‘SUSTAINABLE SECURITY, HOW DOES CYBERSECURITY FIT WITHIN ENVIRONMENTAL, SOCIAL & GOVERNANCE (ESG) REPORTING?’

CISO360 event
Barcelona,
6th July 2023

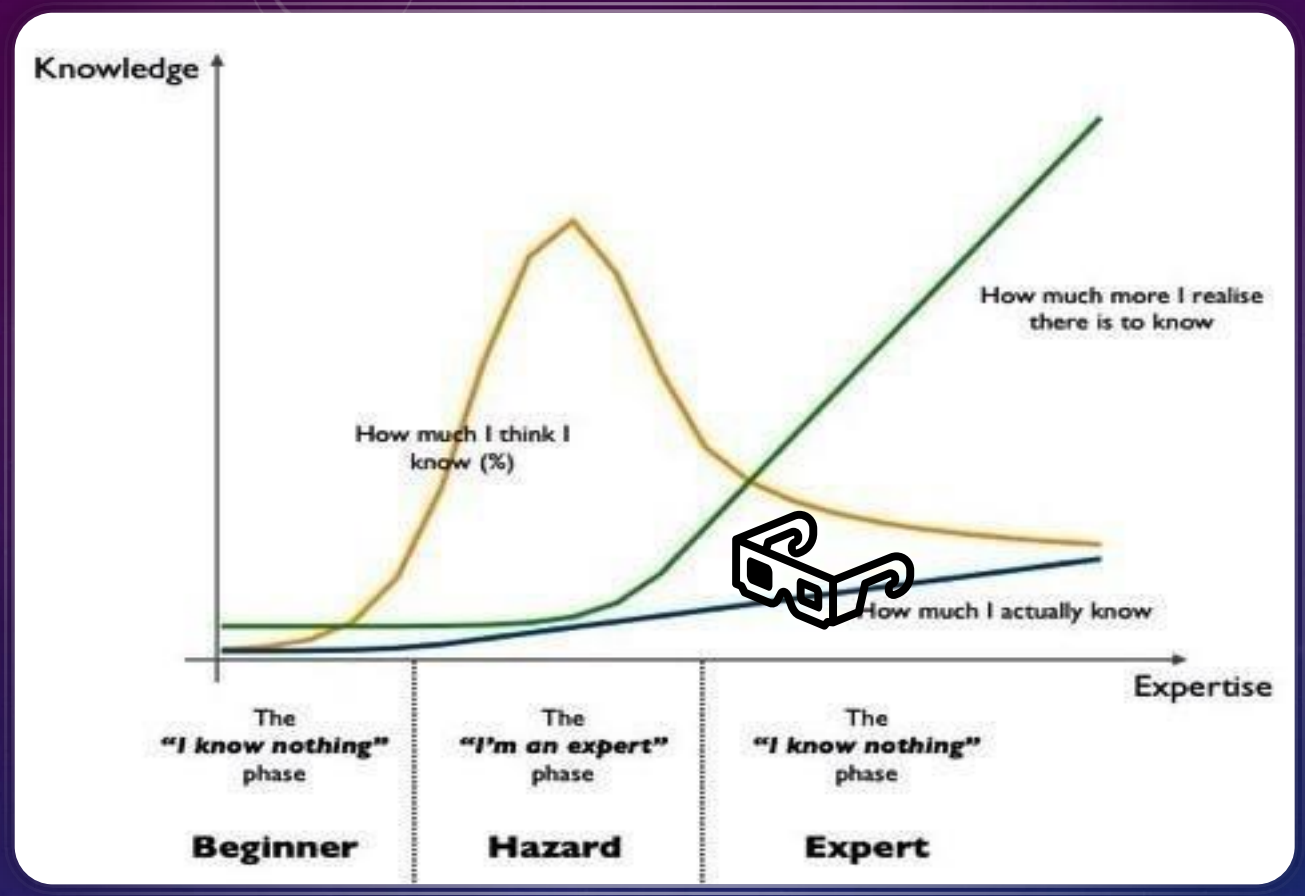
ALAN JENKINS,

INDEPENDENT CONSULTANT, THE CYBER SECURITY NAVIGATOR LTD

SECURITY PRACTITIONER, INTERIM/VIRTUAL CISO, TRUSTED ADVISOR

@THECYBRSECNAV

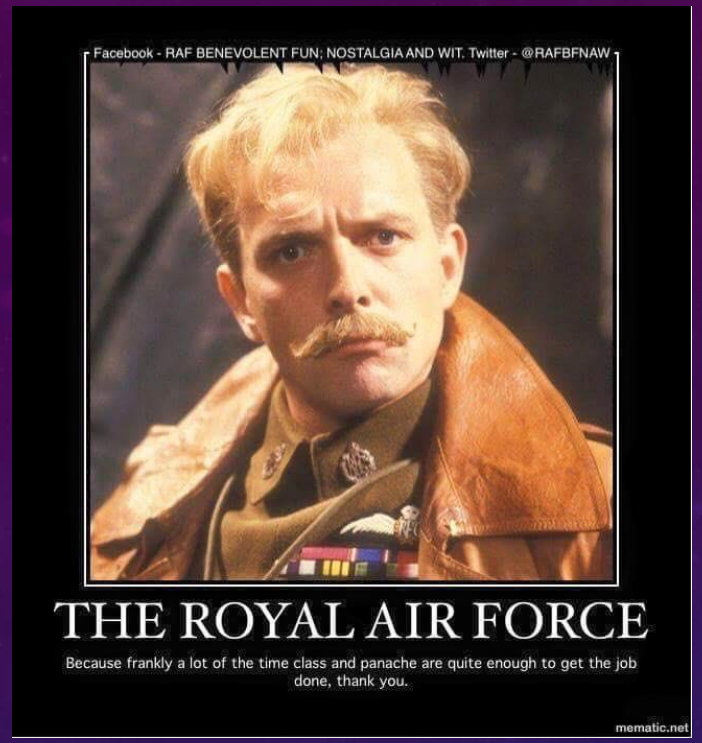
Copyright © 2023 Cyber Security Navigator LTD. All rights reserved



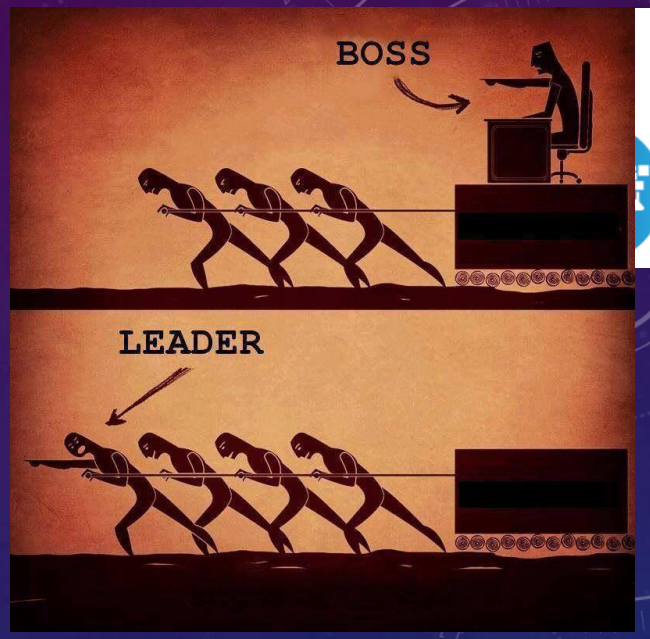
WHO IS ALAN JENKINS?

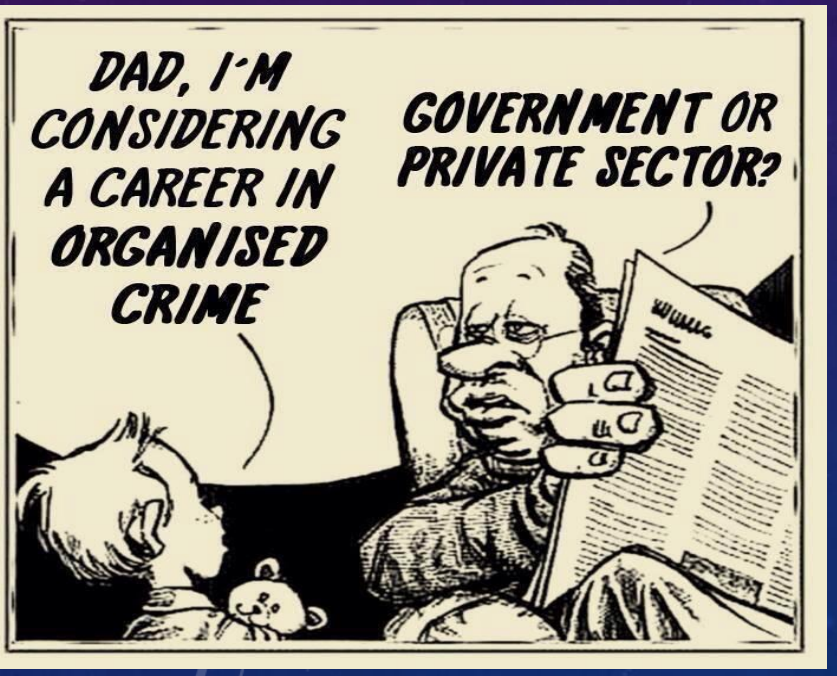
Does he know what he's talking about? *I hope so but I don't know everything!*

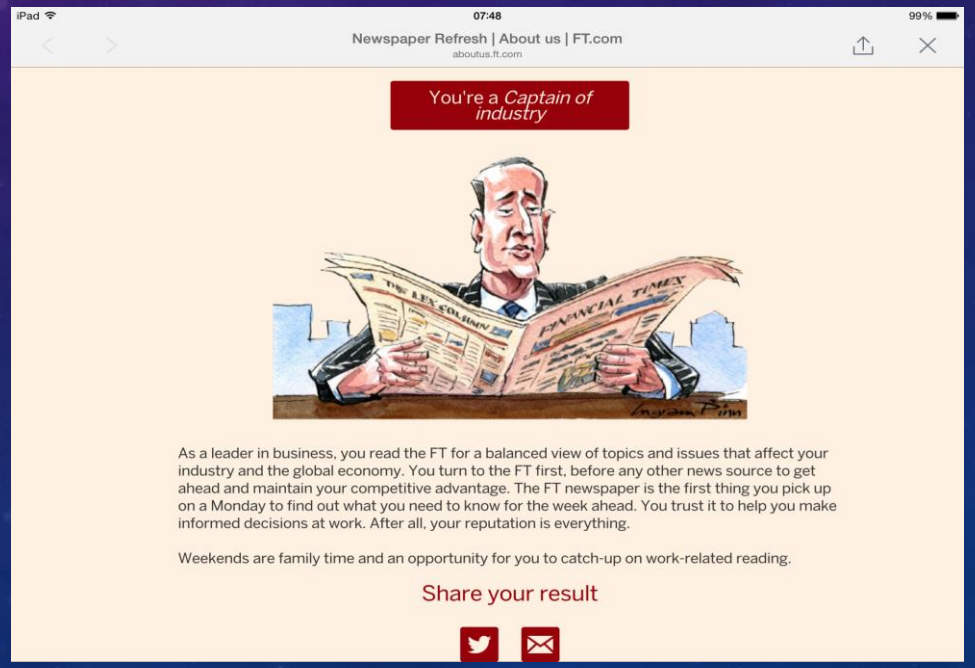
linkedin.com/in/alanjenkins

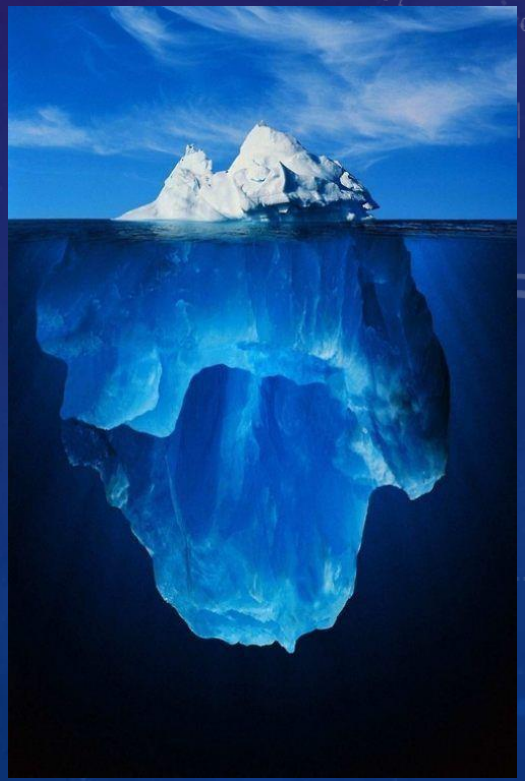

Facebook - RAF BENEVOLENT FUN; NOSTALGIA AND WIT. Twitter - @RAFBFNAW
THE ROYAL AIR FORCE
Because frankly a lot of the time class and panache are quite enough to get the job done, thank you.
mematic.net


I'm a
CONNECTOR
CISO
CISO NEXT
www.protiviti.com/cisotype
protiviti


BOSS
LEADER


DAD, I'M CONSIDERING A CAREER IN ORGANISED CRIME
GOVERNMENT OR PRIVATE SECTOR?


iPad
07:48
99%
Newspaper Refresh | About us | FT.com
aboutus.ft.com
You're a Captain of industry
FINANCIAL TIMES
As a leader in business, you read the FT for a balanced view of topics and issues that affect your industry and the global economy. You turn to the FT first, before any other news source to get ahead and maintain your competitive advantage. The FT newspaper is the first thing you pick up on a Monday to find out what you need to know for the week ahead. You trust it to help you make informed decisions at work. After all, your reputation is everything.
Weekends are family time and an opportunity for you to catch-up on work-related reading.
Share your result



DISCLAIMER …..

- "Investment risks
  - Investors must appreciate that, as with all funds, the funds ….. entail risks, including a possible loss of the invested capital. Past performance …… cannot be taken as a guide to future performance ……. Good past performance may not be repeated in the future. ***The performance indicated does not take into account …… costs***."
- ***What follows are the views of the presenter based on open source reporting, analysis thereof and deductions drawn after some 30 years as a security practitioner in a range of industries and roles***
- It is always possible that the future will throw up events that have not been foreseen ……
  - My 'Crystal Ball' is imperfect and any forecasts should be viewed with caution!
  - The 7 Ps - Prior Planning & Preparation Prevents P??? Poor Performance …..

WHAT IS 'SUSTAINABLE SECURITY'?

- "….. The central premise of ***sustainable security*** is that we cannot successfully control all the consequences of insecurity, but must work to resolve the causes. In other words, 'fighting the symptoms' will not work, we must instead 'cure the disease'.

- **By aiming to cooperatively resolve the root causes of threats using the most effective means available, sustainable security is inherently preventative in that it addresses (the) likely causes of conflict and instability well before (any) effects are felt."**
  - ***Source: Oxford Research Group https://sustainablesecurity.org/what-is-sustainable-security/the-concept/***

- **'Pets vs Cattle, CIA vs DIA Triad' Sunnil Yu www.cyberdefensematrix.com**

WHAT IS ESG? WHY DOES IT MATTER?

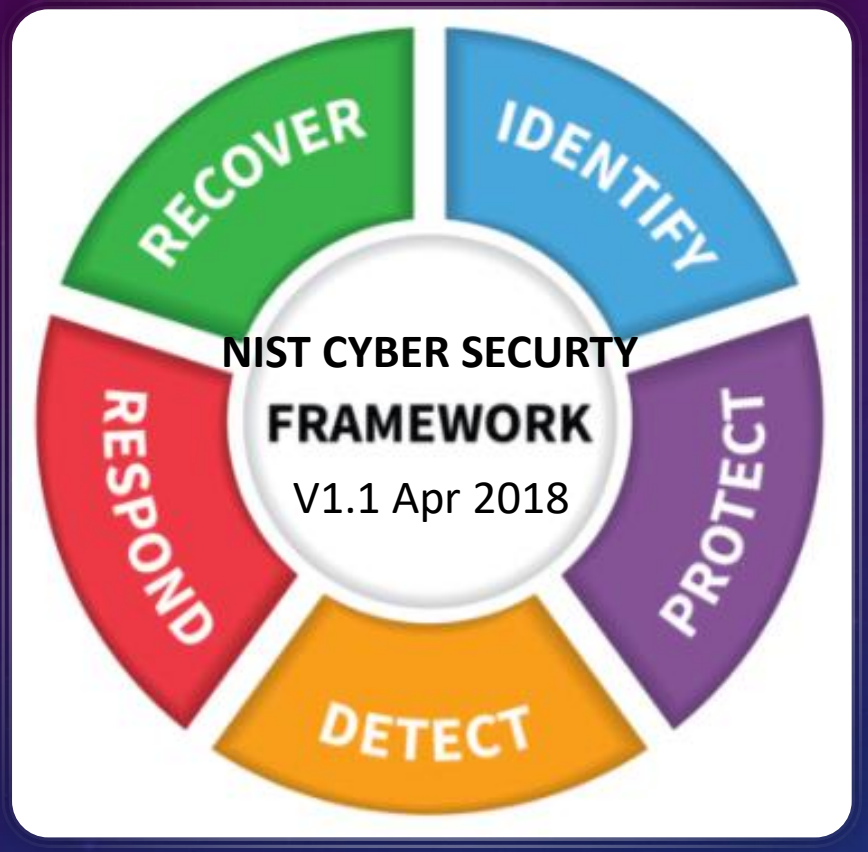
- "ESG – short for Environmental, Social and Governance – is a set of standards measuring a business's impact on society, the environment, and how transparent and accountable it is.
- It measures how your business integrates environmental, social, and governance practices into operations, as well as your business model, its impact, and its sustainability.
- Examples of good Governance practices include:
  - Accurate reporting to stakeholders on financial performance, business strategy and operations
  - Ensuring business leaders and managers are accountable for risk and performance management (while behaving in an ethically sound manner)
- Ensuring good governance in your business can appeal to investors and your supply chain; practising good governance may also help enable businesses to grow."
  - According to the CBI, "***2/3 of investors take ESG factors into account when investing in a company***"

- ***Source:*** ***https://www.british-business-bank.co.uk/finance-hub/business-guidance/sustainability/what-is-esg-a-guide-for-smaller-businesses/***

SUSTAINABLE SECURITY, HOW DOES THIS RELATE TO ESG?

- Key deductions:
  - "….. The central premise of ***sustainable security*** is that ……. it must be based on an integrated analysis of security ***threats*** and a ***preventative*** approach to ***response***.'
    - Prevention is better than cure
    - Emphasis on Secure-By-Design coupled with Threat modelling & improved Resilience
    - The linkage to ESG is important to bear in mind such that Security aligns to the needs of the business particularly with respect to good Governance
    - Good enterprise security risk management provides an opportunity to link Cost to Effectiveness and, therefore, Value
- **So, what is the connection between *Sustainable* and *Resilient* in the context of Cyber?**
- **And what is the *Value* proposition to your business to support continued, if not increasing, expenditure on Cyber Security? It's a cost to business……**
  - **Recognising increasing cost pressures across both geopolitical boundaries and all business sectors**

WHAT DO WE MEAN BY CYBER RESILIENCE?



NB NIST v2.0 is out for comment

- **Cyber resilience** refers to an entity's ability to continuously deliver the intended output despite adverse cyber events[1]
- Cyber resilience is an evolving term that is rapidly gaining recognition. The concept essentially brings the areas of information (cyber) security, business continuity, and operational resilience together
- It encompasses the 5 pillars that form the basis of NIST's Cyber Security Framework but particularly 3 of them:
  - PROTECT, RESPOND & RECOVER
- ***It is not the 'Mean-time-to-Detect' that matters to the business; it is the outage time before system(s) are recovered to >(80)% of normal service/output that matters more***
- ***This gives rise to Acceptable Outage time, a familiar term used in relation to business continuity***
  - ***This is an indicator of a business' risk appetite***

1. Cyber Resilience - Fundamentals for a Definition. Advances in Intelligent Systems and Computing (2015)
2. https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework

‘YOU CAN’T MANAGE WHAT YOU CAN’T MEASURE’ – THE FOUNDATION OF ENTERPRISE RISK MANAGEMENT

Business truism attributed to Peter Drucker, ‘Father of Management Theory’

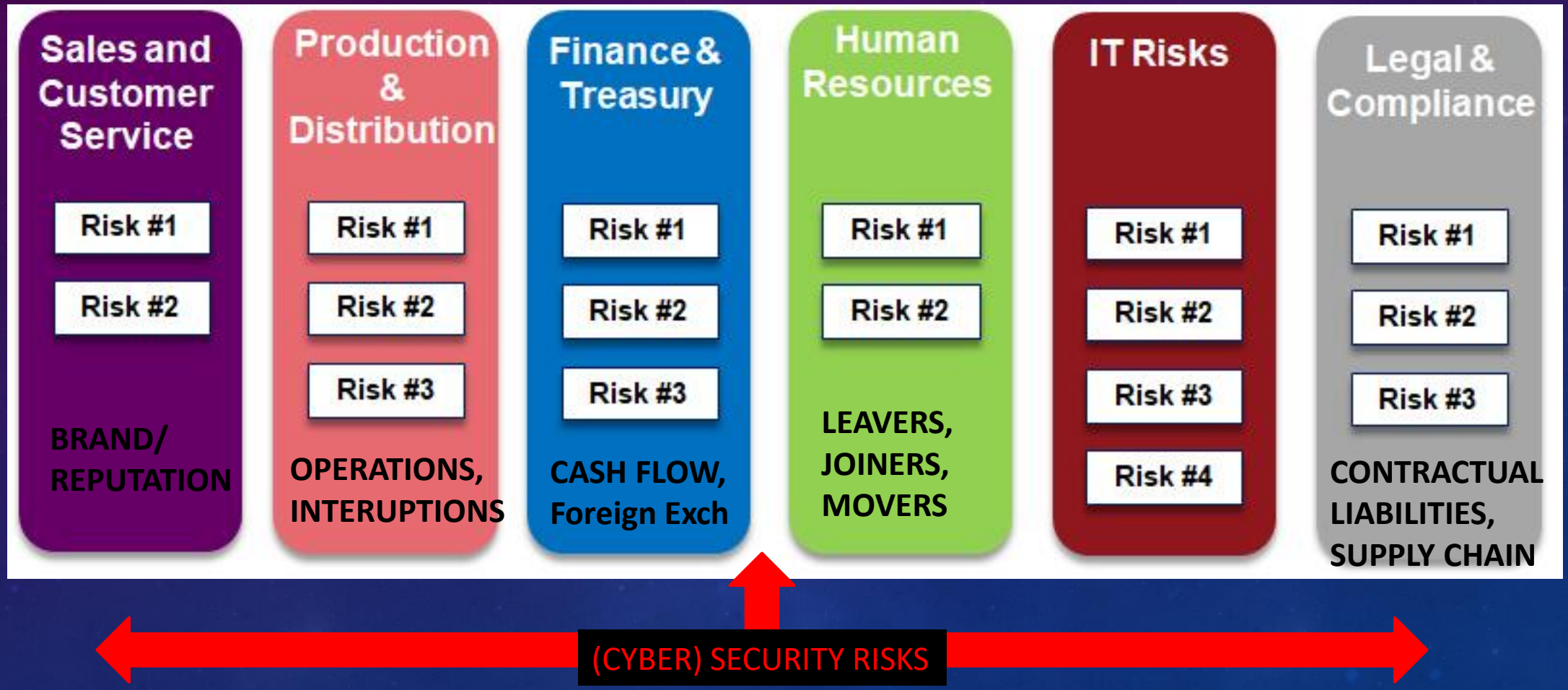
Table 0.1: Top risks according to the World Economic Forum’s *Global Risks Report 2018*

	2008	2013	2018
Top 5 global risks in terms of likelihood	Asset price collapse	Severe income disparity	Extreme weather events
	Middle East instability	Chronic fiscal imbalances	Natural disasters
	Failed and failing states	Rising greenhouse gas emissions	Cyberattacks
	Oil and gas price spike	Water supply crises	Data fraud or theft
	Chronic disease, developed world	Mismanagement of population aging	Failure of climate-change mitigation and adaptation
Top 5 global risks in terms of impact	Asset price collapse	Major systemic financial failure	Weapons of mass destruction
	Retrenchment from globalization (developed)	Water supply crises	Extreme weather events
	Slowing Chinese economy (<6%)	Chronic fiscal imbalances	Natural disasters
	Oil and gas price spike	Diffusion of weapons of mass destruction	Failure of climate-change mitigation and adaptation
	Pandemics	Failure of climate-change mitigation and adaptation	Water crises

?

● Economic ● Environmental ● Geopolitical ● Societal ● Technological

ENTERPRISE RISK MANAGEMENT COVERS A BROAD SPECTRUM



BUSINESS IMPACTS ARISING FROM CYBER INCIDENTS

1. **Fines levied by Privacy Regulators across Europe and beyond for multiple breaches eg British Airways fined £20M for incident effecting 400k customers (June 2018)[1]**

2. **WannaCry[2] (NHS, May 2017) & NotPetya (Maersk/$300M cost, June 2017)[3]**

3. **SolarWinds (Dec 2020)[4] – nation state hack of vendor infrastructure**

4. ***Colonial Pipeline (May 2021)[5] – $4.4M ransom reportedly paid; regulatory fines/class action lawsuits are pending***

5. ***Many others before and since, not all reported …….***

6. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers
7. https://www.europol.europa.eu/wannacry-ransomware
8. https://www.i-cio.com/management/insight/item/maersk-springing-back-from-a-catastrophic-cyber-attack
9. https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12?r=US&IR=T
10. https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

3 TRENDS DRIVING BUSINESSES TO REVIEW CYBER RESILIENCE AS FACTOR IN ENTERPRISE RISK MANAGEMENT

1. **Privacy** - Ever increasing friction between regulators & data processors as a result of abuses & breaches, leading to ever larger fines & increased regulatory constraints

2. **Evident impact of ransomware on business operations** - Increasing impacts felt by citizens, companies and nations as a result of Cyber events

3. **Operational Resilience** - Regulatory interest in stress testing and assessment of control effectiveness (driven by #1 & #2)

Note: Not the only trends!

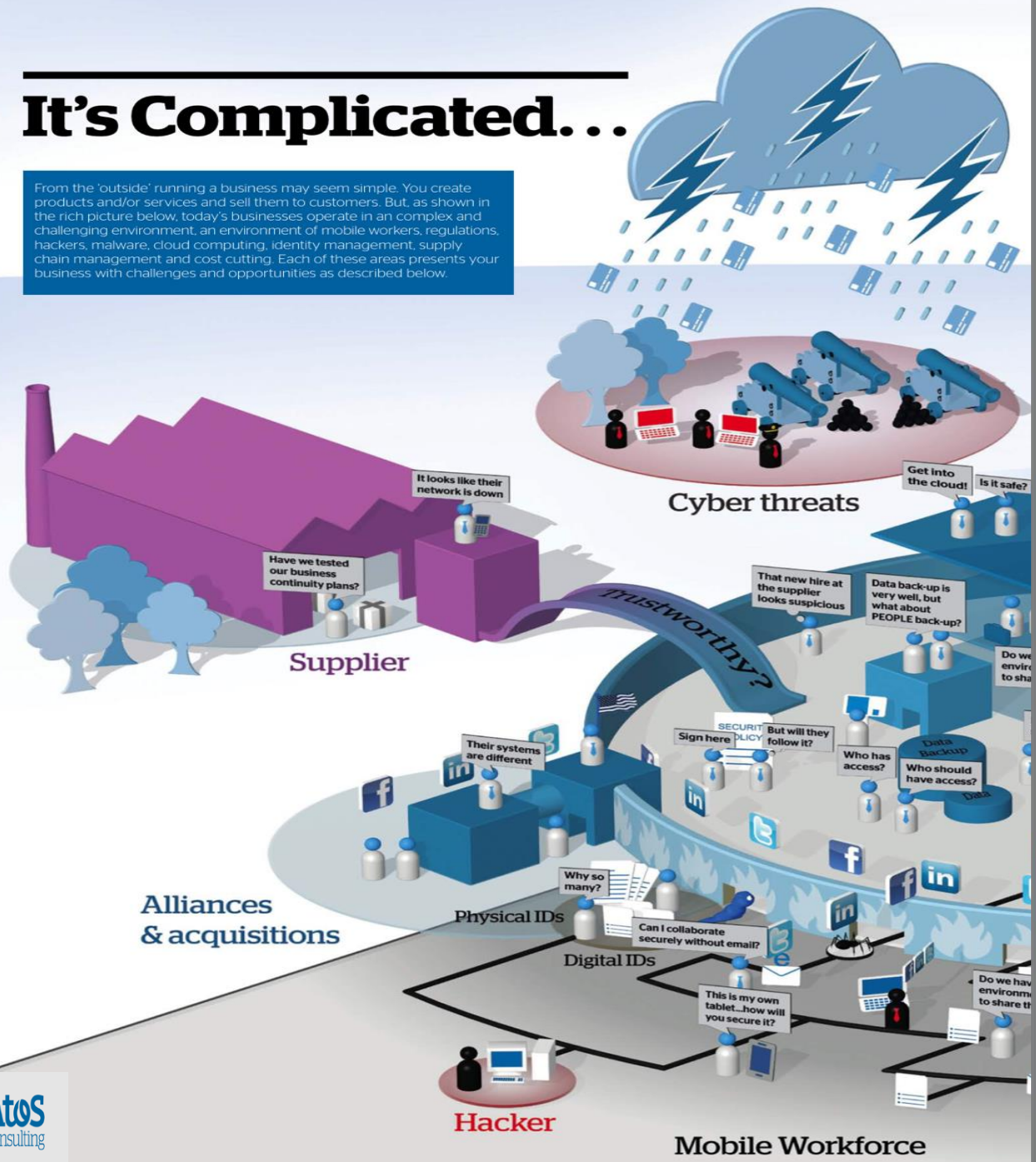
SO, HOW DO WE IMPROVE OUR CYBER RESILIENCE?
WHAT ARE THE BUSINESS DRIVERS? VALUE-AT-RISK? VALUE GAINED?

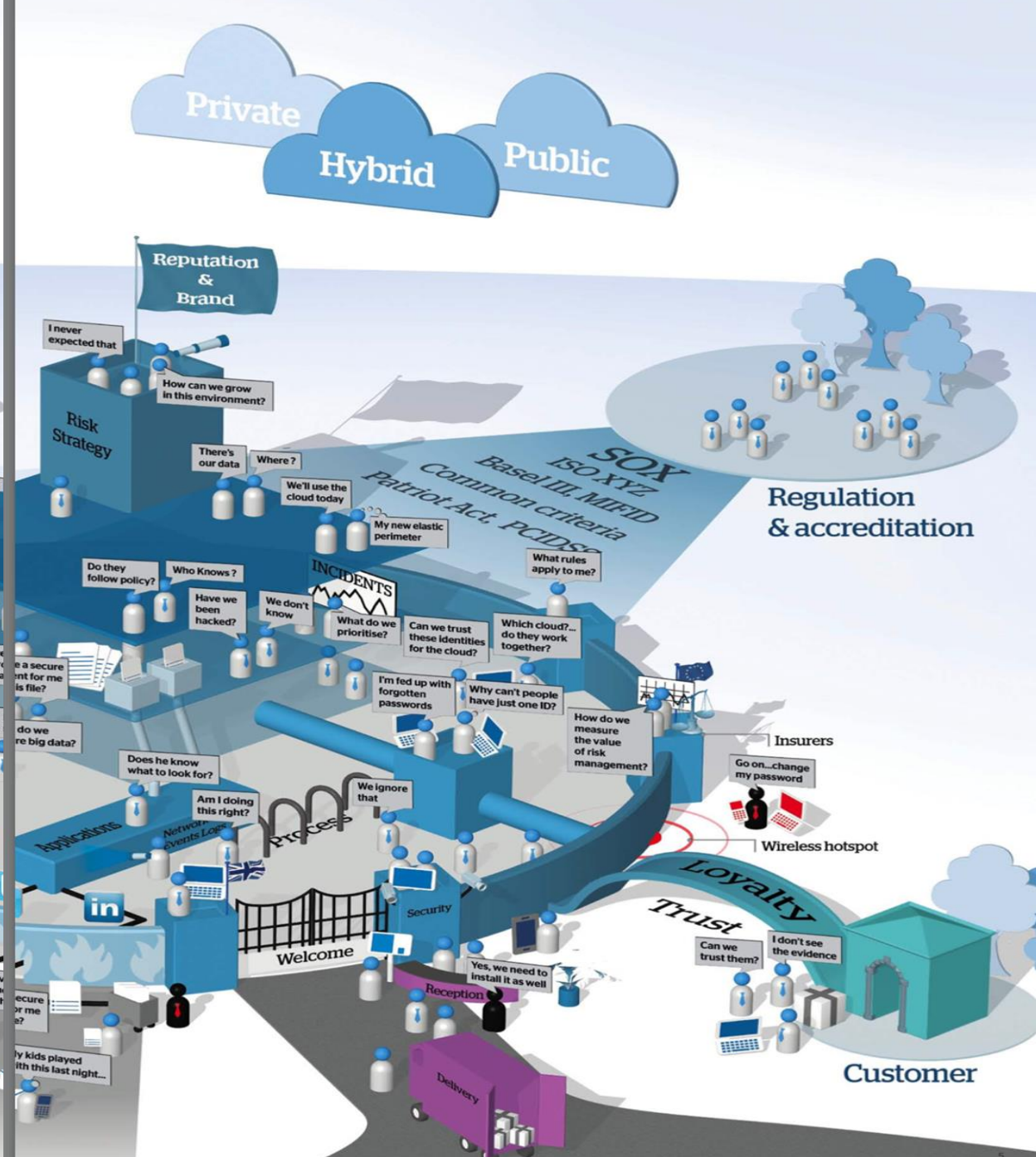
What does good look like? At what cost?

Compliance = Secure, doesn't it? ***No!!!!***

It's Complicated...

From the 'outside' running a business may seem simple. You create products and/or services and sell them to customers. But, as shown in the rich picture below, today's businesses operate in an complex and challenging environment, an environment of mobile workers, regulations, hackers, malware, cloud computing, identity management, supply chain management and cost cutting. Each of these areas presents your business with challenges and opportunities as described below.





Atos Consulting

CONCLUSIONS – SO WHAT?

- 3 Trends only called out and explored:
  Privacy, CNI & Operational Resiliency
  There are others eg Pandemic risk/effect on supply chain eg Auto industry

- ERM is being extended to encompass Environmental & Societal risks also, hence ESG
- Much effort goes into demonstrating compliance eg ISO27002/136 controls
- Multiple compliance frameworks eg NIST CSF vs ISO27002 vs IS031000
- Compliance effort is a business overhead, 'cost of doing business'
- Status reporting requires common risk taxonomy across risk silos
- Value gained from compliance has to be tangible, else lip service
- But being Compliant does not equate to being Secure ……
- Businesses need to review their approach to Cyber Resilience given evident Impacts ……
- ***Time to look again at Security Convergence to reduce silo effects & cost/effort duplication***

THANK YOU

AJ@cybersecnav.onmicrosoft.com

+44(0)7725096098

Copyright © 2023 Cyber Security Navigator LTD. All rights reserved