

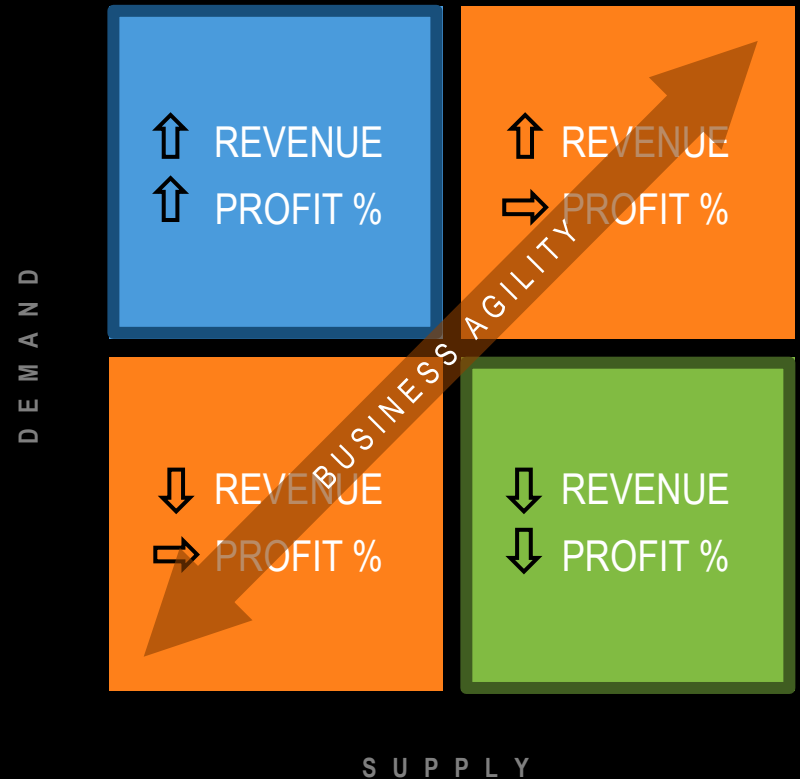


EFFECTIVELY REPRESENTING CYBERSECURITY TO BOARDS AND SENIOR EXECUTIVE TEAMS

A fronte praecipitium a tergo lupi

AHEM....THE REAL WORLD

- Is cyber-physical, not digital
- It is made up of producers, manufacturers, suppliers, sellers and buyers
- Is complex and driven by forces you will likely not understand
- You are a messenger who has to bridge the cyber-physical world to the world of business
- “Digital transformation” is mostly a marketing term that has limited impact in the real world



UNPACKING RISK

- More is less
- The most critical thing to your business is????
- Use a “business”, not an “Cyber/ICT” lens, think SHE
- Don’t forget people, paper & pens. Or audit. Or Policy....
- Understand the Risk, the likelihood and the Impact **before** you design the policy, controls, monitoring & review
 - Balancing routine and predictable against improbable and unpredictable - response depends on probability, also likelihood, vulnerability and costs
 - System of systems. FMEA & FMECA are lessons from the real world
 - Sector, Supply chain need to be factored in as well
- Be a [proper] gatekeeper – AI anyone?

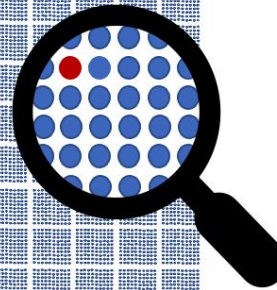
....RISK IS PERCEIVED

There are 100,000 dots on this slide. Imagine each represented a person aged 25-34

If they were all unvaccinated we'd
expect 2 per week to be hospitalized
with COVID-19



If they were all vaccinated we'd
expect less than 1 per week to be
hospitalized with COVID-19

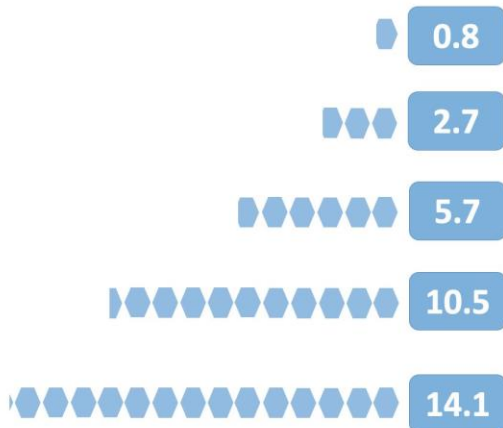


....A FRAMEWORK EXAMPLE

Weighing up the potential benefits and harms of the Astra-Zeneca COVID-19 vaccine

Potential benefits

ICU admissions due to COVID-19 prevented every 16 weeks:



Other potential benefits not shown include prevention of COVID-19 cases not leading to ICU and reduction of transmission

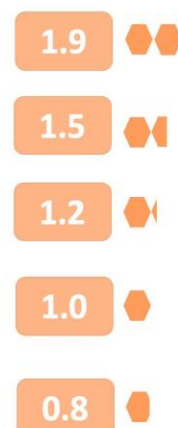
* Based on coronavirus incidence of 2 per 10,000 per day (140 per 100,000 per week): roughly UK in March 2021

For 100,000 people with low exposure risk*

Age group

Potential harms

Specific blood clots associated with the vaccine:



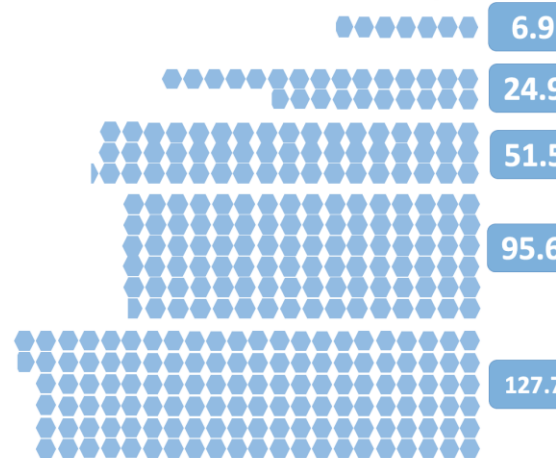
Other potential harms not shown include short-term side effects
Data from reactions to first dose only

Data from

Weighing up the potential benefits and harms of the Astra-Zeneca COVID-19 vaccine

Potential benefits

ICU admissions due to COVID-19 prevented every 16 weeks:



Other potential benefits not shown include prevention of COVID-19 cases not leading to ICU and reduction of transmission

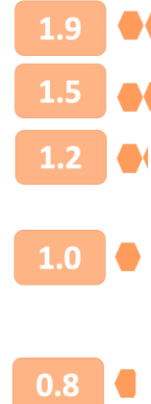
* Based on coronavirus incidence of 20 per 10,000 per day (1391 per 100,000 per week): roughly UK at peak

For 100,000 people with high exposure risk*

Age group

Potential harms

Specific blood clots associated with the vaccine:



Other potential harms not shown include short-term side effects
Data from reactions to first dose only

Data from UK up until 28th April 2021

PRESENTING RISK

- First principles: The Business is a meta collection of processes using technology to manage data, in order to make money
- Use a Framework for communicating the Risk, the likelihood and the Impact
 - A “point in time” that allows tracking
 - Underpins all activities and your improvement plane
 - Lets risk drive policy, controls, monitoring & review
- Don't forget People
- Qualify impact/severity
 - Value at Risk is not always the only measure
 - Don't forget the cost of remediation/impairment
 - Don't assume: check, benchmark, & extrapolate

Risk Framework & Controls

LIKELIHOOD	Almost certain (71-100%) The risk is expected to occur in most circumstances and at least 3 times in 12 months.	Medium	High	Very High	Extreme	Extreme
	Likely (41-70%) The risk will probably occur once within the next 12 months.	Medium	High	Very High	Very High	Extreme
	Possible (16-40%) The risk could occur at least once in the next 3 years.	Low	Medium	High	Very High	Very High
	Unlikely (6-15%) Not expected to occur more than once in 10 years.	Low	Low	Medium	High	Very High
	Rare (0-5%) May occur only in exceptional circumstances less than once per 10 years.	Low	Low	Low	Medium	High
		Negligible	Minor	Moderate	Major	Catastrophic
IMPACT / CONSEQUENCE						

Inherent Rating (circled in red)

Controls (vertical arrow pointing down)

Target Rating (circled in red)

KNOW YOUR AUDIENCE

- Uncommon ground: Boards don't understand Cyber*, you're not there to "Just take care of it"
- Common ground: your audience understands risk & controls and their impact on trust & reputation in the SHE & financial worlds (e.g. HSE)
- The Board is about investments and strategy, but also have a critical role in incidents (communications; customers, suppliers, employees, regulatory etc)
- Feel comfortable to talk about incidents – they give context and inform
- Be ready to be tested. Expect to be. Confidence, reasonableness
- Bottom line: gain trust, gain a champion

**PwC's 2022 Annual Corporate Directors Survey: only 41% of corporate directors think that they understand cybersecurity risks "very well"*

MAKE YOUR PITCH

- Translate cyber into business terms: value, cost, risk & reputation
- Present the Cyber Framework as the context for your plan
- Start small – BCP? And you DO have an improvement plan don't you?
- Assessment is a Good Thing (e.g. NIST-based review) but caveat emptor
- Bring regulatory & compliance into the picture (NZPA 2019, GDPR)
- Where is your IR Plan? How do you know it will work? How is the Board involved?
- Understand and articulate trade-offs, priorities and what you can live without
- Jargon
- Bottom line: what is it?



SUCCESS IS...

- Your business will be better protected **because** of your pitch
- Dialogue is established
- Agreement on the things you want
- You feel comfortable that your business can respond to an incident (BCP anyone?)
- You can sleep easier
- Trust
- You get asked back