Measuring the state of cyber resilience

Building a framework of cyber resilience metrics

PVIB session 15-06-2017
Paul Samwel

Rabobank

Paul Samwel

audIT

EY

hip '97 Hacking In Progress August 8th, 9th, 10th

TU Delft

vrije Universiteit amsterdam

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL
CISSP®

LID VAN PvIB
Platform voor InformatieBeveiliging

ENISA
CURRENT THREAT LANDSCAPE EMERGING
ETL 2015

CYBERCRIME TASK FORCE

Rabobank

Enterprise Architect Skills – simplicable.com

SecurityInnovation

Shared research program Cyber Security

Rabobank

ABN·AMRO

Rabobank

TNO innovation for life

ING

achmea

Share costs

Share workload

Share experiences

Why metrics

- The need to show and provide **assurance and evidence** on the level of resilience and/or security achieved;
- The need of a metrics system for **validating the conformance with regulations**, policies and business requirements;
- The **practical need to analyse** in an effective and efficient manner the increasing number and complexity of technical logs;
- The **identification of trends** in the different communica l of attacks, common failure causes, etc.

Background:
Cyber resilience

Rabobank

Cyber resilience is the ability of an ecosystem (e.g. an organization, infrastructure, system) to

…withstand deliberate attacks on technical infrastructure that are conducted from cyberspace

…rapidly recover from the negative effects of such attacks

…limit the damage of such attacks on business, people and society

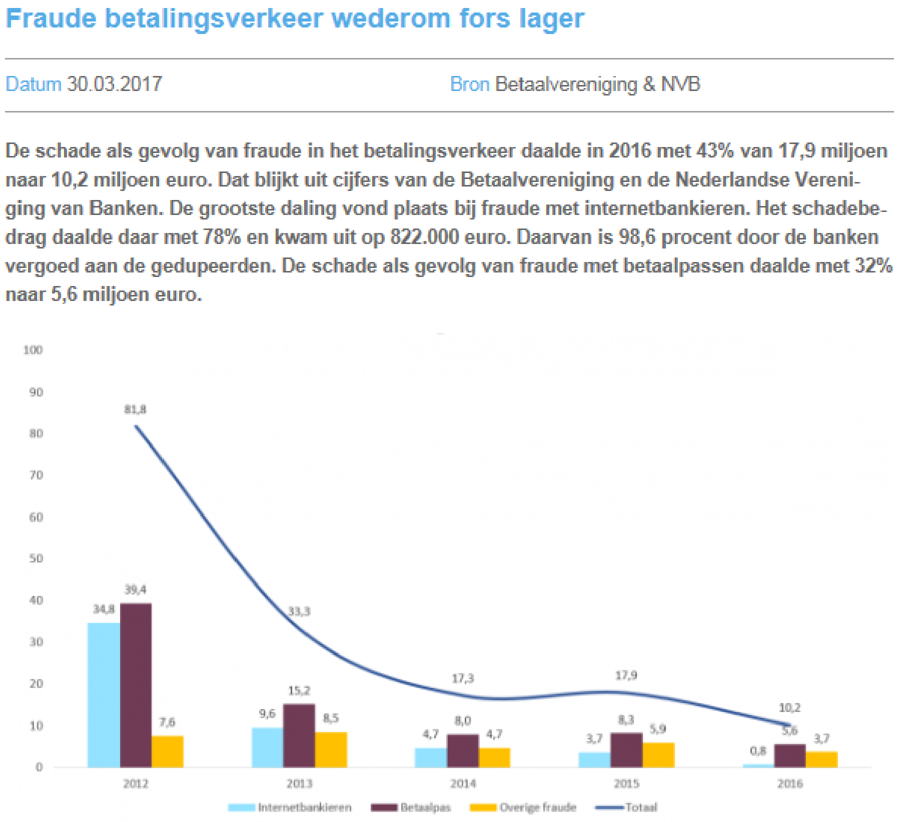
…prepare for and adapt to changing conditions e.g. changes in attacker methods or the organisation's IT infrastructure

Background:
Experience with benchmarking between banks

Losses in electronic payments collected by "betaalvereniging"

Totals of internet banking fraud are published
Banks benchmarking:

- Own figures against totals
- Reported developments at other banks.

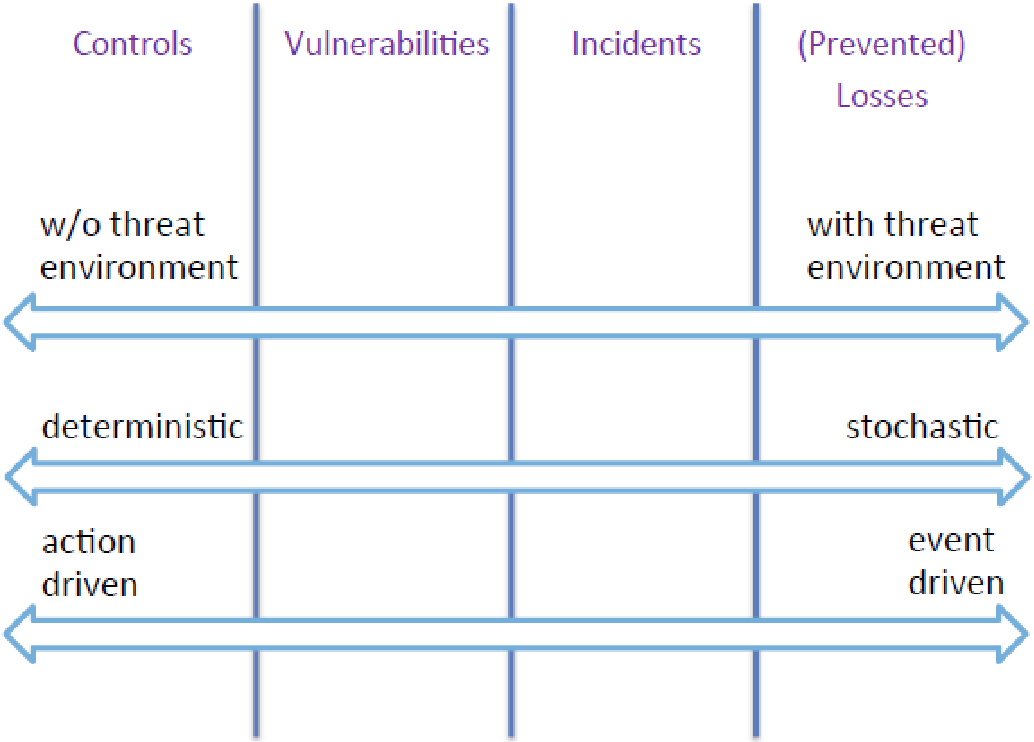


Fraude betalingsverkeer wederom fors lager

Datum 30.03.2017 Bron Betaalvereniging & NVB

De schade als gevolg van fraude in het betalingsverkeer daalde in 2016 met 43% van 17,9 miljoen naar 10,2 miljoen euro. Dat blijkt uit cijfers van de Betaalvereniging en de Nederlandse Vereniging van Banken. De grootste daling vond plaats bij fraude met internetbankieren. Het schadebedrag daalde daar met 78% en kwam uit op 822.000 euro. Daarvan is 98,6 procent door de banken vergoed aan de gedupeerden. De schade als gevolg van fraude met betaalpassen daalde met 32% naar 5,6 miljoen euro.

Background:
Types of metrics



Controls

Vulnerabilities

Incidents

(Prevented) Losses

w/o threat environment

with threat environment

deterministic

stochastic

action driven

event driven

Source: Michel van Eeten: Measuring security levels

strong desire to measure and quantify status of cyber resilience provisions
- fortify basis for operational governance and investment decisions

traditional metrics system

compliance with policies and regulation

measures/ controls and actions taken

parameters that are easily measured

➡

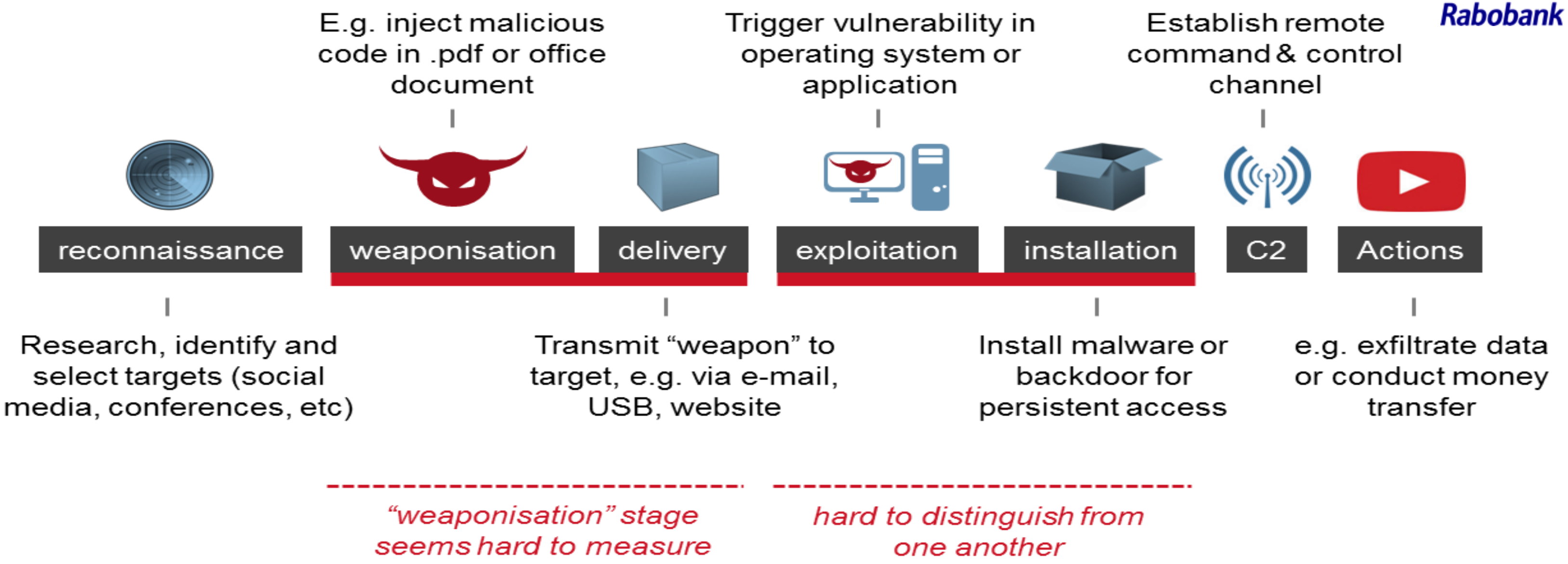
framework of cyber resilience metrics

resilience against targeted attacks

abilities and effects achieved

demonstrably meaningful information

Kill chain to check for completeness



E.g. inject malicious code in .pdf or office document

Trigger vulnerability in operating system or application

Establish remote command & control channel

reconnaissance | weaponisation | delivery | exploitation | installation | C2 | Actions

Research, identify and select targets (social media, conferences, etc)

Transmit “weapon” to target, e.g. via e-mail, USB, website

Install malware or backdoor for persistent access

e.g. exfiltrate data or conduct money transfer

“weaponisation” stage seems hard to measure

hard to distinguish from one another

cyber kill chain embraced as top level structure

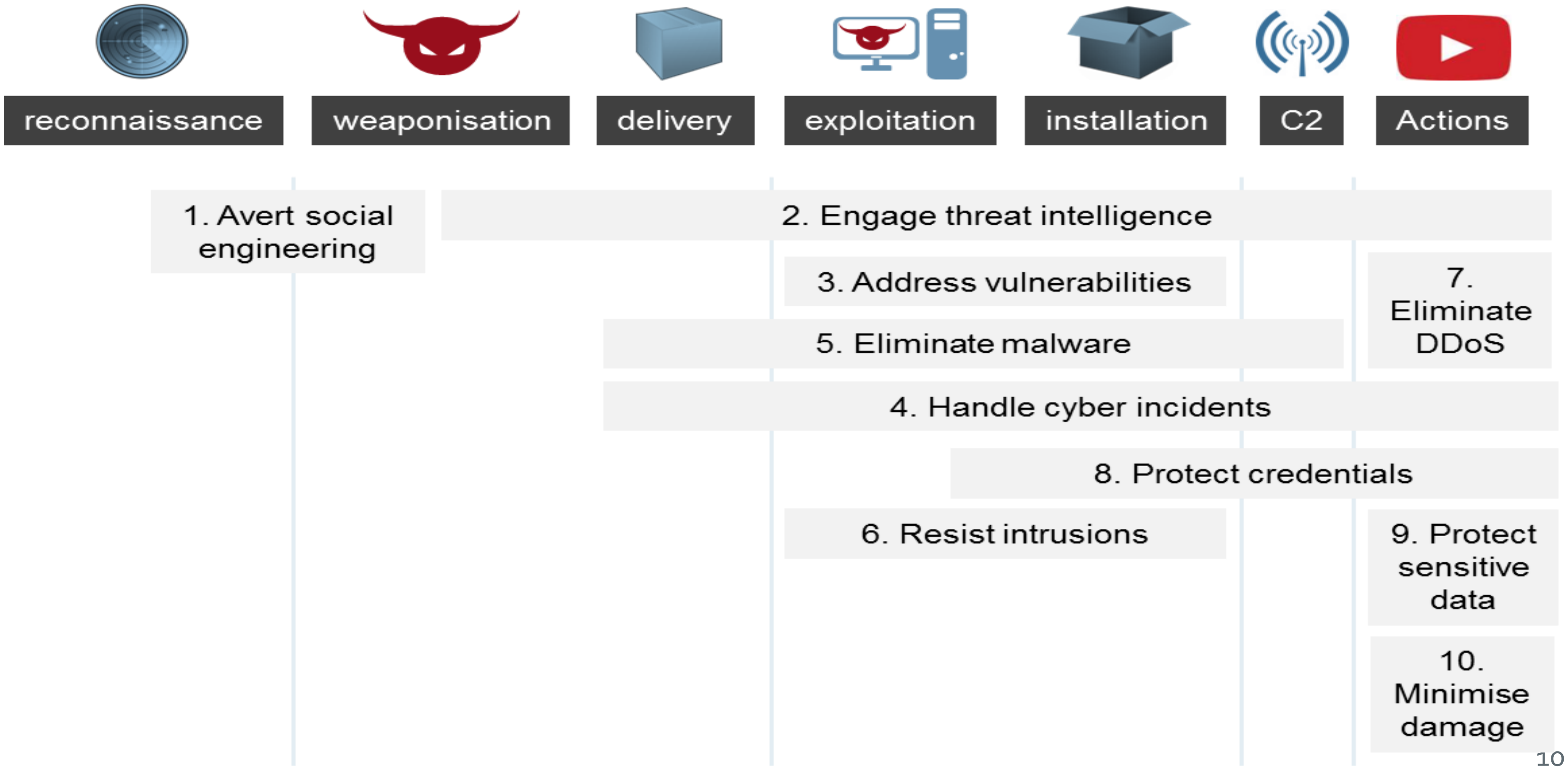
a) acknowledged model for targeted attacks

b) facilitates differentiation by attack stage

some stages merged for the purpose of this work

Building a meaningful framework

Rabobank



reconnaissance

weaponisation

delivery

exploitation

installation

C2

Actions

1. Avert social engineering

2. Engage threat intelligence

3. Address vulnerabilities

5. Eliminate malware

7. Eliminate DDoS

4. Handle cyber incidents

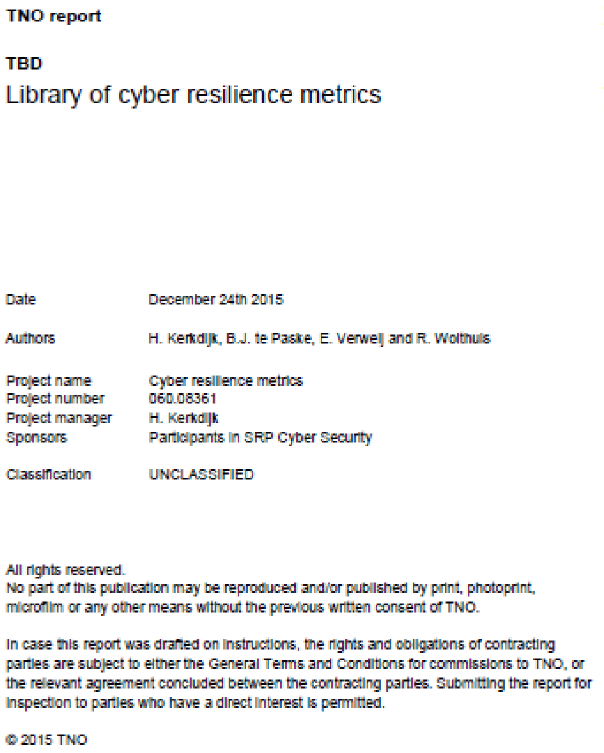
8. Protect credentials

6. Resist intrusions

9. Protect sensitive data

10. Minimise damage

Library of metrics



TNO report

TBD

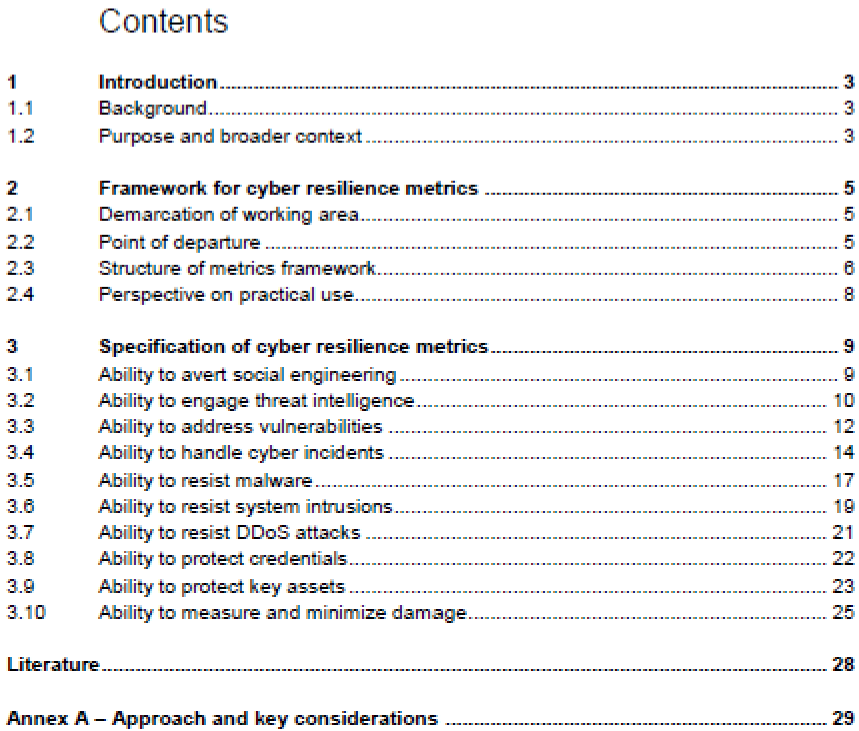
Library of cyber resilience metrics

Date	December 24th 2015
Authors	H. Kerkdijk, B.J. te Paske, E. Verweij and R. Wolthuis
Project name	Cyber resilience metrics
Project number	060.08361
Project manager	H. Kerkdijk
Sponsors	Participants in SRP Cyber Security
Classification	UNCLASSIFIED

All rights reserved.
No part of this publication may be reproduced and/or published by print, photoprint, microfilm or any other means without the previous written consent of TNO.

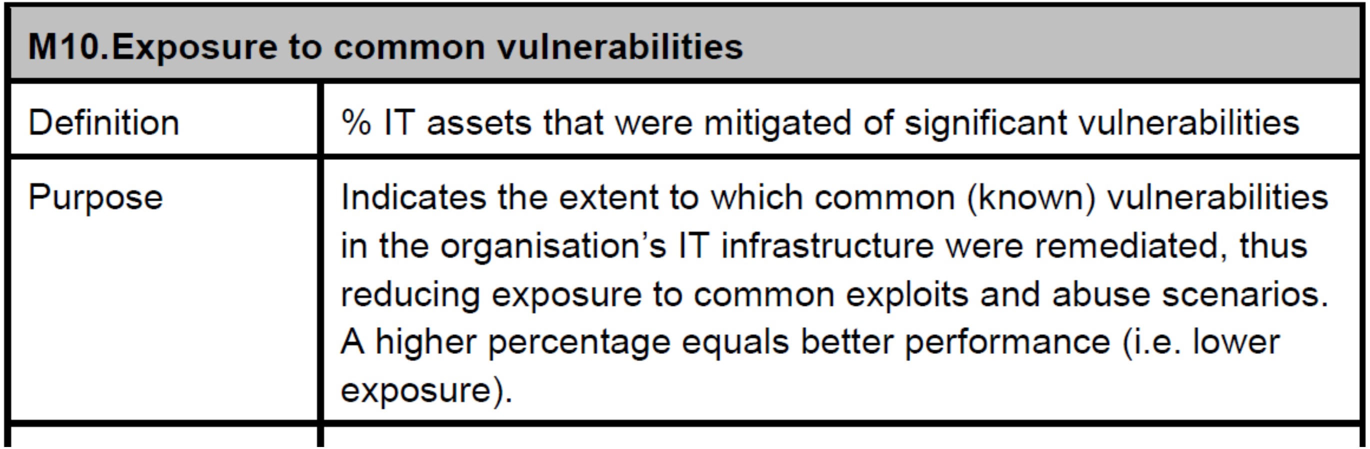
In case this report was drafted on instructions, the rights and obligations of contracting parties are subject to either the General Terms and Conditions for commissions to TNO, or the relevant agreement concluded between the contracting parties. Submitting the report for inspection to parties who have a direct interest is permitted.

© 2015 TNO

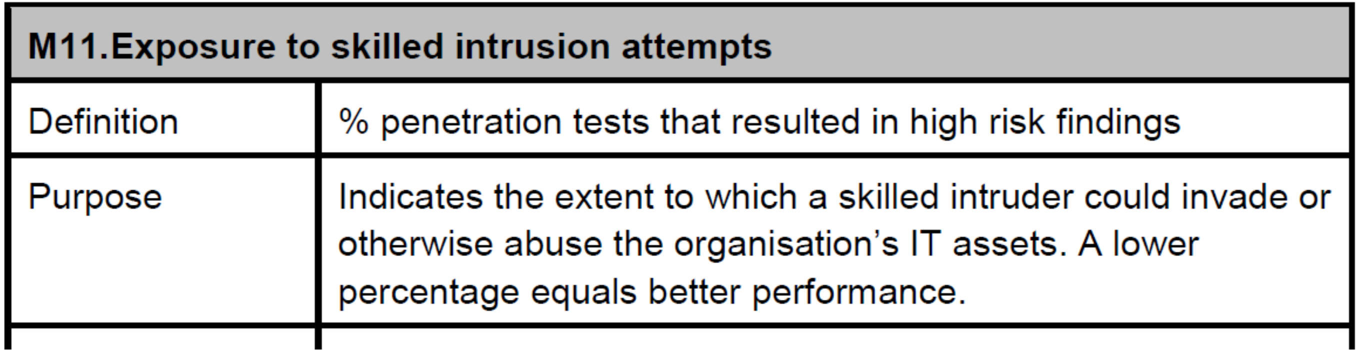


Contents

some reasonably doable

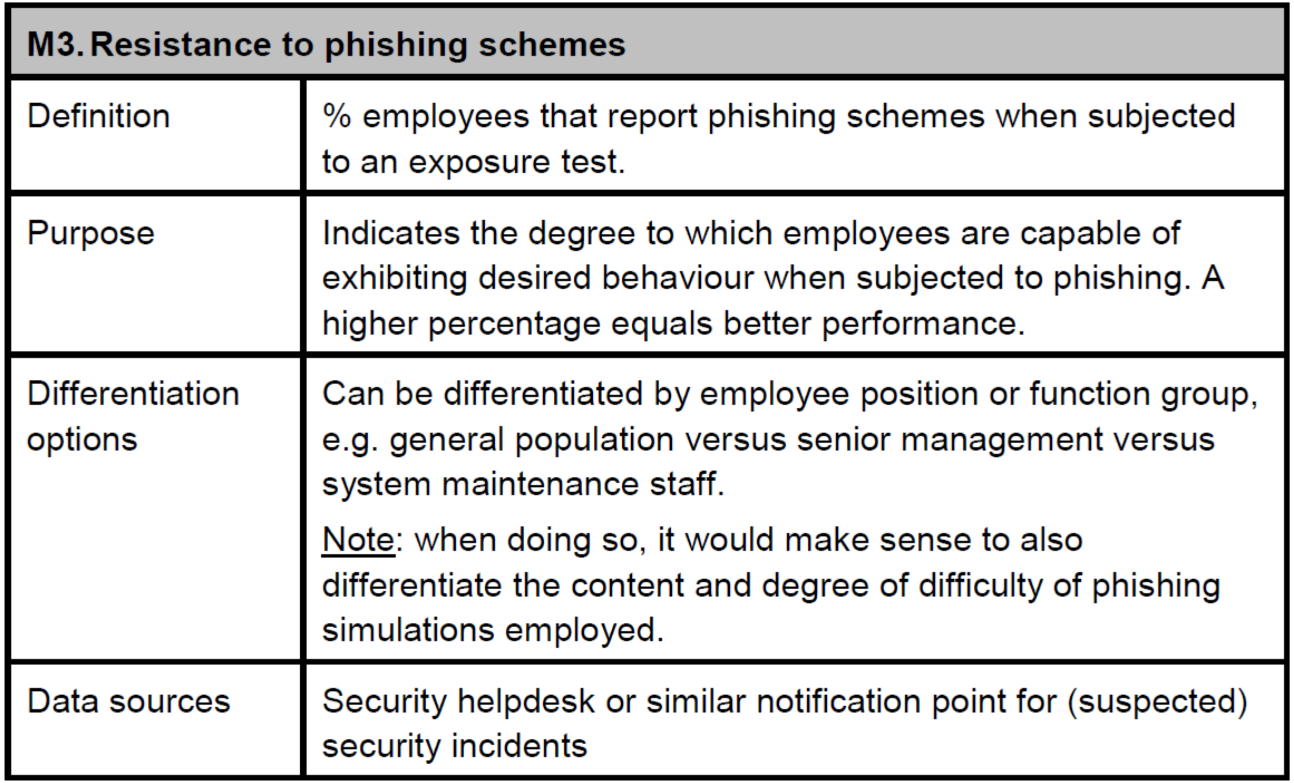


M10.Exposure to common vulnerabilities	
Definition	% IT assets that were mitigated of significant vulnerabilities
Purpose	Indicates the extent to which common (known) vulnerabilities in the organisation's IT infrastructure were remediated, thus reducing exposure to common exploits and abuse scenarios. A higher percentage equals better performance (i.e. lower exposure).



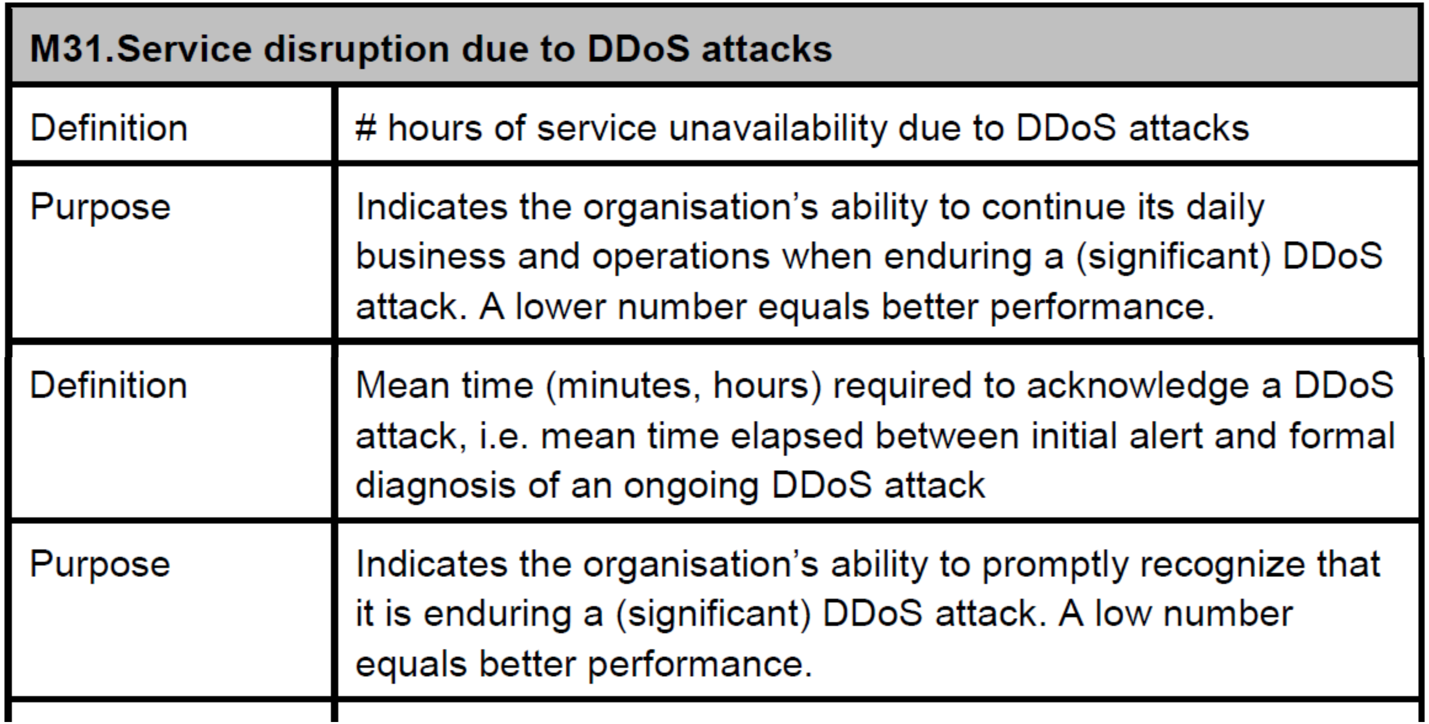
M11.Exposure to skilled intrusion attempts	
Definition	% penetration tests that resulted in high risk findings
Purpose	Indicates the extent to which a skilled intruder could invade or otherwise abuse the organisation's IT assets. A lower percentage equals better performance.

others less trivial



M3. Resistance to phishing schemes	
Definition	% employees that report phishing schemes when subjected to an exposure test.
Purpose	Indicates the degree to which employees are capable of exhibiting desired behaviour when subjected to phishing. A higher percentage equals better performance.
Differentiation options	Can be differentiated by employee position or function group, e.g. general population versus senior management versus system maintenance staff. Note: when doing so, it would make sense to also differentiate the content and degree of difficulty of phishing simulations employed.
Data sources	Security helpdesk or similar notification point for (suspected) security incidents

Oversight vs detail



M31.Service disruption due to DDoS attacks	
Definition	# hours of service unavailability due to DDoS attacks
Purpose	Indicates the organisation’s ability to continue its daily business and operations when enduring a (significant) DDoS attack. A lower number equals better performance.
Definition	Mean time (minutes, hours) required to acknowledge a DDoS attack, i.e. mean time elapsed between initial alert and formal diagnosis of an ongoing DDoS attack
Purpose	Indicates the organisation’s ability to promptly recognize that it is enduring a (significant) DDoS attack. A low number equals better performance.

Lessons learned

- *effect oriented metrics that reflect cyber resilience capabilities offers value but such metrics are often hard to measure.*
- *Stakeholders are rarely interested in the full set of cyber resilience metrics.*
- *Embracing the full set of cyber resilience metrics is challenging and perhaps to much. (less is more….)*
- *Comparing actual cyber resilience measurements across organisations requires a level of alignment that is presently not in place.*
- *Set of metrics focusses on content. Converting it to fancy pictures is not included but necessary to attract public.*

Way forward

1. Choose feasible metrics
2. Collect data
3. Compare over time ➔ benchmark against yourself
4. Share experiences amongst SRP partners
5. Choose metrics to benchmark with partners

Final remarks

- Questions?
- Download Security Metrics document?
- Participate in Shared research program?

https://www.tno.nl/nl/samenwerken/partners-van-tno/shared-research-programme-cybersecurity/