Managing Business Risks Related to Cybersecurity

Cloud ERP – bookkeeping

- QuickBooks Online account was highjacked and you were asked to pay a ransom
- QuickBooks Online servers were attacked, and you lost all your accounting and customer data
- A former employee made error deleting customer data from QuickBooks

Social Media Accounts – YouTube, Facebook

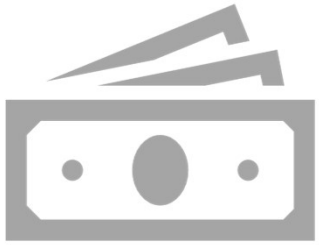
- Someone impersonate you, made sales, collect payment and never send orders to customers

Possibilities

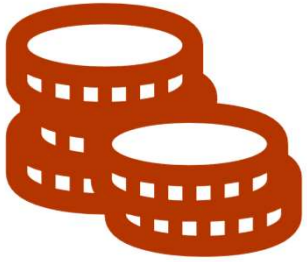
Risk level = probability x impact

- Computer crimes
- Computer viruses and destructive codes
- Natural disasters

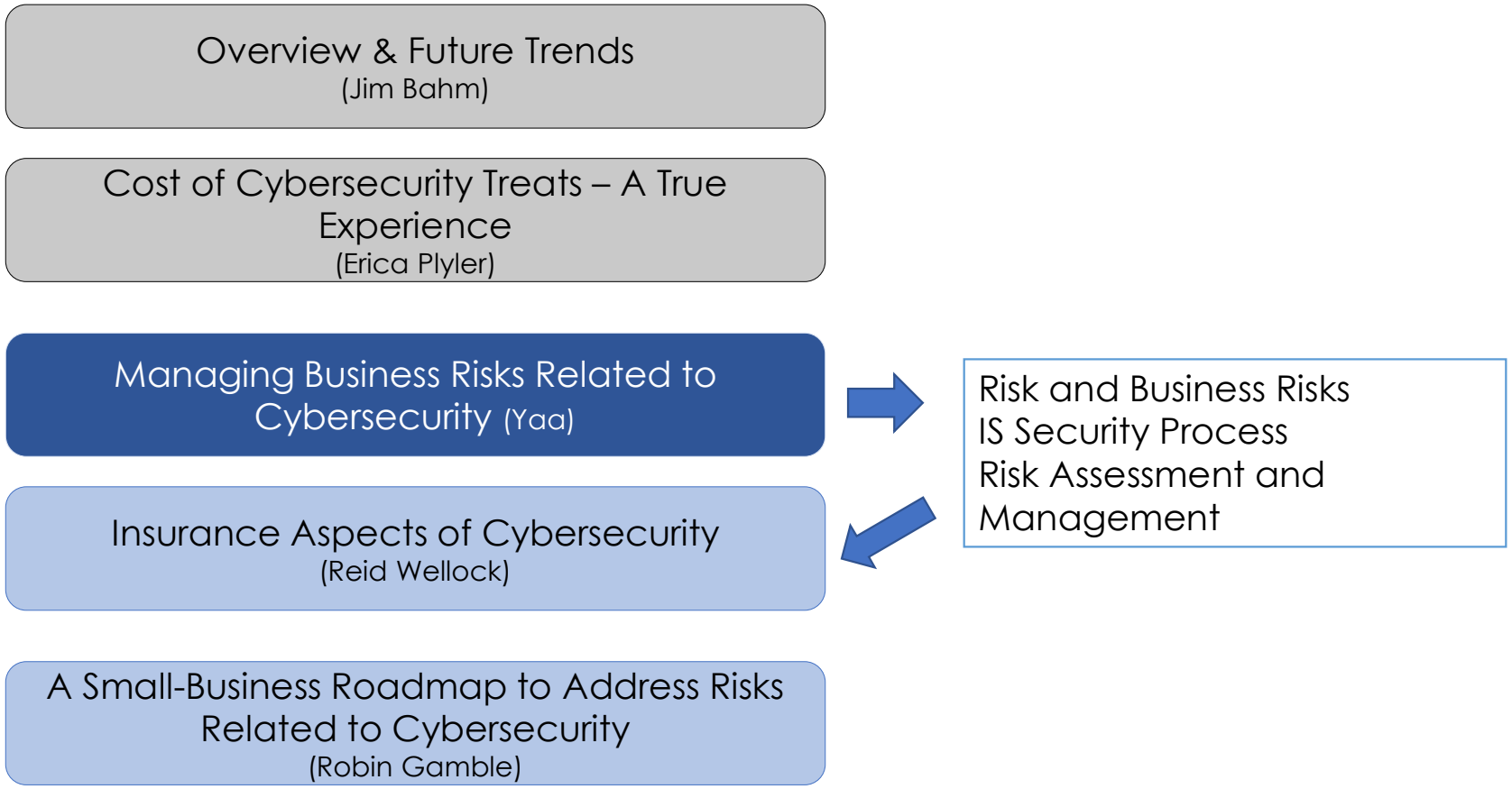
Would this make sense?



Budget spent: $2 million



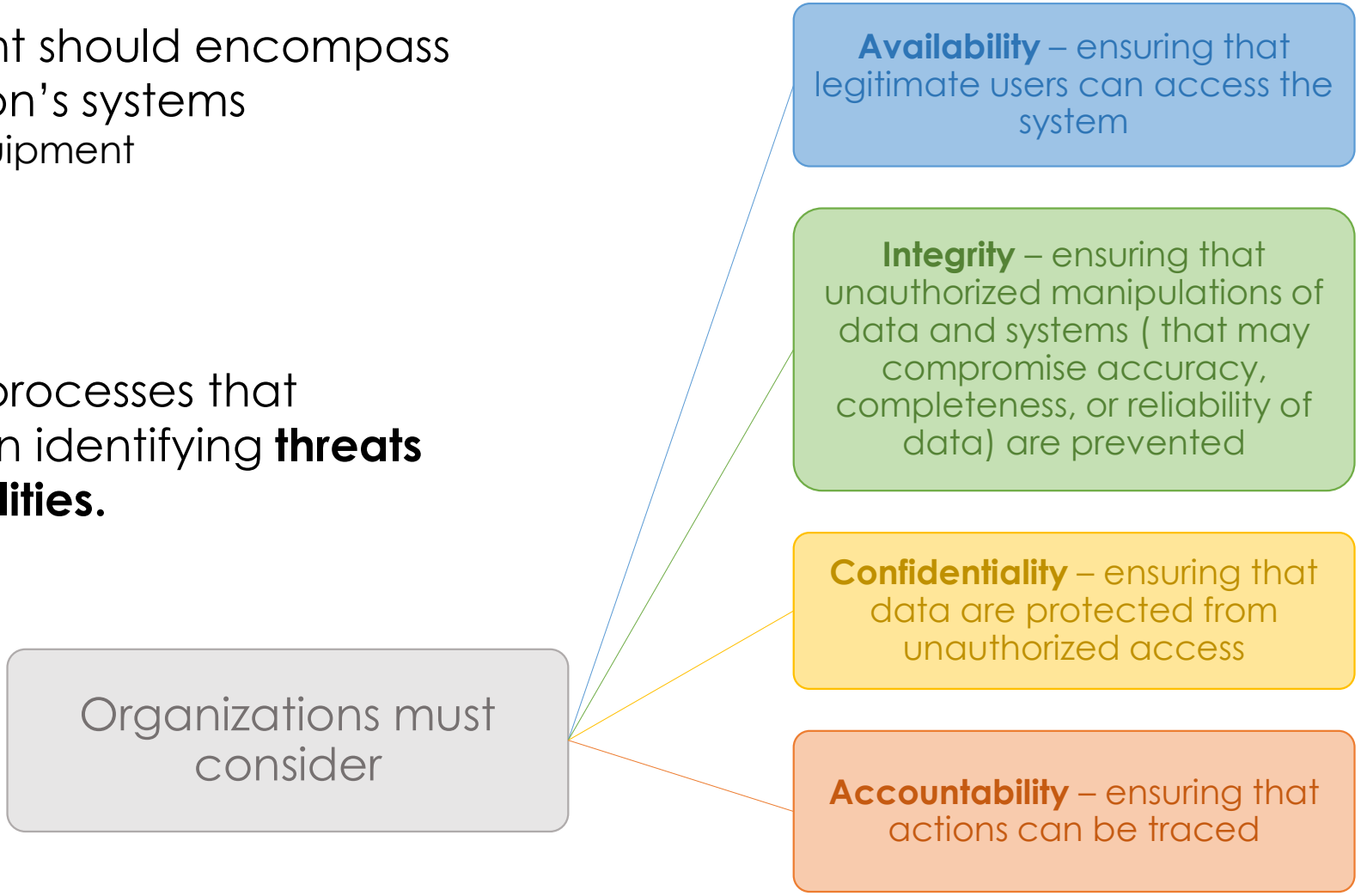
The loss of an asset: $5,000


Overview & Future Trends
(Jim Bahm)
Cost of Cybersecurity Treats – A True Experience
(Erica Plyler)
Managing Business Risks Related to Cybersecurity (Yaa)
Insurance Aspects of Cybersecurity
(Reid Wellock)
A Small-Business Roadmap to Address Risks Related to Cybersecurity
(Robin Gamble)
Risk and Business Risks
IS Security Process
Risk Assessment and Management

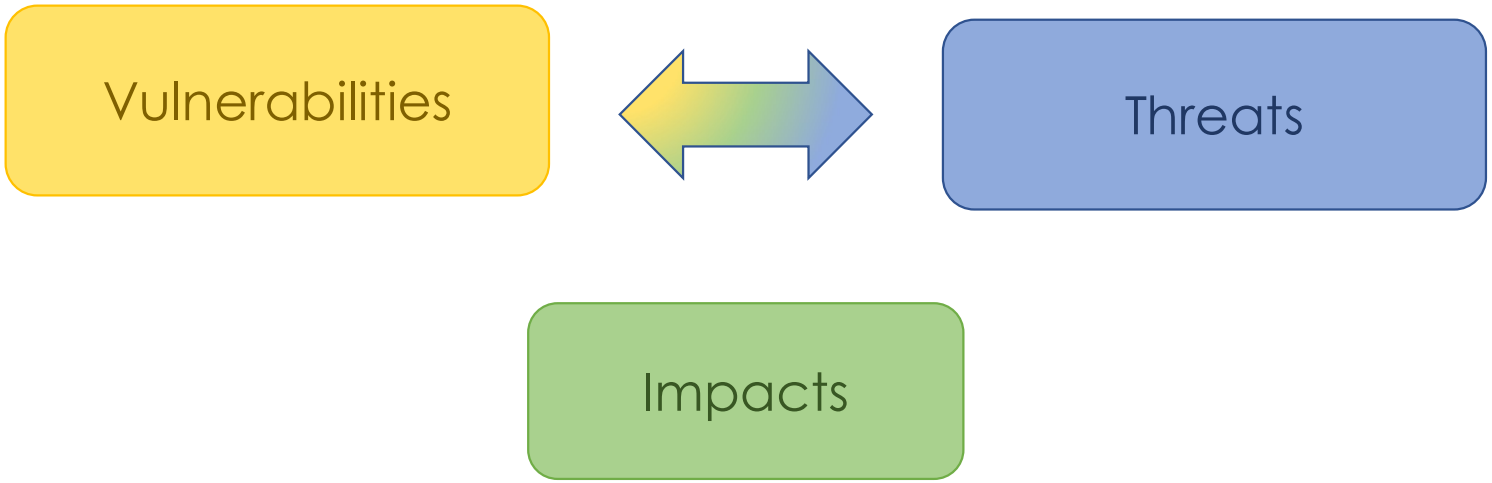
The assessment should encompass an organization's systems

- Hardware, Equipment
- Software
- Data
- Networks

Any business processes that involve them in identifying **threats** and **vulnerabilities.**



Information Systems
Risk Assessment



How to best manage the risks - Controls
Design and implement a security strategy that make the best use of the available resources to eliminate vulnerabilities or reduce impacts.

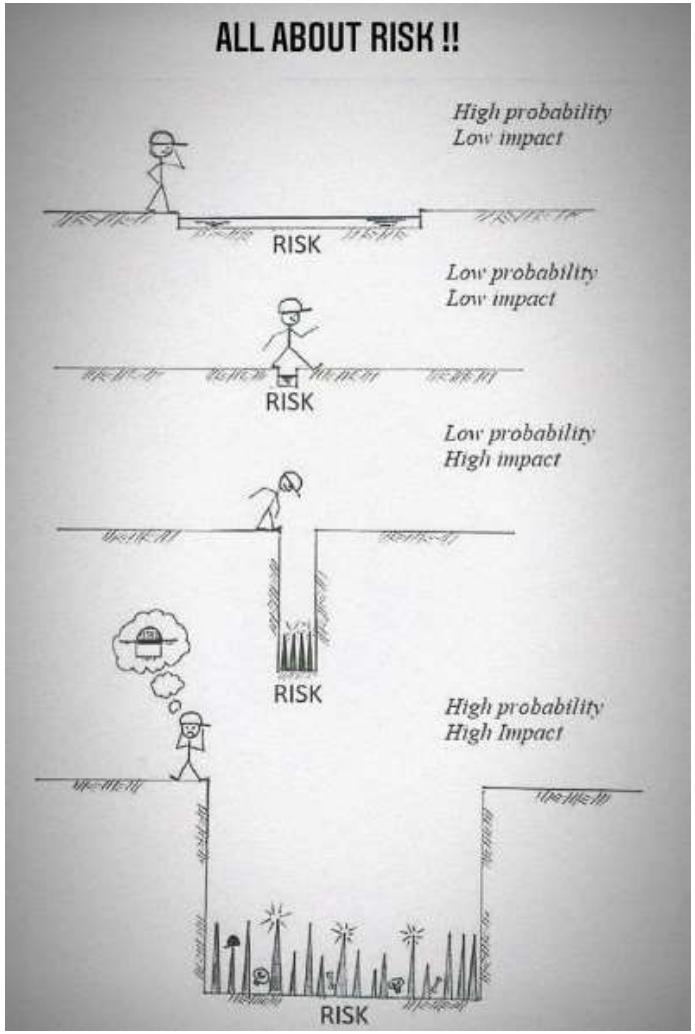
Business Risks
- Strategic
- Operational
- Reputational
- Compliance/Legal
- Institutional

Category
- Availability
- Integrity
- Confidentiality
- Accountability

Business Risk	Risk Category	Possibility	Impact (1-5)	Probability (1-5 or 0-1)	Risk Level (Impact x Probability)

Balancing Different Approaches
- Risk reduction
- Risk acceptance
- Risk transference
- Risk avoidance

Strategy
- Preventive controls
- Detective controls
- Corrective controls



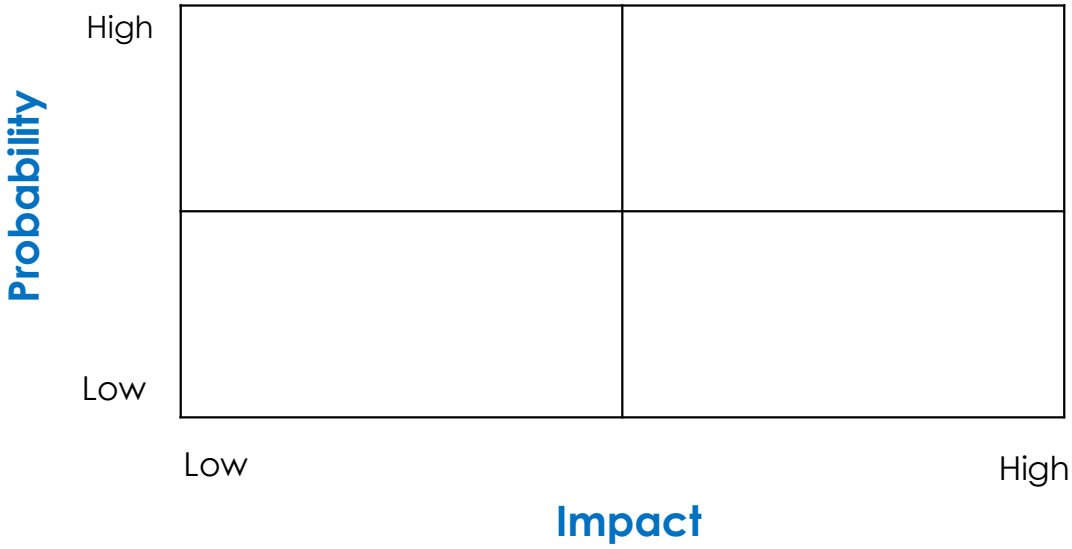


Image Source: https://twitter.com/SJosephBurns/status/1376146974580355081/photo/1

Thorough Understanding of Risks – to determine and assess the threats and vulnerabilities

Technical Information

- Cloud Providers
- Network
- Hardware
- Software

Non-technical Information

- Processes and procedures related to physical or personnel security

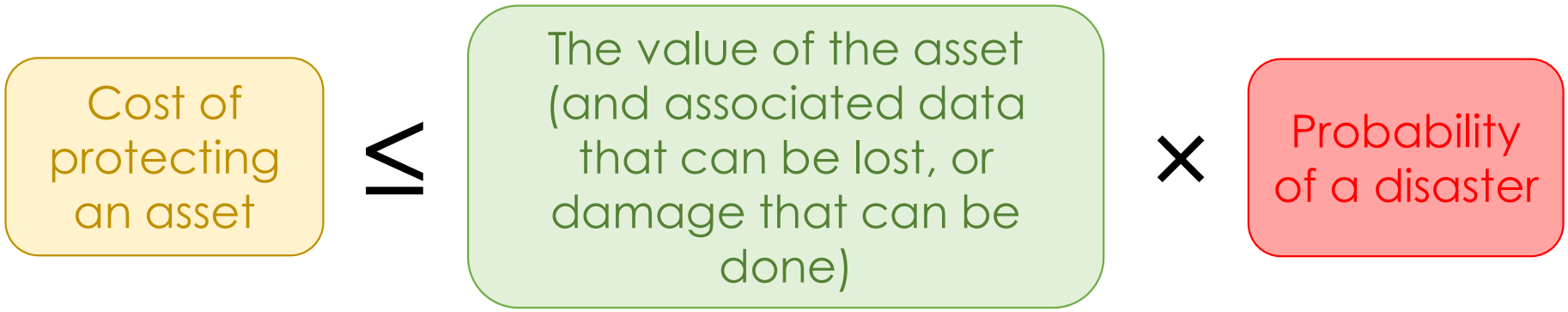
Quantitative data

- Value of an asset or implementation costs of security measures

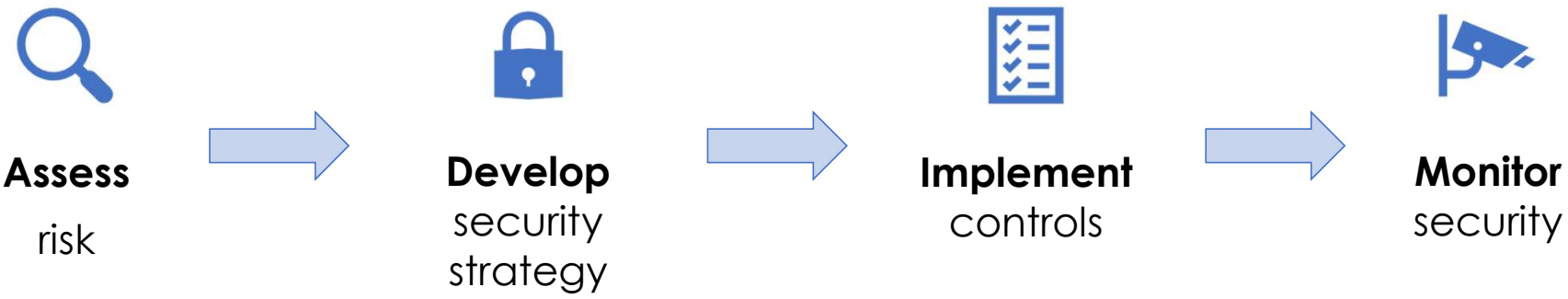
Qualitative data

- Results from interviews or walkthroughs

Rule of thumb – managing multiple risks



Information system security is an ongoing process

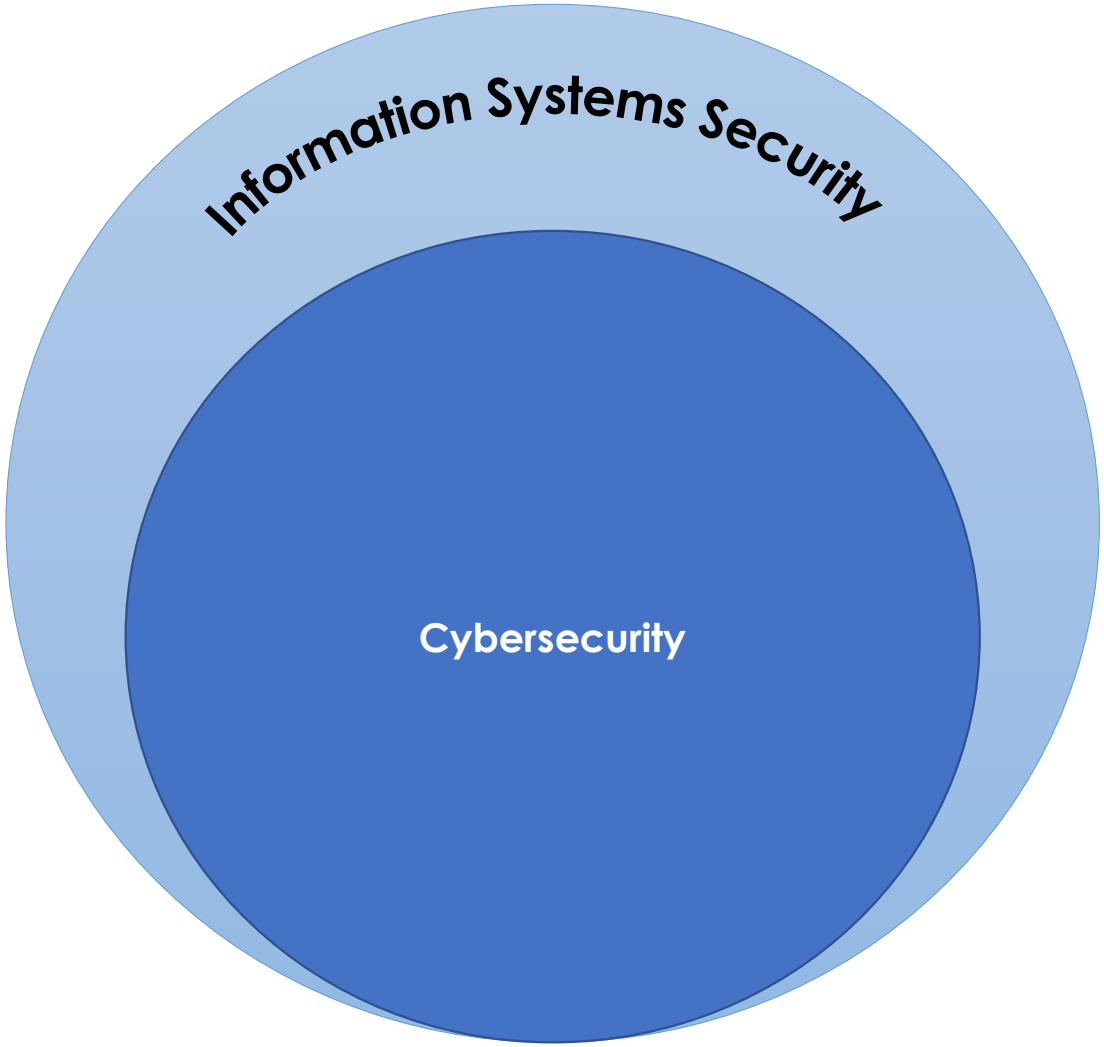


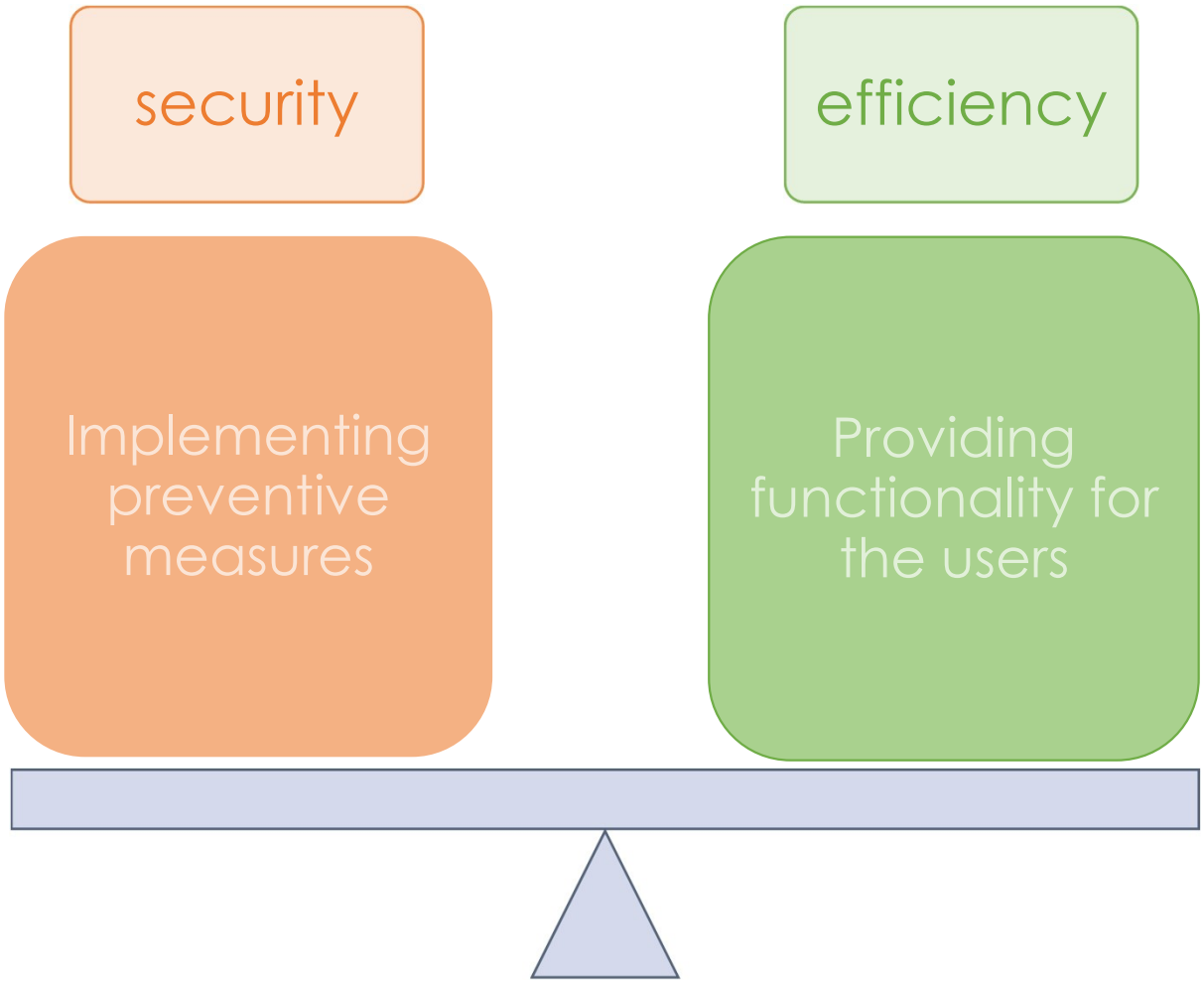
Review and update security process – watch for emerging threats, vulnerabilities, and attacks (including ones on other organizations)

Cybersecurity is the art of

- **protecting networks, devices, and data from unauthorized access or criminal use** and
- the practice of **ensuring confidentiality, integrity, and availability of information**.

Source: https://www.cisa.gov/uscert/ncas/tips/ST04-001





Suggested approach:

Least permissions and least privileges

Users should **only be given access** to the systems, data, or resources that are **needed to perform their duties** and should be **restricted from accessing other resources**.

Common components

- Confidential information policy
- Security policy
- Use policy
- Backup policy
- Account management policy
- Incident handling procedures
- Disaster recovery plan

Having an AUP is not enough

- Clearly communicated
- Having mechanism in place for enforcing the AUP
- AUP should be continually reviewed and updated to account for environmental changes

Source: https://www.techtarget.com/whatis/definition/acceptable-use-policy-AUP

End Notes

Mitigation: firewall, software, SOP, training, etc.

Don't overlook:
Make every effort to **hire trustworthy employees** and treat them well - less likely to commit offenses affecting the organization's information systems.

Selecting a cloud provider is a mitigation approach.

Have a plan in place and have peace of mind ☺
Don't let worries take over your mind.

References

- Book: How to Measure Anything in Cybersecurity Risk by Hubbard and Seieren (2016)
- Book: Cyber Risk Management: Prioritize Threats, Identify Vulnerabilities and Apply Controls by Hodson (2019)
- Book: Information Systems Today: Managing in the Digital World, e9
- CISA.gov
  - CISA CYBERSECURITY AWARENESS PROGRAM SMALL BUSINESS RESOURCES https://www.cisa.gov/publication/cisa-cybersecurity-awareness-program-small-business-resources
  - Resources for Small and Midsize Businesses (SMB) https://www.cisa.gov/uscert/resources/smb
  - CYBER GUIDANCE FOR SMALL BUSINESSES https://www.cisa.gov/small-business
- NIST.gov
  - Cybersecurity Framework https://www.nist.gov/cyberframework
  - NIST Risk Management Framework https://csrc.nist.gov/projects/risk-management/about-rmf
- SBA.gov
  - Strengthen your cybersecurity https://www.sba.gov/business-guide/manage-your-business/strengthen-your-cybersecurity
  - https://www.sba.gov/event/4730
  - https://www.sba.gov/blog/protect-your-small-business-cybersecurity-attacks
- DHS.gov
  - Risk Management Fundamentals https://www.dhs.gov/xlibrary/assets/rma-risk-management-fundamentals.pdf
- EPA.gov
  - Fundamentals of Asset Management https://www.epa.gov/sites/default/files/2016-01/documents/epa-8-capital.pdf

NIST Cybersecurity Framework (CSF)

Function	Category
Identify	Asset Management Business Environment Governance Risk Assessment Risk Management Strategy Supply Chain Risk Management
Protect	Identity Management, Authn & Access Control Awareness and Training Data Security Information Protection Processes & Procedures Maintenance Protective Technology
Detect	Anomalies and Events Security Continuous Monitoring Detection Processes
Respond	Response Planning Communications Analysis Mitigation Improvements
Recover	Recovery Planning Improvements Communications

- Helps organizations ask:
  - What are we doing today?
  - How are we doing?
  - Where do we want to go?
  - When do we want to get there?

Source: https://www.nist.gov/cyberframework