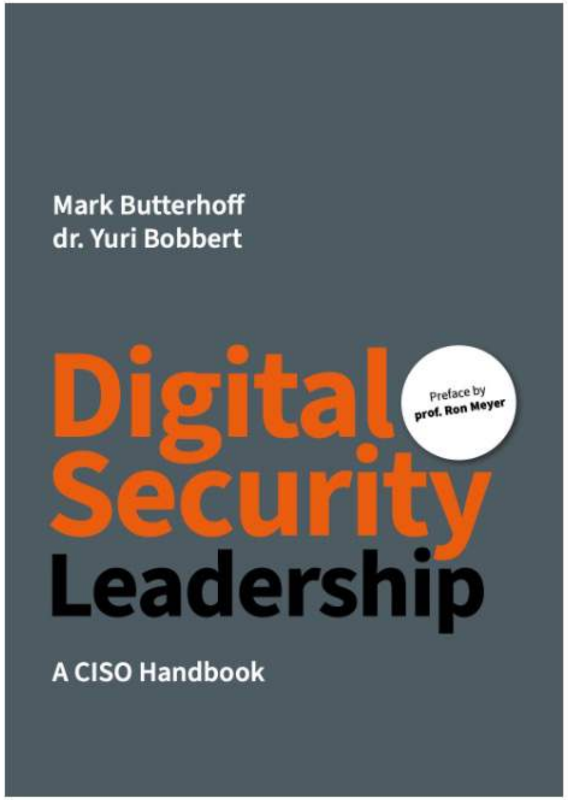
Digital Security Leadership

Mark Butterhoff
19 March 2025


Mark Butterhoff
dr. Yuri Bobbert

Digital Security Leadership

Preface by prof. Ron Meyer

A CISO Handbook

Who am I?

Discover the IT Cherry

How to become the most valued cherries

De IT Kersen sensatie

Mark Butterhoff
Barry Derksen
Aart van der Vlist

Mark Butterhoff
dr. Yuri Bobbert

Digital Security Leadership

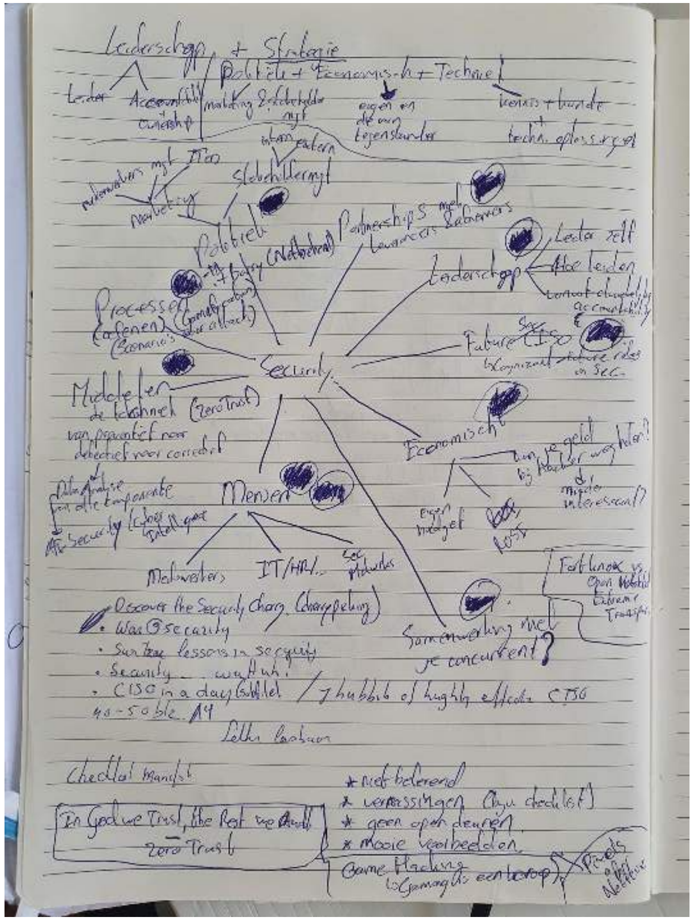
A CISO Handbook

KPMG

BAUHAUS ARTITECH

VU UNIVERSITY AMSTERDAM

inc
I'm in control


Leiderschap + Strategie
Politiek + Economisch + Techniek
Leider
Accountability + ownership
marketing & stakeholder mgt
eigen en die van tegenstander
kennis + kunde + techn. oplossingen
intern / extern
stakeholdermgt
medewerkers mgt / ITeo
marketing
Politiek
Partnerships met leveranciers & afnemers
Leider zelf
Hoe leiden
Leiderschap
context ownership accountability
Processen (oefenen) (Scenario's)
(Gamification of an attack)
Future Sec CISO
Security
Middelen
de techniek (Zero Trust)
van preventief naar detectief naar correctief
Data Analyse van alle componente
Security Intelligence
Mensen
Medewerkers
IT/HR/..
Sec afdelingen
Economisch
kun je geld bij hacker weghalen?
minder interessant?
eigen budget
kost
Samenwerking met je concurrent?
Fort Knox vs open
Checklist Manifest
In God we Trust, the Rest we Audit
Zero Trust
Game Hacking
Pixels of Niet

- Discover the Security Charm (Charm offensive)
- War @ security
- Sun Tzu lessons in security
- Security ... wa huh!
- CISO in a day / 7 habits of highly effective CISO

40-50 blz A4

* niet belerend
* verrassingen (bijv. checklist)
* geen open deuren
* mooie voorbeelden

What started with an idea

Why this book?

WRONG
FOCUS

The problem we all face

- Increase in cyber security threats
- Increase in compliance pressure
- Complex landscape to secure
- Insufficient skilled staff
- Budgetpressure
- ....and all the rest....

How we usually solve these issues

HIRING MORE AND MORE (UNSKILLED) STAFF

- MORE IS LESS -

DEFINE MORE POLICIES, PROCEDURES AND PROCESSES

- PEOPLE WILL ALWAYS FOLLOW RULES -

FOCUS ON COMPLIANCY NOT ON SECURITY

COMPLIANCE ≠ SECURE

USE NON-COMPLIANCES TO GET MORE BUDGET

- MORE PRESSURE INCREASES WILLING TO CORPORATE -

WANTING TO CHANGE PEOPLE IN “HUMAN FIREWALLS”

- THE END USER IS THE KEY TO SUCCESS -

BUY MORE “FLASHY” TOOLS AND SERVICES

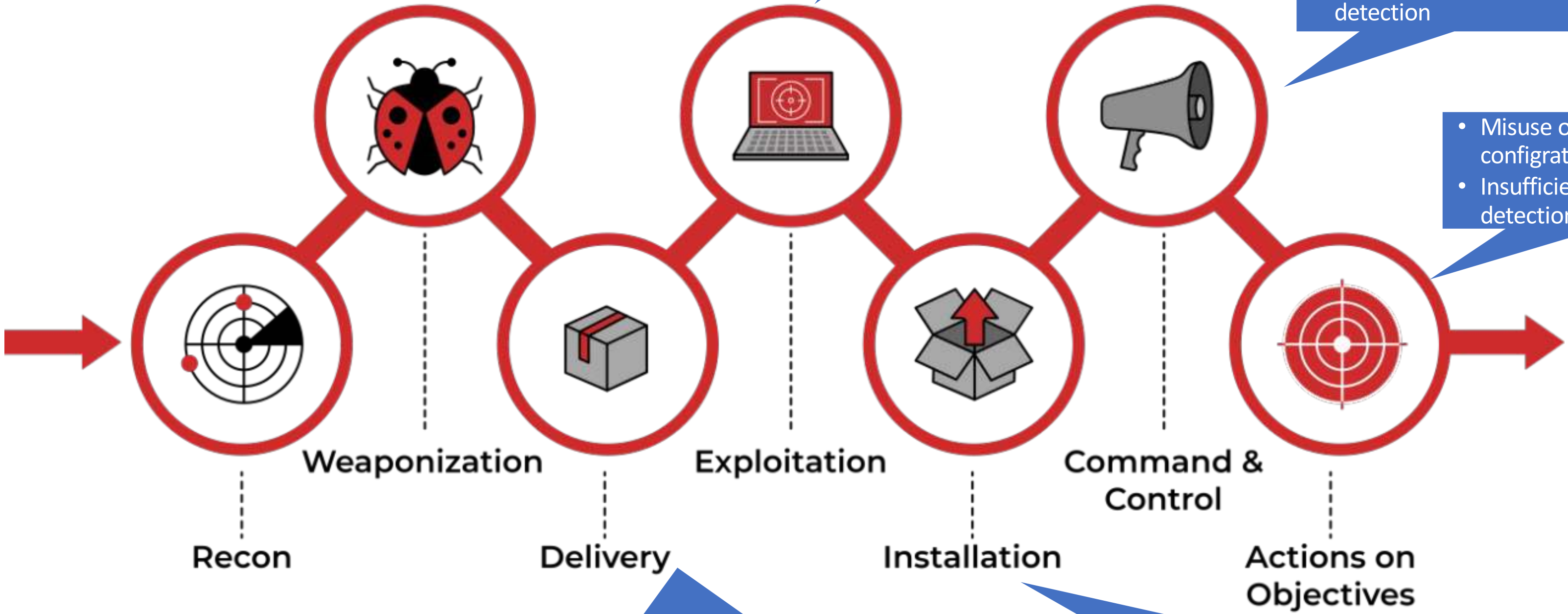
- TOOLS PREVENT US FROM BEING HACKED -

The result?

- More security staff creates more work….for others to execute
- A security function that is a risk management-role (assessments, monitor progress and report), which is very inefficient
- More tools that people don’t know or don’t want to work with

And allthough we might be certified and compliant – we still get hacked

The reason we get hacked



- Misuse of insecure coding, configration / lack of hardening
- Misuse of vulnerabilities in software

- Misuse of insecure coding, configration / lack of hardening
- Insufficient monitoring & detection

- Misuse of insecure coding, configration / lack of hardening
- Insufficient monitoring & detection

- User makes a mistake
- Mail Gateway does not detect phish
- Computer is not sufficiently hardened

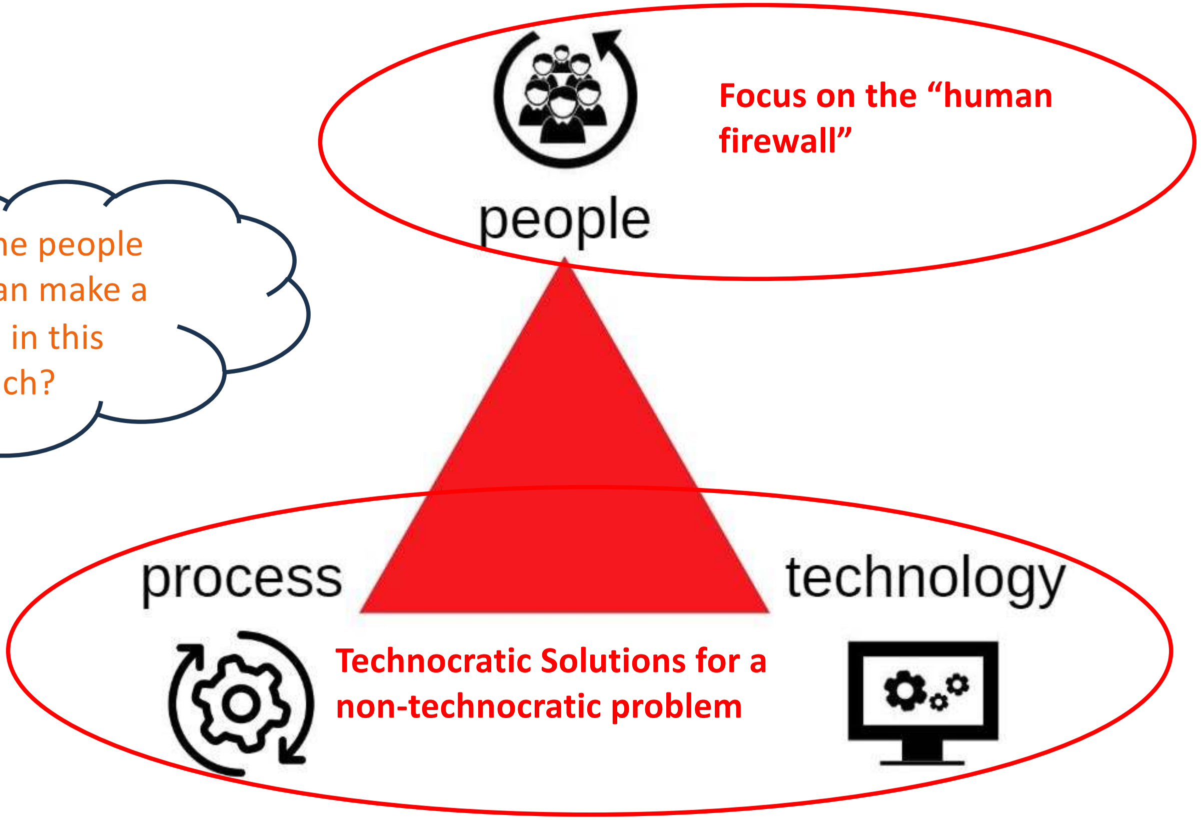
- Misuse of insecure coding, configration / lack of hardening
- Insufficient monitoring & detection

No Influence

Much Influence

Main focus in Information Security

Where are the people that actual can make a difference in this approach?



people

Focus on the “human firewall”

process

technology

Technocratic Solutions for a non-technocratic problem

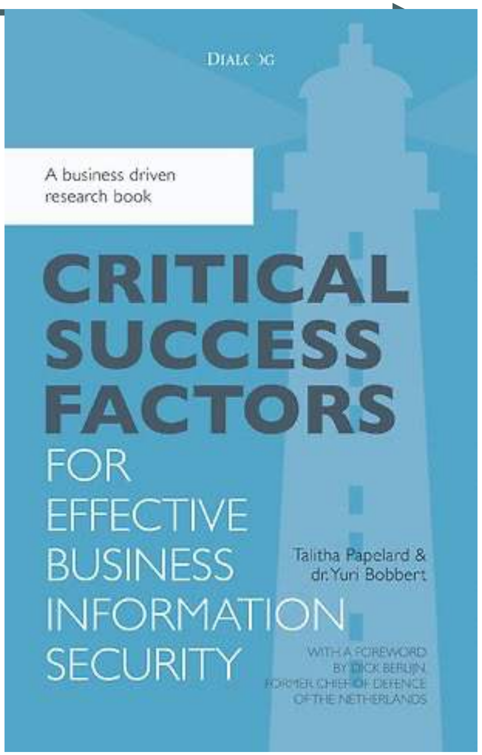
What are the Main Critical Success factors for Digital Security?

- ❑ Management & Board Commitment
- ❑ Creating a Security Aware Culture
- ❑ The quality at the top (leadership)
- ❑ Cultivating lessons learned

Years have passed and we still see any significant change in the way digital security is led, managed, and/or implemented.

Human "error" is still the main cause of security incidents leading to e.g. data breaches and ransomware

Budgets are still mainly focused on technology and services and not improving behavior and culture…….including the one of IT staff



A business driven research book

CRITICAL SUCCESS FACTORS FOR EFFECTIVE BUSINESS INFORMATION SECURITY

Talitha Papelard & dr.Yuri Bobbert

WITH A FOREWORD BY DICK BERLIJN FORMER CHIEF OF DEFENCE OF THE NETHERLANDS

The Book

Leading

About the digital security leader and about how to lead the company through the cybersecurity challenges. Also, on how the CISO role emerges to a Chief Information Security Orchestrator balancing and leading multiple stakeholders

Strategizing

How to bring the security maturity from the current to the future state, considering the *technical*, *economical* and *political* aspects

Changing

Changing the people working in digital security and the people who need to act in a secure manner

Governing

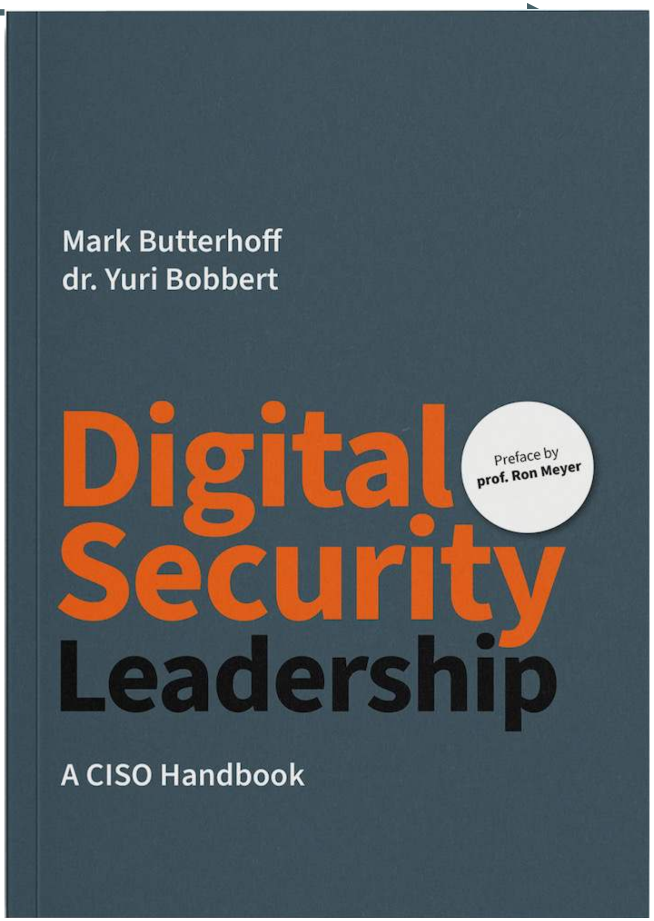
Tangible practices and metrics to measure and govern your digital security as well as the way to work practically and proactively with your governance, including regulators

Funding

All change has financial consequences that stakeholders want to know about and understand. With economic models we bring more rational arguments, which enables more balanced decision-making and, in the end, more "bang for your buck."

Trending

Possible digital security future in Trending, because as a wise man once said: "It's not the strongest of the species that survives, nor the most intelligent that survives. It's the one that is most adaptable to change".



Mark Butterhoff
dr. Yuri Bobbert

Digital Security Leadership

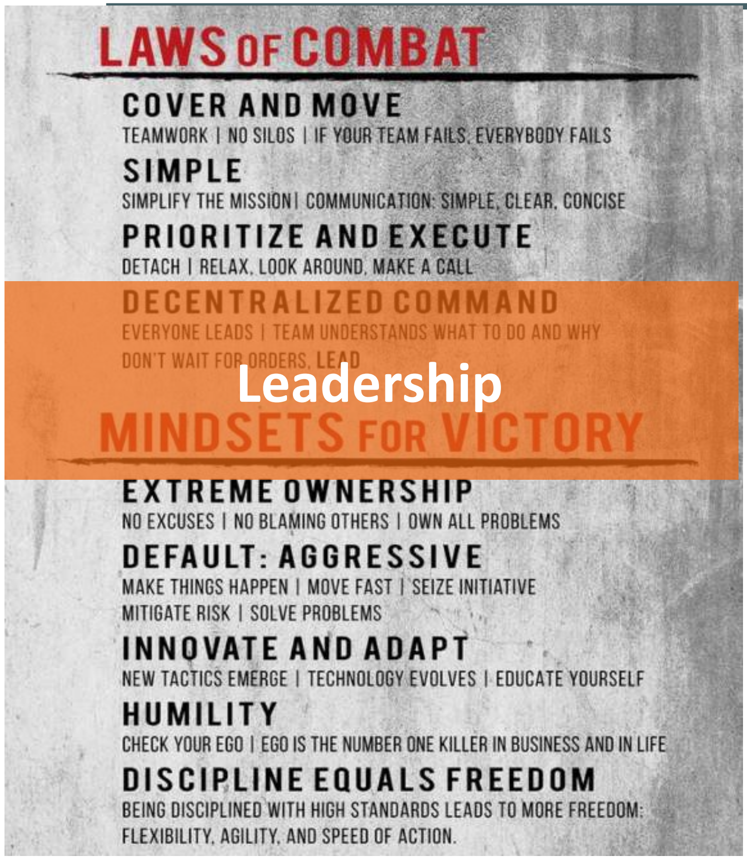
Preface by prof. Ron Meyer

A CISO Handbook

Operations Checklist
CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

Sneak Peek

Leadership



LAWS OF COMBAT

COVER AND MOVE

TEAMWORK | NO SILOS | IF YOUR TEAM FAILS, EVERYBODY FAILS

SIMPLE

SIMPLIFY THE MISSION| COMMUNICATION: SIMPLE, CLEAR, CONCISE

PRIORITIZE AND EXECUTE

DETACH | RELAX, LOOK AROUND, MAKE A CALL

DECENTRALIZED COMMAND

EVERYONE LEADS | TEAM UNDERSTANDS WHAT TO DO AND WHY

DON'T WAIT FOR ORDERS, LEAD

Leadership

MINDSETS FOR VICTORY

EXTREME OWNERSHIP

NO EXCUSES | NO BLAMING OTHERS | OWN ALL PROBLEMS

DEFAULT: AGGRESSIVE

MAKE THINGS HAPPEN | MOVE FAST | SEIZE INITIATIVE

MITIGATE RISK | SOLVE PROBLEMS

INNOVATE AND ADAPT

NEW TACTICS EMERGE | TECHNOLOGY EVOLVES | EDUCATE YOURSELF

HUMILITY

CHECK YOUR EGO | EGO IS THE NUMBER ONE KILLER IN BUSINESS AND IN LIFE

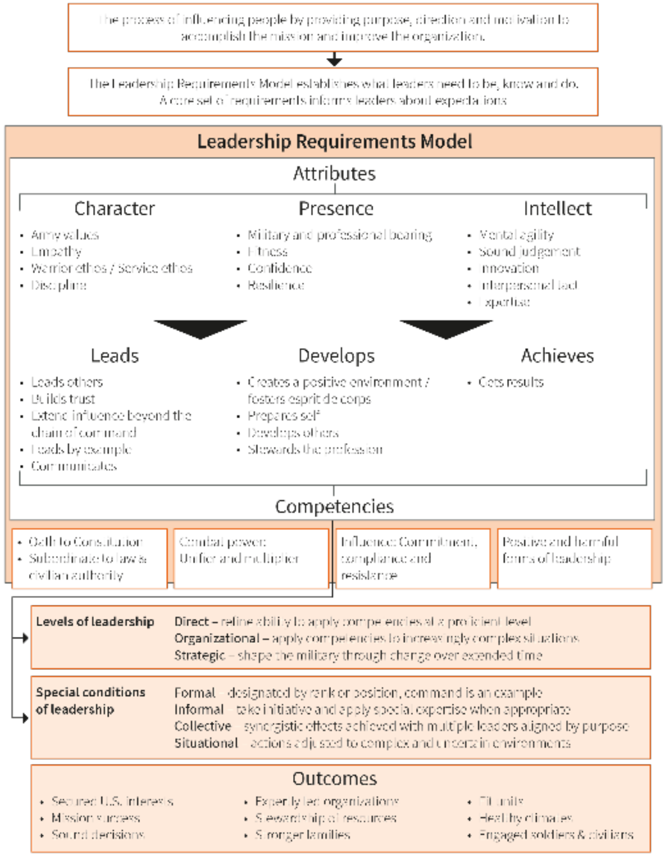
DISCIPLINE EQUALS FREEDOM

BEING DISCIPLINED WITH HIGH STANDARDS LEADS TO MORE FREEDOM: FLEXIBILITY, AGILITY, AND SPEED OF ACTION.

'The art of getting someone else to do something you want done because he wants to do it' (Dwight D. Eisenhower)

- **Other people**, which means that it's not about the leader in isolation, but about the interaction between leader and followers, not about what the leader does, but also how the followers react.'
- **Influencing**, which ranges from using formal powers, such as hire, fire, reward, reprimand and reassign, to informal powers such as the ability to convince, charm, inspire, support and challenge. Informal powers are usually more effective and more lasting than formal powers.
- **Is capable of** and willing to influence followers. leaders must be willing to take the responsibility of the leadership role and invest in winning authority among potential followers.
- **To move in a certain direction** and to realize objectives. It's not the goal to gain powers as an end in itself, but as a means toward achieving objectives. (Ron Meyer and Ronald Meijers)

Leadership Requirements



The process of influencing people by providing purpose, direction and motivation to accomplish the mission and improve the organization.

The Leadership Requirements Model establishes what leaders need to be, know and do. A core set of requirements informs leaders about expectations

Leadership Requirements Model

Attributes

Character
- Army values
- Empathy
- Warrior ethos / Service ethos
- Discipline

Presence
- Military and professional bearing
- Fitness
- Confidence
- Resilience

Intellect
- Mental agility
- Sound judgement
- Innovation
- Interpersonal tact
- Expertise

Leads
- Leads others
- Builds trust
- Extend influence beyond the chain of command
- Leads by example
- Communicates

Develops
- Creates a positive environment / fosters esprit de corps
- Prepares self
- Develops others
- Stewards the profession

Achieves
- Gets results

Competencies

- Oath to Constitution
- Subordinate to law & civilian authority

Combat power: Unifier and multiplier

Influence: Commitment, compliance and resistance

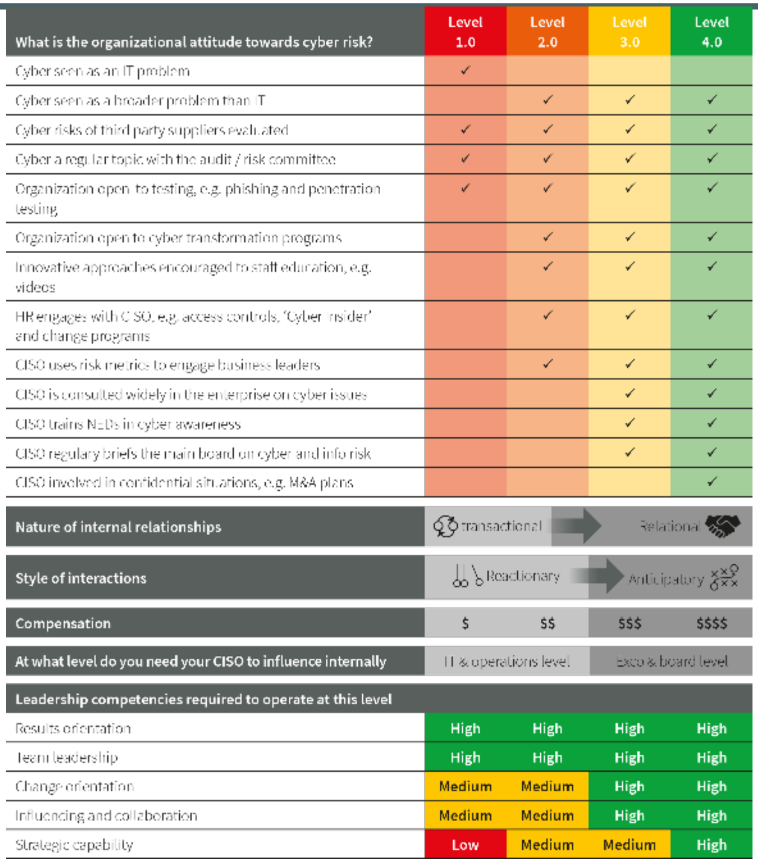
Positive and harmful forms of leadership

Levels of leadership
Direct – refine ability to apply competencies at a proficient level
Organizational – apply competencies to increasingly complex situations
Strategic – shape the military through change over extended time

Special conditions of leadership
Formal – designated by rank or position, command is an example
Informal – take initiative and apply special expertise when appropriate
Collective – synergistic effects achieved with multiple leaders aligned by purpose
Situational – actions adjusted to complex and uncertain environments

Outcomes
- Secured U.S. interests
- Mission success
- Sound decisions
- Expertly led organizations
- Stewardship of resources
- Stronger families
- Fit units
- Healthy climates
- Engaged soldiers & civilians

Underlying logic of Army leadership (taken from ADRP 6.22, Army Leadership – August 2019, Headquarters, Department of the Army)



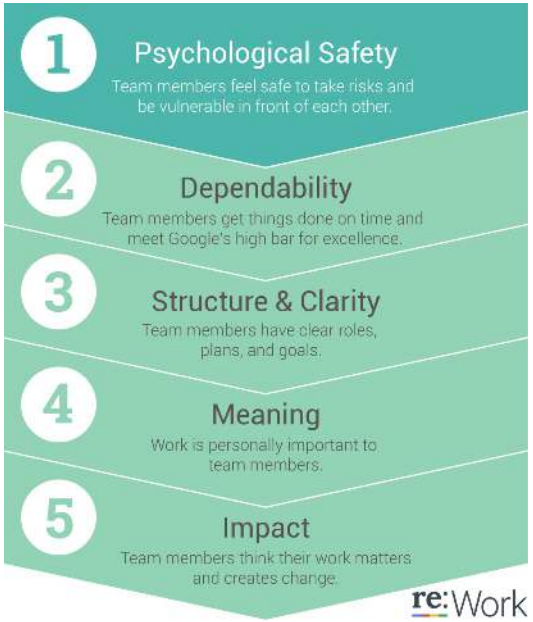
What is the organizational attitude towards cyber risk?	Level 1.0	Level 2.0	Level 3.0	Level 4.0
Cyber seen as an IT problem	✓			
Cyber seen as a broader problem than IT		✓	✓	✓
Cyber risks of third party suppliers evaluated	✓	✓	✓	✓
Cyber a regular topic with the audit / risk committee	✓	✓	✓	✓
Organization open to testing, e.g. phishing and penetration testing	✓	✓	✓	✓
Organization open to cyber transformation programs		✓	✓	✓
Innovative approaches encouraged to staff education, e.g. videos		✓	✓	✓
HR engages with CISO, e.g. access controls, 'Cyber insider' and change programs		✓	✓	✓
CISO uses risk metrics to engage business leaders		✓	✓	✓
CISO is consulted widely in the enterprise on cyber issues			✓	✓
CISO trains NEDs in cyber awareness			✓	✓
CISO regulary briefs the main board on cyber and info risk			✓	✓
CISO involved in confidential situations, e.g. M&A plans				✓
Nature of internal relationships	transactional		Relational	
Style of interactions	Reactionary		Anticipatory	
Compensation	$	$$	$$$	$$$$
At what level do you need your CISO to influence internally	IT & operations level		Exco & board level	
Leadership competencies required to operate at this level				
Results orientation	High	High	High	High
Team leadership	High	High	High	High
Change orientation	Medium	Medium	High	High
Influencing and collaboration	Medium	Medium	High	High
Strategic capability	Low	Medium	Medium	High

'CISO leadership competencies required per level (Taken from the Russell Reynolds Capability Model).'

CISO Team

I can do things you can’t, you can do things I can’t: together we can do great things

Google’s five-year study of highly productive teams



1 Psychological Safety
Team members feel safe to take risks and be vulnerable in front of each other.

2 Dependability
Team members get things done on time and meet Google's high bar for excellence.

3 Structure & Clarity
Team members have clear roles, plans, and goals.

4 Meaning
Work is personally important to team members.

5 Impact
Team members think their work matters and creates change.

re:Work

Formula 1 vital aspects of a winning culture

- A no-blame philosophy
- The one-team mindset

Teams have several key traits:

- Share a clear, common goal
- Work at building trust
- Are willing to learn and collaborate
- Communicate openly and often.'

Show them the way

Everybody has a strategy until they get punched in the mouth

Plan vs Strategy

Digital Security Strategy ≠

- Implementation of ISO27001/2
- GAP analysis with recommendations
- Improvement Activities planned in a happy flow
- Etc

Three perspectives of Strategy

Technical

Having the right people, processes and technology

Economical

Funding of Digital Security and showing value

Political

Influencing internal and external stakeholders

- Internal: Staff, Management, Board
- External: Sector, Intelligence Agencies, Regulators, etc

'Total Competition, Lessons in strategy from Formula One, Ross Brawn and Adam Parr, 2016'

I have a Dream

Compelling vision

- "*we need to comply to ISO27001 or COBIT*" is not Compelling
- Why, How and What – Simon Sinek

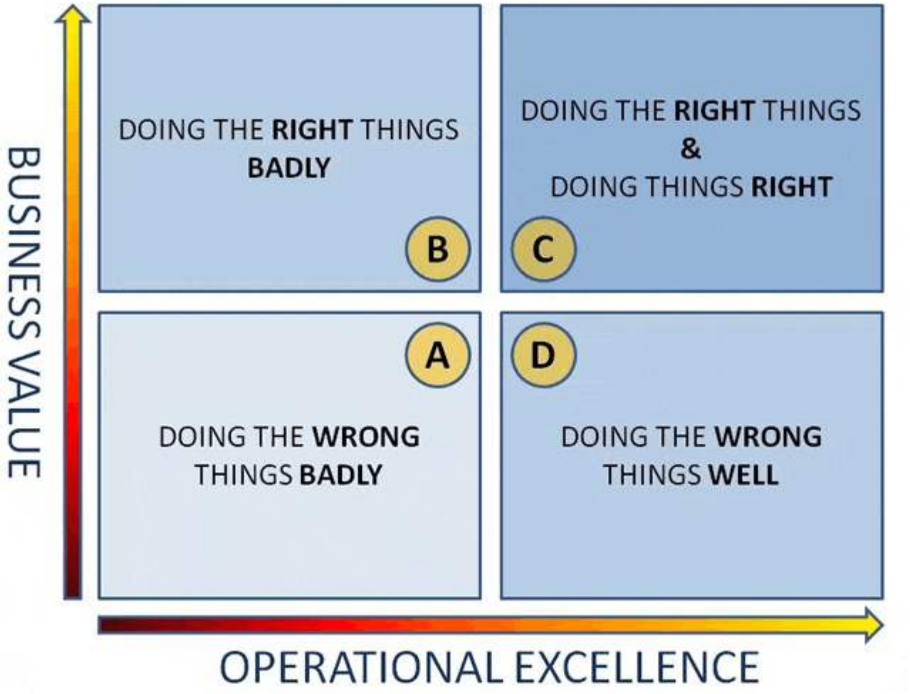
If Apple were like everyone else, a marketing message from them might sound like this:

"We make great computers. They're beautifully designed, simple to use and user friendly. Want to buy one?"

Then way Apple does it:

"Everything we do, we believe in challenging the status quo. We believe in thinking differently. The way we challenge the status quo is by making our products beautifully designed, simple to use and user friendly. We just happen to make great computers. Want to buy one?"

Security is a Change Program


DOING THE **RIGHT** THINGS **BADLY**
B
DOING THE **RIGHT** THINGS & DOING THINGS **RIGHT**
C
A
DOING THE **WRONG** THINGS **BADLY**
D
DOING THE **WRONG** THINGS **WELL**
BUSINESS VALUE
OPERATIONAL EXCELLENCE

Security is very dependent on IT staff ***doing the right things right*** every day

DISCIPLINE EQUALS FREEDOM

discipline

[dis-uh-plin] noun

Discipline is the consistency of action

(also if you don’t feel like doing it)

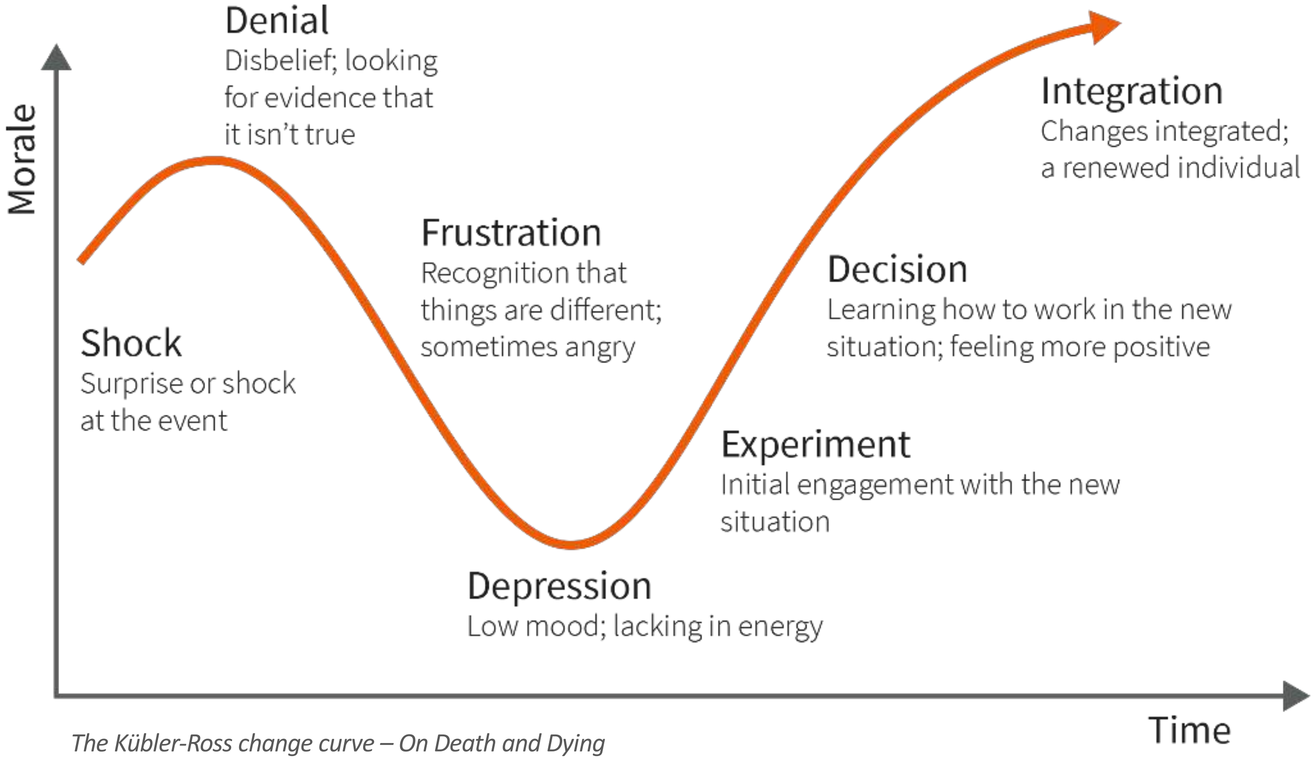
Eight reasons why Digital Security Change fails

Change Management

- Lacking a Sense of Urgency
- Lacking a Powerful Guiding Smart Coalition
- Lacking a Vision
- Under-communicating the Vision by a Factor of Ten
- Not Removing Obstacles to the New Vision
- Not Systematically Planning and Creating Short-Term Wins
- Declaring Victory too soon
- No Anchoring Changes in the Corporation’s Culture

Leading Change: Why transformation Efforts Fail, John P. Kotter, Harvard Business Review, 1994

The Change Curve



Denial
Disbelief; looking for evidence that it isn't true

Shock
Surprise or shock at the event

Frustration
Recognition that things are different; sometimes angry

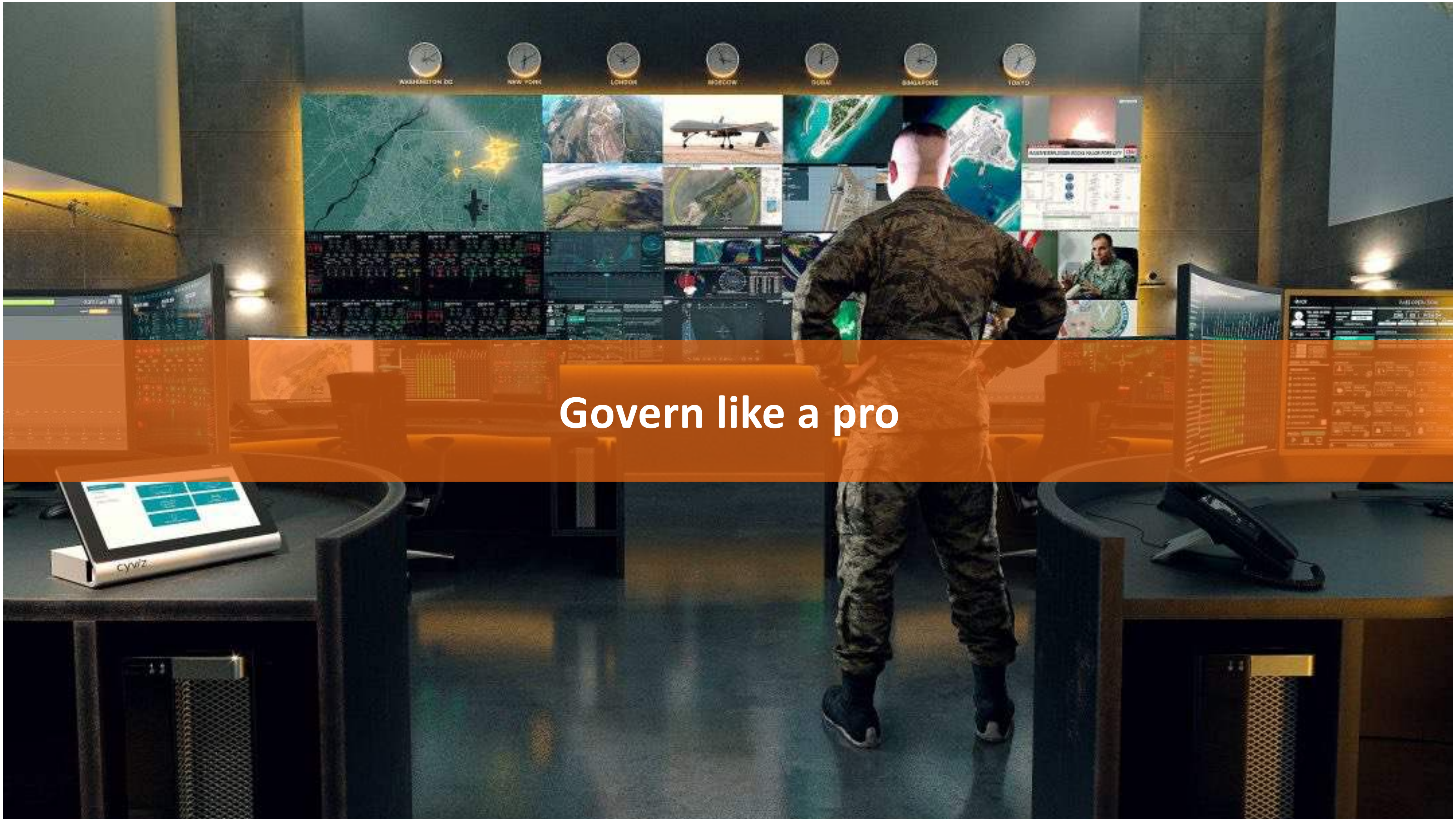
Depression
Low mood; lacking in energy

Experiment
Initial engagement with the new situation

Decision
Learning how to work in the new situation; feeling more positive

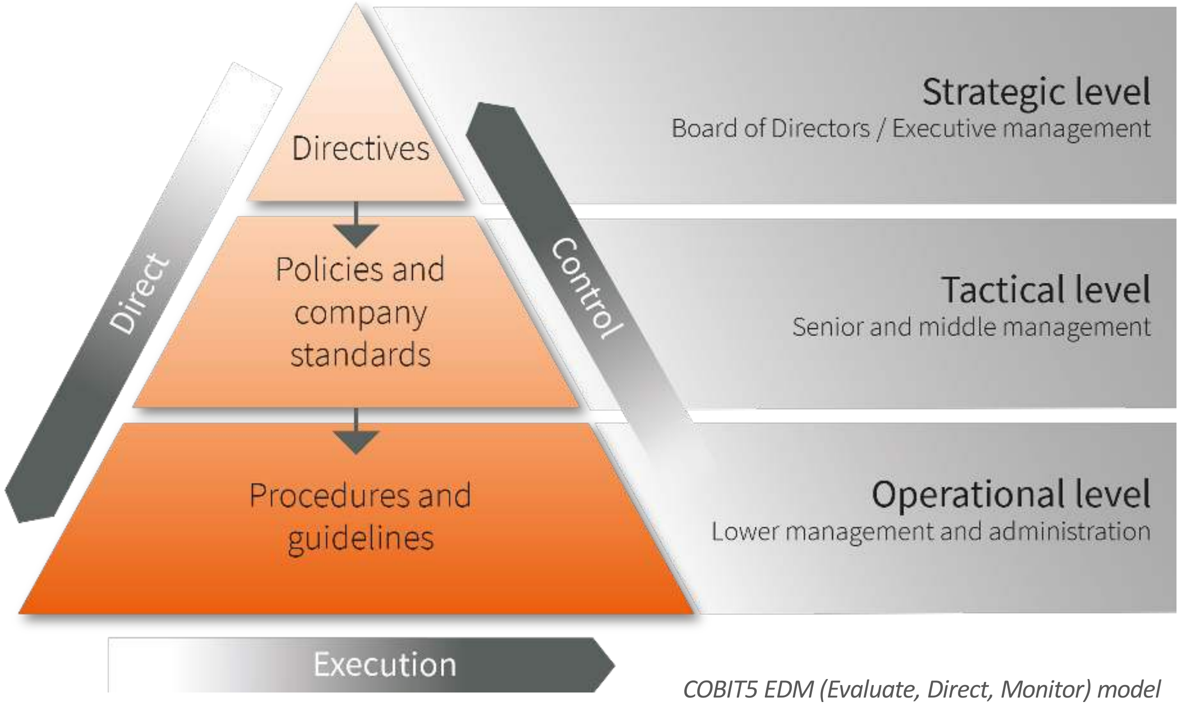
Integration
Changes integrated; a renewed individual

The Kübler-Ross change curve – On Death and Dying



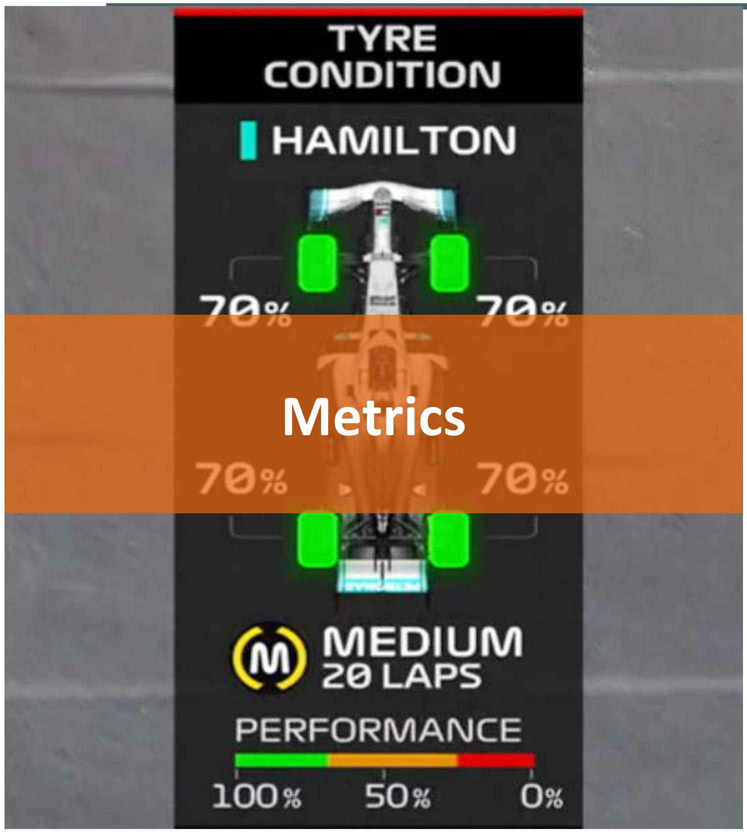
Govern like a pro

COBIT


Directives
Policies and company standards
Procedures and guidelines
Direct
Control
Execution
Strategic level
Board of Directors / Executive management
Tactical level
Senior and middle management
Operational level
Lower management and administration

COBIT5 EDM (Evaluate, Direct, Monitor) model for defining processes (taken from ISACA)

Measuring Digital Security



Measure digital security at three levels with metrics:

- Strategic Level (Board and Executive Management)
  - Overview realized vs planning improvements per period
  - Level of compliance with internal and external policies
  - Presence of a Security Organization
- Tactical Level (senior and middle management), e.g.
  - #security incidents, effectiveness of security controls, development of maturity level
  - Level of awareness at management level
  - Follow ups to previously set KPIs
- Operational Level (lower management and administration)
  - Level of awareness of security with operational personnel
  - Level of compliance with the security baseline
  - MTBF and MTTR as a result of security incidents

Note: This was an outcome of working with 38 security experts. Consider involving the Board, Business Management and end users for a different angle about what is important

Governance vs. Regulation

- If you can't win, you have to make sure you don't lose. (Johan Cruijff)
- From explaining to telling: Take Ownership!
  - Show that you own what needs to be done
  - Have a plan and show progress
- Assurance reports and ISO27001/2 certificates ≠ Being secure
  - Focussed on Financial Risk
  - Focussed on the ISMS, not the latest threats or in depth

Questions

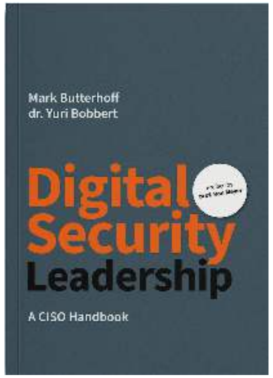
Contact details

Mark Butterhoff

Mark Butterhoff has gained experience over the last 20 years in various roles. He has a long history in one of the Big Four accounting firms, where he worked in information security, IT auditing, and management consulting. After that he worked for several years as program manager and interim manager restructuring and changing mainly IT organizations as well as a post as Interim Chief Information Security Officer. So far he has helped over 80 companies in 17 countries. Alongside his work he also teaches at the TIAS Business School in the Netherlands. Mark has completed studies in various topics, including Business Informatics and IT Auditing.

In 2016 he published a book entitled “Discover the IT Cherry,” which describes how to become the most valued IT organization by building trust and creating experiences instead of using the latest technology or implementing new processes. His experiences from work and the insights gained from writing this book were also the basis for writing this book. Solid technology and processes are massively important in cyber- security; however, they won’t help you win the war against this silent enemy. Just as in sports, the army, aviation, healthcare, etc., it’s mostly leadership and the people in your organization that make the difference.

Mark@i-inc.nl



Find Out More & Order Here:

https://12ways.net/shop/