Cyber Strategy Optimization for Risk Management

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

Ru
Ma
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

"What is the ROI on the money you want to spend on that cyber project?"

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

NIST

MIT MANAGEMENT SLOAN SCHOOL — INTERDISCIPLINARY CONSORTIUM for IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY — (IC)³

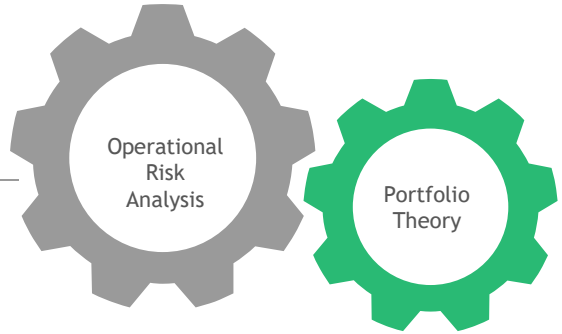
Novel approach yields big benefits

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 ...

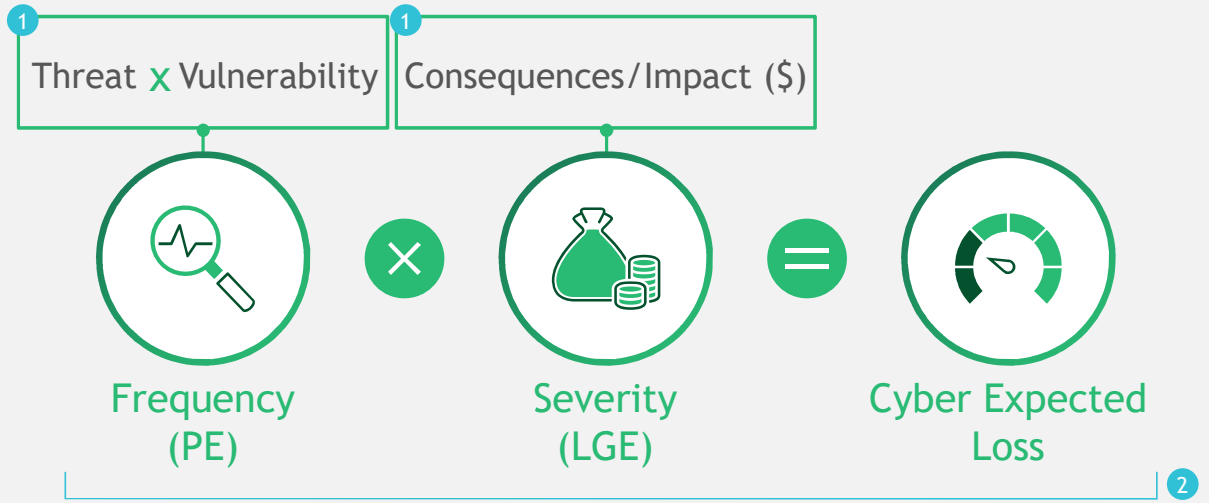
Traditional components of operational risk and portfolio theory



ROI on Implementing a Portfolio of Cyber Initiatives = $\frac{\$ \text{ Cyber Risk After Project Portfolio} - \$ \text{ Cyber Risk Before Project Portfolio}}{\$ \text{ Cost of Implementing Cyber Project Portfolio}}$

Cyber Doppler utilizes proven techniques from operational risk management to estimate expected loss

CYBER DOPPLER



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

STACHT 1

Attack scenarios are customized to account for assets, attacks, and outcomes relevant to your organization

Assets

What are you trying to protect?

Attacks[1]

How are attackers getting to the asset?

Outcomes

What happens to the asset?

Scenarios

List of applicable scenarios

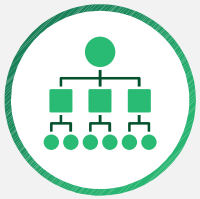
1. Attacks follow the cyber kill chain to model the full steps of an attack from delivery to actions on objectives

STACHT[1] has its roots in the system-theoretic accident model and processes (STAMP[1]) methodology

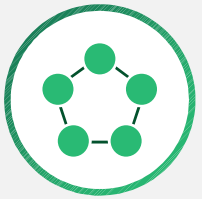
To understand why we have created STACHT, a review of the origin will provide some basic concepts to understand the foundation and implications to cybersecurity.

STAMP is constructed from three basic concepts:

Constraints



Hierarchical Control Structures



Process Models

- 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.

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"

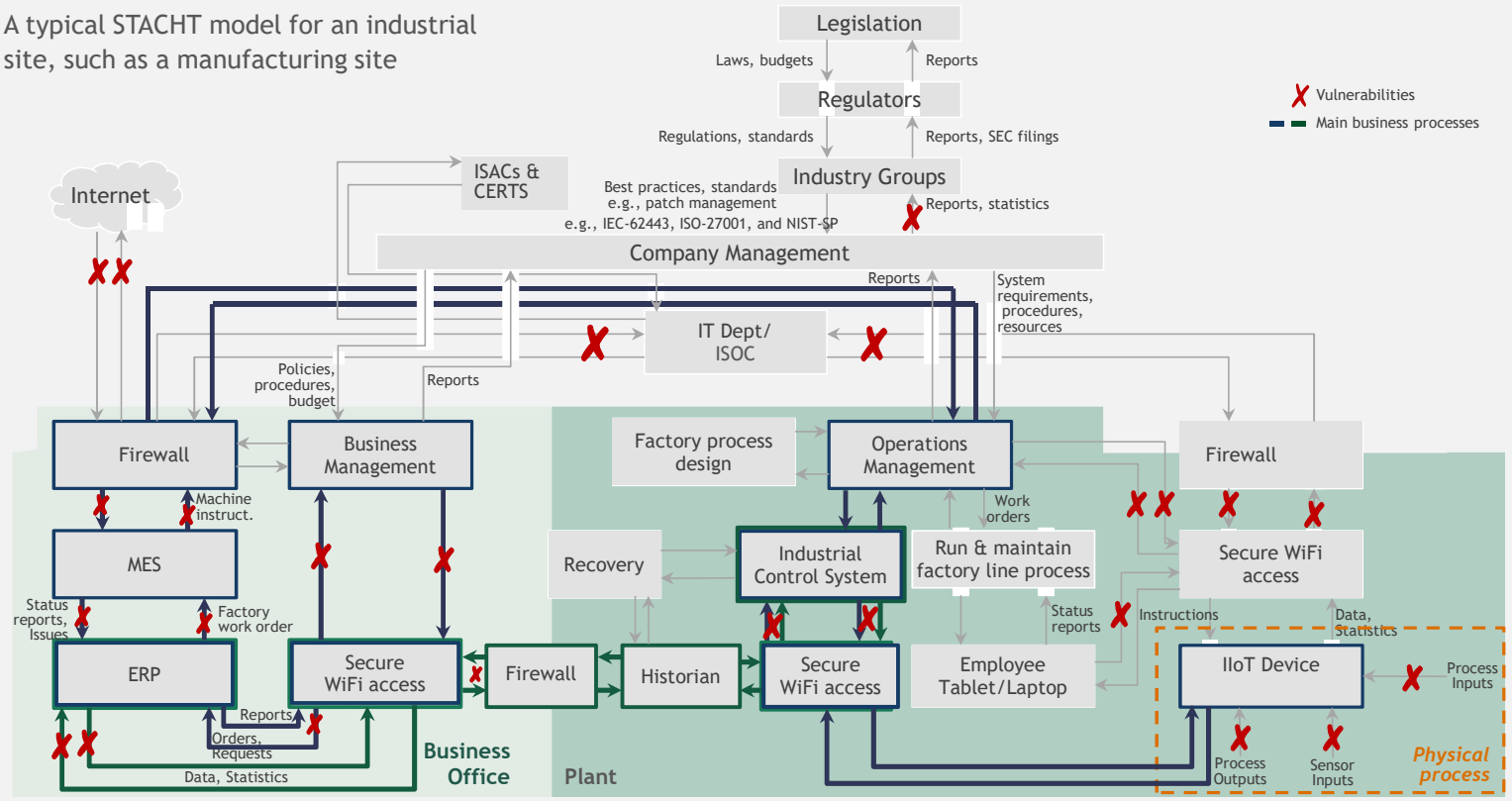
Layered Security Control Structure

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

STACHT

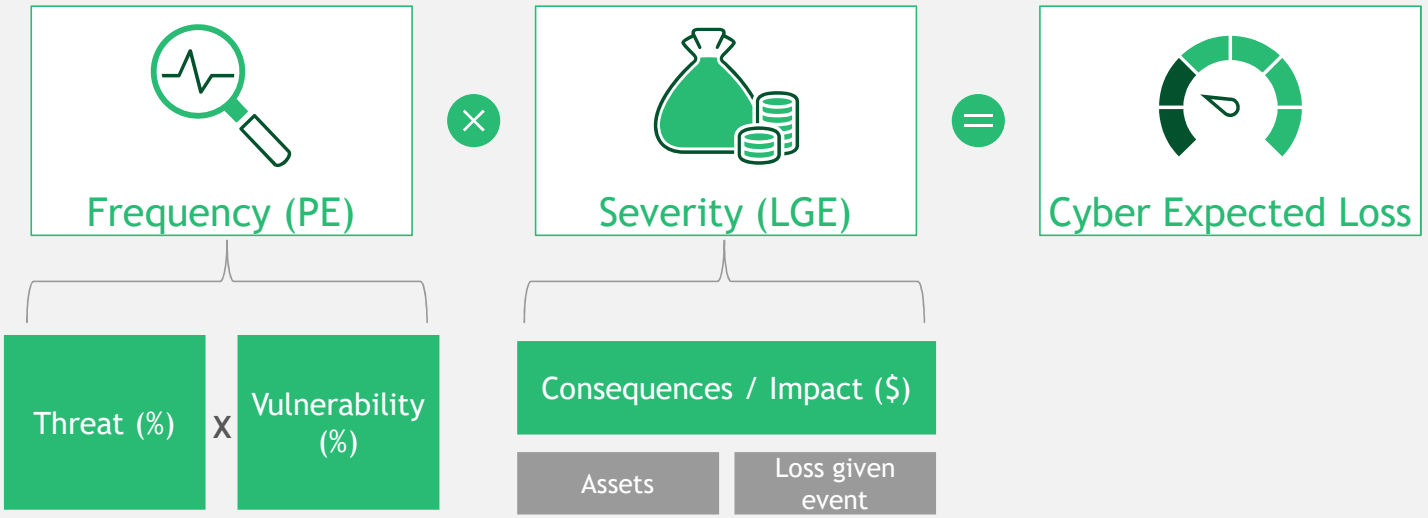
A typical STACHT model for an industrial site, such as a manufacturing site



1. ISOC—Information Security Operations Center, 2. ERP—Enterprise resource planning, 3. MES—Manufacturing execution system, 4. ISAC—Information Sharing and Analysis Center, 5. CERT—Computer Emergency Readiness Team
Source: BCG Analysis

Recap: Framework

Recap



Vulnerability and threat determines the Frequency estimate

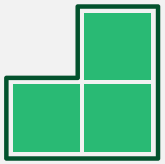
Industry / firm specific data determines the Severity estimate

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

Attack Vector

Malware wipe data

Process

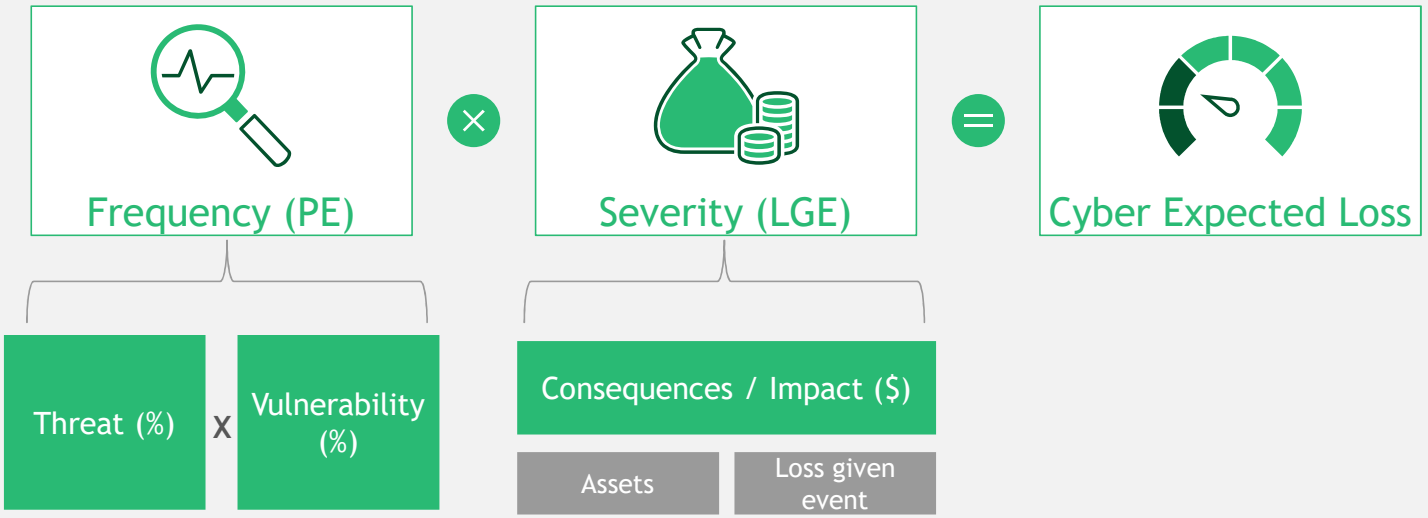
1. Conduct mapping of FSR NIST CSF controls against attack vector
2. Socialise and iterate on mapping

Mapped Functions	Mapped Categories	
Governance	Policy Technology	
Identify	Asset management Risk assessment	
Protect	ID mgmt. and Access Control Awareness and training Data security Info. protection Proc. and Proc.	Maintenance Protective technology
Detect	Anomalies and events Security Cont. monitoring	
Respond	Response planning Communications Analysis Mitigation	
Recover	Not Applicable	
Supply chain/ dependency management	Not Applicable	

- 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

Recap



Vulnerability and threat determines 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

Questionnaire tailoring & development

Stakeholder identification

Guided interviews / workshops

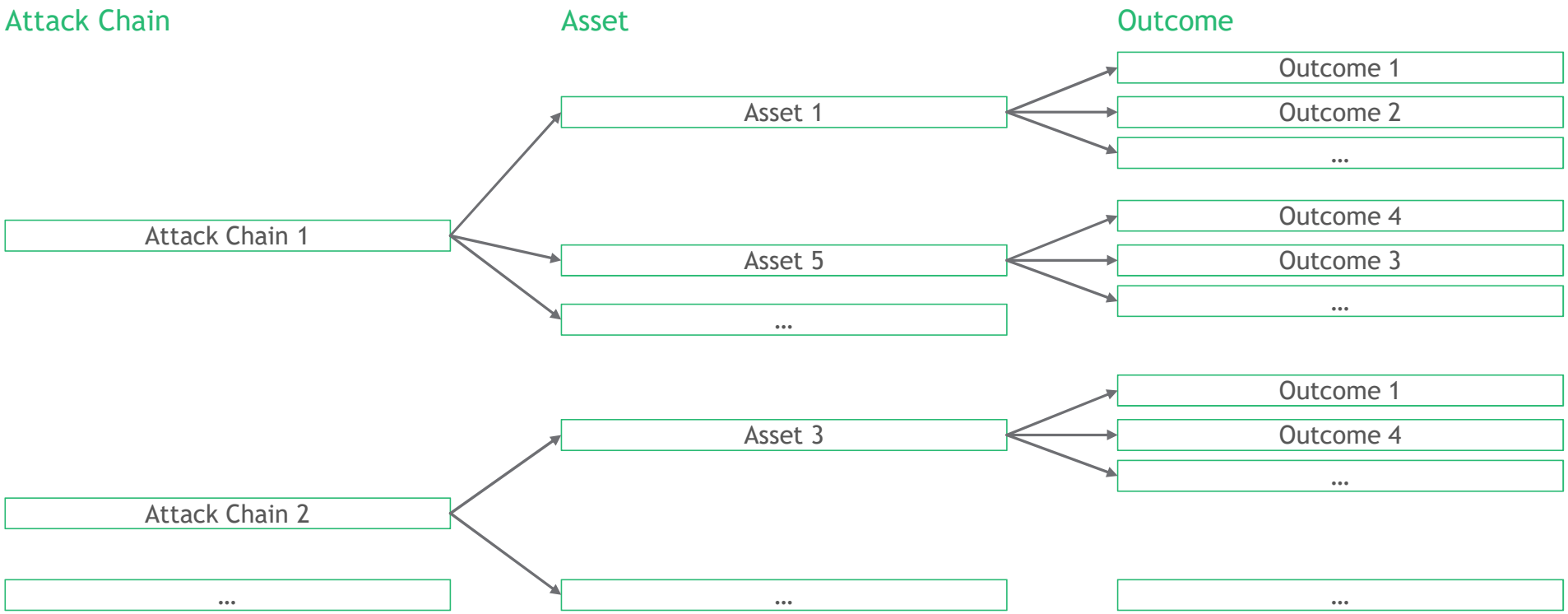
Data gathering

Calibration & refinement

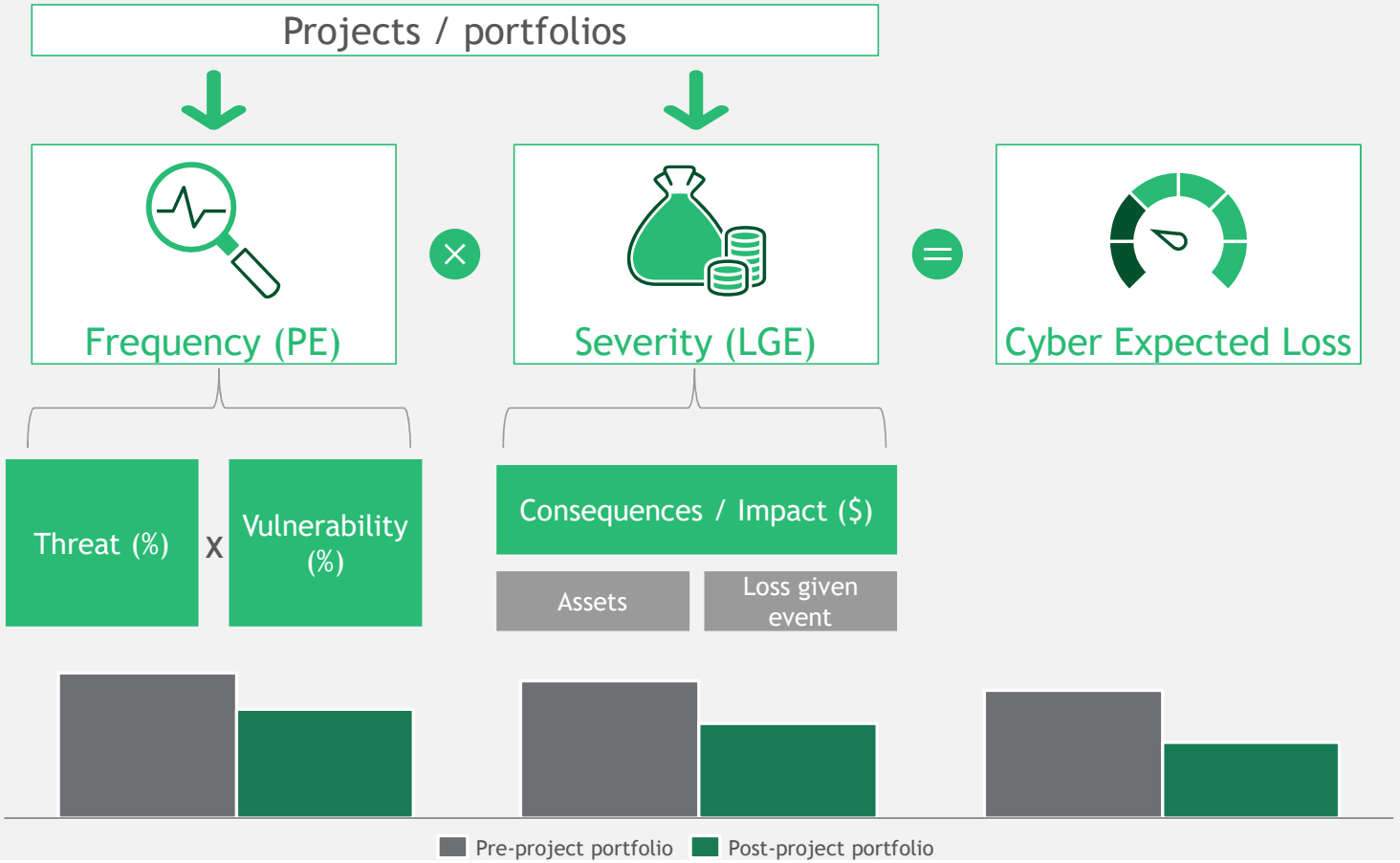
Cyber Doppler

We then focus on the controls that will either disrupt the attack chain, or reduce the undesirable outcome

Illustrative



Risks are inevitable; to minimize risk, we optimize reduction of vulnerability and reduction of impact



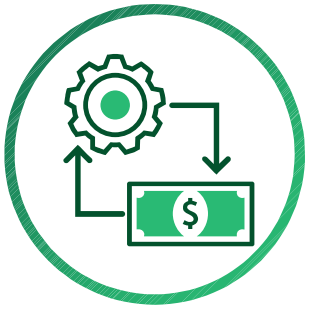
Rank projects and portfolios based on their reduction of expected loss

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...

BCG PLATINION | 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)

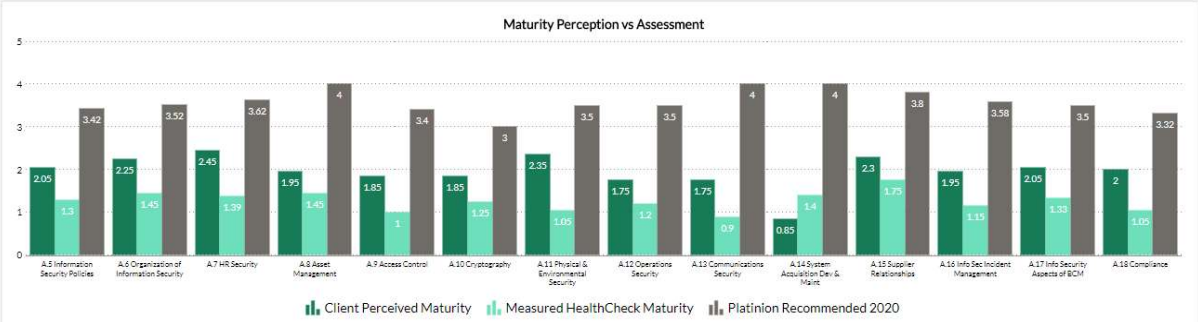
- Review or perform cyber security current state assessment and potential future states

Step 1: Cyber Security Maturity Assessment (ISO)

BCG PLATINION | CYBER DOPPLER

Ray

Cyber Maturity Chart

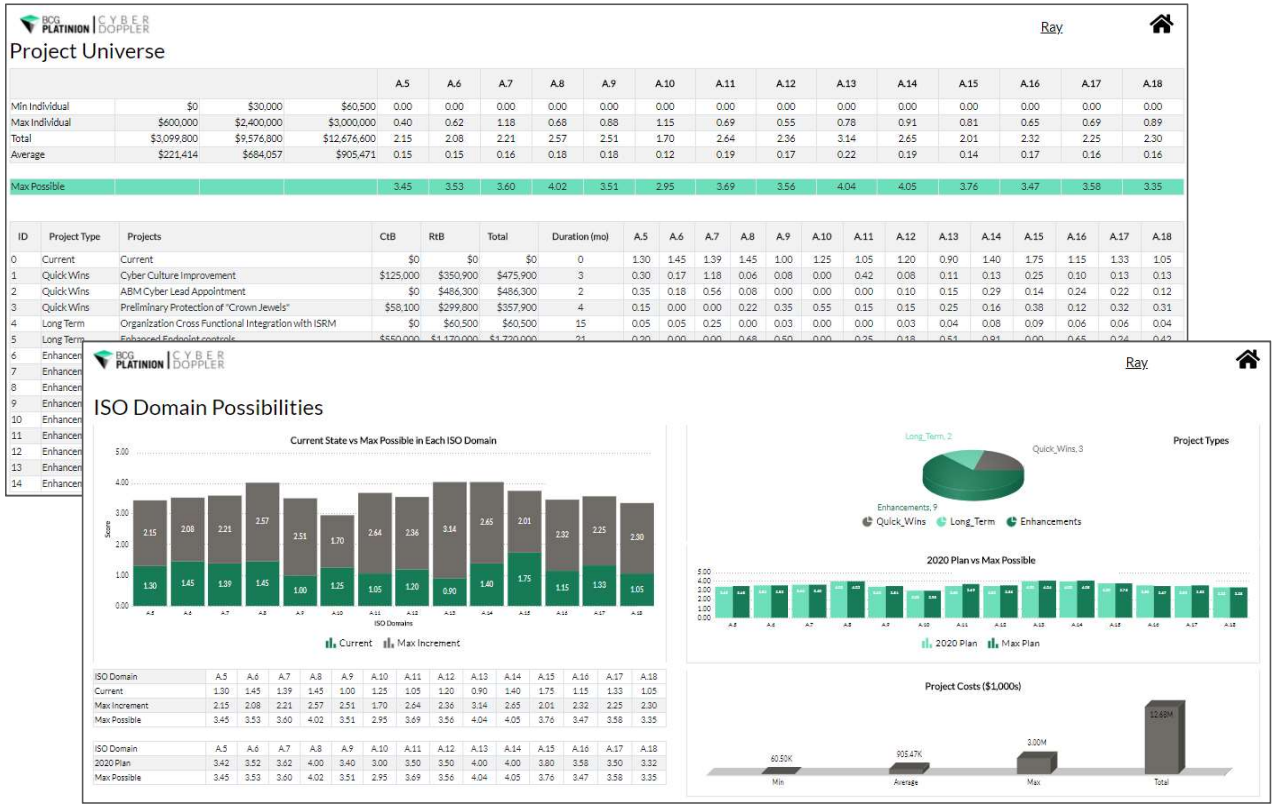


ISO Function	ISO Domains	Client Perceived Maturity	Measured HealthCheck Maturity	Platinion Recommended 2020
A.5	A.5 Information Security Policies	2.05	1.30	3.42
A.6	A.6 Organization of Information Security	2.25	1.45	3.52
A.7	A.7 HR Security	2.45	1.39	3.62
A.8	A.8 Asset Management	1.95	1.45	4.00
A.9	A.9 Access Control	1.85	1.00	3.40
A.10	A.10 Cryptography	1.85	1.25	3.00
A.11	A.11 Physical & Environmental Security	2.35	1.05	3.50
A.12	A.12 Operations Security	1.75	1.20	3.50
A.13	A.13 Communications Security	1.75	0.90	4.00
A.14	A.14 System Acquisition Dev & Maint	0.85	1.40	4.00
A.15	A.15 Supplier Relationships	2.30	1.75	3.80
A.16	A.16 Info Sec Incident Management	1.95	1.15	3.58
A.17	A.17 Info Security Aspects of BCM	2.05	1.33	3.50
A.18	A.18 Compliance	2.00	1.05	3.32

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 bu constraints, dur types of cyber i

Step 2: Project Universe Analysis



BCG PLATINION | CYBER DOPPLER

Ray

Project Universe

				A.5	A.6	A.7	A.8	A.9	A.10	A.11	A.12	A.13	A.14	A.15	A.16	A.17	A.18
Min Individual	$0	$30,000	$60,500	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Max Individual	$600,000	$2,400,000	$3,000,000	0.40	0.62	1.18	0.68	0.88	1.15	0.69	0.55	0.78	0.91	0.81	0.65	0.69	0.89
Total	$3,099,800	$9,576,800	$12,676,600	2.15	2.08	2.21	2.57	2.51	1.70	2.64	2.36	3.14	2.65	2.01	2.32	2.25	2.30
Average	$221,414	$684,057	$905,471	0.15	0.15	0.16	0.18	0.18	0.12	0.19	0.17	0.22	0.19	0.14	0.17	0.16	0.16
Max Possible				3.45	3.53	3.60	4.02	3.51	2.95	3.69	3.56	4.04	4.05	3.76	3.47	3.58	3.35

ID	Project Type	Projects	CtB	RtB	Total	Duration (mo)	A.5	A.6	A.7	A.8	A.9	A.10	A.11	A.12	A.13	A.14	A.15	A.16	A.17	A.18
0	Current	Current	$0	$0	$0	0	1.30	1.45	1.39	1.45	1.00	1.25	1.05	1.20	0.90	1.40	1.75	1.15	1.33	1.05
1	Quick Wins	Cyber Culture Improvement	$125,000	$350,900	$475,900	3	0.30	0.17	1.18	0.06	0.08	0.00	0.42	0.08	0.11	0.13	0.25	0.10	0.13	0.13
2	Quick Wins	ABM Cyber Lead Appointment	$0	$486,300	$486,300	2	0.35	0.18	0.56	0.08	0.00	0.00	0.00	0.10	0.15	0.29	0.14	0.24	0.22	0.12
3	Quick Wins	Preliminary Protection of "Crown Jewels"	$58,100	$299,800	$357,900	4	0.15	0.00	0.00	0.22	0.35	0.55	0.15	0.15	0.25	0.16	0.38	0.12	0.32	0.31
4	Long Term	Organization Cross Functional Integration with ISRM	$0	$60,500	$60,500	15	0.05	0.05	0.25	0.00	0.03	0.00	0.00	0.03	0.04	0.08	0.09	0.06	0.06	0.04
5	Long Term	Enhanced Endpoint controls	$550,000	$1,170,000	$1,720,000	21	0.20	0.00	0.00	0.68	0.50	0.00	0.25	0.18	0.51	0.81	0.00	0.65	0.24	0.42
6	Enhancem																			
7	Enhancem																			
8	Enhancem																			
9	Enhancem																			
10	Enhancem																			
11	Enhancem																			
12	Enhancem																			
13	Enhancem																			
14	Enhancem																			

BCG PLATINION | CYBER DOPPLER

Ray

ISO Domain Possibilities

Current State vs Max Possible in Each ISO Domain

Project Types

2020 Plan vs Max Possible

ISO Domain	A.5	A.6	A.7	A.8	A.9	A.10	A.11	A.12	A.13	A.14	A.15	A.16	A.17	A.18
Current	1.30	1.45	1.39	1.45	1.00	1.25	1.05	1.20	0.90	1.40	1.75	1.15	1.33	1.05
Max Increment	2.15	2.08	2.21	2.57	2.51	1.70	2.64	2.36	3.14	2.65	2.01	2.32	2.25	2.30
Max Possible	3.45	3.53	3.60	4.02	3.51	2.95	3.69	3.56	4.04	4.05	3.76	3.47	3.58	3.35

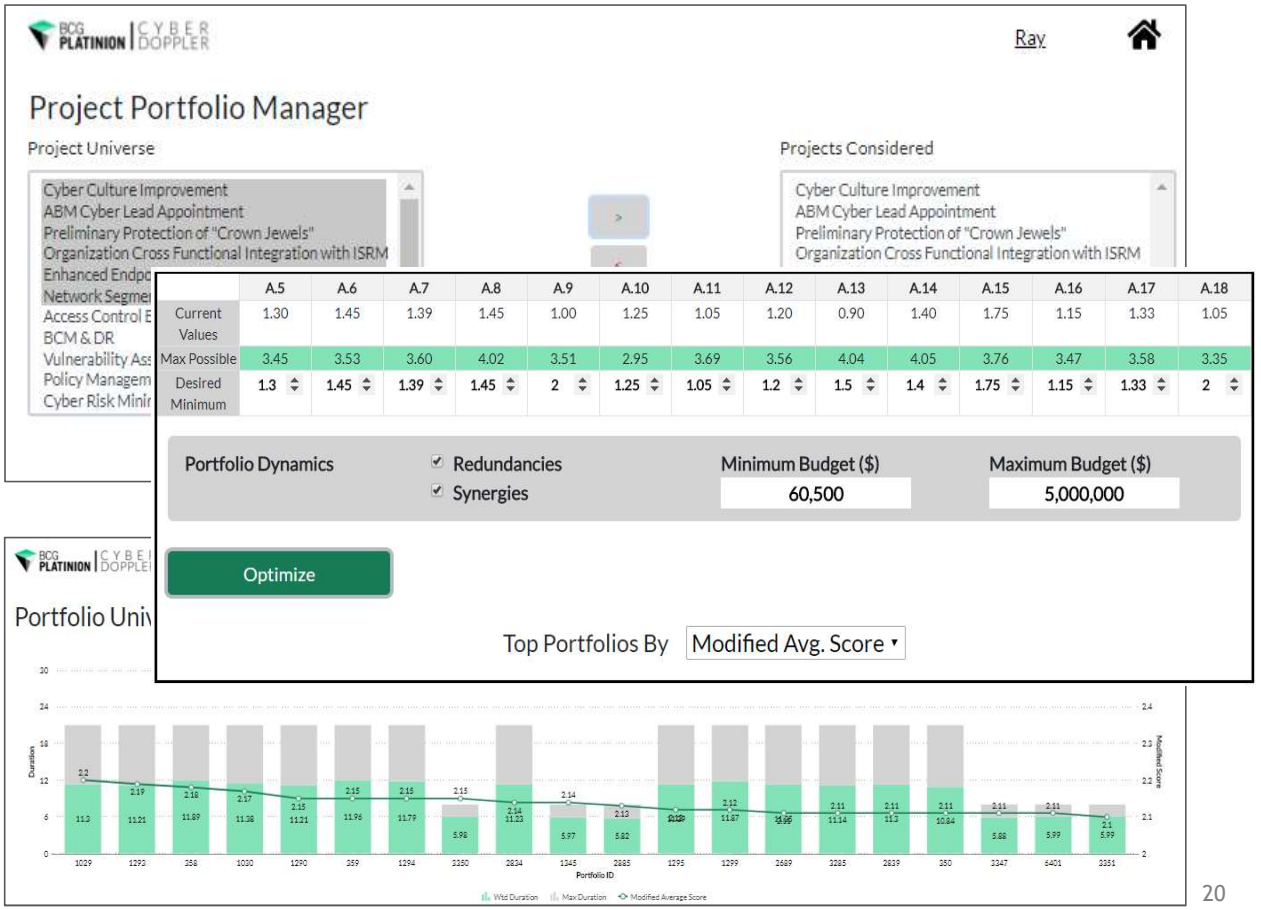
ISO Domain	A.5	A.6	A.7	A.8	A.9	A.10	A.11	A.12	A.13	A.14	A.15	A.16	A.17	A.18
2020 Plan	3.42	3.52	3.62	4.00	3.40	3.00	3.50	3.50	4.00	4.00	3.80	3.58	3.50	3.32
Max Possible	3.45	3.53	3.60	4.02	3.51	2.95	3.69	3.56	4.04	4.05	3.76	3.47	3.58	3.35

Project Costs ($1,000s)

Step 3: Portfolio Creation and Optimization

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

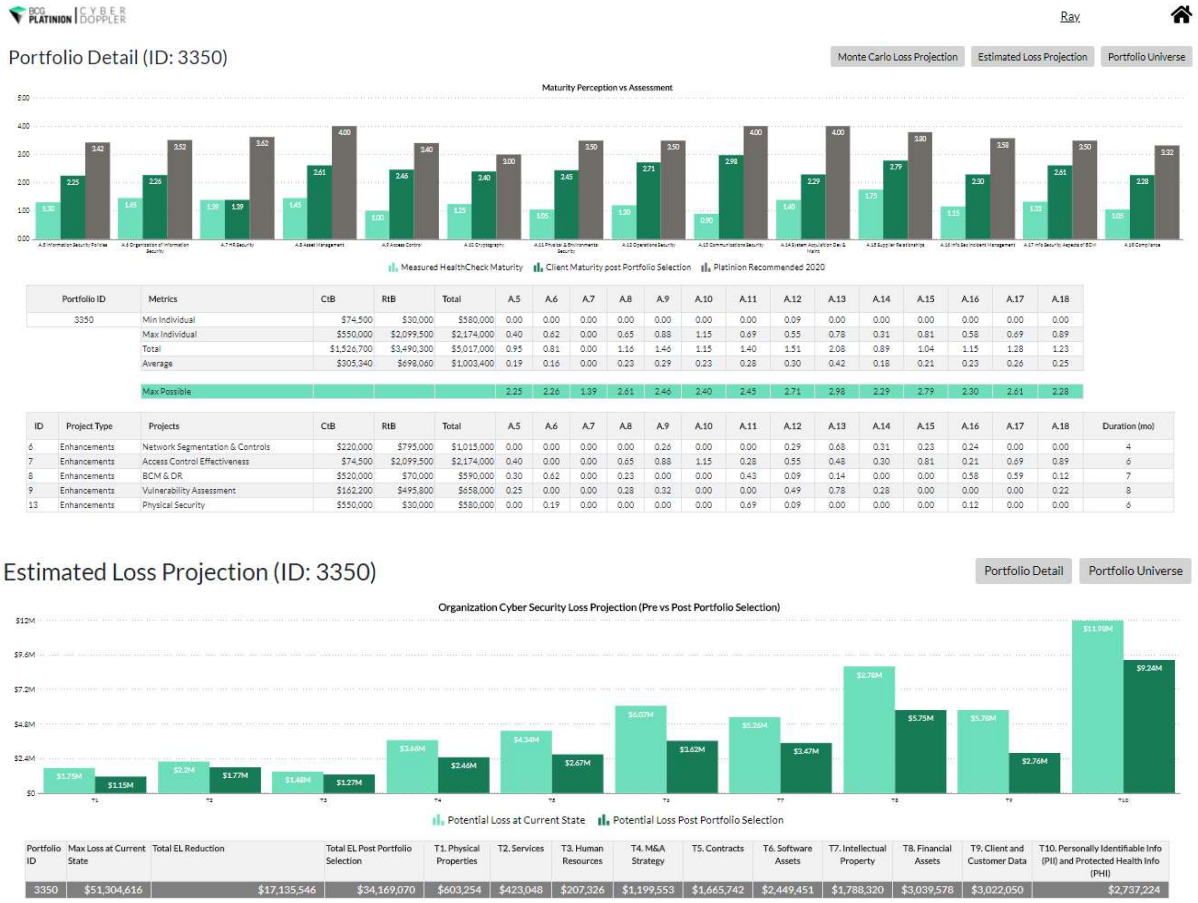
Step 3: Portfolio Creation and Optimization



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: Optimal portfolio of projects / initiatives is identified



PCG PLATINION | CYBER DOPPLER

Ray

Portfolio Detail (ID: 3350)

Monte Carlo Loss Projection | Estimated Loss Projection | Portfolio Universe

Maturity Perception vs Assessment

Measured HealthCheck Maturity | Client Maturity post Portfolio Selection | Platinion Recommended 2020

Portfolio ID	Metrics	CtB	RtB	Total	A.5	A.6	A.7	A.8	A.9	A.10	A.11	A.12	A.13	A.14	A.15	A.16	A.17	A.18
3350	Min Individual	$74,500	$30,000	$580,000	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.09	0.00	0.00	0.00	0.00	0.00	0.00
	Max Individual	$550,000	$2,099,500	$2,174,000	0.40	0.62	0.00	0.65	0.88	1.15	0.69	0.55	0.78	0.31	0.81	0.58	0.69	0.89
	Total	$1,526,700	$3,490,300	$5,017,000	0.95	0.81	0.00	1.16	1.46	1.15	1.40	1.51	2.08	0.89	1.04	1.15	1.28	1.23
	Average	$305,340	$698,060	$1,003,400	0.19	0.16	0.00	0.23	0.29	0.23	0.28	0.30	0.42	0.18	0.21	0.23	0.26	0.25
	Max Possible				2.25	2.26	1.39	2.61	2.46	2.40	2.45	2.71	2.98	2.29	2.79	2.30	2.61	2.28

ID	Project Type	Projects	CtB	RtB	Total	A.5	A.6	A.7	A.8	A.9	A.10	A.11	A.12	A.13	A.14	A.15	A.16	A.17	A.18	Duration (mo)
6	Enhancements	Network Segmentation & Controls	$220,000	$795,000	$1,015,000	0.00	0.00	0.00	0.00	0.26	0.00	0.00	0.29	0.68	0.31	0.23	0.24	0.00	0.00	4
7	Enhancements	Access Control Effectiveness	$74,500	$2,099,500	$2,174,000	0.40	0.00	0.00	0.65	0.88	1.15	0.28	0.55	0.48	0.30	0.81	0.21	0.69	0.89	6
8	Enhancements	BCM & DR	$520,000	$70,000	$590,000	0.30	0.62	0.00	0.23	0.00	0.00	0.43	0.09	0.14	0.00	0.00	0.58	0.59	0.12	7
9	Enhancements	Vulnerability Assessment	$162,200	$495,800	$658,000	0.25	0.00	0.00	0.28	0.32	0.00	0.00	0.49	0.78	0.28	0.00	0.00	0.00	0.22	8
13	Enhancements	Physical Security	$550,000	$30,000	$580,000	0.00	0.19	0.00	0.00	0.00	0.00	0.69	0.09	0.00	0.00	0.00	0.12	0.00	0.00	6

Estimated Loss Projection (ID: 3350)

Portfolio Detail | Portfolio Universe

Organization Cyber Security Loss Projection (Pre vs Post Portfolio Selection)

Potential Loss at Current State | Potential Loss Post Portfolio Selection

Portfolio ID	Max Loss at Current State	Total EL Reduction	Total EL Post Portfolio Selection	T1. Physical Properties	T2. Services	T3. Human Resources	T4. M&A Strategy	T5. Contracts	T6. Software Assets	T7. Intellectual Property	T8. Financial Assets	T9. Client and Customer Data	T10. Personally Identifiable Info (PII) and Protected Health Info (PHI)
3350	$51,304,616	$17,135,546	$34,169,070	$603,254	$423,048	$207,326	$1,199,553	$1,665,742	$2,449,451	$1,788,320	$3,039,578	$3,022,050	$2,737,224

Results: (cont'd)

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

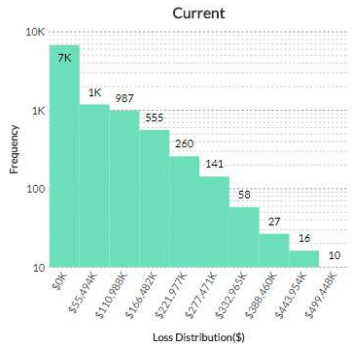
Results: Current and post portfolio estimated loss distribution analyzed (Monte Carlo methodology)

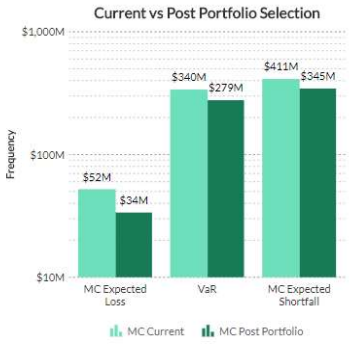
BCG PLATINION | CYBER DOPPLER

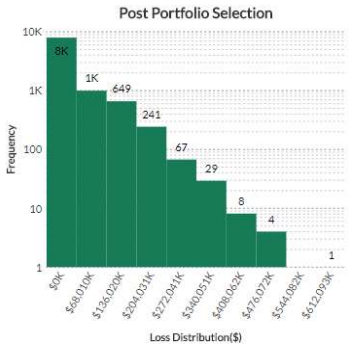
Ray

Monte Carlo Estimated Loss Projection (ID: 3350)

Portfolio Detail | Portfolio Universe







Min Loss Distribution	$0	Max Loss Distribution	$554,943,201
Static Expected Loss	$51,611,245		
MC Expected Loss	$51,657,992	Confidence Interval	99
MC Unexpected Loss	$288,162,011		
VaR	$339,820,003		

Min Loss Distribution	$0	Max Loss Distribution	$680,103,599
Static Expected Loss	$34,357,953		
MC Expected Loss	$33,562,589	Confidence Interval	99
MC Unexpected Loss	$245,457,640		
VaR	$279,020,229		

Results: (cont'd)

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

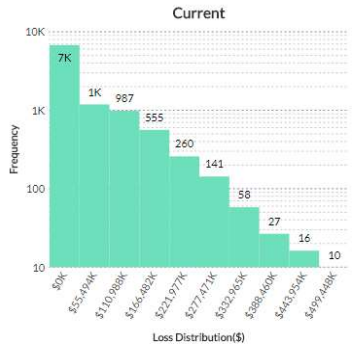
Results: Current and post portfolio estimated loss distribution analyzed (Monte Carlo methodology)

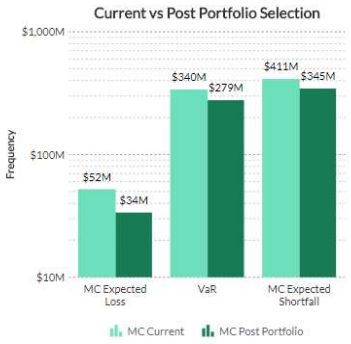
BCG PLATINION | CYBER DOPPLER

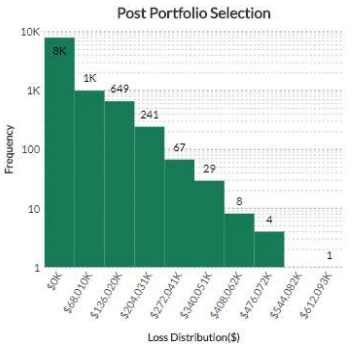
Ray

Monte Carlo Estimated Loss Projection (ID: 3350)

Portfolio Detail | Portfolio Universe







Min Loss Distribution	$0	Max Loss Distribution	$554,943,201
Static Expected Loss	$51,611,245		
MC Expected Loss	$51,657,992	Confidence Interval	99
MC Unexpected Loss	$288,162,011		
VaR	$339,820,003		

Min Loss Distribution	$0	Max Loss Distribution	$680,103,599
Static Expected Loss	$34,357,953		
MC Expected Loss	$33,562,589	Confidence Interval	99
MC Unexpected Loss	$245,457,640		
VaR	$279,020,229		

Portfolio x

Portfolio y

Disclaimer

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


BCG
PLATINION
platinion.com