Week 11 Research

2020-04-12

Chaz Davis

Chapters 17-26 (minus a couple chapters omitted - will post next week.)

1. List and briefly define the five alternatives for treating identified risks.

- Risk acceptance
- Risk avoidance - not proceeding with the activity that creates this risk
- Risk transferal - sharing responsibility for the risk with a third party, eg. insurance
- Reduce the consequence - modifying the structure to reduce impact, eg. off–site backup, disaster recovery plan
- Reduce the likelihood - implementing suitable controls, eg. deploying firewalls and access tokens

2. Define consequence and likelihood.

Consequence: The analyst must then specify the consequences of a specific threat eventuating and consider the appropriate responses; minor - moderate - major - catastrophic

Likelihood: is the probability of an event taking place. The likelihood for a threat to occur is typically described qualitatively with words like rare - unlikely - possible - likely- almost certain.

3. List the steps in the detailed security risk analysis process.

- System characterization
- Threat identification
- Vulnerability identification
- Control analysis
- Likelihood determination
- Impact analysis
- Risk determination
- Control recommendations
- Results documentations.

4. List some of the key national and international standards that provide guidance on IT security management and risk assessment.

ISO27000–ISO27005 and ISO13335

5. List the three fundamental questions IT security management tries to address.

- What assets do we need to protect?
- How are those assets threatened?
- What can we do to counter those threats?

6. Define security control or safeguard.

Safeguards or security control are practices, procedures or mechanisms which may protect against a threat, reduce vulnerability, limit the impact of an unwanted incident, detect unwanted incidents and facilitate recovery.

7. List and briefly define the elements from the implementation of controls phase of IT security management.

- **Implementation of Security Plan** - may require system configuration changes, upgrades, new system installation, development of new procedures to document practices
- **Security Training** - for personnel responsible
- **Security Awareness** - general security training for all personnel, including workshops etc. to explain the need for security and increase awareness

8. What is the relation between change and configuration management as a general systems administration process, and an organization's IT security risk management process?

9. What are the principal concerns with respect to inappropriate temperature and humidity?

Computer are designed to operate within a certain temperature range (most between 10–32°C). Outside this range, resources might continue to operate but produce undesirable results and components might be damaged. Another concern is the internal temperature of equipment, which can be significantly higher than room temperature. The cooling mechanisms may rely on, or be affected by, external conditions. Relative humidity should be maintained between 40% and 60%. Too high humidity can result in corrosion, condensation (threat to magnetic and optical storage as well as circuit boards). Too low humidity can cause some materials to change shape and static electricity becomes a risk.

10. What are the threats posed by loss of electrical power?

3 groups of power utility problems:

- **Under–voltage** - events range from temporary dips in voltage supply to brownouts, to power outages. Generally no damage is done, but service is interrupted

- **Over–voltage** - a surge of over–voltage caused by a supply anomaly, some internal wiring fault or lightning can destroy electrical components
- **Noise** - noise can interfere with signals inside electronic devises, causing logical errors.

11. Briefly define the three major sub-systems in the FIPS 201 PIV Model illustrated in Figure 16.2.

- **Front end subsystem** - supports up to three-factor authentication; the number of factors used depends on the level of security required. The front end makes use of a smart card, known as a PIV card, which is a dual-interface contact and contactless card. The card holds a cardholder photograph, X.509 certificates, cryptographic keys, biometric data, and a cardholder unique identifier (CHUID), explained subsequently.
- **PIV card issuance** - and management subsystem. This subsystem includes the components responsible for identity proofing and registration, card and key issuance and management, and the various repositories and services (e.g., public key infrastructure [PKI] directory, certificate status servers) required as part of the verification infrastructure.
- **Access Control System** - includes components responsible for determining a particular PIV cardholder's access to a physical or logical resource.

12. Briefly define the four protected area types described in NIST SP 800-116.

- **Visual (VIS):** Visual identity verification of a PIV card is done by a human guard. The human guard checks to see that the PIV card looks genuine, com- pares the cardholder's facial features with the picture on the card, checks the expiration date printed on the card, verifies the correctness of other data elements printed on the card, and visually verifies the security feature(s) on the card.
- **Cardholder unique identifier (CHUID):** The CHUID is a PIV card data object. Authentication is implemented by transmission of the CHUID from the PIV card to PACS.
- **Biometric (BIO):** Authentication is implemented by using a fingerprint or iris data object sent from the PIV card to the PACS.
- **Attended biometric (BIO-A):** This authentication mechanism is the same as BIO authentication, but an attendant supervises the use of the PIV card and the submission of the PIN and the sample biometric by the cardholder.
- **PIV authentication key (PKI):** PACS may be designed to perform public key cryptography-based authentication using the PIV authentication key. Use of the PKI provides two-factor authentication, since the cardholder must enter a PIN to unlock the card in order to successfully authenticate.
- **Card authentication key (CAK):** The CAK is an optional key that may be present on any PIV card. The purpose of the CAK authentication

mechanism is to authenticate the card and therefore its possessor. The CAK is unique among the PIV keys in several respects: The CAK may be used on the contactless or contact interface in a challenge/response protocol; and the use of the CAK does not require PIN entry.