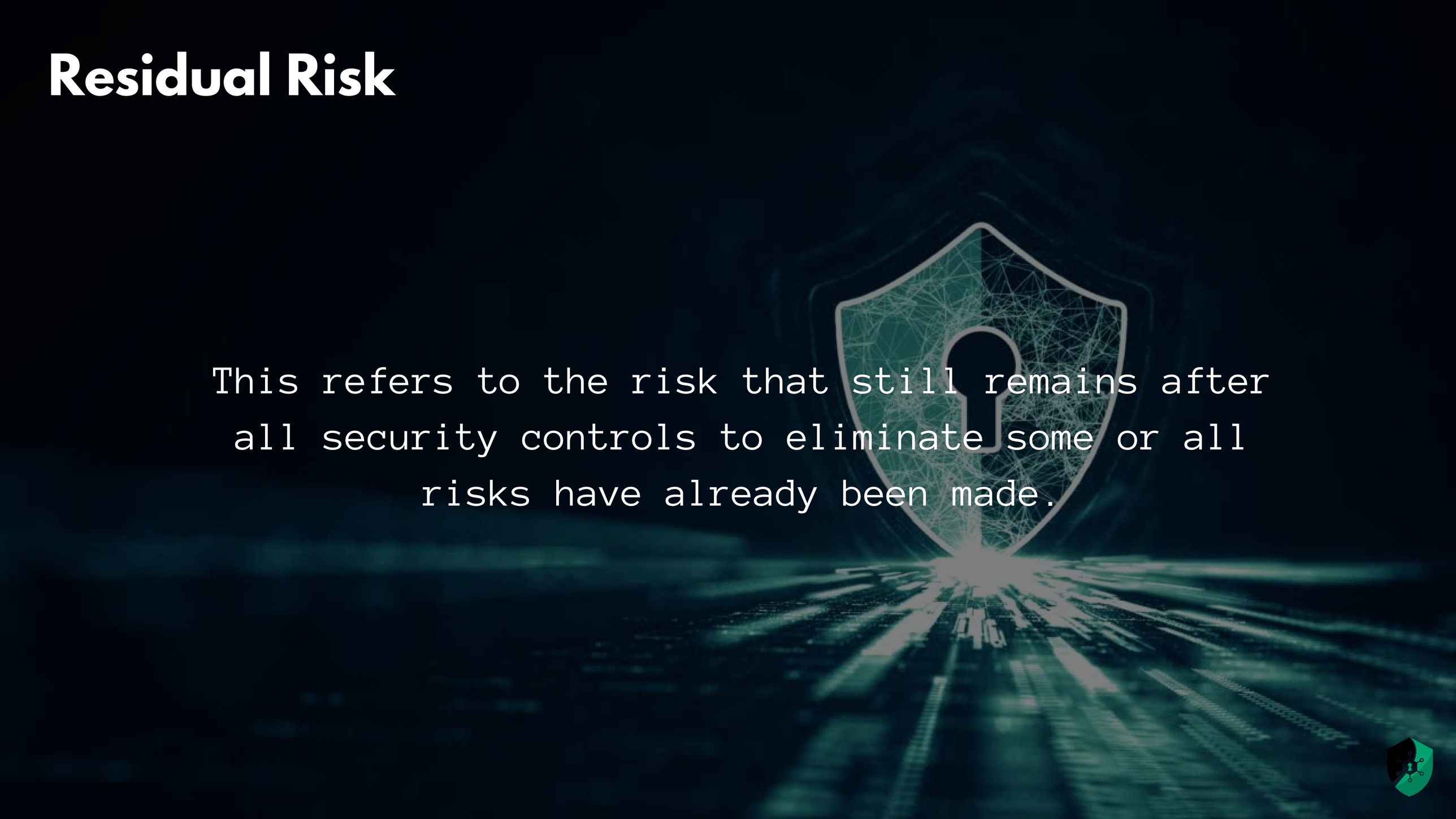

RISK
MANAGEMENT
SALES
RESEARCH
CUSTOMER
PLAN
ASSESSMENT
COMPLEX
ANALYSIS
IMPACT
PLANNING
IMPLEMENTATION
RETENTION
MONITOR
MANAGEMENT
ORGANIZATION
OPPORTUNITY
DATA
IDENTIFICATION
PROCESS
COST
EVALUATION
SCOPE
TREATMENT
STRATEGY
IMPORTANT
SOURCES
PLAN
SOLUTION
PROJECT
EVALUATION
PROBABILITY
CUSTOMER

Residual Risk



This refers to the risk that still remains after all security controls to eliminate some or all risks have already been made.

Residual Risk

It basically refers to the risk that companies will have to live with based on the decisions they have made regarding risk mitigation.

Residual Risk

It is also important to consider residual risk for compliance and regulatory requirements.

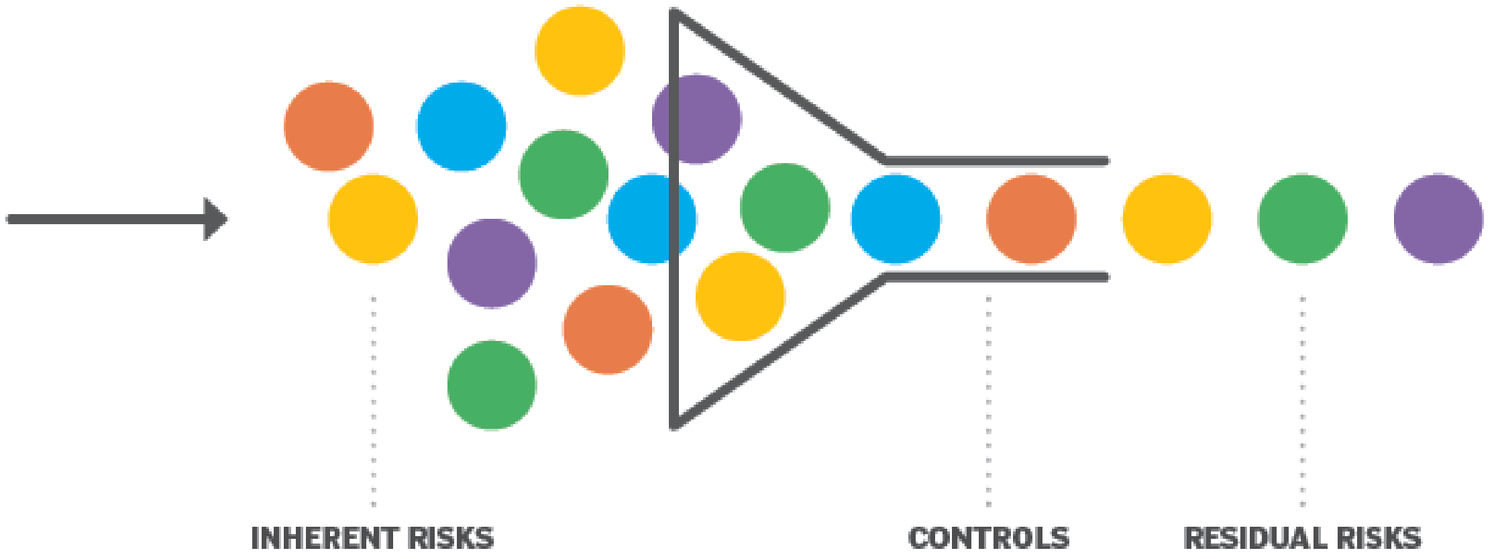
Residual Risk

Also important for determining the appropriate types of security controls and processes that get priority over time.

Inherent Risk

This is the risk that exists prior to any attempts at mitigation.

Inherent risk vs. residual risk



Residual risk is the risk remaining after efforts have been made to reduce the inherent risk.

Residual Risk

Residual risk = Inherent risk - impact of risk controls

Residual Risk

Assuming there is an inherent risk of a ransomware attack and the impact of such an attack could be $3 million but the cost of mitigating such an attack could cost $1 million, then the residual risk is $2 million.

Residual Risk

With qualitative analysis, let's say the possibility of the ransomware attack being successful is 9 out of 10 but by applying necessary anti-malware and backups in place, the score is reduced to 3. In this case the residual risk is 3.

Residual Risk

Such risks can be managed by:

- Doing nothing
- Update or increase controls implemented already