RISK
MANAGEMENT
SALES
RESEARCH
COMPLEX
CUSTOMER
PLAN
ASSESSMENT
ANALYSIS
PLANNING
IMPLEMENTA
IMPACT
RETENTION
MONITOR
MANAGEMENT
ORGANIZATION
OPPORTUNITY
DATA
IDENTIFICATION
PROCESS
COST
EVALUATION
SCOPE
TREATMENT
STRATEGY
IMPORTANT
SOURCES
PLAN
SOLUTION
PROJECT
EVALUATION
RISK
EXT
PROBABILITY
CUSTOMER
RCH

Risk management involves all processes from assessing the risk to managing it

The four phases under risk management are

- Risk Assessment
- Risk Analysis
- Risk Mitigation
- Risk Monitoring

Risk Assessment

All assets, threats and vulnerabilities are identified

Risk Analysis

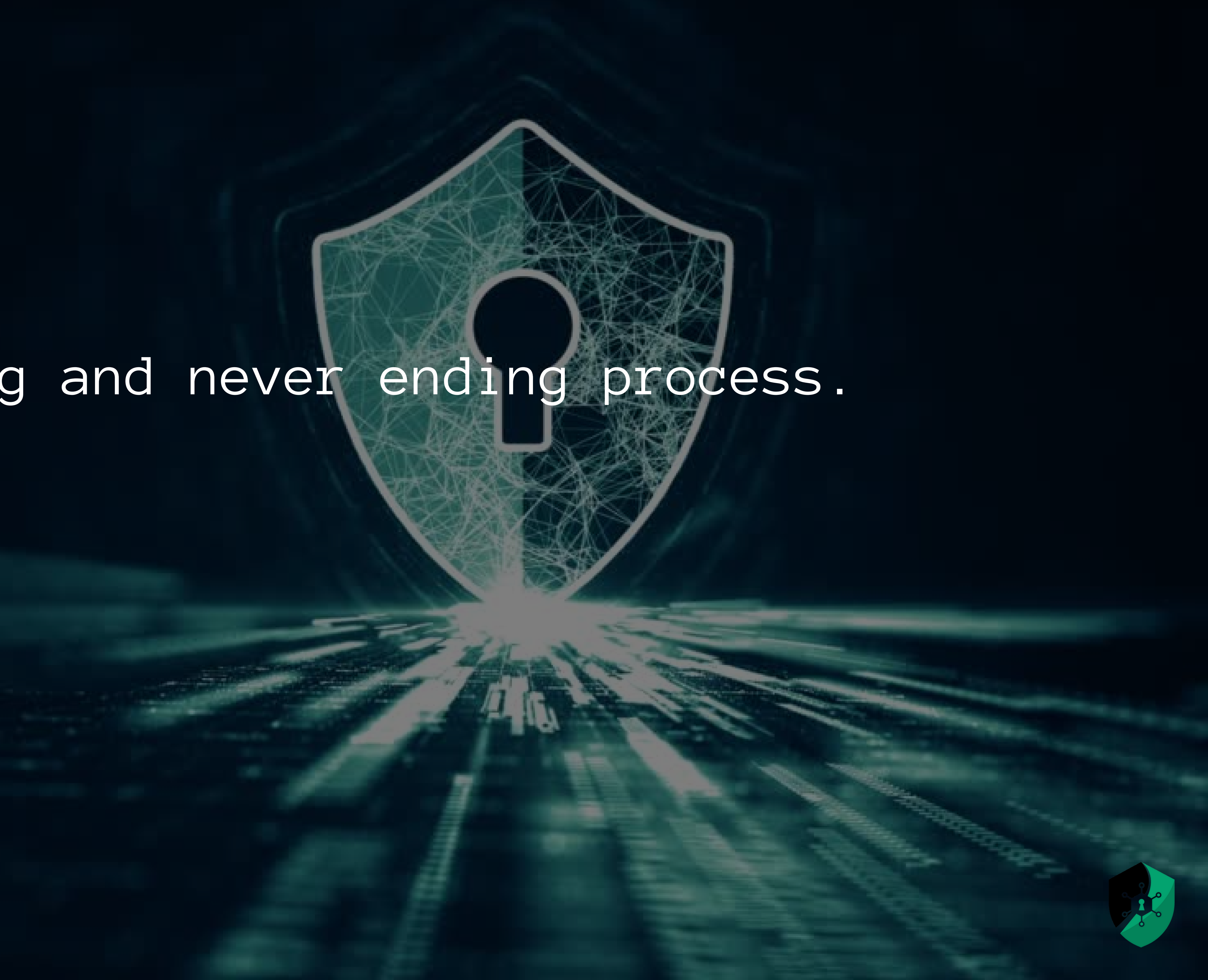
The impact of the risk to the assets

Risk Mitigation

- Reduce the risk
- Avoid the risk
- Transfer the risk
- Accept the risk
- Reject the risk

Risk Monitoring

This is an ongoing and never ending process.



Risk Controls

- Administrative (awareness training, disaster recovery plans, background checks etc)
- Technical (Access control lists, authentication, encryption)
- Physical (trip alarms, security guards, biometrics etc)

Risk Treatment

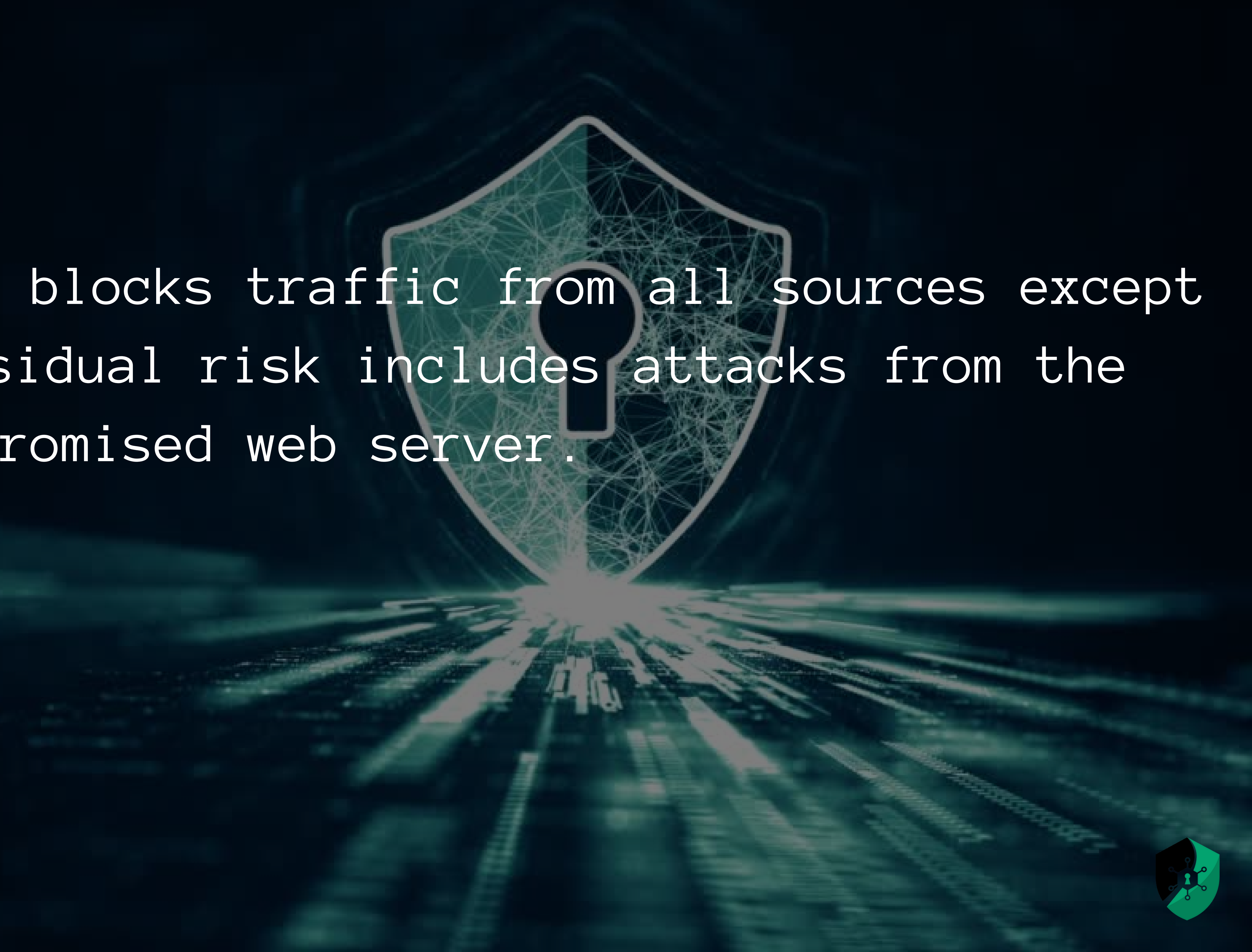
- Preventive (system hardening)
- Detective (logs, security audits)
- Corrective (back up restores, self healing system)
- Compensating (use of disaster recovery site, pen & paper)

Residual Risk

Those risks that are expected to remain after the planned response of risk has been taken, as well as those that have been deliberately accepted. They are acceptable to the organization's risk tolerance level. Sometimes a residual risk has no reasonable response either.

PMBOK DEFINITION

Residual Risk



If an application server blocks traffic from all sources except the webserver, the residual risk includes attacks from the compromised web server.

Residual Risk

All risks can never be fully covered at an acceptable level of cost or usability. At some point, risk will have to be accepted.