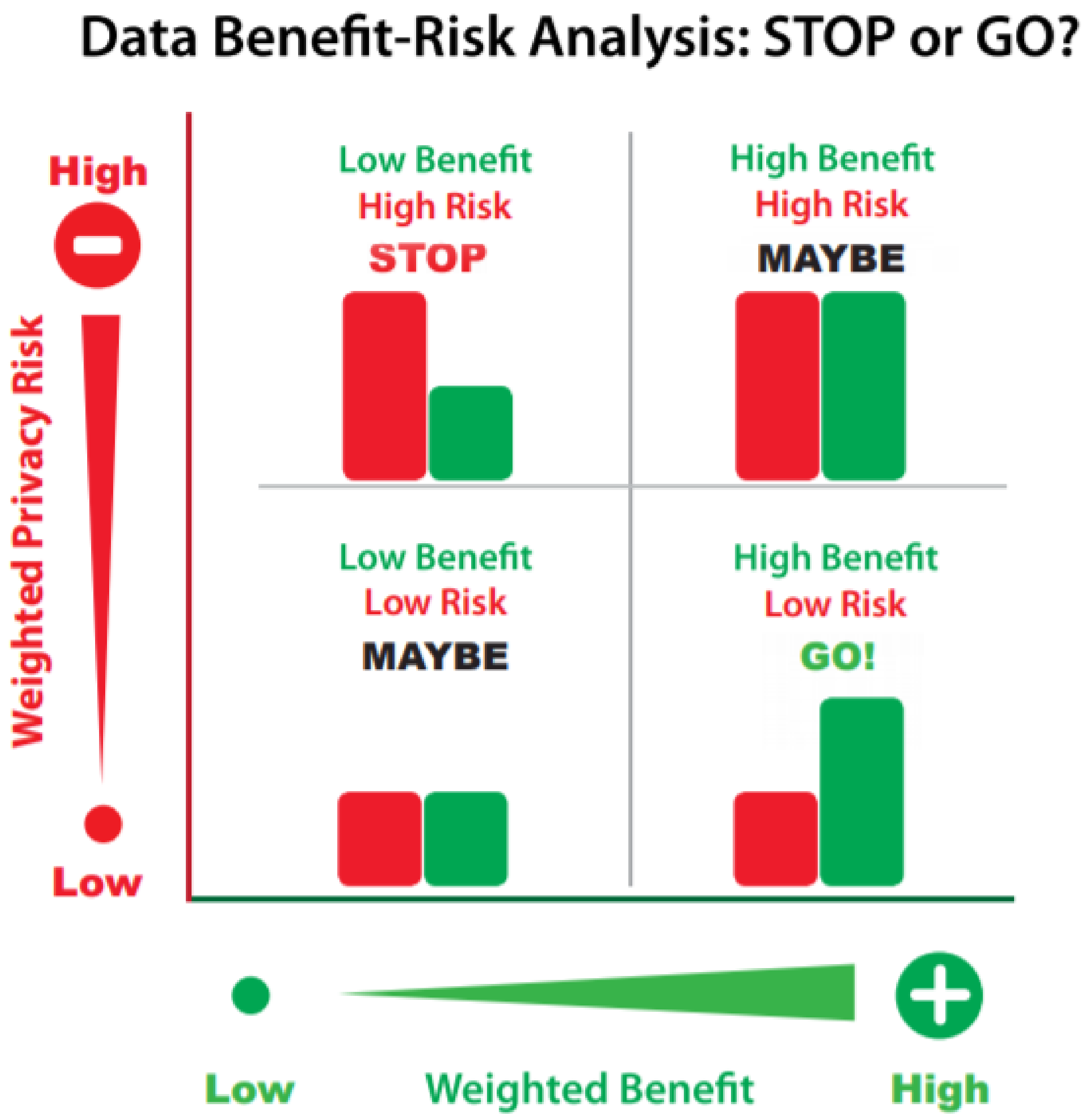
- Screens
- E-mail
- Keystrokes per minute
- Length of breaks
- What computer files are used and for how long

Steganography

- ❑ The Art of Hiding Communications
- ❑ While Encryption Conceals the Data, Steganography Denies the Data Exists
- ❑ Files Can Be Hidden within an Image
- ❑ May be used as a digital watermarking, an efficient solution for the protection of copyright and property
- ❑ Disguising Data as Innocent Text

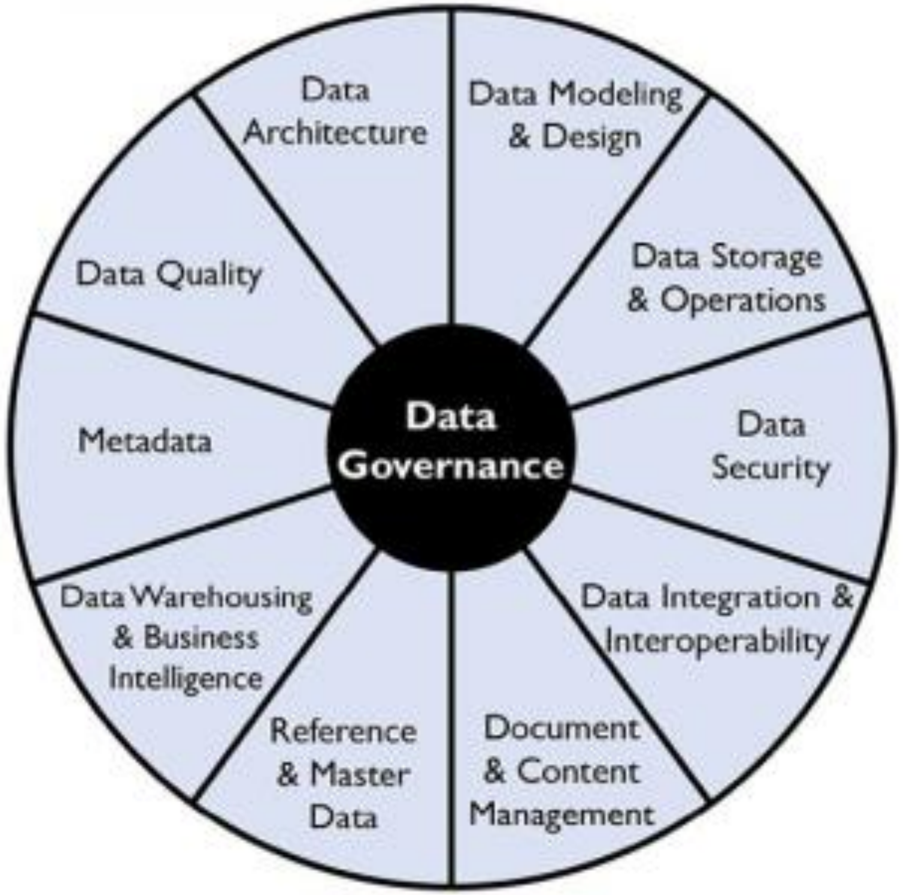
Evaluate benefit and risk

[Polonetsky et al., 2014, Future of Privacy Forum]



Data governance

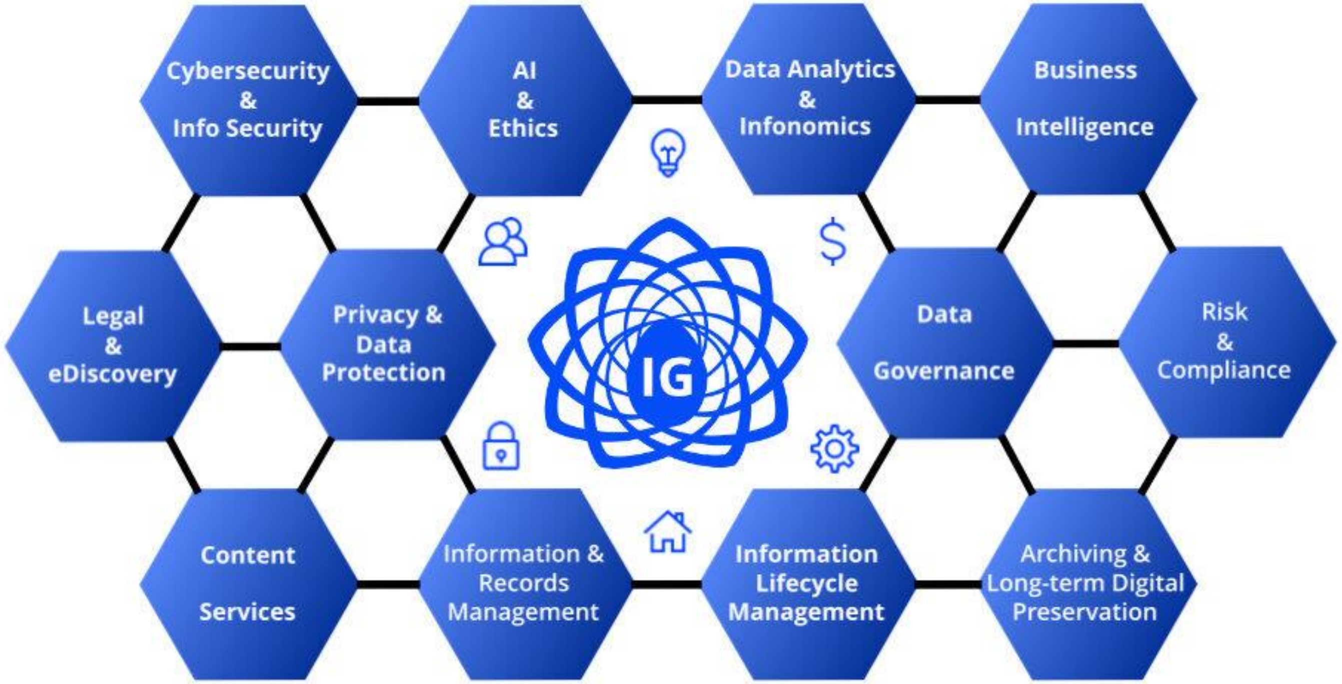
- Maximizing data value with minimizing risk and c
- Managing the availability, usability, integrity and s based on internal data standards and policies that
- Example of framework: DAMA


Data Governance
Data Architecture
Data Modeling & Design
Data Storage & Operations
Data Security
Data Integration & Interoperability
Document & Content Management
Reference & Master Data
Data Warehousing & Business Intelligence
Metadata
Data Quality

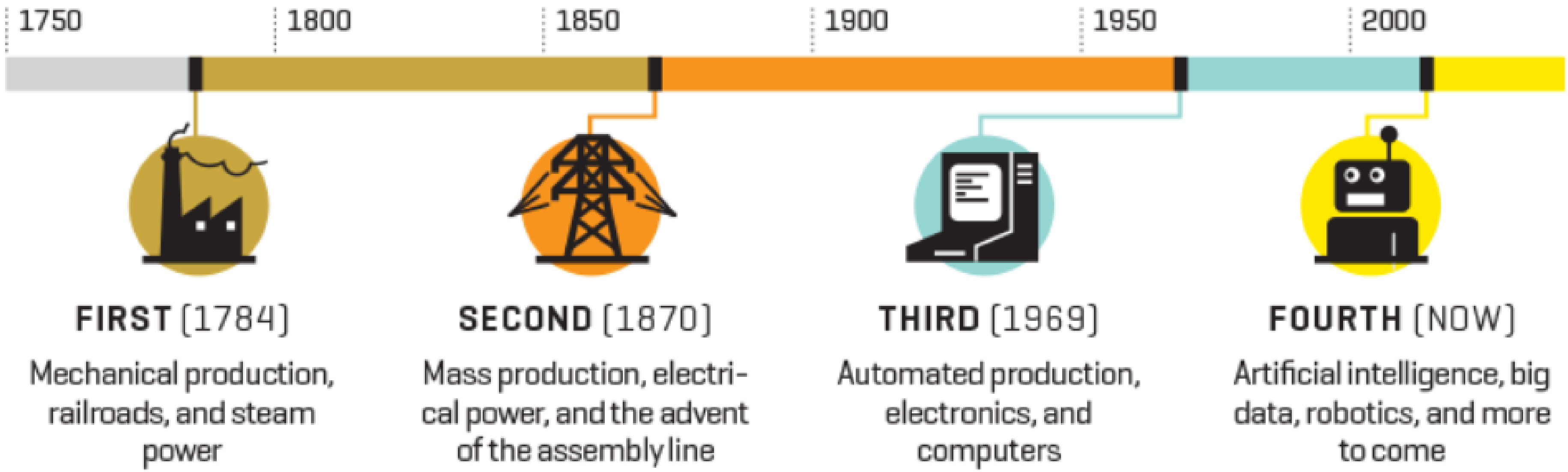
DAMA-DMBOK2 Data Management Framework

Information Governance

- Concentrates on governing information content that is gathered, stored, processed, and exchanged through IT assets
- Infonomics (Information Economics): **Treat Your Information Like an Asset**


Cybersecurity & Info Security
AI & Ethics
Data Analytics & Infonomics
Business Intelligence
Legal & eDiscovery
Privacy & Data Protection
IG
Data Governance
Risk & Compliance
Content Services
Information & Records Management
Information Lifecycle Management
Archiving & Long-term Digital Preservation

Information in the Digital Age



FIRST (1784)
Mechanical production, railroads, and steam power

SECOND (1870)
Mass production, electrical power, and the advent of the assembly line

THIRD (1969)
Automated production, electronics, and computers

FOURTH (NOW)
Artificial intelligence, big data, robotics, and more to come

Source: World Economic Forum

Risks related to Information

- Information protection and security
- Leak, loss, alteration of information content
- Compliance requirements
- Integrity and availability of information content and information systems
- Protection of sensitive information
- Diversity of mechanisms and tools for the production, organization and storage of information
- Diversity of information management practices (formal and informal, institutional and individual)
- Lack of a strong and shared information culture

Information Governance

- A subset of Corporate Governance: Strategic rather than tactical
- Top-down approach to:
  - managing all aspects of information within the organization
  - in line with the strategic objectives of that organization
- A cross-departmental framework consisting of the policies, procedures and technologies designed to:
  - optimize the value of information
  - manage the risks and to control the associated costs

Value of Information Governance Risk Mitigation

- Helps organisations avoid or mitigate **information-related risk,** including regulatory and legal risks
- Supports an improved ability to proactively meet compliance obligations, by introducing the right systems, policies and processes in relation to **information usage and retention**
- It understands **key risks events**, including growing risk of cyber attack

Value of Information Governance Efficiency

- Control over the dysfunction, duplication and waste created by information silos
- Reduction in storage and document discovery (eDiscovery) costs
- Common approach to information management, more consistent rules

Value of Information Governance Business Value

- Better decision-making
- Improved trust in the quality of information
- Drive activities that extract business value from information, including data analytics
- Delivers tangible bottom line benefits including: Lower storage costs, countless hours are spent by employees locating information to do their jobs
- IGI study: 40% of an organization's network drive content is junk
  - 10% is of no business value
  - 25% is superseded / out of date / older than legal retention periods / beyond technical viability
  - 5% is duplicated

Conclusion

- Govern and not only manage
- All information and not only data
- Three dimensions of value:
  - Exploit data and information
  - Manage risks related to information
  - Being more efficient