A secure network??

- Secure network devices with AAA, SSH, role-based CLI, syslog, SNMP, and NTP.
- Secure services using AutoSecure and one-step lockdown.

A secure network??

- Protect network endpoints, such as workstations and servers, against viruses, Trojan Horses, and worms with Cisco NAC, Cisco IronPort, and Cisco Security Agent.
- Use Cisco IOS Firewall and accompanying ACLs to secure resources internally while protecting those resources from outside attacks.

A secure network??

- Supplement Cisco IOS Firewall with Cisco IPS technology to evaluate traffic using an attack signature database.
- Protect the LAN by following Layer 2 and VLAN recommended practices and by using a variety of technologies, including BPDU guard, root guard, PortFast, and SPAN.

A secure network??

Cisco.com

- Failures
- Fail-open
- Attack possibilities
- Exploitation
- End users
- Attacks under unexpected conditions
- Check all assumptions with other people

Threats-Risk analysis

Quantitative risk analysis

SLE = AV * EF

- AV is asset value.
- EF is the exposure factor - the loss, represented as a percentage, that a realized threat could have on an asset.
- SLE is Single Loss Expectancy - the result of AV * EF, or the cost of a single instance of a threat.

Incident

Cisco.com

Flood threat

- Exposure Factor is 60 percent
- AV of the enterprise is 80,000,000 SEK
- SLE is 80,000,000 * .60 = 48,000,000 SEK

Incident

Cisco.com

Data entry error

- Exposure Factor is .001 percent
- AV of data and databases is 8,000,000 SEK
- SLE is 8,000,000 * 0.00001 = 80 SEK

Quantitative risk analysis

ALE = SLE * ARO

- ARO (Annualized Rate of Occurrence) represents the estimated frequency that a threat is expected to occur.
- ALE (Annualized Loss Expectancy) is the expected financial loss that an individual threat will cause an organization. It is a monetary value derived from the formula SLE * ARO.
- ALE is the number used to justify the least-cost security measures.

Incident

Cisco.com

Flood threat

- A flood-of-the-century event = 1/100

- SLE is 48,000,000 SEK
- ARO is .01
- ALE is 48,000,000 SEK * .01 = 480,000 SEK

Incident

Cisco.com

Data input error

- 500 times a day
- 250 days per year

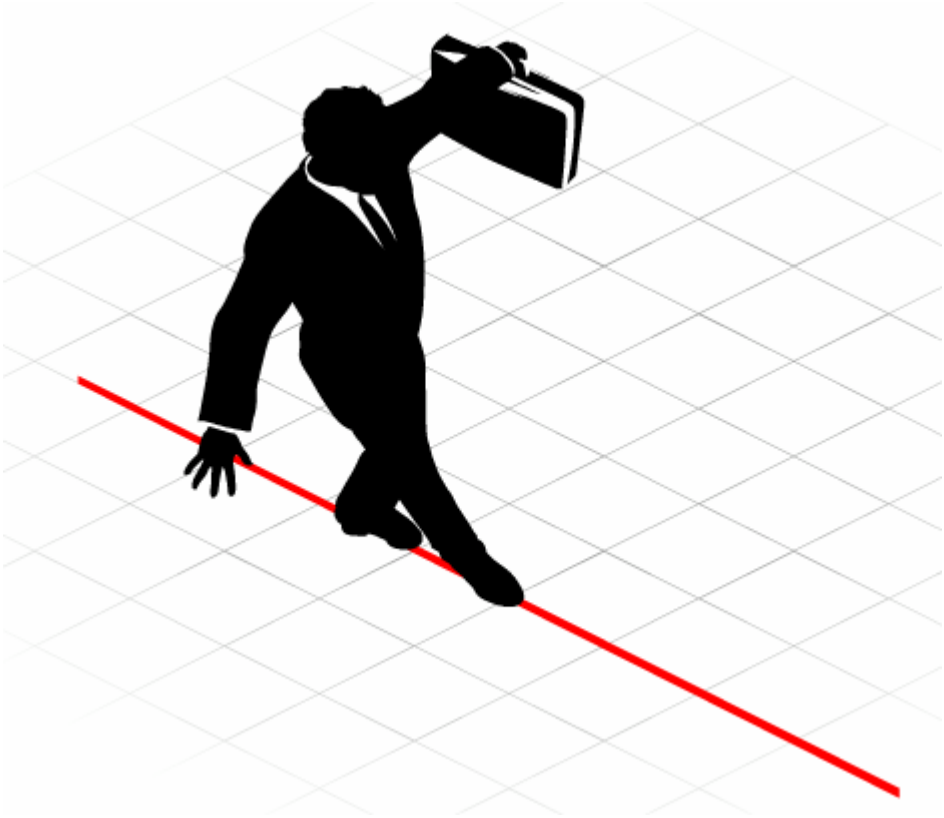
- SLE is 80 SEK
- ARO is 125,000
- ALE is 80 SEK * 125,000 = 10 000 000 SEK

Risk analysis

- Insider network abuse - 8,000,000 SEK in lost productivity
- Data input error - 4000,000 SEK
- Worm outbreak - 800,000 SEK
- Viruses - 80,000 SEK
- Laptop theft - 80,000 SEK
  - In incidents that involve national security, it is not advisable to base decisions on cost.

Walk the tight rope

- Risk management
- Risk avoidance



Risk management

Internal system compromise

- Provide the minimum necessary privileges to internal users to perform specific tasks, and use secure applications that minimizes inside access.

Stolen customer data

- Keep all customer data on inside servers, and only transfer data to the outside on demand.

Phony transactions

- if external server is broken into
- Allow only man-in-the-middle attacks on the external server, and design the external server application so that it does not allow arbitrary transactions to be called for any customer account.

Phony transactions

Cisco.com

- if customer PIN or smart card is stolen –
- Use a quick refresh of revocation lists, and have a contract with the user that forces the user to assume responsibility for stolen token cards.

Insider attack on the system

- Strictly limit inside access to the application, and provide strict auditing of all accesses from the inside.

Data input error

- Enhance the security of database applications, and provide a redundant checking system to reduce data entry errors.

Data center destruction

- Ensure that backups are kept off campus and that additional equipment is on hand. Enhance defenses against flooding by raising equipment off the ground and taking other precautions.

Risk avoidance