GRC be connected

28 MARCH BLEUPOINT BRUSSELS

Leveraging Cyber Risk Quantification for Robust Cybersecurity Governance

– Robert Kloots, TrustMatters

ORGANIZED BY

CYBER SECURITY COALITION.be

ISACA Belgium Chapter

CGEIT CISA CISM CRISC CSX-P COBIT

SUPPORTED BY

Solvay Lifelong Learning
BRUSSELS SCHOOL. ECONOMICS. MANAGEMENT

Agenda

1	Business is the driver
2	Cyber security risk
3	Appropriate measures
4	Conclusion

TRUSTMATTERS

GRC be connected

Business is the driver

ORGANIZED BY

CYBER SECURITY COALITION.be

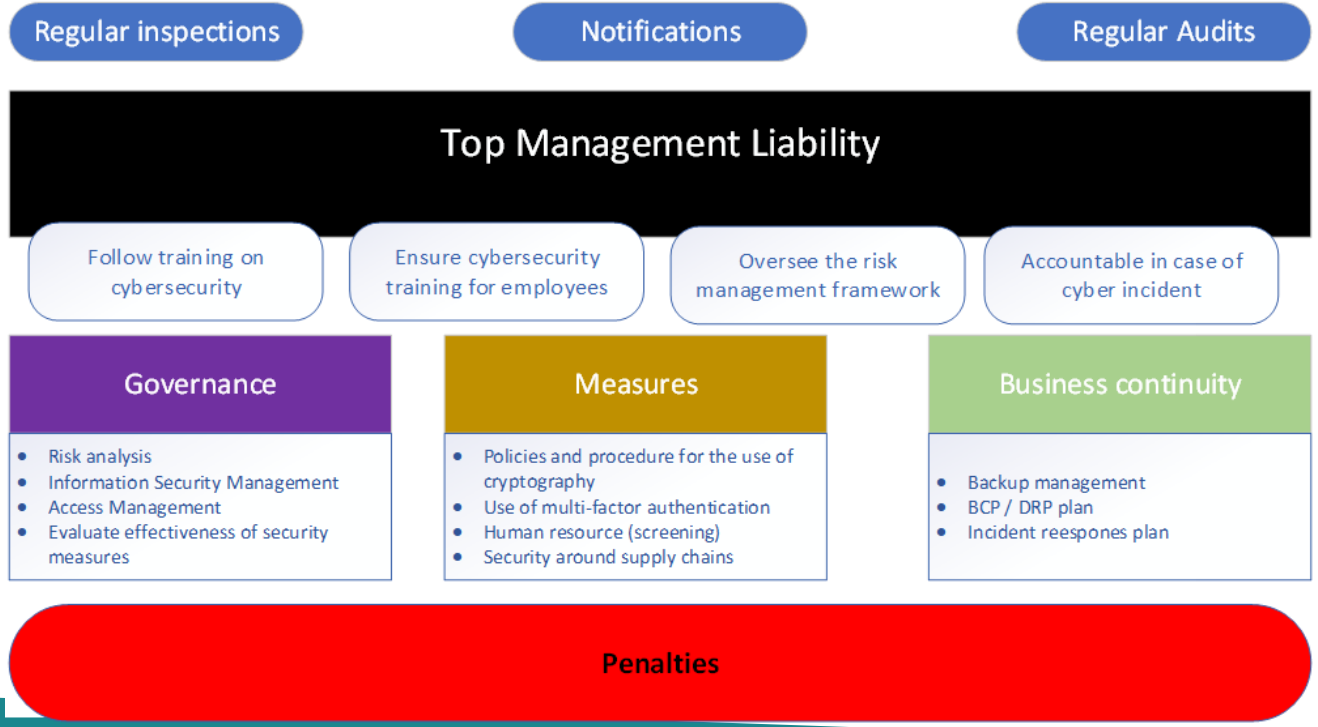
ISACA Belgium Chapter

CGEIT CISA CISM CRISC CSX-P COBIT

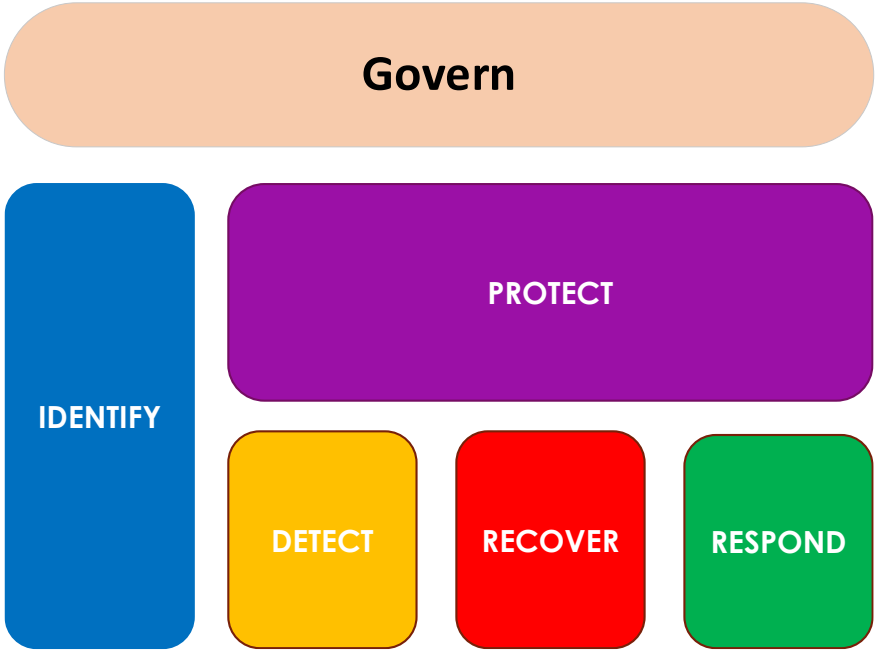
SUPPORTED BY

Solvay Lifelong Learning
BRUSSELS SCHOOL. ECONOMICS. MANAGEMENT

NIS2 Requirements



Cyber Security Framework (CSF)



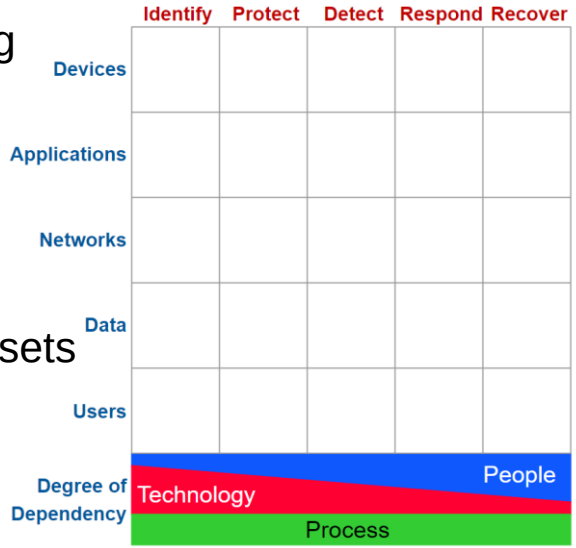
Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

Cyber Security Function Deployment

Actions

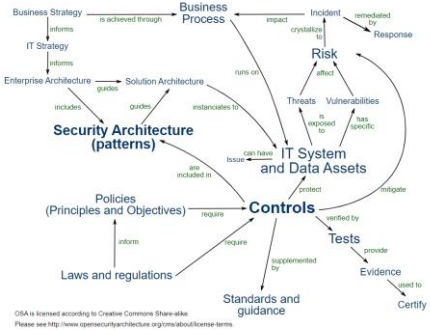
- Take inventory of existing CySec services and/or solutions,
- Allocate control(s) to appropriate matrix-cell
- Repeat for asset type:
  - Corporate digital assets
  - Employee assets
  - Customer assets
  - Vendor assets
  - Threat actor assets

Operational functions



Asset types

Do we have something (inventory)...
That we care about (impact)...
That has weaknesses (vulnerabilities)...
That someone is after (threats)?



TRUSTMATTERS

GRC be connected

Cyber security risk

ORGANIZED BY

CYBER SECURITY COALITION.be

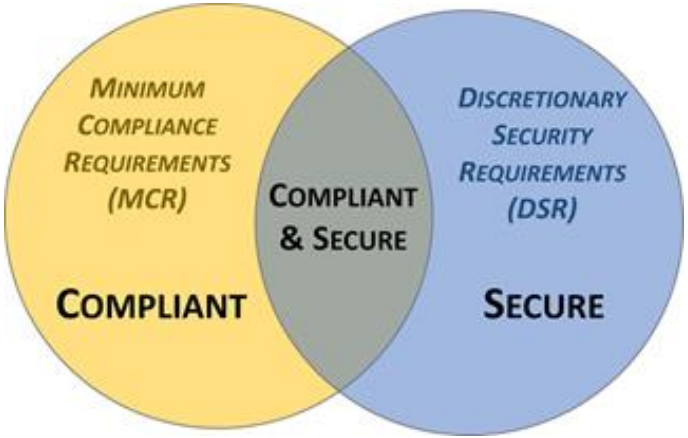
ISACA Belgium Chapter

CGEIT CISA CISM CRISC CSX-P COBIT

SUPPORTED BY

Solvay Lifelong Learning
BRUSSELS SCHOOL. ECONOMICS. MANAGEMENT

Compliance & Secure



•**Compliance Focused** - this is aiming for mediocrity by focusing on only the bare minimums to comply with a law, regulation or framework.

•**Security Focused** - this is focused on hard-core secure engineering practices and compliance is not a concern.

•**Compliance & Security Focused** - this is a holistic approach that is focused on making sure systems, applications and services are secure by design and default, where compliance is viewed as a natural byproduct by having the proper blend of cybersecurity and privacy practices.

The Risk Management Stack

The Risk Management Stack explains the value of quantitative risk analysis models.

The objective is to achieve **cost-effective risk management.**

Risk management is a decision making discipline, which means we try to make **well-informed decisions**.

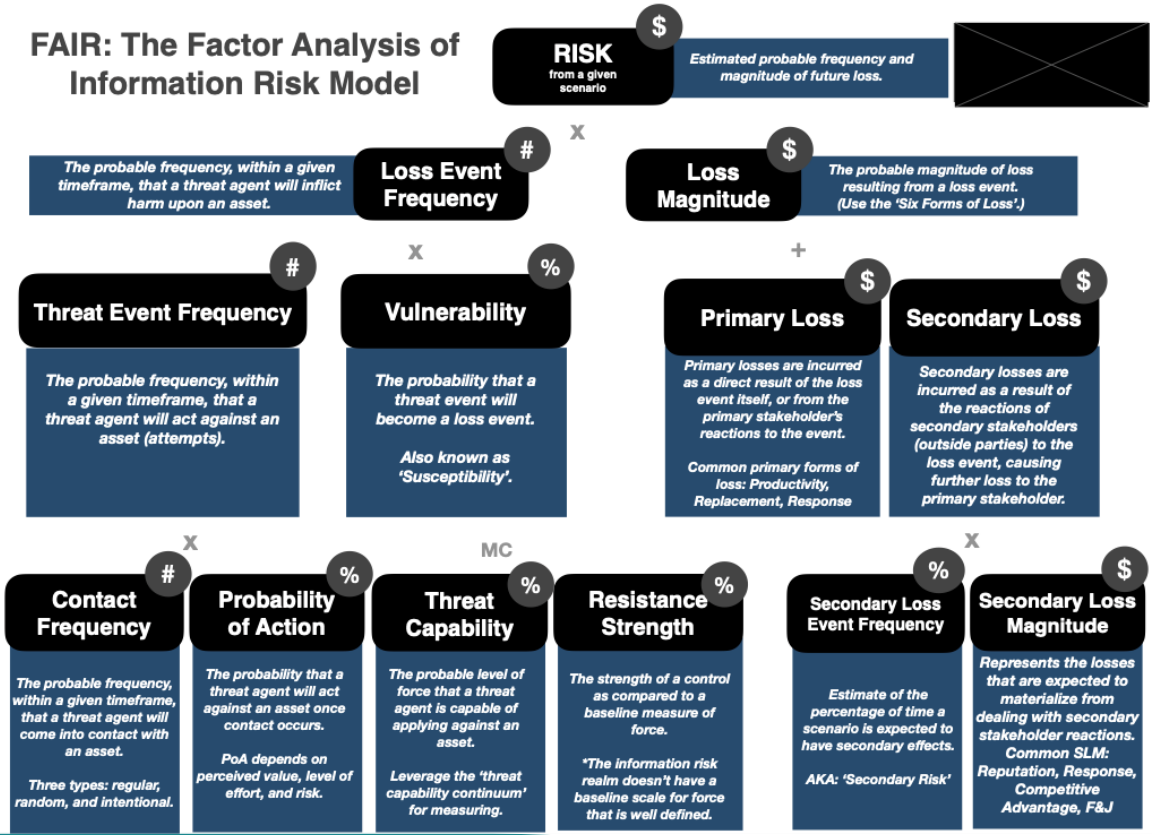
Decisions are typically trade offs between multiple options. We can only decide on which is best for our particular context by making **effective comparisons**.

Effective comparisons are objectively enabled through **meaningful measurements**.

For measurements to be meaningful, logical, consistent and defensible they need to be based on **accurate models**.

FAIR Model

Risk is a **measurement** of future loss from a given scenario derived from **probable frequency** and **probable magnitude** of loss events.



Focus on Loss Event Frequency

Our objective is to feed data into the LEF side of the model with the ATT&CK matrix.

1. Leverage the Real Data
2. Reduce the Guesswork
3. Increase Confidence
4. Dynamically Change Scenario Results

Ingredients…

1. Leverage Threat-Informed Defense with ATT&CK Matrix
2. ATT&CK Components
3. Leverage Attack Flow
4. FAIR
5. Accurate Assumptions :)

TRUSTMATTERS

GRC be connected

Appropriate measures

ORGANIZED BY

CYBER SECURITY COALITION.be

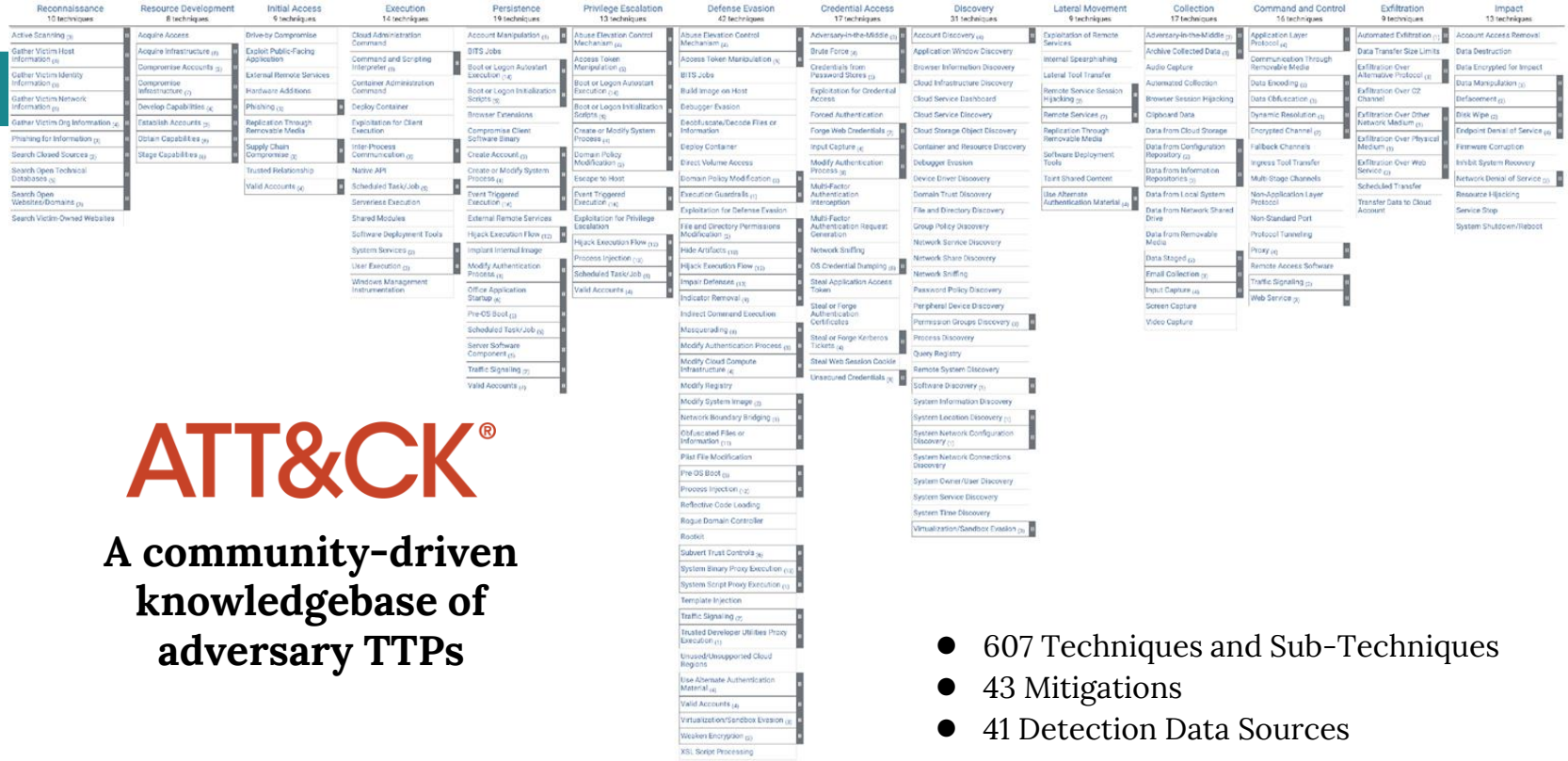
ISACA Belgium Chapter

CGEIT CISA CISM CRISC CSX-P COBIT

SUPPORTED BY

Solvay Lifelong Learning
BRUSSELS SCHOOL. ECONOMICS. MANAGEMENT

TRUSTMATTERS



ATT&CK®

A community-driven knowledgebase of adversary TTPs

- 607 Techniques and Sub-Techniques
- 43 Mitigations
- 41 Detection Data Sources

ORGANIZED BY

CYBER SECURITY COALITION.be

ISACA Belgium Chapter

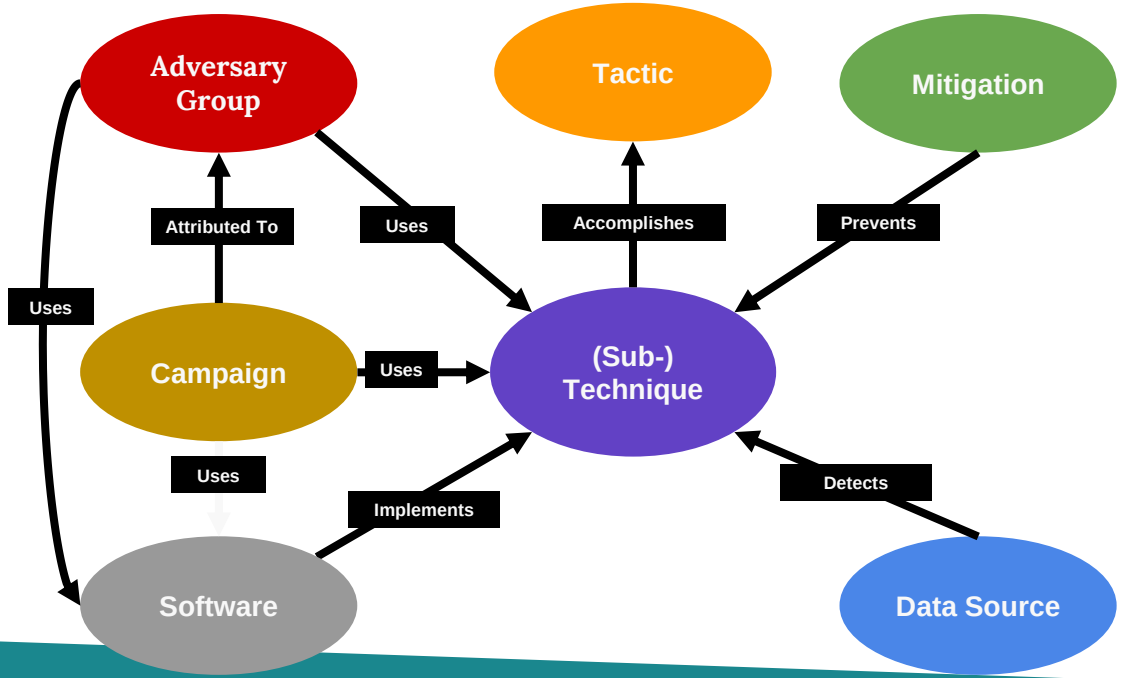
CGEIT CISA CISM CRISC CSX-P COBIT

SUPPORTED BY

Solvay Lifelong Learning
BRUSSELS SCHOOL. ECONOMICS. MANAGEMENT

CRC be connected

From TTPs to Mitigation and Detection



Example Technique

Technique: Bruteforce
(https://attack.mitre.org/techniques/T1110/)

4 Sub-techniques

19 Threat Actors

19 Campaigns

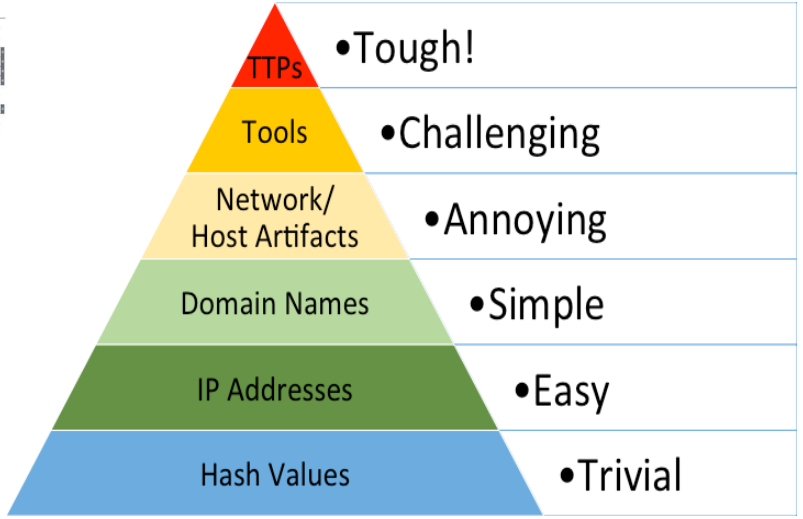
Mitigations

ID	Mitigation	Description
M1036	Account Use Policies	Set account lockout policies after a certain number of failed login attempts to prevent passwords from being guessed. Too strict a policy may create a denial of service condition and render environments un-usable, with all accounts used in the brute force being locked-out. Use conditional access policies to block logins from non-compliant devices or from outside defined organization IP ranges.[25]
M1032	Multi-factor Authentication	Use multi-factor authentication. Where possible, also enable multi-factor authentication on externally facing services.
M1027	Password Policies	Refer to NIST guidelines when creating password policies.[26]
M1018	User Account Management	Proactively reset accounts that are known to be part of breached credentials either immediately, or after detecting bruteforce attempts.

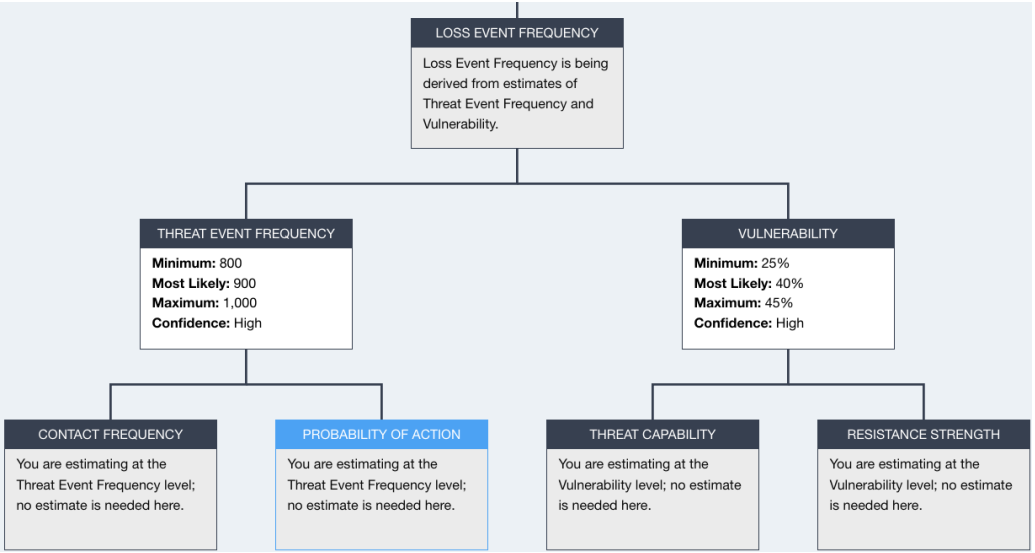
Detection

ID	Data Source	Data Component	Detects
DS0015	Application Log	Application Log Content	Monitor authentication logs for system and application login failures of Valid Accounts. If authentication failures are high, then there may be a brute force attempt to gain access to a system using legitimate credentials.
DS0017	Command	Command Execution	Monitor executed commands and arguments that may use brute force techniques to gain access to accounts when passwords are unknown or when password hashes are obtained.
DS0002	User Account	User Account Authentication	Monitor for many failed authentication attempts across various accounts that may result from password spraying attempts. It is difficult to detect when hashes are cracked, since this is generally done outside the scope of the target network.

Increasing the Cost for the Adversary



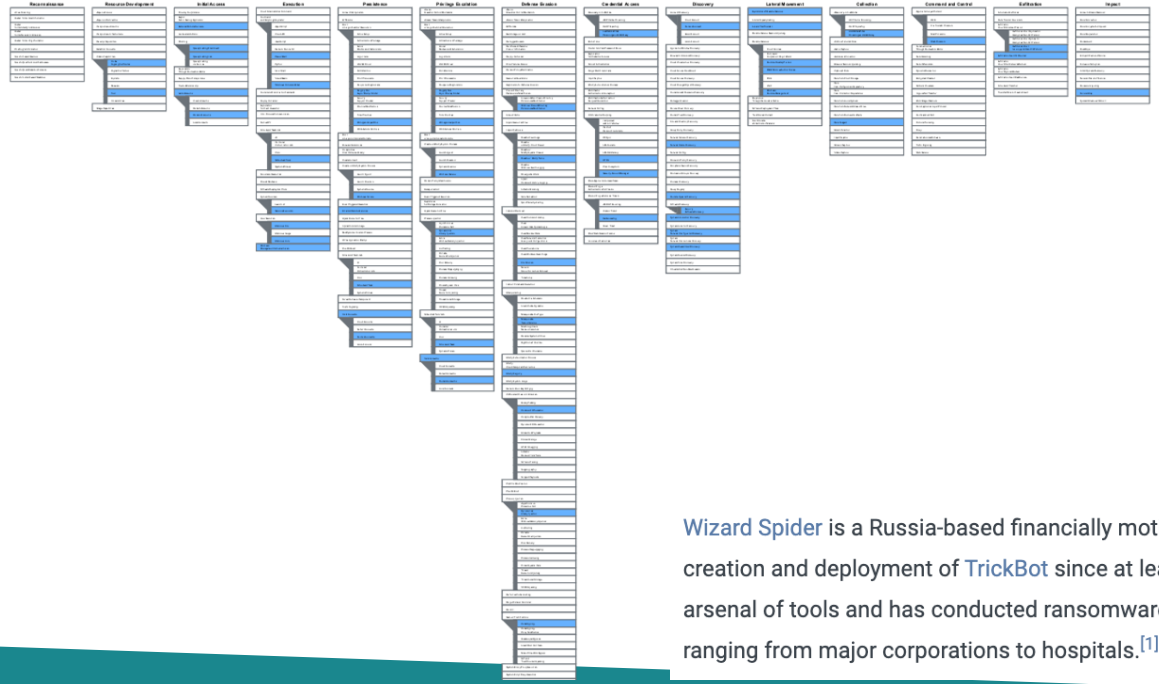
Leverage ATT&CK and Real Data in FAIR Model



- Map your security findings and controls against ATT&CK Techniques, Subtechniques, Mitigations and Detections to better understand your **Resistance Strength and Probability of Action**
- Use Attack Flow to understand frequently used Techniques and Sub-techniques by Threat Groups during a specific attack type (method) to better understand **Threat Capability**

SIEM | Failing Techniques | Threat Group + Software + Campaign Techniques | Mitigations & Detections

ATT&CK Techniques used by Wizard Spider Group



37 Documented Techniques

Wizard Spider is a Russia-based financially motivated threat group originally known for the creation and deployment of TrickBot since at least 2016. Wizard Spider possesses a diverse arsenal of tools and has conducted ransomware campaigns against a variety of organizations, ranging from major corporations to hospitals.[1][2][3]

Leverage ATT&CK and Real Data in FAIR Model

1. Asset - PII Data
2. Threat - Wizard Spider Group
3. Effect - Availability Impact
4. Method - Data Encrypted using Ransomware

Fortune-10 Healthcare Win

Risk
Min: $3.2
Most Likely: $4.6M
Max:$6.2M

Loss Event Frequency
Min: 9
Most Likely: 12
Max: 15

Loss Magnitude
Min: $1.6M
Most Likely: $3.4M
Max: $5.3M

Threat Event Frequency
Min: 400
Most Likely: 65(
Max:900

Vulnerability
Min: 26%
Most Likely: 60%
Max:78%

Primary Loss
Min: $1.1M
Most Likely: $2.2M
Max: $3.1M

Secondary Loss
Min: $0.5M
Most Likely: $1.2M
Max: $2.2M

Success Story :)

Business Enablement:

Enabled business to continue securely

Board Engagement:

Effective Communication with the Board and the business leadership

Cross Team Alignment:

Focused Execution towards common goal with accurate context setting between Security and Risk teams.

Risk Based Security:

Crown Jewels protection

Build encryption

Key management and enhanced DB security program

Cost: $2.1M

Value:

Loss Exposure: Reduced from $8M to $1.9M

Increased Data Protection: Secured 33M PHI records vs 5M PHI records that were at risk

Increased Maturity: Enhanced Cyber program maturity by securing all DBs and implementing enhanced monitoring and Access.

TRUSTMATTERS

GRC be connected

Conclusion

ORGANIZED BY

CYBER SECURITY COALITION.be

ISACA Belgium Chapter

CGEIT CISA CISM CRISC CSX-P COBIT

SUPPORTED BY

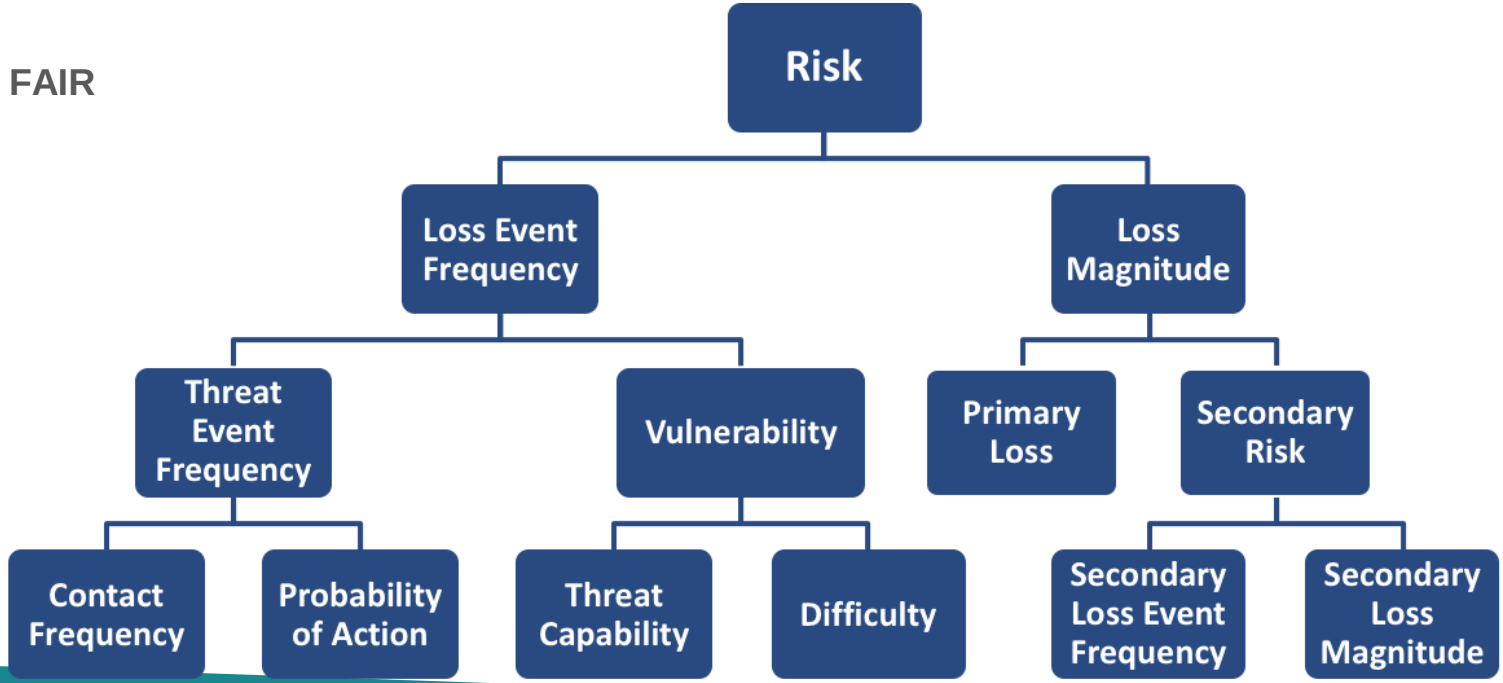
Solvay Lifelong Learning
BRUSSELS SCHOOL. ECONOMICS. MANAGEMENT

Leveraging Cyber Risk Quantification for Robust Cybersecurity Governance

- Choose your Framework wisely
- Structure the Cyber Security Function accordingly
- Move from Qualified Risk to Quantified Risk
- Align Threat modelling with Quantified Risk Analysis
- Implement Risk based mitigating measures
- Deliver Business aligned Decisions

Manage the Cyber Risk

- FAIR



GRC be connected

Thank you!

TRUSTMATTERS

Email: robert.Kloots@trustmatters.eu

ORGANIZED BY

CYBER SECURITY COALITION.be

ISACA Belgium Chapter

CGEIT CISA CISM CRISC CSX-P COBIT

SUPPORTED BY

Solvay Lifelong Learning
BRUSSELS SCHOOL. ECONOMICS. MANAGEMENT