infosecurity® ISACA®
NORTH AMERICA EXPO AND CONFERENCE
20-21 NOVEMBER 2019

Andrej Volchkov

Security key performance indicators or "How to measure security from the governance perspective"

#INFOSECNA

Volchkov
consulting

Volchkov
consulting

Objectives of the session

Having reliable metrics or KPI in the field of security is a *sine qua non* to assess risks and achieve a reliable security program.

This session aims to provide elements allowing CISOs to develop pragmatic metrics to facilitate security program management.

The objectives are:

- Have a broader view on how to build useful and pragmatic security metrics or KPI for governance / management purpose.
- Envision a catalog of metrics that can be adapted to your particular organization.

Why is it important to measure security?

- Answer questions such as: "How our investments contribute to better security?",
- Assess the effectiveness of security controls to be able to adjust program and decide on investments,
- Bring hard facts for Management / Board to achieve their role of accountable for security,
- Measure probability and impact in Risk management process,
- Achieve compliance,
- Estimate a return on security investments (ROSI),
- Steering efforts towards defined strategy,
- …

Why is it difficult to measure security?

- Information security has no dimensions of its own.
- The adequacy of security is relative.
- There is no universally accepted standards to measure the adequacy of the security controls.
- Incident, protection, value, asset, cost, loss, etc. means different thing to different people.
- High-level metrics require additional efforts to collate technical data.
- Organizations do not share information on security events, breaches or costs.
- There is absence of events to measure (known / unknown incidents in our or other companies).

Short exercise:

Think of examples of security metrics you are currently using for Governance / Management.

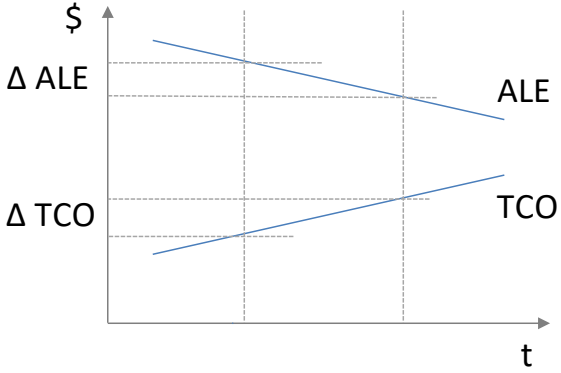
- How did you decide what / how to measure?
- What was the real need behind?

Attempt to categorize IS metrics for Governance and Management

1. Financial metrics
2. Modeling
3. Maturity assessment
4. Assumption-based metrics
5. Measurement of progress toward objective
6. Operational metrics
7. Security Cost Analysis
8. Benchmarking

1. Financial metrics

- Annualized Loss Expectancy (ALE) = potential annual losses as the result of risk impacts,
- Total Cost of Ownership (TCO) = all costs related to security in an organization,
- Economic Value Added (EVA) or ROSI = Δ ALE / Δ TCO (potential loss reduction with investments in security).
- Benefit (EVA) = Impact of inherent risk - Impact of residual risk.
- ROSI = Benefit - Cost of countermeasures.



1. Financial metrics (continues)

Example of pragmatic usage: evaluating ROSI of some specific security solution.

Financial metrics help assess investment opportunities in protection solutions. Security investments are considered justified if their cost is less then potential losses.

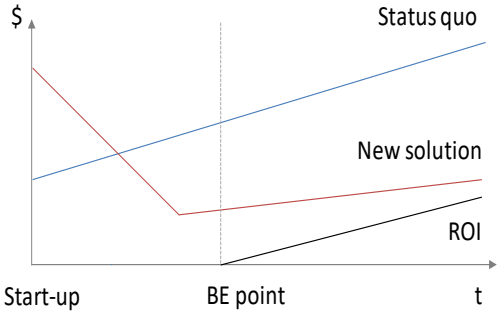
The main difficulties with these metrics are:

- The estimate of a loss must be associated with its probability of occurrence for all processes/assets and controls deployed, which can be very inaccurate.
- Requires statistics over several years.
- Impossible to collect at reasonable cost.

2. Modeling / Simulation

Example of pragmatic usage: for justifying (explaining) the investments in new projects

- Many disciplines use models to represent reality in order to simulate or observe the behavior of a system, make "what if" analyses or extrapolate the trends.
- To measure the effectiveness of investments (in security) one can use simple cost evolution models to visualize the ROSI.



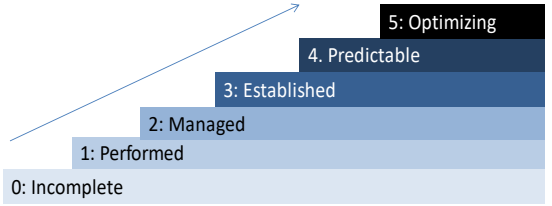
Example:

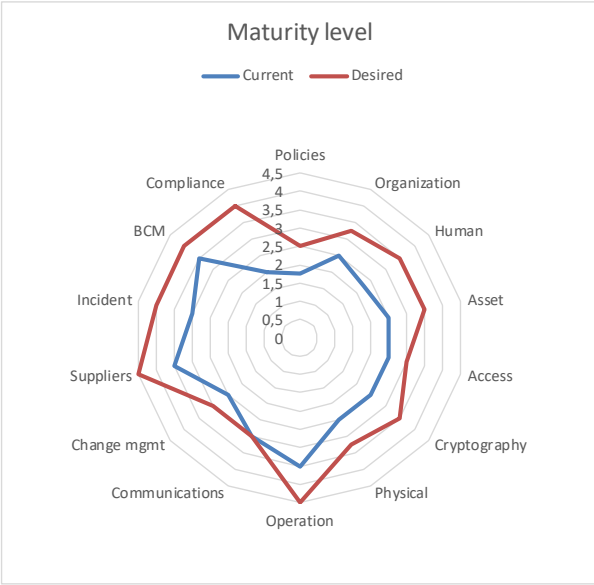
ROSI analysis for IS change projects such as building a SOC (Security Operations Center), new intrusion detection system, new means of authentication, new role-based access management system (RBAC), etc.

3. Maturity Assessment

Example of pragmatic usage: presenting the main IS capacity (protection) gaps

- Security program posture, capacity or maturity are synonyms for means that allow the state of security to be presented in a concise and standardized way.
- Use maturity models to evaluate processes according to a scale of values (based on ISO 27001/2, NIST, or some other).
- Each model presents the evaluation criteria for each evaluation point or process (based on some standards such as ISO 15504, CMMI).





4. Assumption-based metrics

Example of pragmatic usage: remove doubts about assumptions on security controls

Setting measurement objectives facilitates the choice of metrics.

- Make an initial assumption (with sub assumptions), then choose metrics which will help confirm or reject the assumptions.
- The more complex the measurement goals, the less metrics will be easy to build.

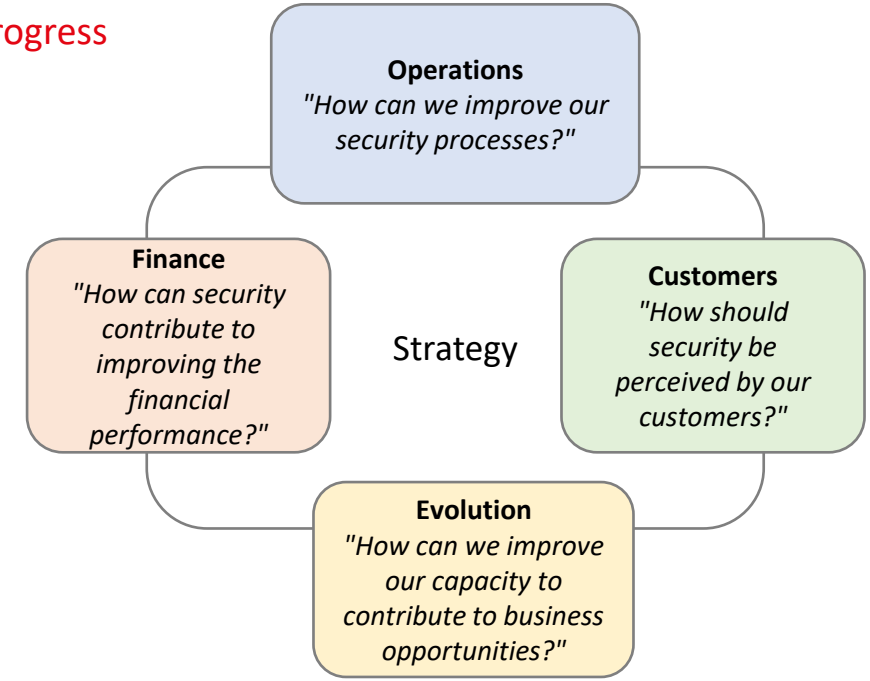
***Example** (excerpt) Measure the "time to recovery" capacity of a BCM (Business Continuity Management) program*

Assumption/Objective	Sub-assumption	Metrics
There is a clear SLA on the time to recovery for critical processes	All critical processes are formally identified.	N**o** of critical processes not formally identified.
	There is an SLA for time to recovery for all identified critical processes.	N**o** of SLAs for time to recovery.
	Recovery tests include all critical processes.	N**o** of critical processes tested during a period.

5. Measurement of progression toward objective

Example of pragmatic usage: annual review of progress

- The Balanced Scorecard (BSC) is a popular tool for tracking performance and progression toward goals that support the business strategy.
- As a well-known management tool, it provides a formal basis to establish and communicate results also in the domain of information security (IS).



6. Operational metrics

Example of pragmatic usage: annual review or management dashboard

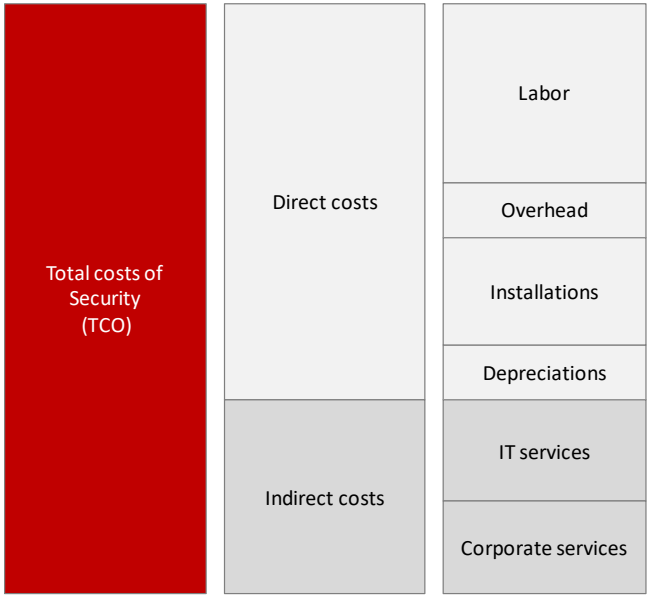
- Security operations can be assimilated into the *controls* set up within the framework of a security program.
- Operational performance can be measured and presented through figures, ratios and trends.

MEASUREMENT OBJECTIVE	METRIC	Trend
Awareness efficiency	Percentage of employees trained on high risks.	↘
Efficiency in resolving audit findings	Average delays in the processing of security audit findings.	↗
Configuration management	Number of patched systems/Number of systems to be patched.	↘
Incident handling	Mean time to resolve incidents.	↗
	Average effort for specific analyses and requests over a period of time/Number of employees.	↘

7. Security Costs

Example of pragmatic usage: annual reporting and program / strategy revision

- Use cost accounting principles already in place in the organization to analyze security costs
- Good indicator for governing bodies especially if it is related to other figures, such as the evolution of the company's overall expenses, the number of employees, the evolution of risks, factors generating cost, etc.



8. Benchmarking

Example of pragmatic usage: security organization / program adjustments

Benchmarking is appreciated by senior executives to compare results of different strategies.

- Studies or surveys.
- Results of surveys.
- Forums or associations.
- Business associations conduct studies of the practices of their members and share this information.
- Firms specialized in conducting benchmarking.

Short exercise:

What category (type) of metrics would you suggest for the following examples:

1.	Evaluate the effectiveness of a newly established SOC.	→ Operational metrics
2.	Decide to invest in a new IAM tool.	→ Modeling
3.	Figure out if your security organization is similar to others.	→ Benchmarking
4.	Demonstrate that the protection of personal data is accurate.	→ Assumption-based metrics
5.	Highlight gaps in your Cybersecurity posture.	→ Maturity assessment
6.	Calculate ROSI on a newly acquired intrusion detection system.	→ Financial metrics
7.	Present the structure of security costs.	→ Security Cost Analysis
8.	Evaluate the progress towards the new strategy.	→ Balanced Scorecard

TAKEAWAYS

www.volchkov.ch
avolchkov@volchkov.ch

1. *As a Security Officer, you are responsible to provide IS metrics for management / governance.*
2. *Limit the scope of measurement: simple metric is sometimes more useful (and less expensive) than the more elaborate one.*
3. *Don't try to use available (technical) metrics for management reporting. Don't bother your executives!*
4. *Building metrics is a hard work: start small and build while listening. Respond to "So What?" questions.*
5. *Put priority on metrics for risk analysis.*

Andrej Volchkov

www.volchkov.ch

avolchkov@volchkov.ch