CIA Triad

Confidentiality

Integrity — Availability

Confidentiality

- permitting authorized access to information while at the same time protecting it from improper disclosure.

Integrity

- property of info whereby it is recorded, used, and maintained in a way that ensures its completeness, accuracy, internal consistency, & usefullness for a stated purpose.

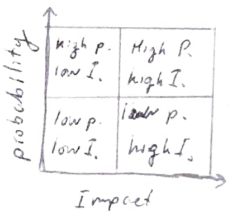
Availability

Systems & data are accessible at the time users need them.

Privacy

- the right of an individual to control the distribution of info. about themselves.
- Privacy legislation can impact companies regardless of location.
- In 2016, the EU passed legislation that addresses personal privacy, deeming it an individual human right.
  - EU's General Data Protection Regulation (GDPR) - Applies to anyone dealing with or in the EU, on top of national & state-level laws.

Risk Management



- Evaluate risk,
- Implement security controls to mitigate risk.

Risk Sources

- Cyberattacks,
  - malware
  - social engineering
  - denial of service
- Other
  - fire,
  - violent crime
  - nat. disasters

If a pickpocket is a threat, their technique and approach is their attack vector.

Ex. of Threat & Impact.

- Unauthorized charges on your credit card.
  - don't store credit info on phone or browser

mitigation

- multi-factor authorization

Booking Vacation

Threat: Bad weather cancelling cruise.

Mitigation: Travel Insurance to transfer risk

Protecting Information

PII - Personaly identifiable information

- Information that, when combined with other pieces of data, significantly narrows the possibility of association with more individuals.

Making Connections

Threats to CIA triad

- Sharing password
  - could lead to furious individuals deleting company files or
  - intro. of software full of malware.
- Remote worker's laptop left unlocked and/or unattended.
  - could lead to compromised integrity.
- Power outtage
- Fires
  - Can destroy digital / analog info.

Solution

Assessments of technical, human and environmental threats must be completed, then steps to mitigate those risks could be put in place

Code of Ethics

States that information security professionals must act honorably, honestly, justly, responsibly, and legally.

- Violating the code of ethics is not acceptable.

Authentication

Confidentiality

When users have stated their identity, its necessary to validate that they are the rightful owners of that identity. Verifying or proving the user's identification is called authentication.

Common methods of auth.:

- Something you know: passwords or pass phrases
- Something you have: tokens, memory cards, smart cards
- Something you Are: Biometrics, measurable characteristics

Privacy in the Working Environment

- Information has different levels of confidentiality
- Different regions have different policies on personal information.

Privacy of Medicaid Info. in U.S.:

- governed by HIPAA

Risk Management Terminology

- An asset: is something in need of protection
- A vulnerability: is a gap or weakness in those protection efforts.
- A threat: something or someone that aims to exploit a vulnerability to thwart efforts.

Professional Code of Conduct

ISC2 Code of Ethics Preamble:

- The safety & welfare of society and the common good, duty to our principles, and duty to each other require that we adhere to the highest ethical standards of behavior.
- Therefore, strict adherence to this code is a condition of certification

ISC2 Code of Ethics Canons:

- Protect society, the common good, necessary public trust and confidence, and the infrastructure.
- Act honorably, honestly, justly, responsibly, & legally
- Provide diligent & competent service to principles.
- Advance & protect the profession.

Decision Making Based on Risk Priorities

- Organizations must evaluate the likelihoods and impact of the risk as well as their tolerance for different sorts of risk.
- Determining risk tolerance is up to the executive mangement and board of directors.

Importance of Risk Management

- A threat can harm an asset by exploiting a vulnerability
- In order to mitigate the risk associated with a threat, it is recommended to evaluate how likely an event is to take place and take appropriate actions to mitigate the risk associated with the threat.

Importance of Governance Elements

Regulations and associated fines can be imposed by governments at the national, regional or local level

Organizations with a presence in multiple jurisdictions must comply with the most restrictive regulations.

Standards cover a broad range of issues and ideas

ISO - International. Org. for Standardization
NIST - Natl. Institute of Standards & tech
IETF - Internet Engineering Task Force

Risk Identification

- Recurring process of identifying different possible risks, characterizing them, and then estimating their potential for disrupting the organization.
  - identify risk to communicate it clearly
  - employees at all levels are responsible for identifying risk.
  - identify risk to protect against it
- Security professionals are likely to assist in risk assessment at a system level, focusing on process, control, monitoring or incident response & recovery.

Governance Elements

- Procedures are the detailed steps to complete a task that support departmental or organizational policies.
- Policies are put in place by organizational governance, such as executive mangemt, to provide guidance in all activities to ensure that the organization supports industry standards and regulations
- Standards are often used by governance teams to provide a framework to introduce policies & procedures in support of regulations
- regulations are commonly issued in the form of laws, usually from government and typically carry financial penalties for non-compliance