Date:

ICS

lecture 3

Security Control and risk managment.

Security controls devided into 3 main categories.

- Physical Controls
- Technical / Logical controls
- Administrative Controls.

Physical control.

- Security mesures that took to provide Safety for Sensitive material.

CCTV, Security guard, ID access

Technical / Logica Controls.

- Using technology Controlling the aceess and usage of data and rescources.

Encryption, Smart card, Access control.

Administrative control.

- providing security using human factors. Who Can aceess to what resources.

Troining, and awareness.
Policy and procedures
recovery plans.

Controls Categorized using functionality

(6)

- Preventive Controls
- Detective Controls
- Deterrent Controls
- Corrective Controls
- Recovery Controls
- Compensating Controls.

- Preventive Controls - ~~prot~~ Controls that took to prevent from something happen bad.

- Detective Controls - Controls that took to find error or unauthorized activities that happen or occured.

- Deterrent Controls - Controls that took to discourage attakers not to do/attake.

- Corrective Controls - Controls that took to Correct the issues that happen after a attack.

- Recovery Controls - ~~Co~~ Same as Corrective. but more often they are used in serious situations to restore information.

- Compensating Controls - Controls that took as backup to the original Controls.

Date: / /

Risk apatite - max risk level that can hold.

Risk - possibilitie of damage happening.

Information risk managment (IRM) - process of identify the risk and reduce it using right mechanisms.

Managing risks (4 ways)

- Accept
- Transfer
- Mitigate
- Avoid.

~~Accept~~ Avoid - trying to avoid a risk by identifying assets that exposure a risk.

Transfer - hand over the some part of the risk to a third party.

Mitigate - reducing the risk to acceptable level.

Accept - after mitigating to acceptable level Accept the risk.

Quantitative risk analysis.

- total assests = 10 computers
- income = $50 per hour → from 1 computer

  - total earning for 1 hour = 10 x 50
  - from 10 computers = $500 per hour

Recover from malware = 4 hours

if malware infected = 4 x 500
expected loose
SLE = $2000 (loose)

Single lose Expectancy (SLE) - if an insidence happen What will be lose. (its $2000).

Annualized Rate of Occurrence (ARO) - how many times threat can be happen withing year.

eg: Withing 5 years malware infected 25 times.

5 → 25

annual rate = 25/5

ARO = 5

Annualized Lose Expectancy (ALE) - how much expected to loose withing a year (SEE x ARO)

SLE = $2000 , ARO = 5

= 2000 x 5

ALE = $10000

Date: / /

Safeguard cost & benefit -

after control ,

Anti virus = $ 1000

ARO = 0

new ALE after control = 2000 x 0

= 0

Cost / Benefit = ALE before Safeguard - ALE after Safeguard - Safeguard annual cost.

= $10000 - 0 - $1000

= $9000

+ → benefit

- → lose.

Eg : if after Safeguard ARO is 2.

ALE after = 2000 x 2

= 4000

Cost / benefit = 10 000 - 4000 - 1000

= $ 5000

NO. Date: / /

Eg ; if

AV = cost is 7000

Cost / benefit = 10 000 - 4000 - 7000

= - 1000 (loose)