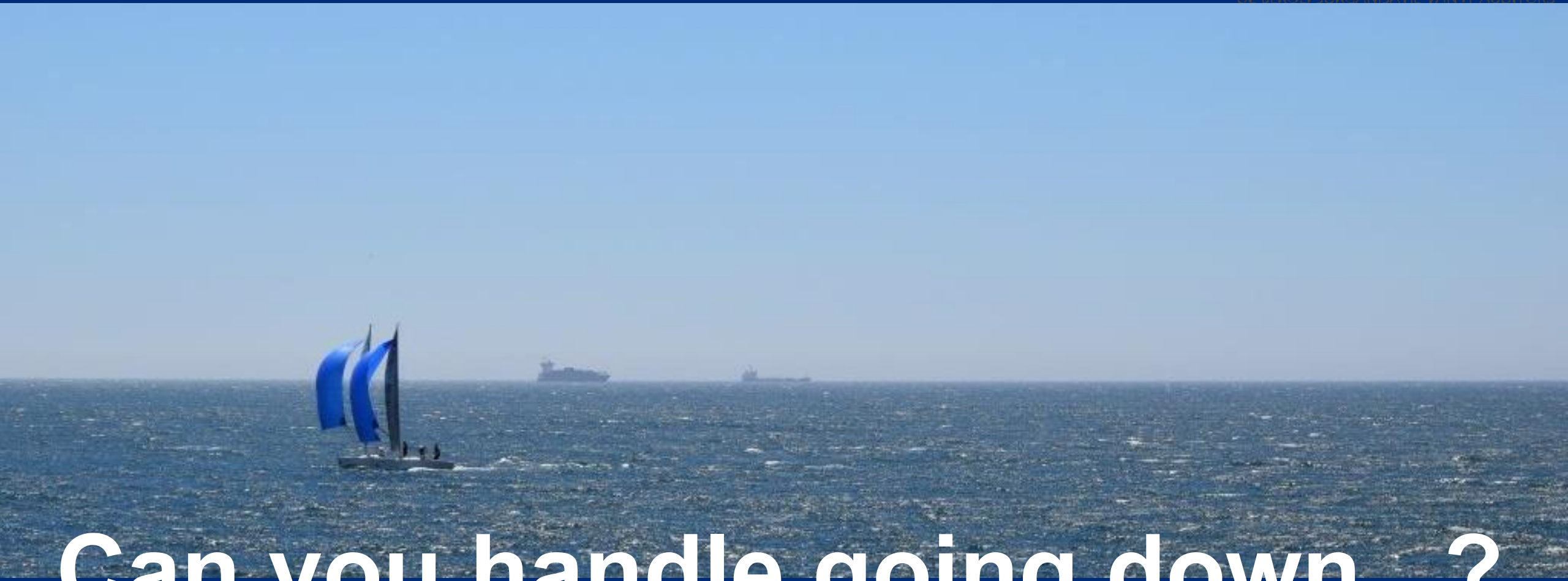


Can you handle going down ..?

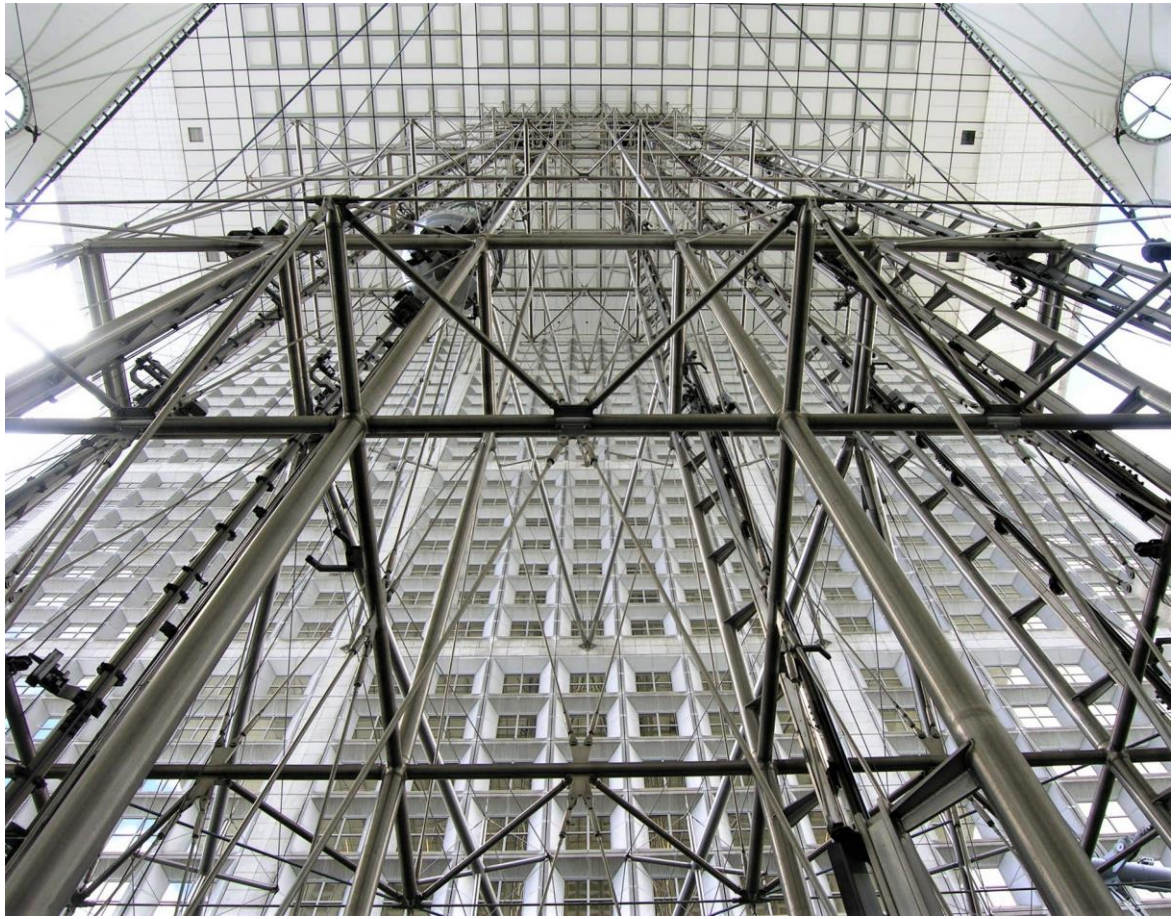
ISACA / NOREA Roundtable 1 June, 2022

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

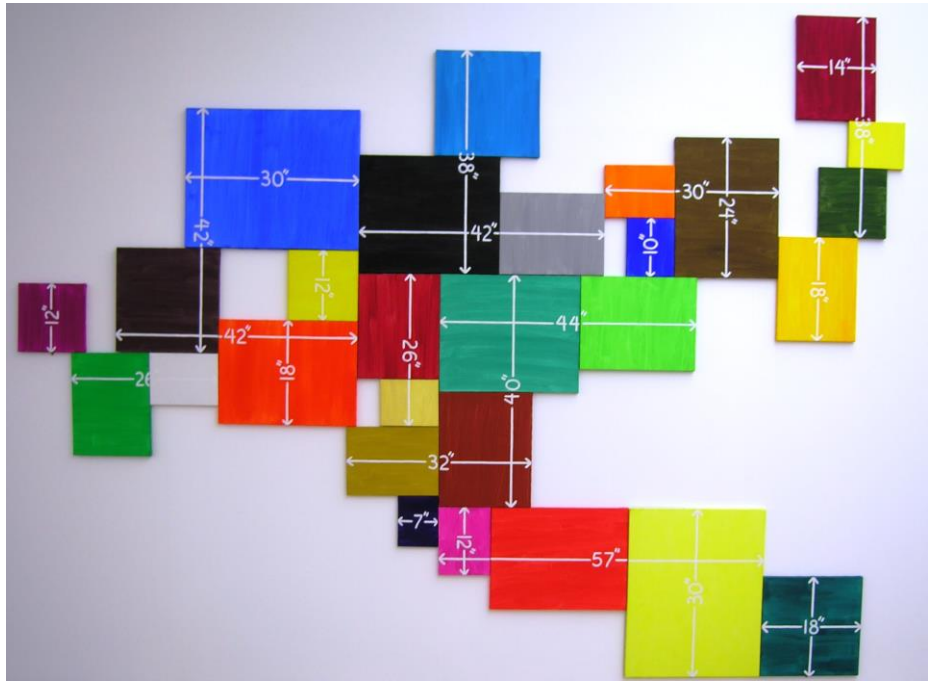


Intro

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

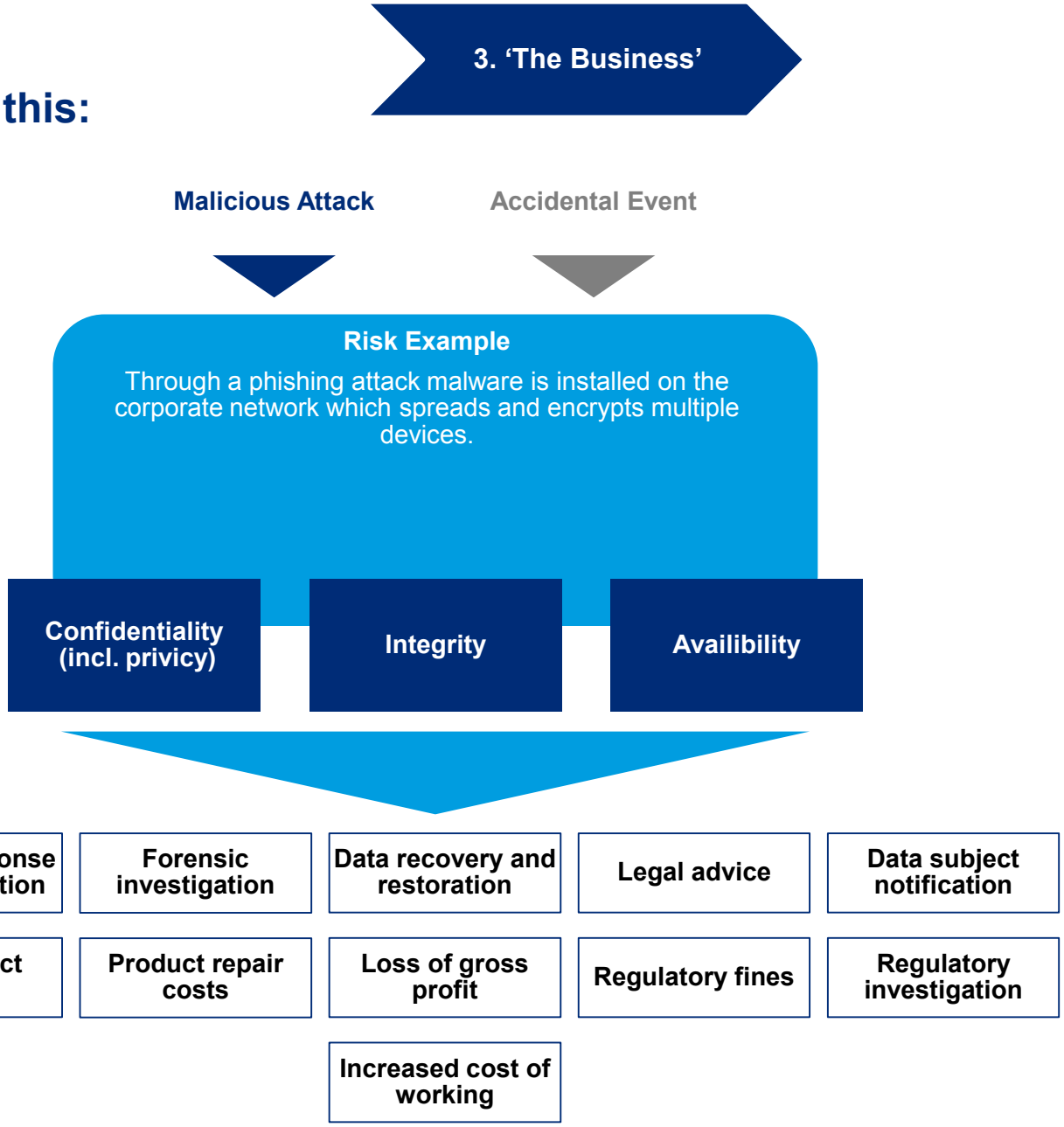
‘The Business’

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?

‘The Business’

Whatever. Just don’t give us this:



Eat Your Greens, too

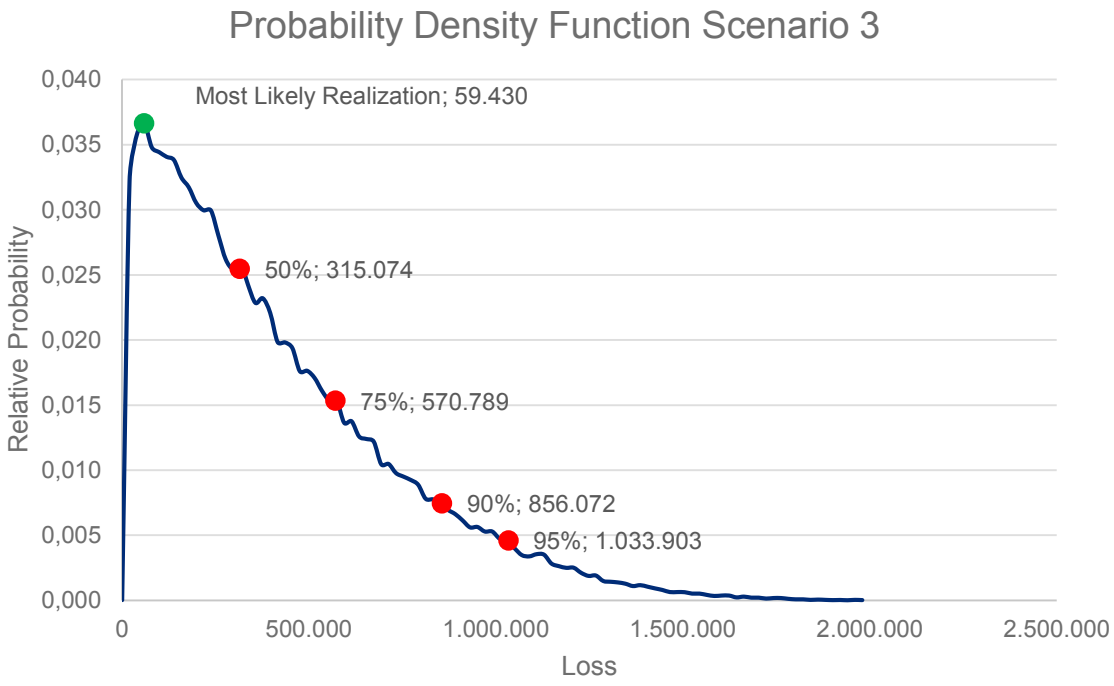
And Plan B is only the yellow

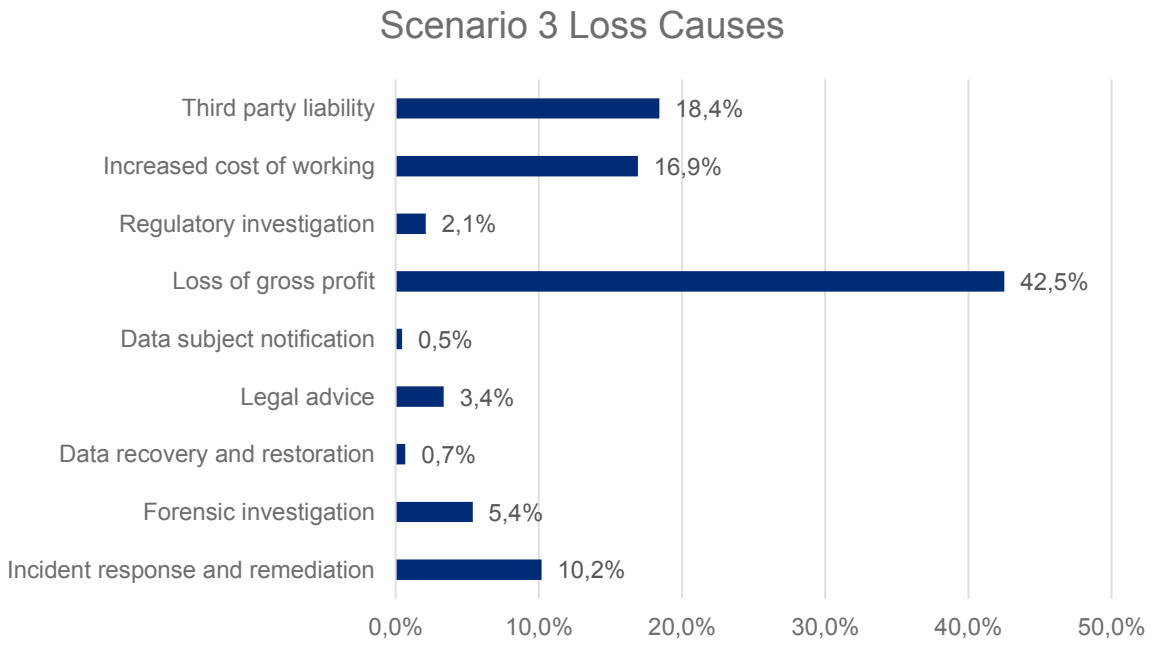
3. ‘The Business’

Quantify. Improve.

Be safe, then save. *And* insure

3. 'The Business'





[* Just your regular malware attack]

Who cares ..?

IT go figure it out yourself (?)

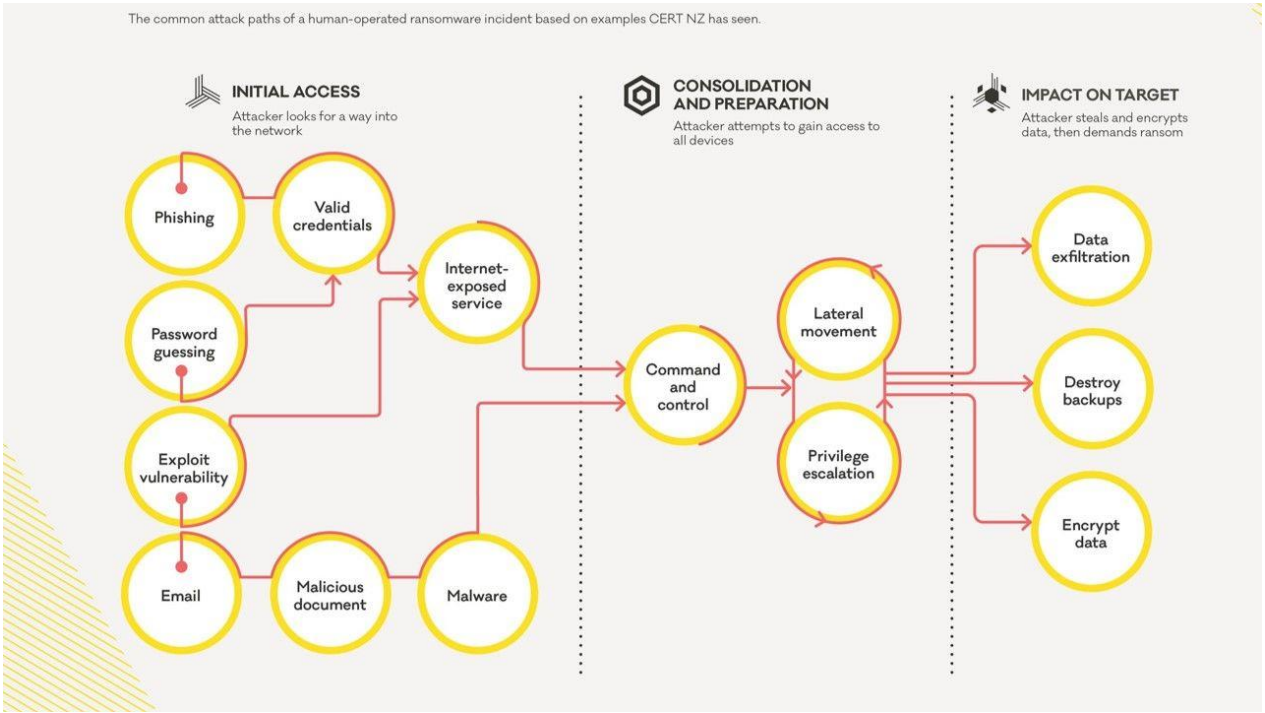
4. What about IT?

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 ..!*



[Yeah, plucked from a LI post]

Who cares

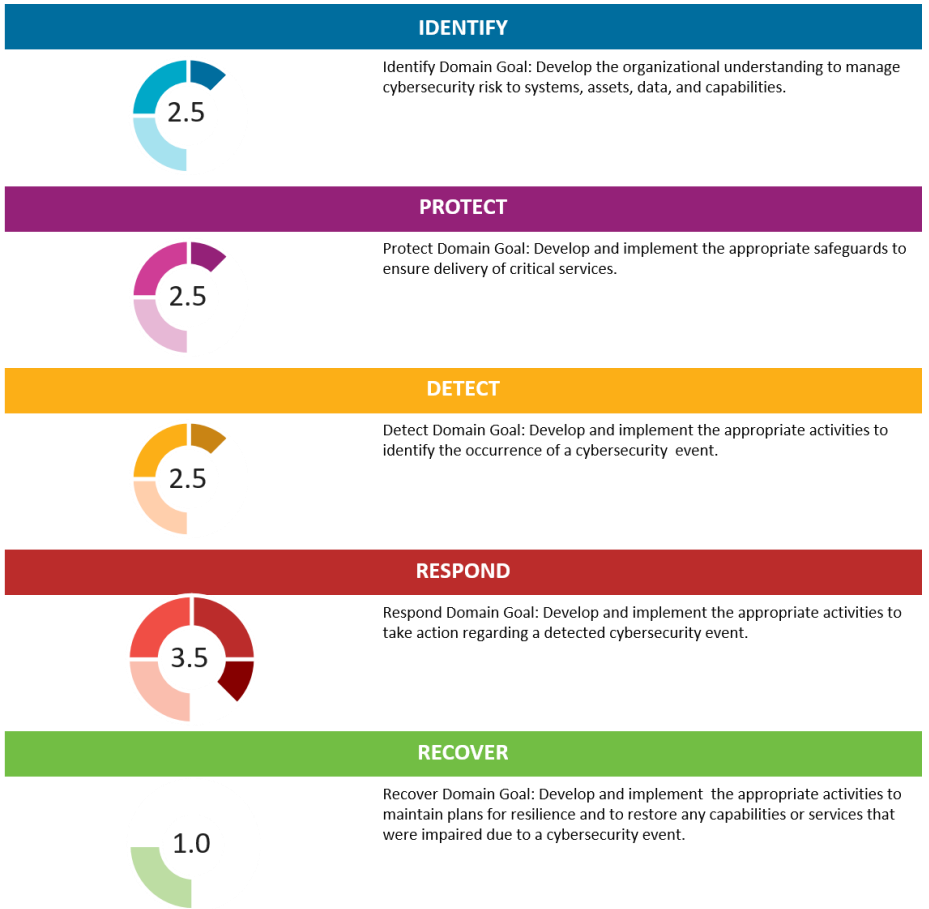
Part II, the Colby's

4. What about IT?

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



WIP re kill chain et al.

4. What about IT?

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.

4. What about IT?

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

And they lived happily ever after

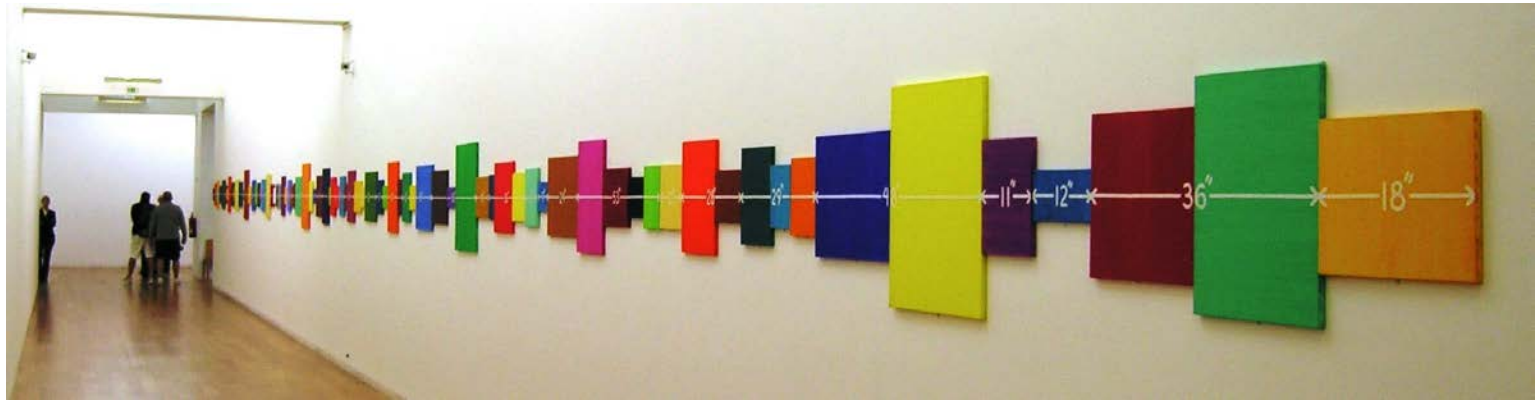
[Fairy tale]

- *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. 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

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

A business of Marsh McLennan