Cyber Strategy Optimization for Risk Management

Michael Coden
Managing Director
Head of Cybersecurity Practice
coden.michael@bcgplatinion.com

Russell Schaefer
Manager
Cybersecurity Practice
schaefer.russell@bcgplatinion.com

NOVEMBER 2018
Wanted: A Systematic Method for Developing a Cyber Strategy

Selecting cyber security initiatives is a complex process

Current state:

- qualitative and subjective measures
- attempts to prioritize without metrics
- lack of consideration for synergies and redundancies among initiatives

Desired state:

- quantify maturity increases
- quantify risk reduction in dollars
- quantify synergies and redundancies
- Identify optimal portfolio of cyber security initiatives with an objective to
  - maximize cyber maturity (target state)
  - maximize decrease in $ cyber-risk
Novel approach yields big benefits

Enhancing & enabling dynamic tactical, strategic and operational decision making process requires sophisticated analytics capabilities

Cyber Doppler - Mechanics

To enhance decision making processes & strive to achieve optimal solutions, BCG Platinion developed Cyber Doppler, which combines ...

Traditional components of operational risk and portfolio theory

Operational Risk Analysis

Portfolio Theory

ROI on Implementing a Portfolio of Cyber Initiatives = $ Cyber Risk After Project Portfolio - $ Cyber Risk Before Project Portfolio

$ Cost of Implementing Cyber Project Portfolio
Cyber Doppler utilizes proven techniques from operational risk management to estimate expected loss.

1. Identify and visualize key business assets
   - Understand threat profile for assets w/ threat tree analysis of attack vectors
   - Review current cybersecurity maturity to understand controls in place and consequent vulnerabilities

2. Define event and human-based attack scenarios per asset
   - Estimate loss given event for each scenario

Cyber Doppler

\[ \text{Threat} \times \text{Vulnerability} \times \text{Severity (LGE)} = \text{Cyber Expected Loss} \]
Attack scenarios are customized to account for assets, attacks, and outcomes relevant to your organization.

1. Attacks follow the cyber kill chain to model the full steps of an attack from delivery to actions on objectives.
STACHT\textsuperscript{1} has its roots in the system-theoretic accident model and processes (STAMP\textsuperscript{1}) methodology

To understand why we have created STACHT, a review of the origin will provide some basic concepts to understand the foundation and implications to cybersecurity.

STAMP is constructed from three basic concepts:

- Instead of viewing accidents as the result of an initiating (root cause) event in a series of events leading to a loss, accidents are viewed as resulting from interaction among multiple components that violate the system safety constraints.

- Using the STAMP Model, accidents can be understood in terms of why the controls that were in place did not prevent or detect changes by identifying the safety constraints that were violated and determining why the controls in place were inadequate at enforcing them.

---

\textsuperscript{1} System Theoretic Analysis of Cyber Hazards and Threats
Source: A New Accident Model for Engineering Safer Systems, Nancy Leveson, MIT
STACHT provides a structured approach to help prevent cyber incidents before they occur

Precise Security Requirements - "Security by Design"

Layered Security Control Structure

Security process weaknesses
To find the points of vulnerability we use Cyber-STACHT models to focus on the controls that can lead to a hazardous state.
Recap: Framework

Vulnerability and threat determines the Frequency estimate. Industry / firm specific data determines the Severity estimate. Expected loss is estimated from combining these two.
Vulnerabilities are estimated from the current control environment

- **Comprehensive**
  Controls take into account people, process, and technology globally and across different locations

- **Framework flexibility**
  Ability to utilize industry standard frameworks (ISO, NIST CSF, etc.)

- **Attack analysis**
  Identify and analyze controls best suited to reduce chances of successful attacks
Control mapping to attack vector uses a control framework such as NIST CSF, ISO/IEC-27001, or other, tying back to maturity and compliance.

### Process
1. Conduct mapping of FSR NIST CSF controls against attack vector
2. Socialise and iterate on mapping

<table>
<thead>
<tr>
<th>Attack Vector</th>
<th>Mapped Functions</th>
<th>Mapped Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware wipe data</td>
<td>Governance</td>
<td>Policy</td>
</tr>
<tr>
<td></td>
<td>Identify</td>
<td>Technology</td>
</tr>
<tr>
<td></td>
<td>Protect</td>
<td>Asset management</td>
</tr>
<tr>
<td></td>
<td>Detect</td>
<td>Risk assessment</td>
</tr>
<tr>
<td></td>
<td>Respond</td>
<td>ID mgmt. and Access Control</td>
</tr>
<tr>
<td></td>
<td>Recover</td>
<td>Awareness and training</td>
</tr>
<tr>
<td></td>
<td>Supply chain/dependency management</td>
<td>Data security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Info. protection Proc. and Proc.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Anomalies and events</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security Cont. monitoring</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Not Applicable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Not Applicable</td>
</tr>
</tbody>
</table>

- **PR.IP-1**: A baseline configuration of information technology/industrial control systems is created and maintained incorporating appropriate security principles (e.g., concept of least functionality).
- **PR.IP-4**: Backups of information are conducted, maintained, and tested periodically.
Recap: Framework

Vulnerability and threat determine the Frequency estimate.

Industry / firm specific data determines the Severity estimate.

Expected loss is estimated from combining these two.
Data is used to determine the impact of a cyber event for crown jewels
We then focus on the controls that will either disrupt the attack chain, or reduce the undesirable outcome.
Risks are inevitable; to minimize risk, we optimize reduction of vulnerability and reduction of impact.

```
<table>
<thead>
<tr>
<th>Projects / portfolios</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency (PE)</td>
</tr>
<tr>
<td>-</td>
</tr>
<tr>
<td>Severity (LGE)</td>
</tr>
<tr>
<td>-</td>
</tr>
<tr>
<td>Cyber Expected Loss</td>
</tr>
</tbody>
</table>

Threat (%) \times Vulnerability (%) = Consequences / Impact ($)

Assets \times Loss given event

Pre-project portfolio  Post-project portfolio
```

Rank projects and portfolios based on their reduction of expected loss.

Select project portfolios optimized for budget and return on investment.

Identify and prioritize areas of investment.
This approach can determine the maximum risk reduction for a given budget, or the minimum budget to achieve a desired residual risk level.

- **Project analysis**
- **Portfolio selection**
  - Optimization algorithm selects project portfolio within proposed budget
  - Calculate portfolio expected loss reduction
- **Optimized portfolio**
  - Iteratively re-select, re-run, and compare new portfolios
  - Optimization achieved when a selected portfolio of projects has not been beaten in a set amount of time
Appendix: Example with ISO Framework
Cyber Doppler Plattform

Key set of inputs...

1. Current State Maturity Assessment (ISO Maturity Framework)

2. Projects / Initiatives Assessment (ISO Maturity Framework)

3. Loss factor identification (BCG Approach)

...run through Cyber Doppler...

...to determine optimal project portfolios

- Optimizes cyber risk mitigating projects / initiatives
- Minimizes project portfolio costs
- Quantifies project portfolio benefits using ISO maturity framework values and expected loss reduction
- Measures return of cyber security project investments
Step 1: Cyber Security Maturity Assessment (ISO)

- Review or perform cyber security current state assessment and potential future states.
Step 2: Project Universe Analysis

- Analyze existing and potential cyber initiatives to understand the different possibilities and the score impact of the individual projects across ISO domains.
- Evaluate the budget constraints, duration, and types of cyber initiatives.

ISO Domain Possibilities

<table>
<thead>
<tr>
<th>ISO Domain</th>
<th>Current</th>
<th>Maint</th>
<th>Enhanc</th>
<th>Low Term</th>
<th>ISOL</th>
<th>Non Possible</th>
<th>On</th>
<th>Project Costs ($1000s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current</td>
<td>1.35</td>
<td>1.41</td>
<td>1.56</td>
<td>1.67</td>
<td>1.75</td>
<td>1.81</td>
<td>1.8</td>
<td>4.32</td>
</tr>
<tr>
<td>Maint</td>
<td>1.10</td>
<td>1.45</td>
<td>1.86</td>
<td>2.09</td>
<td>2.39</td>
<td>2.51</td>
<td>2.6</td>
<td>7.15</td>
</tr>
<tr>
<td>Enhanc</td>
<td>0.68</td>
<td>0.74</td>
<td>0.79</td>
<td>0.83</td>
<td>0.86</td>
<td>0.88</td>
<td>0.9</td>
<td>2.23</td>
</tr>
<tr>
<td>Low Term</td>
<td>0.35</td>
<td>0.39</td>
<td>0.39</td>
<td>0.39</td>
<td>0.39</td>
<td>0.39</td>
<td>0.4</td>
<td>0.72</td>
</tr>
<tr>
<td>Enhanc</td>
<td>0.05</td>
<td>0.06</td>
<td>0.06</td>
<td>0.06</td>
<td>0.06</td>
<td>0.06</td>
<td>0.1</td>
<td>0.17</td>
</tr>
<tr>
<td>Low Term</td>
<td>0.05</td>
<td>0.06</td>
<td>0.06</td>
<td>0.06</td>
<td>0.06</td>
<td>0.06</td>
<td>0.1</td>
<td>0.17</td>
</tr>
<tr>
<td>Enhanc</td>
<td>0.05</td>
<td>0.06</td>
<td>0.06</td>
<td>0.06</td>
<td>0.06</td>
<td>0.06</td>
<td>0.1</td>
<td>0.17</td>
</tr>
</tbody>
</table>
Step 3: Portfolio Creation and Optimization

- Select list of cyber initiatives to create all possible portfolios
- Optimize portfolio based on the budget, and ISO targets
- Incorporate cost synergies, and score redundancies
- Prioritize portfolios by maturity score, and duration

```
Project Portfolio Manager

Selected Cyber Initiatives:
- Cyber Culture Improvement
- ABM Cyber Lead Appointment
- Preliminary Protection of "Crown Jewels"
- Organization Cross Functional Integration with ISRM

Enhanced Environments:
- Access Control
- BCM & DR
- Vulnerability
- Policy Management
- Cyber Risk Management

Portfolio Universe:

- Projects Considered:
  - Cyber Culture Improvement
  - ABM Cyber Lead Appointment
  - Preliminary Protection of "Crown Jewels"
  - Organization Cross Functional Integration with ISRM

Portfolio Dynamics:
- Redundancies
- Synergies

Minimum Budget ($) | Maximum Budget ($)
---------------------|---------------------
60,500               | 5,000,000

Top Portfolios by Modified Avg. Score
```

Copyright © 2018 by The Boston Consulting Group, Inc. All rights reserved.
Results: Most optimized and favorable portfolio selection, and estimated loss reduction analysis

- Post execution of the optimization exercise, the firm selects the most optimal and favorable portfolio
- The portfolio can be deconstructed to show incremental benefits of each project
- Estimated ISO Maturity Score benefits and expected loss reduction for the chosen portfolio is calculated
Results: (cont'd)

- Estimated expected loss distribution for the chosen portfolio is calculated and compared with the estimated loss in the current state.

Results: Current and post portfolio estimated loss distribution analyzed (Monte Carlo methodology)

Monte Carlo Estimated Loss Projection (ID: 3350)

<table>
<thead>
<tr>
<th>Min Loss Distribution</th>
<th>Max Loss Distribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static Expected Loss</td>
<td>$1,611,245</td>
</tr>
<tr>
<td>MC Expected Loss</td>
<td>$1,657,992</td>
</tr>
<tr>
<td>MC Unexpected Loss</td>
<td>$2,088,162,011</td>
</tr>
<tr>
<td>VaR</td>
<td>$3,398,020,003</td>
</tr>
<tr>
<td>$0</td>
<td>$554,943,201</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Min Loss Distribution</th>
<th>Max Loss Distribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static Expected Loss</td>
<td>$3,357,953</td>
</tr>
<tr>
<td>MC Expected Loss</td>
<td>$3,562,589</td>
</tr>
<tr>
<td>MC Unexpected Loss</td>
<td>$2,454,576,640</td>
</tr>
<tr>
<td>VaR</td>
<td>$2,792,020,229</td>
</tr>
</tbody>
</table>

Copyright © 2018 by The Boston Consulting Group, Inc. All rights reserved.
Results: (cont'd)

- Estimated expected loss distribution for the chosen portfolio is calculated and compared with the estimated loss in the current state.

Monte Carlo Estimated Loss Projection (ID: 3350)

<table>
<thead>
<tr>
<th>Min Loss Distribution</th>
<th>$0</th>
<th>Max Loss Distribution</th>
<th>$554,943,201</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static Expected Loss</td>
<td>$1,611,245</td>
<td>MC Expected Loss</td>
<td>$1,657,992</td>
</tr>
<tr>
<td>MC Expected Loss</td>
<td>$288,162,011</td>
<td>Confidence Interval</td>
<td>99</td>
</tr>
<tr>
<td>MC Unexpected Loss</td>
<td>$339,820,003</td>
<td>VaR</td>
<td>$333,562,589</td>
</tr>
<tr>
<td></td>
<td>$245,457,640</td>
<td>VaR</td>
<td>$279,020,279</td>
</tr>
</tbody>
</table>

Portfolio x

Portfolio y
The services and materials provided by The Boston Consulting Group (BCG) are subject to BCG’s Standard Terms (a copy of which is available upon request) or such other agreement as may have been previously executed by BCG. BCG does not provide legal, accounting, or tax advice. The Client is responsible for obtaining independent advice concerning these matters. This advice may affect the guidance given by BCG. Further, BCG has made no undertaking to update these materials after the date hereof, notwithstanding that such information may become outdated or inaccurate.

The materials contained in this presentation are designed for the sole use by the board of directors or senior management of the Client and solely for the limited purposes described in the presentation. The materials shall not be copied or given to any person or entity other than the Client (“Third Party”) without the prior written consent of BCG. These materials serve only as the focus for discussion; they are incomplete without the accompanying oral commentary and may not be relied on as a stand-alone document. Further, Third Parties may not, and it is unreasonable for any Third Party to, rely on these materials for any purpose whatsoever. To the fullest extent permitted by law (and except to the extent otherwise agreed in a signed writing by BCG), BCG shall have no liability whatsoever to any Third Party, and any Third Party hereby waives any rights and claims it may have at any time against BCG with regard to the services, this presentation, or other materials, including the accuracy or completeness thereof. Receipt and review of this document shall be deemed agreement with and consideration for the foregoing.

BCG does not provide fairness opinions or valuations of market transactions, and these materials should not be relied on or construed as such. Further, the financial evaluations, projected market and financial information, and conclusions contained in these materials are based upon standard valuation methodologies, are not definitive forecasts, and are not guaranteed by BCG. BCG has used public and/or confidential data and assumptions provided to BCG by the Client. BCG has not independently verified the data and assumptions used in these analyses. Changes in the underlying data or operating assumptions will clearly impact the analyses and conclusions.

Michael Coden  
Managing Director  
Head of Cybersecurity Practice  
coden.michael@bcgplatinion.com

Russell Schaefer  
Manager  
Cybersecurity Practice  
schaefer.russell@bcgplatinion.com