Security and Risk Management

Understand and apply concepts of confidentiality, integrity and availability

Definitions and examples

- Confidentiality - Making sure the right people can access the material. Data must be classified so the administrators knows exactly who should have access. Users must Identify themselves, authenticate, and then be given authorization before having access. Contents must be encrypted or restricted for users who don't do the above.
    - End to End symetric encryption holds confidentiality because only users with a key can see the data
    - File permissions only allow authorized users to view the contents
- Integrity - Protected from changes
    - Hashing
    - Segregation of duties
    - approval checkpoints (SDLC)
    - RSA(uses HMC)
    - IPSec
- Availability - Information is available to users when they need it
    - Not vulnerable to DOS
    - Has backups and redundancy to ensure no downtime

How do they relate to each other?

CIA TRIAD - You can't have maximum levels of everything

Evaluate and apply security governance principles

English please?? - These are just defined roles, and processes for each role, to make sure executive management is informed about IT decisions being made. This makes sure that information is appropriately secured, communicated, documented, and budgeted for. It's like a questionaire. Look at ISO 27000 to get requimrents for which security frameworks you should impliment. Think of security frameworks as blue prints and governance principles(iso 27000 or togaf) as guides for how to draw blueprints.

- Alignment of security function to business strategy, goals, mission, and objectives
    - Have to analyze cost of loss/thieft information, cost to impliment controls, and the benefit to organization by certain controls.
- Organizational processes (e.g., acquisitions, divestitures, governance committees)
    - if the business changes at all, security needs to be involved in that changing process. apply frameworks to those processes.
- Organizational roles and responsibilities
    - different job titles have to work with others and be aware of things. each job has a checklist of things to be concerend about. some positions will be reponsible for risk on certain decisions.
- Security control frameworks
    - the blue prints to how security in the organization is done. ex. if you are going to label an area on a blueprint as a "bed room", it needs to meet certain requirements. certain frameworks need to be applied to your organization based off what you contain.
- Due care/due diligence

    - legal perspective. What would a "reasonable person" due in the same circumstance if they were being responsible?

      Difference between Process/architecture/framework/standard?

- Process: A set up steps to accomplish a task.
- Architecture: specifies when and where to apply security controls. Describes interactions and roles
- Framework: A set up processes with implimentation guidance
- Standard: A set of requirements, roles, and controls/frameworks to impliment

Determine compliance requirements

Governments are required to impliment NIST 800-53. Private sector is required to implimented COBIT. Many businesses end up implimenting part of each framework to meet its business objectives.

Organizations operate in environments where laws, regulations, and compliance requirements must be met. Want to handle peoples cred cards? - must meet certain requirements and impliment certain frameworks. Want to be a defense contractor? - same as before.

- Contractual, legal, industry standards, and regulatory requirements
    - one example is all federal agencies are required to ahere to FISMA. Gives list of requirements because they handle mission information as well as PIV.
- Privacy requirements
    - Mitre has a good framework for dealing with privacy. You just need to identify what data you process and see if it applies in your TOGAF or other blueprint guidlines you are following.

Understand legal and regulatory issues that pertain to information security in a global context

- Cyber crimes and data breaches
- Licensing and intellectual property requirements
- Import/export controls

- Trans-border data flow
- Privacy

Difference between Criminal Law/Common Law/Private law/Civil Law/Federal Law/

- Criminal Law: punished by jail, fine, or death
- Common Law: jury makes decision. then judge decides punishment
- Civil Law: never incarcerated or executed. Have to reimburse the plaintiff
- Private Law: deals with relations between individuals and institutions. Part of civil law
- Federal Law: body of law consisting of a constitution, enacted laws, and the court decisions pertaining to them

Understand, adhere to, and promote professional ethics

- $(ISC)^2$ Code of Professional Ethics - be a nice boy or girl
- Organizational code of ethics - basically that anything you invent/design/consult is for good. you do your due diligence

Develop, document, and implement security policy, standards, procedures, and guidelines

Examples below

- Policy: write policy for people who use lab at work. no usb allow, need to take this training, etc etc
- standards: FIPS 140-2 is a common cryptographic standard in the military. must do certain things to have your device certifed.
- procedure: you are tasked with the job of writing a procedure for analyzing computers that may contain malware
- guidlines: this is not mantatory and no penalties happen if not followed. ex. i give guidlines for how to configure SMB shares at work since there are no SMB STIGs we must follow.

Identify, analyze, and prioritize Business Continuity (BC) requirements

- Develop and document scope and plan
- Business Impact Analysis (BIA) - process to determine and evaluate the potential effects of an interruption to critical business operations as a result of a disaster, accident or emergency. If a function went down, could the rest of the business function? Could customers still function? Could customers still purchase things?

Contribute to and enforce personnel security policies and procedures

- Candidate screening and hiring - talk to references. background check. credit history. criminal history. education. drug testing.
- Employment agreements and policies - write policies that people can only use computers for work. NDA. mandatory vacations.

- Onboarding and termination processes - make sure people are given least privilege. take away access, badge, account, change passwords.
- Vendor, consultant, and contractor agreements and controls - your business has security requirements when dealing business with them. if their code is in yours, they must develop securely. their information systems that connect to yours must be hardened
- Compliance policy requirements - PCI is a policy that makes sure you must follow various controls to deal with credit cards
- Privacy policy requirements - FISMA regulates peoples PII info and that is appropriately controlled

Understand and apply risk management concepts

- Identify threats and vulnerabilities - NIST 800-30 defines threat sources. microsoft also has great threat model
- Risk assessment/analysis - find all vulnerabilities and flaws in scope. prioritize them by level of effort to fix and the amount of risk of not fixing that.
- Risk response - If you face risk, you can do one of the following things: avoid it, transfer it, mitigate it, or accept it
- Countermeasure selection and implementation - If risk is identified, need to consider accountabilitiy, reliablility, dependencies, CIA, when implimenting a countermeasure. Think of solution to problem and other supplimental controls to help fix it. soemtimes you won't be able apply a patch to completely fix problem, so you will need some supplimental fixes (band aids)
- Applicable types of controls (e.g., preventive, detective, corrective) - directive, deterrent, preventive, compensating, detective, corrective, recovery. a good plan usually contains most of the types of controls just listed. that is defense in depth
- Security Control Assessment (SCA) -
- Monitoring and measurement - make sure problems, vulnerabilities, failures are monitored. make sure metrics are recorded that document hours spent to fix and recover. cost from failure. for network, get IDS and log server. do bi-weekly analysis to determine information system failures and patterns
- Asset valuation - conduct software and hardware inventories regularly and automatically
- Reporting - document baseline. explain why something is a risk. how severe. provide a fix, supplimental fixes, level of effort to fix, and a mitigation for why this risk could potentially be accepted (if you think it should).
- Continuous improvement - Six Sigma. record metrics on your processes. find bottlenecks. eliminate bottlenecks.
- Risk frameworks - below is list of frameowkrs
    - ISACA
    - ISO 31000
    - ISO 2009
    - NIST RMF Framework

Understand and apply threat modeling concepts and methodologies

- Threat modeling methodologies - make scope, applicable attack vectors, vulnerabilities open, risks, and countermeasures. should result in architecture changes, remediation actions, and good data for a risk report
- Threat modeling concepts - same as above

Apply risk-based management concepts to the supply chain

- Risks associated with hardware, software, and services - look at past CVEs
- Third-party assessment and monitoring - the third party solutions you use could have vulnerabilities or back doors
- Minimum security requirements - decide on requirements for your product. those, and only those things will be delivered. very hard.
- Service-level requirements - requirements for a service from the client viewpoint, defining detailed service level targets and mutual responsibilities

Establish and maintain a security awareness, education, and training program

- Methods and techniques to present awareness and training - need to always train people constantly in security awarness or it doesn't work. always echo it. disaster recovery is always way more expensive.
- Periodic content reviews - make sure as new responsibilities and processes arise that we have security training in mind for them. make sure we are being aware of current threats
- Program effectiveness evaluation - track enforcement and enhancement of security initiatives. periodic walk throughs and quizes to make sure people are staying up to date

Home Page
To next domain! - D2 - Asset Security