Can you handle going down ..?

ISACA / NOREA Roundtable 1 June, 2022   Jurgen van der Vlugt

Marsh Risk Advisory,
A business of Marsh McLennan

To Do

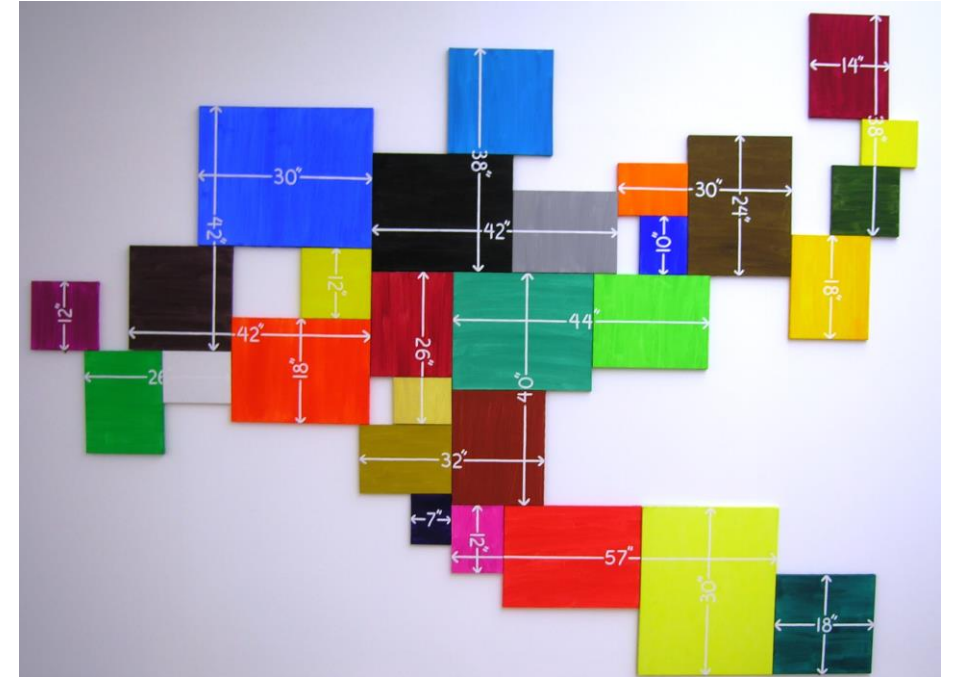| 1. Intro | 2. (No) Panic | 3. 'The Business' | 4. What about IT? | 5. Summary |

Intro

Where we stood, where we stand

Some remarks about where we are:

- Having gone through the work-from-home motions
- What's your Plan C now ..? [© Gert Kogenhop]

- Note:
  Global society on your side ↔ you're on your own again!

- E.g., Rw keeps on exploding

- Have you updated your BCPs already ..?

(No) Panic
The Whack-a-Mole approach

- Running from hype to hype; boy cried 'Wolf'

- [So now already, many think they're OK
  since they survived the physical-office outage]

- BAU is moving towards EoL:
  - ISO 27001 = ... "Who has anything slightly good on <name your subject>?"
  - Setting *boundary* conditions ... To make perfectly square wheels / concrete life vests
  - So much focus on C, with a bit of I (data and systems) → Prevention; better be safe than sorry
  - But A in the opposite! → Provision, you'll be sorry you overly saved me

- ISO 31000: Ermm... Piecemeal approach (4 treatments!?)

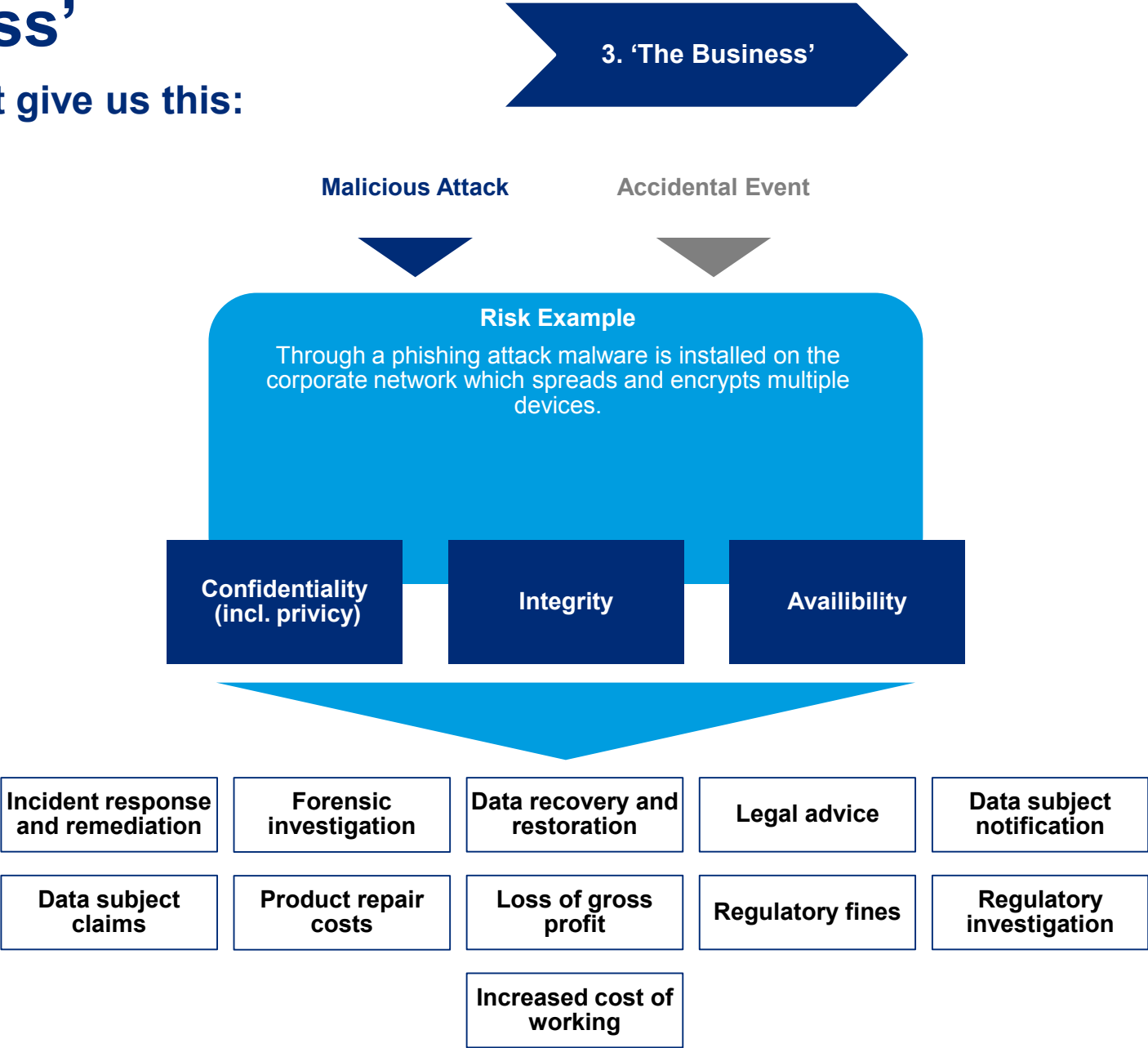- RM1 = compliance oriented
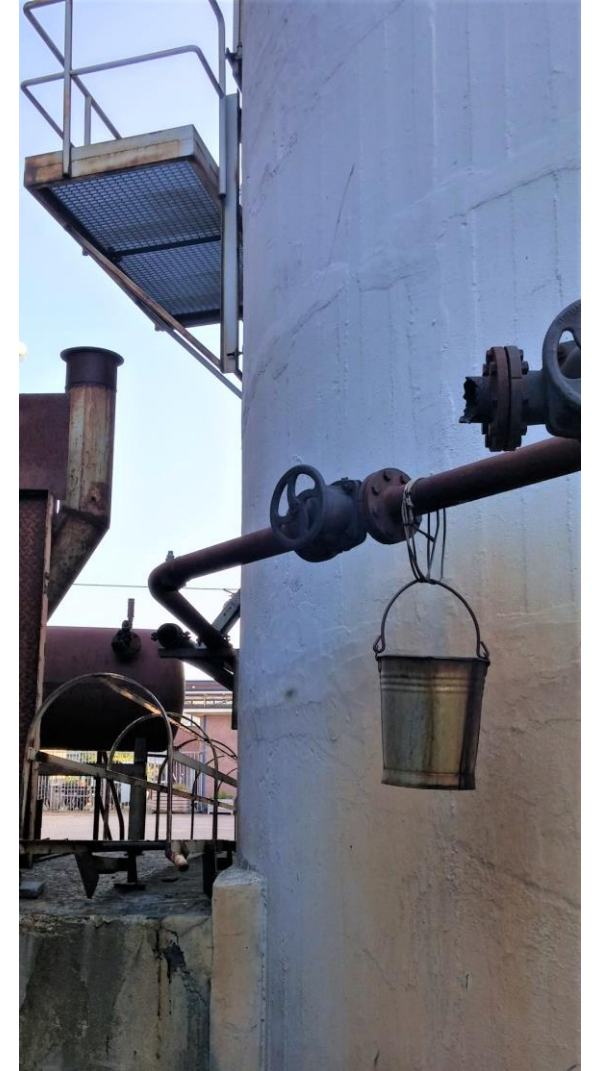
'The Business'

Is what ..?

- Toyota versus the other car makers

- Business processes are the raison d'être of any IT (even when provided aaS)

- Capital, People, Technology (last)

- What scenarios (IT cause, busn damages), what gives?

Marsh

'The Business'

Whatever. Just don't give us this:

Malicious Attack   Accidental Event

Risk Example

Through a phishing attack malware is installed on the corporate network which spreads and encrypts multiple devices.

Confidentiality (incl. privicy)	Integrity	Availibility

Incident response and remediation	Forensic investigation	Data recovery and restoration	Legal advice	Data subject notification
Data subject claims	Product repair costs	Loss of gross profit	Regulatory fines	Regulatory investigation
		Increased cost of working		

Eat Your Greens, too

And Plan B is only the yellow

Marsh
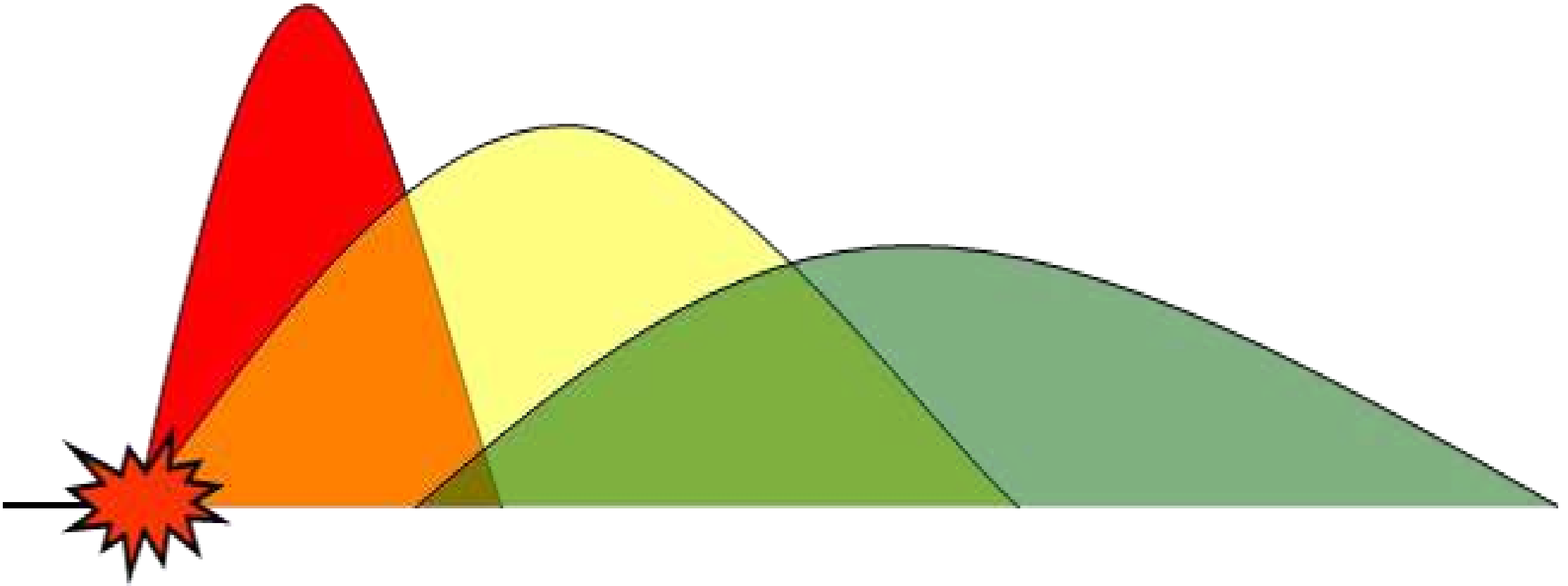
Quantify. Improve.

Be safe, then save. *And* insure

Probability Density Function Scenario 3

Most Likely Realization; 59.430

50%; 315.074

75%; 570.789

90%; 856.072

95%; 1.033.903

Relative Probability

Loss

Scenario 3 Loss Causes

Loss Cause	%
Third party liability	18,4%
Increased cost of working	16,9%
Regulatory investigation	2,1%
Loss of gross profit	42,5%
Data subject notification	0,5%
Legal advice	3,4%
Data recovery and restoration	0,7%
Forensic investigation	5,4%
Incident response and remediation	10,2%

[* Just your regular malware attack]

Marsh

8

Who cares ..?

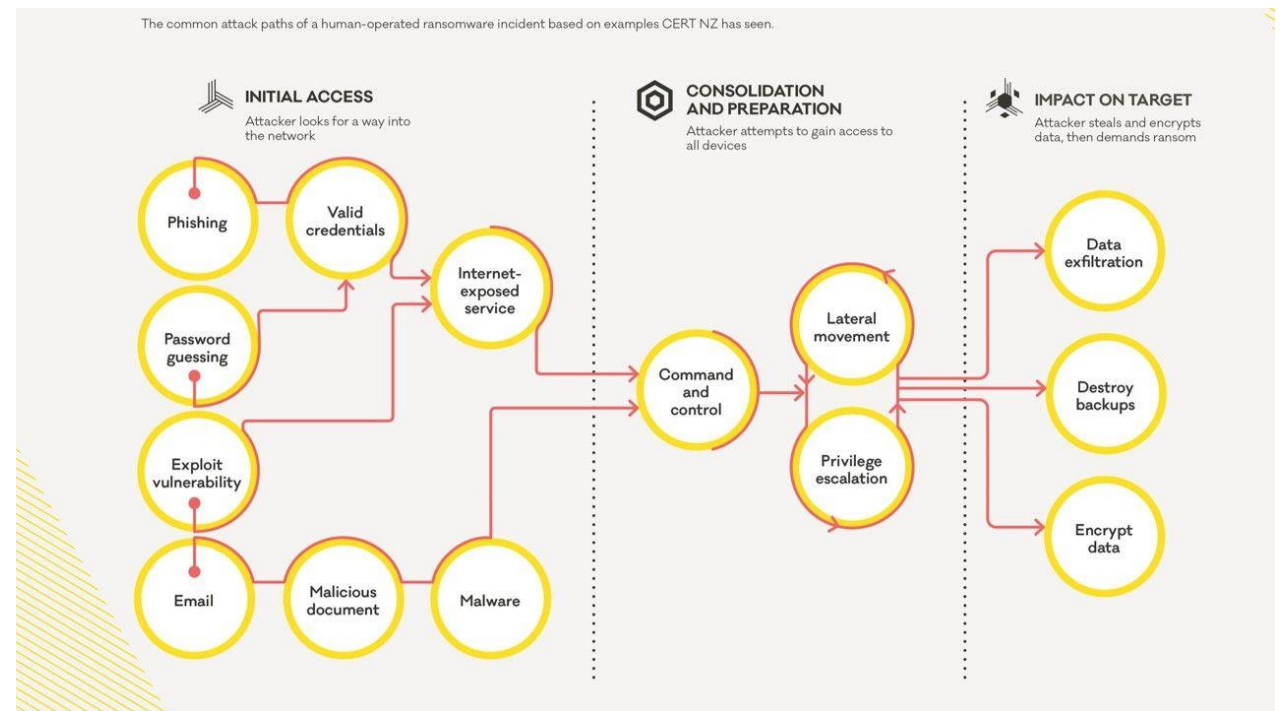## IT go figure it out yourself (?)

Hm, I may have gone overboard:

- Cyber threats are real. Something-something in Eastern (Central ..?) Europe

- "IT butterflies" – even beyond

However, leading should be:

- Vision, mission, strategy, objectives ...

- Assumptions, boundary conditions

- Controls to keep risks to ,, ,, in check

- Controls to keep risks to controls in check

- Etc.

- *RM2 ..!*

The common attack paths of a human-operated ransomware incident based on examples CERT NZ has seen.

INITIAL ACCESS — Attacker looks for a way into the network

CONSOLIDATION AND PREPARATION — Attacker attempts to gain access to all devices

IMPACT ON TARGET — Attacker steals and encrypts data, then demands ransom

Phishing · Valid credentials · Internet-exposed service · Password guessing · Exploit vulnerability · Email · Malicious document · Malware · Command and control · Lateral movement · Privilege escalation · Data exfiltration · Destroy backups · Encrypt data
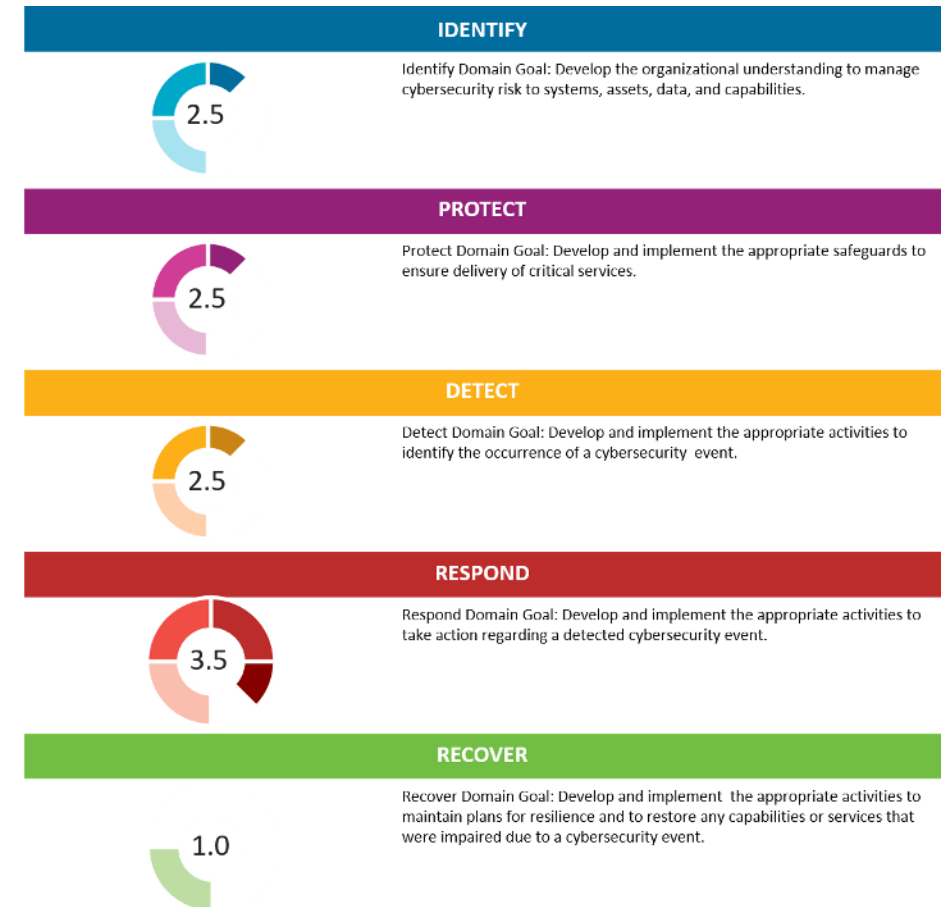
[Yeah, plucked from a LI post]

Who cares

Part II, the Colby's

Plus the staple Control Objectives / Controls cascade, P-P-T, Prev-Detect-... and/or the CSF 5*, and/or ...

Smart control design:

- Treat/Mitigate → Freq of threats, impact of vulnerabilities

- Transfer / share

- Avoid
- Accept/Retain

- Insurance
  On top of the above
  To avoid fat tail fatalities

- And still a lot to do (CIS Top-12 for insurance)

- Too little (tech) controls → expensive insurance

IDENTIFY
2.5
Identify Domain Goal: Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

PROTECT
2.5
Protect Domain Goal: Develop and implement the appropriate safeguards to ensure delivery of critical services.

DETECT
2.5
Detect Domain Goal: Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

RESPOND
3.5
Respond Domain Goal: Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

RECOVER
1.0
Recover Domain Goal: Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

WIP re kill chain et al.

Scene function	Script action	Increase the Effort	Increase the Risks	Reduce the Rewards	Reduce Provocation	Remove Excuses
Preparation	Deliberately gaining access to organisation	Prospective employment screening (4)				
Entry	Already authorised as employee	—				
Pre-condition	Wait for employees absence from offices	Physical segregation of duties (4) Staggered breaks (4)	Signing in/out of offices (8)			
Instrumental Pre-condition	Access colleagues' computers	System time outs (2) Biometric fingerprint authentication (2)				Information security polices (21) Security education (24)
Instrumental Initiation	Access programmes	Password use for access to specific programmes (2)				
Instrumental Actualization	False customer account construction		Two person sign-off on new accounts (9)			
Doing	Authorisation of fictitious invoices		Audit of computer logs (8) Budget monitoring (8)			
Post Condition	Exit programmes		—			
Exit	Exit system		User event viewer (8)			
Doing Later	Spend the transferred money					

[Intermission] Better controls design

We need that. They exist, far, far away[1] from here

Remember, 'your' users (co-workers and you) are psych(ological being)s

[1] https://shrek.fandom.com/wiki/Far_Far_Away

[Intermission] Designing controls

Straightjacket – by and for the boss ..?

[Intermission] Roam free

Within bounds – for all

[Intermission] Monitoring

'Tripwire' controls

- Checklists are OK

- *IF* they focus on tripwire controls: Typical indicators of OK

- *Else* form over substance

- Dashboard to HUD *and* where's the steering wheel *?*

- Don't start me on 'heat maps'

Insurance co's tripwires

It's a choice. A smart one.

Multifactor authentication for remote access and admin/privileged controls

Endpoint Detection and Response (EDR)

Secured, encrypted, and tested backups

Privileged Access Management (PAM)

Email filtering and web security

Patch management and vulnerability management

Cyber incident response planning and testing

Cybersecurity awareness training and phishing testing

Hardening techniques, including Remote Desktop Protocol (RDP) mitigation

Logging and monitoring/network protections

End-of-life systems replaced or protected

Vendor/digital supply chain risk management

Marsh

And they lived happily ever after

[Fairy tale]

- *Don't panic everyone!!!*

- Train like you fight,
  then you'll fight like you trained

- Then you can rest assured,
  that you can handle going down.

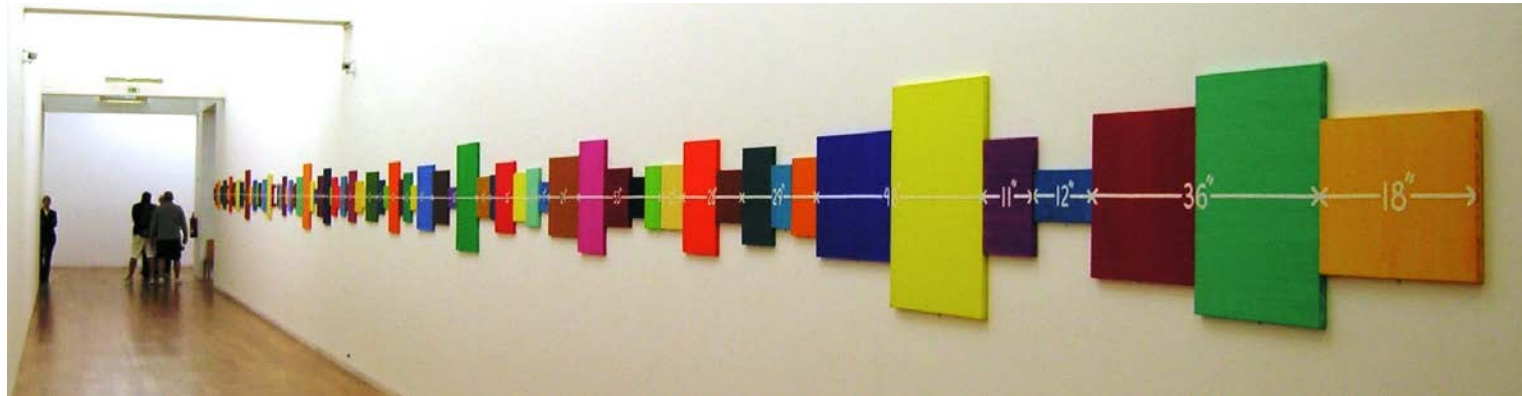# Summary

Should've started here...

1. Intro	2. (No) Panic	3. 'The Business'	4. What about IT?	5. Summary

1. Don't go chasing ever shifting cyber windmills

2. Focus on Continuity – *of the business!*

3. Get ready to
   - Analyse, with 2. in mind
   - Quantify , with 2. in mind
   - Actually improve; smarter controls, with 2. in mind
   - Insure, mind you

Thank you

Marsh

Ir.drs. J. van der Vlugt CISA CRISC (em.RE)

Jurgen van der Vlugt is Senior Consultant with Marsh McLennan, in the Cybersecurity Risk Consultants' team. He advises clients on cyber risks, governance and the improvement of their cyber risk profile.
Jurgen has a background in IS auditing and advisory. As an independent consultant, he advised a large number of clients on optimal GRC, operational risk management, cyber security and privacy. This included e.g., Secura, BDO, ABN AMRO Bank, a range of building companies and health care institutions, the International Criminal Court, and water authorities. Before that, Jurgen for many years was department head, senior manager, IS auditor and advisor with e.g., ABN AMRO Bank and KPMG.
Jurgen had a number of guest lecturer positions with universities and colleges, and is regular author and speaker on risk management, cybersecurity, audit, privacy and operational technology both nationally and internationally. He held a number of committee and chair positions with various trade organisations and associations.

Jurgen *will* maintain that heat maps are a sad joke, damaging your business.

Jurgen.vanderVlugt@marsh.com
+31(0)6 161 29 747
https://www.marsh.com/nl/nl/services/cyber-risk.html