



Measuring Security Success: Unveiling the KPIs of Protection

Mrs. Olga Ghincul
EY Financial services

ORGANIZED BY



CYBER SECURITY
COALITION.be



ISACA
Belgium Chapter



SUPPORTED BY



Solvay Lifelong Learning
BRUSSELS SCHOOL. ECONOMICS. MANAGEMENT

Measuring Security Success: Unveiling the KPIs of Protection

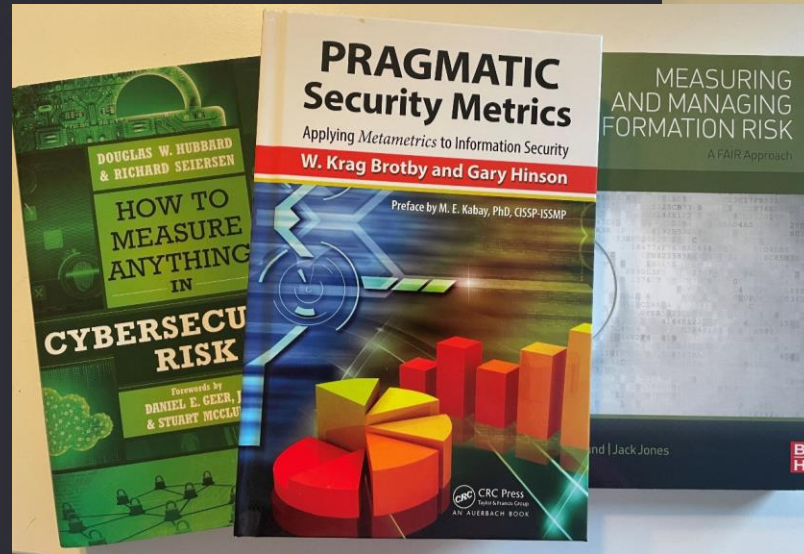
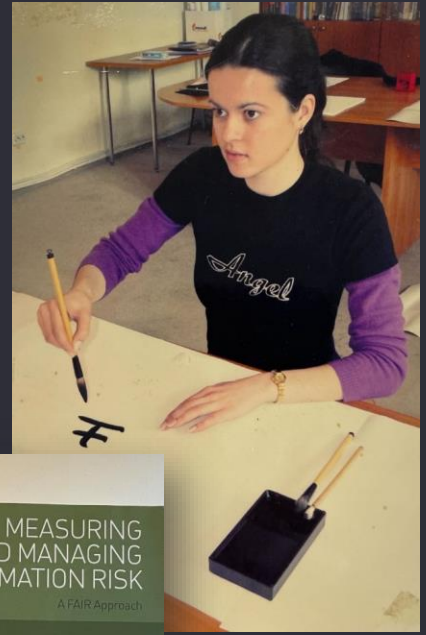
Olga Ghincul, Senior Manager, EY

olga.ghincul@be.ey.com









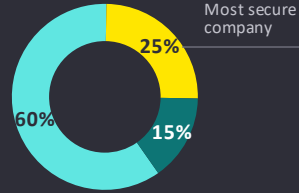
The Security Dashboard

ISO 27001 maturity score



The Security Dashboard

Group targets for information security

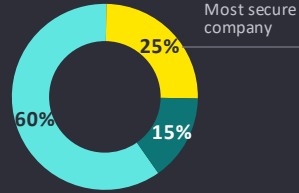


ISO 27001 maturity score



The Security Dashboard

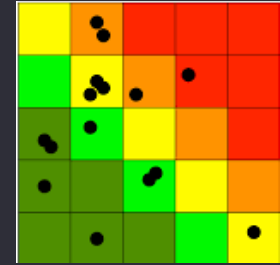
Group targets for information security



ISO 27001 maturity score

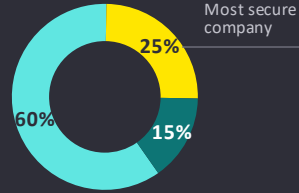


Top security risks treatment status



The Security Dashboard

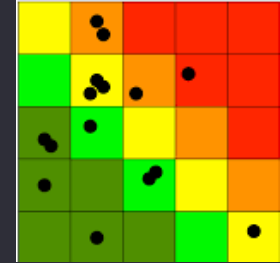
Group targets for information security



ISO 27001 maturity score



Top security risks treatment status

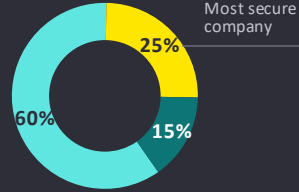


The Security Dashboard

Baseline security controls implementation

Security Baseline controls	Q1	Q2	Q3
	42%	63%	92%

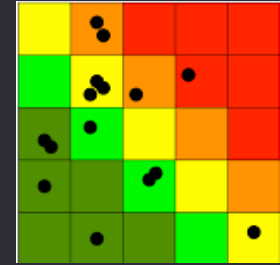
Group targets for information security



ISO 27001 maturity score



Top security risks treatment status



The Security Dashboard

Security control effectiveness



Baseline security controls implementation

Security Baseline controls	Q1	Q2	Q3
	42%	63%	92%

“I need **one** security KPI...”



Replacing fear,
uncertainty and
doubt



The Cobra effect



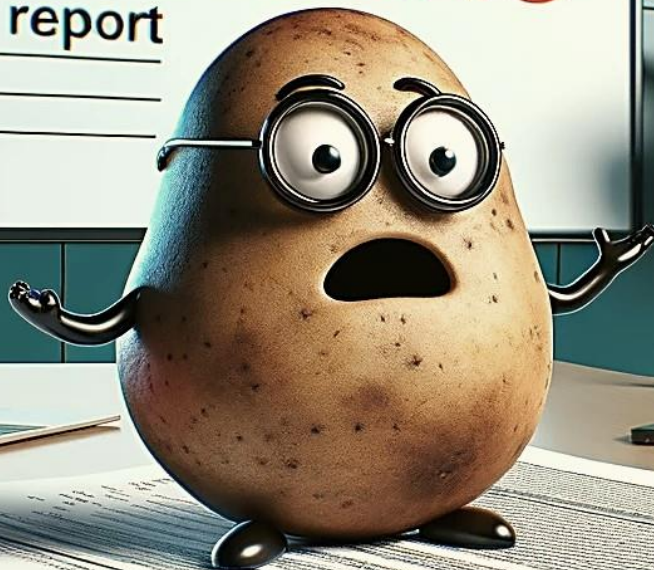
Domesticating information security risk



Be careful **what** to report **to management**

HOT POTATO

Audit report



Striving for
perfection
can be
counterproductive

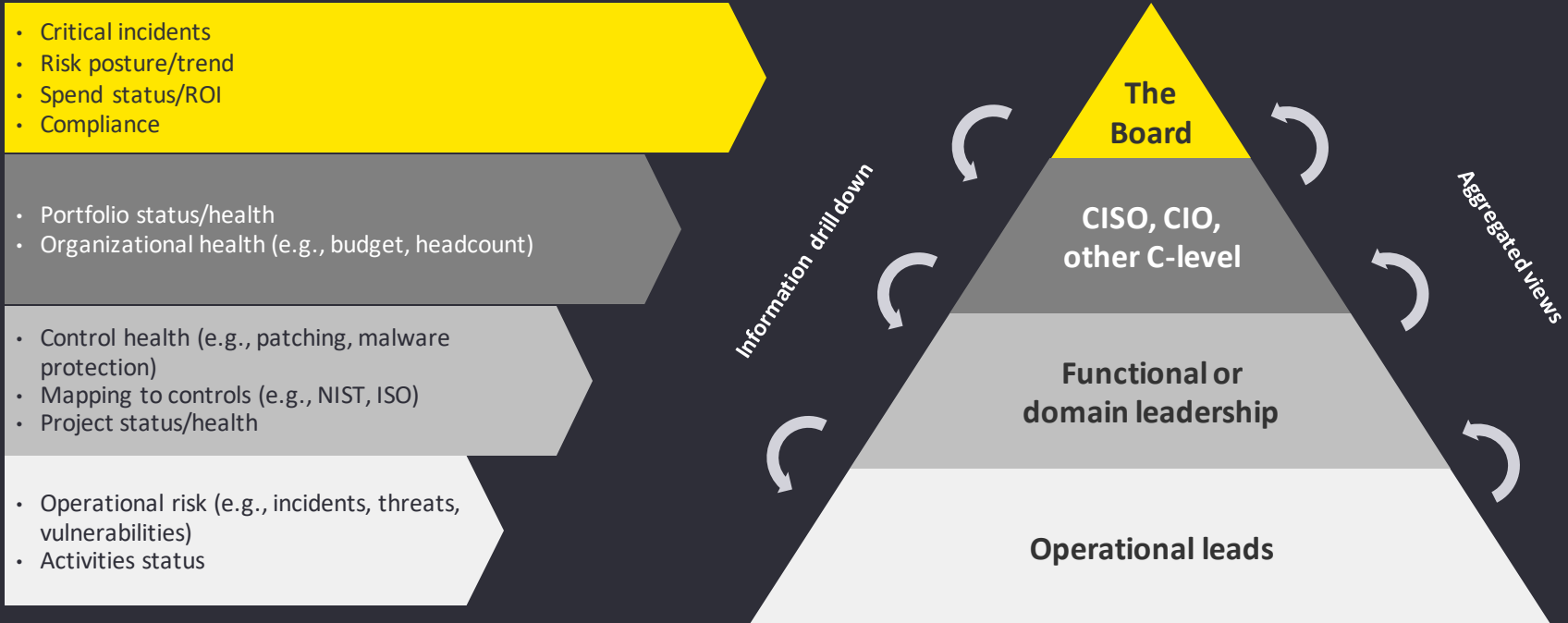


objective actionable
measurable comparable
timely **reliable** achievable
understandable consistent
efficient **effective** quantifiable
relevant

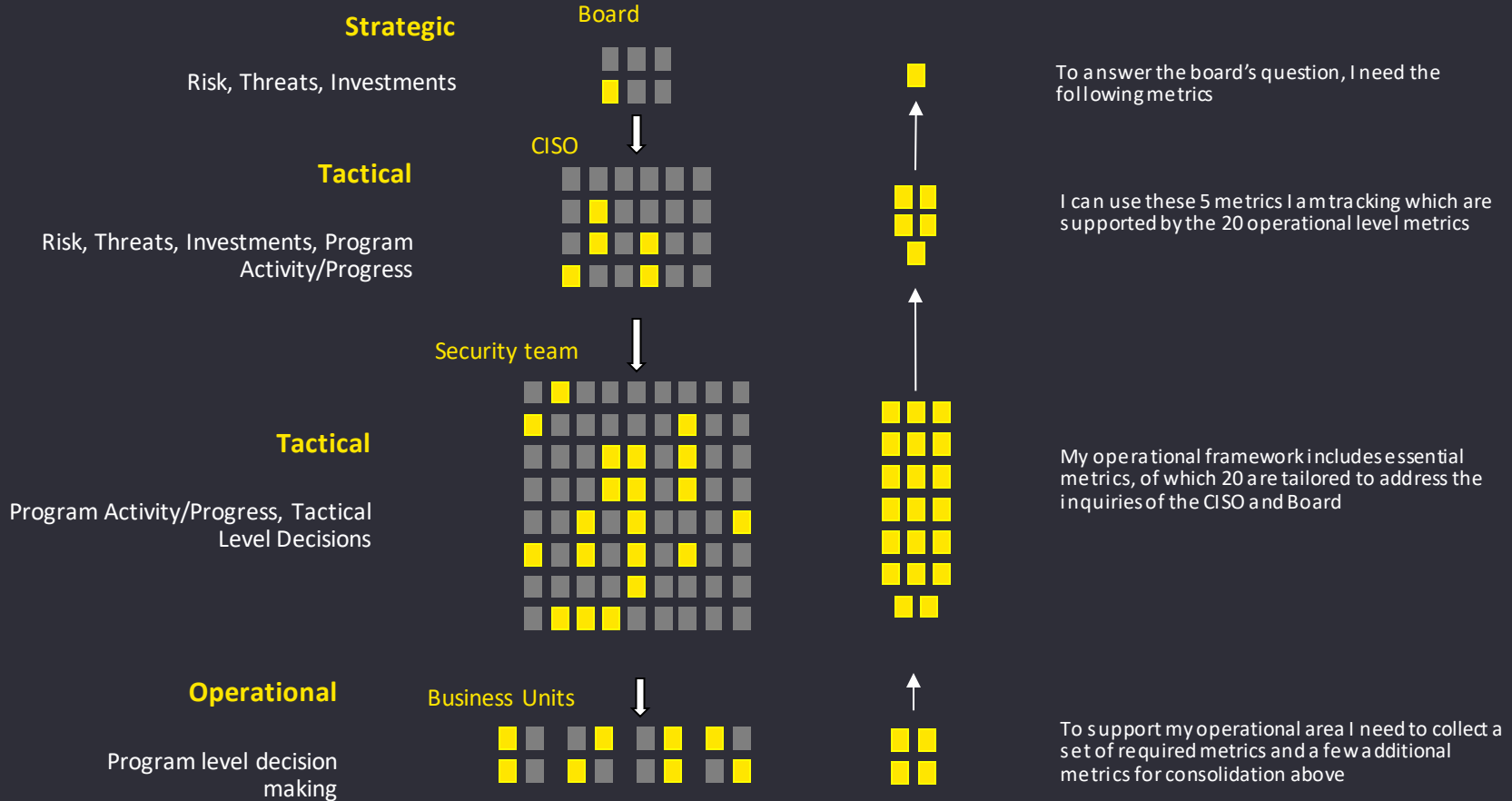
objective actionable
measurable comparable
timely **reliable** achievable
understandable consistent
efficient **effective** quantifiable
relevant

- ✓ Support effective decision making
- ✓ Decrease uncertainty
- ✓ Highlight issues that matter

Change the message for your audience



Top down approach to select metrics



What is board really interested
in?



Revenue



Revenue



Cost

What is board really interested in?



Revenue



Cost



Risk

FSBHFVWE
ROKMKLJOB
SKDUWA.GORME
CHOD AE-ANDNE
PROBNYQME
BAKXNDICORE
SBECYRUM
WANDPULFFIPE
BRPKZLIS
OCSSLBY
DNMFG
IMOCALKREIRE
EDSFTLJODPS
WANDCC.2000



SRSYIM	JACKRMS	UCSTARIB	REBECOS	SEBONECA	212456	NER10S	SEBEGG	JESSEJW
11110	0.11.215	TRE.HI	02965	1.2	1	OFMS	TR	ICA





Executives are advised to...

- ✓ **Target level 5 maturity**
- ✓ **Spend x% of revenue on security**
- ✓ **Be accountable for incidents**
- ✓ **Use benchmarks**
- ✓ **Follow a checklist**

Executives are advised to...

- ✓ **Target level 5 maturity**
- ✓ **Spend x% of revenue on security**
- ✓ **Be accountable for incidents**
- ✓ **Use benchmarks**
- ✓ **Follow a checklist**

We advise CISOs to ask...

- ✓ **What is the board's background?**
- ✓ **What role do they serve on the board?**
- ✓ **Is there a cybersecurity expert in the board?**
- ✓ **What are their biases?**
- ✓ **What are their passions?**

Once upon
a time...



Security can be simple



Focus on your critical assets (errors in configuration, software)

Focus on credentials that control systems

Focus on people that use your critical assets



Balanced security controls

Why security controls matter



Risk tolerance

>130

Risk appetite

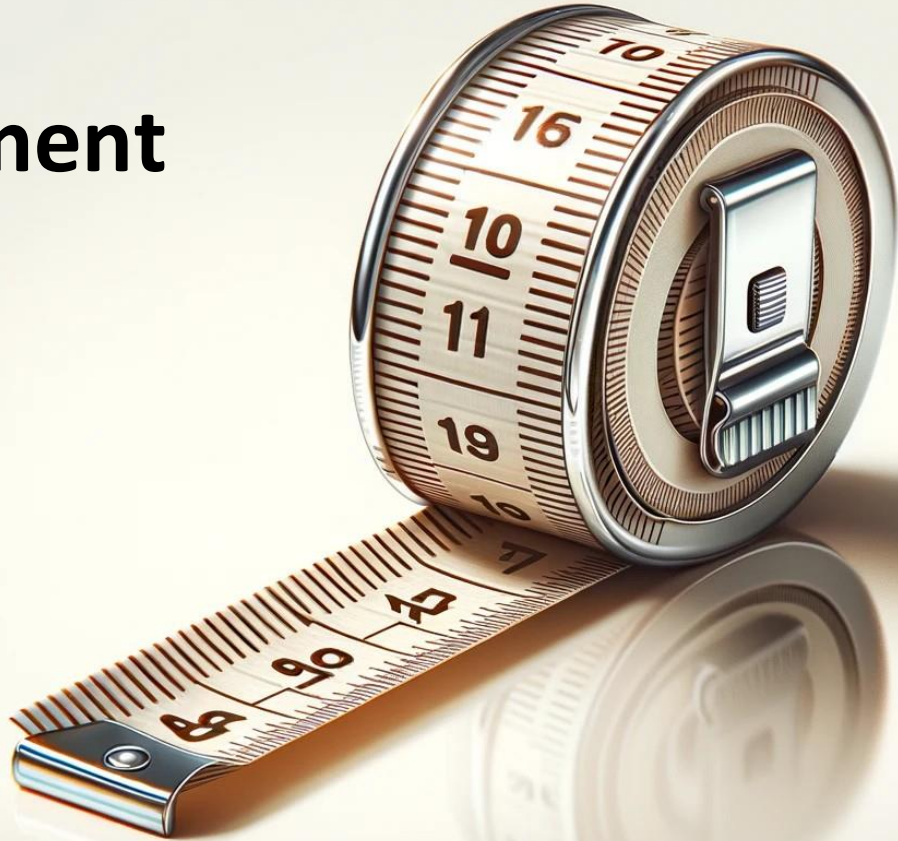
120





NIST CSF – a management-friendly framework

The measurement cycle



Measure effectiveness of controls

Automate

Measure the maturity of the controls

Design a control framework



The measurement cycle



1. Define

- Metric Owner
- Data Owner
- Description
- Assumptions
- Calculation
- Data Sources
- Thresholds
- Frequency
- Status

2. Collect

- Iterative process
- Continual improvements
- A set framework
- Methodology

3. Validate

- Clear steps to validate
- Responsibility of the collector, initially
- Over time, moves to metric and data owner
- Brings confidence level of the data collected

4. Manage

- Begin with manual collection and analysis
- Gradually moving towards automation
- Not take resources away from their main tasks

Building the metrics story

1 Threat actors and threats

- Top 5 threats
- Top 5 threat actors

2 Assets and business at risk

- Top 5 Crown Jewels aligned with business
- Financial value and value at risk

3 Security posture

- Health
- Effectiveness
- Defensibility
- Recoverability
- External security ratings

4 Top risk scenarios

- Risk scenarios
- Risk exposure

5 Ongoing risk reduction efforts

- Ongoing Initiatives
- Risk reduction value

6 Recommended risk reduction efforts

- Recommended initiative
- Initiative cost
- Initiative risk reduction value
- Initiative return on security investment

Building the metrics story

1

Threat actors & threats

The company is in the news, threat actors are highly motivated and well financed



- ATP1
- Lazarus
- Cobalt
- Ransomware
- Spear phishing
- Supply chain attacks

Building the metrics story

1

Threat actors & threats

The company is in the news, threat actors are highly motivated and well financed



- ATP1
- Lazarus
- Cobalt
- Ransomware
- Spear phishing
- Supply chain attacks

2

Assets & business at risk

Loss amount is based on productivity, response, replacement, fines, reputation loss

PII Data



€500 m

IP



€150 m

E-commerce



€200 m

Data centers



€300 m

Applications



€600 m

Building the metrics story

1

Threat actors & threats

The company is in the news, threat actors are highly motivated and well financed



- ATP1
- Lazarus
- Cobalt
- Ransomware
- Spear phishing
- Supply chain attacks

2

Assets & business at risk

Loss amount is based on productivity, response, replacement, fines, reputation loss

PII Data



€500 m

IP



€150 m

E-commerce



€200 m

Data centers



€300 m

Applications



€600 m

3a

Security Posture (Metrics)

Health



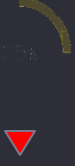
Effectiveness



Defensibility



Recoverability



External monitoring score

725

Building the metrics story

1

Threat actors & threats

The company is in the news, threat actors are highly motivated and well financed



- ATP1
- Lazarus
- Cobalt



- Ransomware
- Spear phishing
- Supply chain attacks

2

Assets & business at risk

Loss amount is based on productivity, response, replacement, fines, reputation loss

PII Data



€500 m

IP



€150 m

E-commerce



€200 m

Data centers



€300 m

Applications



€600 m

3a

Security Posture (Metrics)



3b

Security Posture (Frameworks)

MITRE ATT&CK

	Initial access	Gain control	Lateral mov.	Data access	Data transf.
Coverage	25%	25%	25%	25%	25%
Tested	15%	15%	15%	15%	15%
Detection	65%	65%	65%	25%	25%

NIST CSF

	Identify	Protect	Detect	Respond	Recover
(4) Adaptive					
(3) Repeatable	●	●	●	●	●
(2) Informed	●	●	●	●	●
(1) Partial	●	●	●	●	●

Building the metrics story

1

Threat actors & threats

The company is in the news, threat actors are highly motivated and well financed



- ATP1
- Lazarus
- Cobalt
- Ransomware
- Spear phishing
- Supply chain attacks

2

Assets & business at risk

Loss amount is based on productivity, response, replacement, fines, reputation loss

PII Data



€500 m

IP



€150 m

E-commerce



€200 m

Data centers



€300 m

Applications



€600 m

3a

Security Posture (Metrics)



4

Top risk scenarios

- Successful ransomware attack
- Top executive spear phishing
- IP stolen by internal employee
- Account takeover due to critical vulnerability
- Major disruption to a critical service caused by DDoS

Exposure

€20M

€10M

€5M

€25M

€2M

3b

Security Posture (Frameworks)

MITRE ATT&CK					
	Initial access	Gain control	Lateral mov.	Data access	Data transf.
Coverage	25%	25%	25%	25%	25%
Tested	15%	15%	15%	15%	15%
Detection	65%	65%	65%	25%	25%

NIST CSF					
	Identify	Protect	Detect	Respond	Recover
(4) Adaptive					
(3) Repeatable	●	●	●	●	●
(2) Informed	●	●	●	●	●
(1) Partial	●	●	●	●	●

Building the metrics story

1 Threat actors & threats

The company is in the news, threat actors are highly motivated and well financed



- ATP1
- Lazarus
- Cobalt



- Ransomware
- Spear phishing
- Supply chain attacks

2 Assets & business at risk

Loss amount is based on productivity, response, replacement, fines, reputation loss

PII Data



€500 m

IP



€150 m

E-commerce



€200 m

Data centers



€300 m

Applications



€600 m

3a Security Posture (Metrics)



5 Ongoing risk reduction efforts

	Cost	Reduction	ROI
Revamp vulnerability management	€10M	€5M	50%
PII data inventory & protection	€5M	€5M	50%
Review firewall rules	€5M	€1M	25%

4 Top risk scenarios

- Successful ransomware attack
- Top executive spear phishing
- IP stolen by internal employee
- Account takeover due to critical vulnerability
- Major disruption to a critical service caused by DDoS

Exposure

€20M

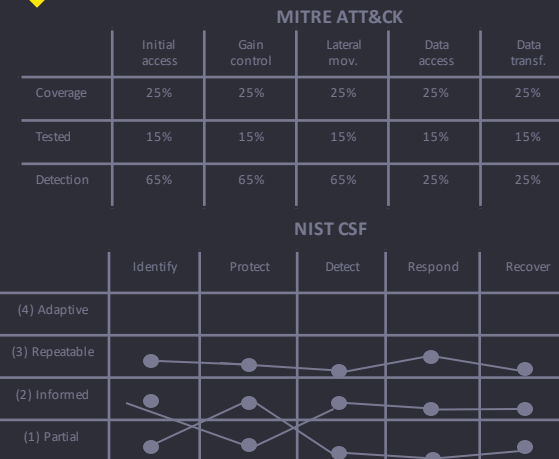
€10M

€5M

€25M

€2M

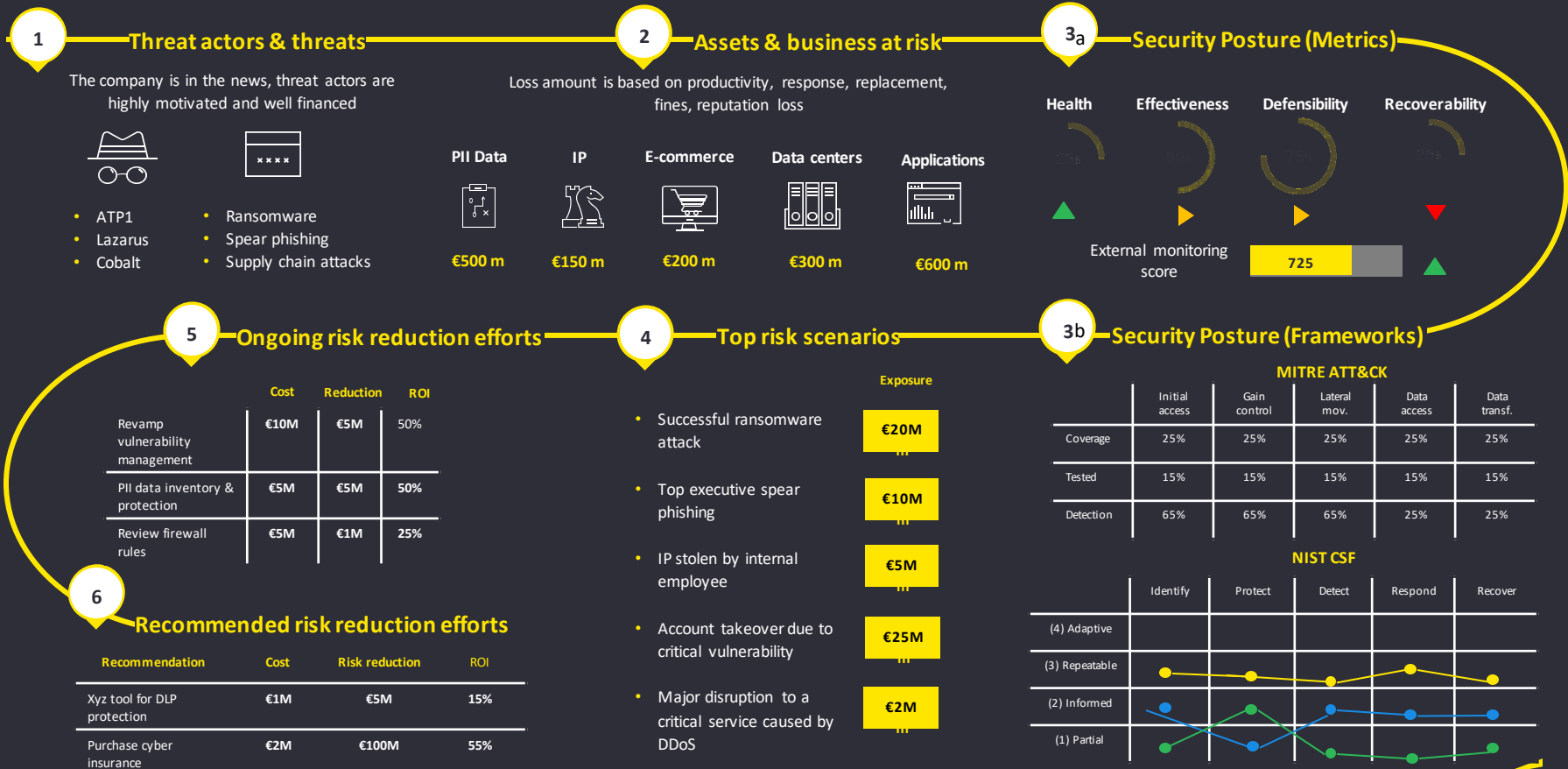
3b Security Posture (Frameworks)



Building the metrics story



Building the metrics story



Thank you!

Olga Ghincul

CISM, CRISC
Senior Manager, EY

olga.ghincul@be.ey.com



EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

© 2024 EYGM Limited.
All Rights Reserved.

ey.com/be

