



Security from scratch...

What would you do if you were starting all over again with your security program?

Andrew Morgan – Chief Information Security Officer

CISO Melbourne : July 2022

Today's Session

1

A brief history

A whirlwind tour of the history of the security discipline and how it has sort of evolved...

2

How did we defend?

The way we have defended these threats has evolved. Let's look at then vs now...

3

Starting again...

If we had the ability to stop time and step back and think again, what would we consider...

4

What about the future?

We know what we know but the great challenge for all of us is the future – how do we set ourselves up for success and what do we need?

A brief history...



1833

First programmer

Augusta Ada King-Noel worked on the Analytical Engine and is the world's first programmer



1949

First Virus

The roots of the computer virus were developed when scientist John von Neumann published "The Theory of Self-Reproducing Automata"

700 BC

Scytale

Used by the Greeks and Romans to send encrypted messages



1903

First Hacker

Nevil Maskelyne interrupted a demonstration of a secure wireless telegraph by hacking projector



A brief history...

The New York Times



Slide 4

1980 1st hacking report

NYT makes 1st report on hackers after FBI investigate a breach at NCSS (mainframe time share company)

1994 More bad guys...

- Vladimir Levin leads a team of hackers who steal \$10 million from Citibank
- AOHell is released
 - SSL encryption protocol released by Netscape

1957

The whistler...

"Joybubbles" Engressia, a blind 7 year old with perfect pitch discovered that by whistling the 4th E above Middle C would interfere with AT&T phone systems



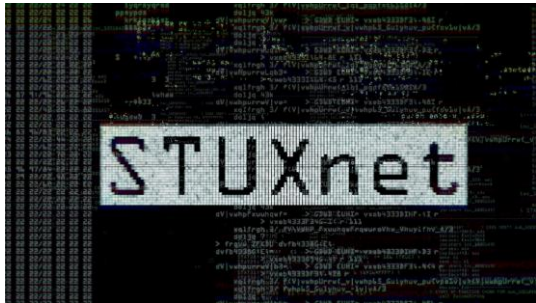
1984

The bad guys...

- Lex Luthor founds "Legion of Doom"
- Cult of Dead Cows forms.
- Hacker magazine "2600" published.
- The Chaos Communication Congress is held in Hamburg, Germany



A brief history...



2010 Stuxnet

The Stuxnet Worm is found by VirusBlokAda and it was responsible for the cyber attack on Iran's nuclear facilities



2017 More bad guys...

- Wannacry infects over 230000 computers in 150+ companies
 - Petya makes Ransomware mainstream and takes out NHS and others
- Las Vegas Casino hack starts with a fishtank

2004

Nation States

North Korea claims to have trained 500 hackers who had hacked Sth Korean, Japanese and other ally's computer systems



2014

The bad guys...

Mt Gox (bitcoin exchange) went bankrupt after \$460 million was stolen by hackers due to "system weaknesses" and another \$27.4 million went missing from its bank accounts



A brief history...

What does this mean?

- There have always been people trying to make it so that people and systems can communicate securely
- There have always been people who are trying to breach the security for their own benefit
- The bad guys have their noses in front and the gap is getting bigger

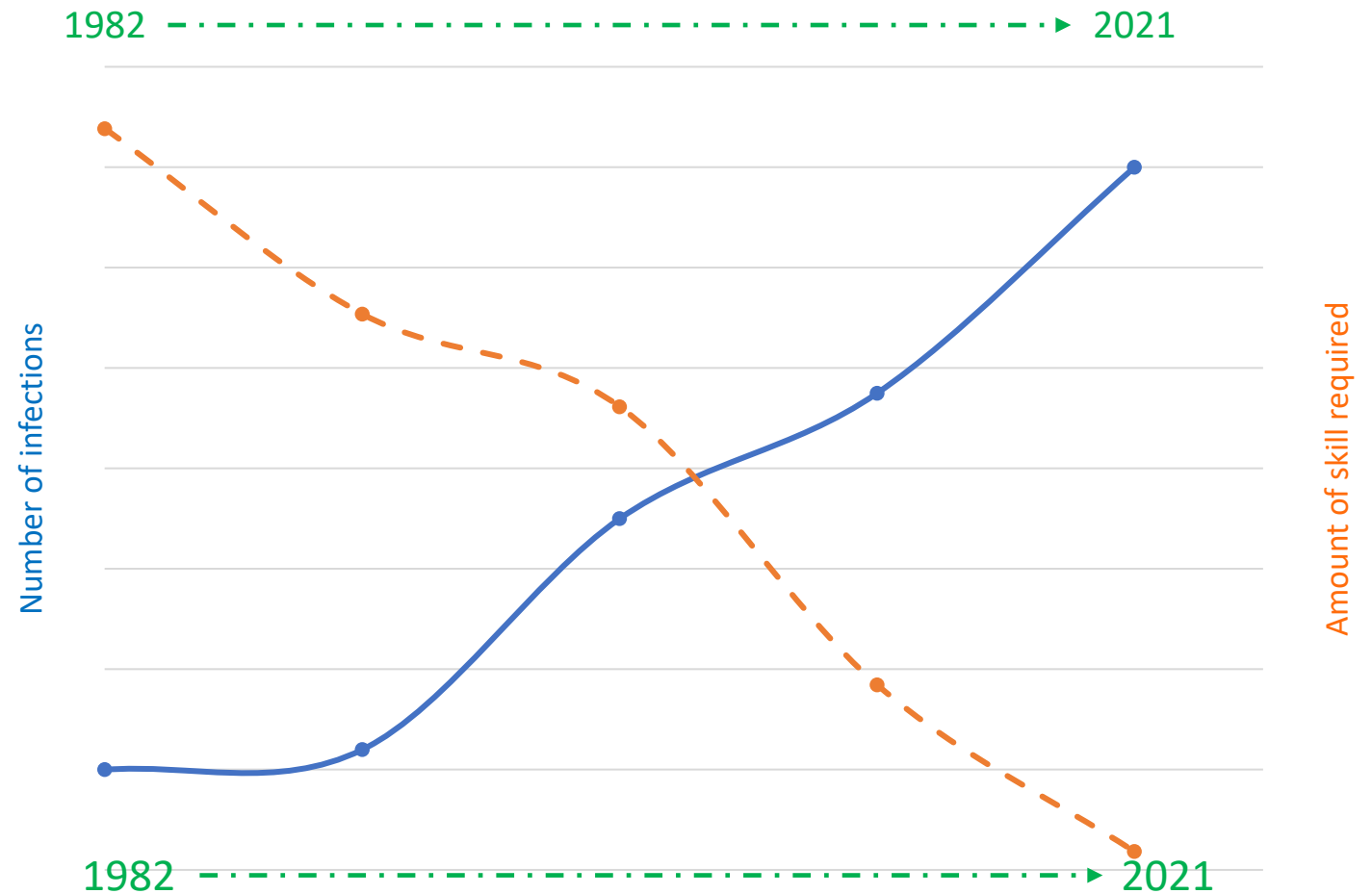
01

The number of malware, viruses and hacking has increased exponentially over time

02

The amount of skills required to carry out these attacks has steadily decreased as the industry has become increasingly commoditised

Skills required vs the number of infections



Today's Session

1

A brief history

A whirlwind tour of the history of the security discipline and how it has sort of evolved...

2

How did we defend?

The way we have defended these threats has evolved. Let's look at then vs now...

3

Starting again...

If we had the ability to stop time and step back and think again, what would we consider...

4

What about the future?

We know what we know but the great challenge for all of us is the future – how do we set ourselves up for success and what do we need?

Way back in the old
days...
It was actually not too
complex



Castle and moat approach

Everything on our premises:

**We assumed that all security threats
came from outside our organization so we
created barriers to stop them getting in.**

These days...
It is incredibly complex

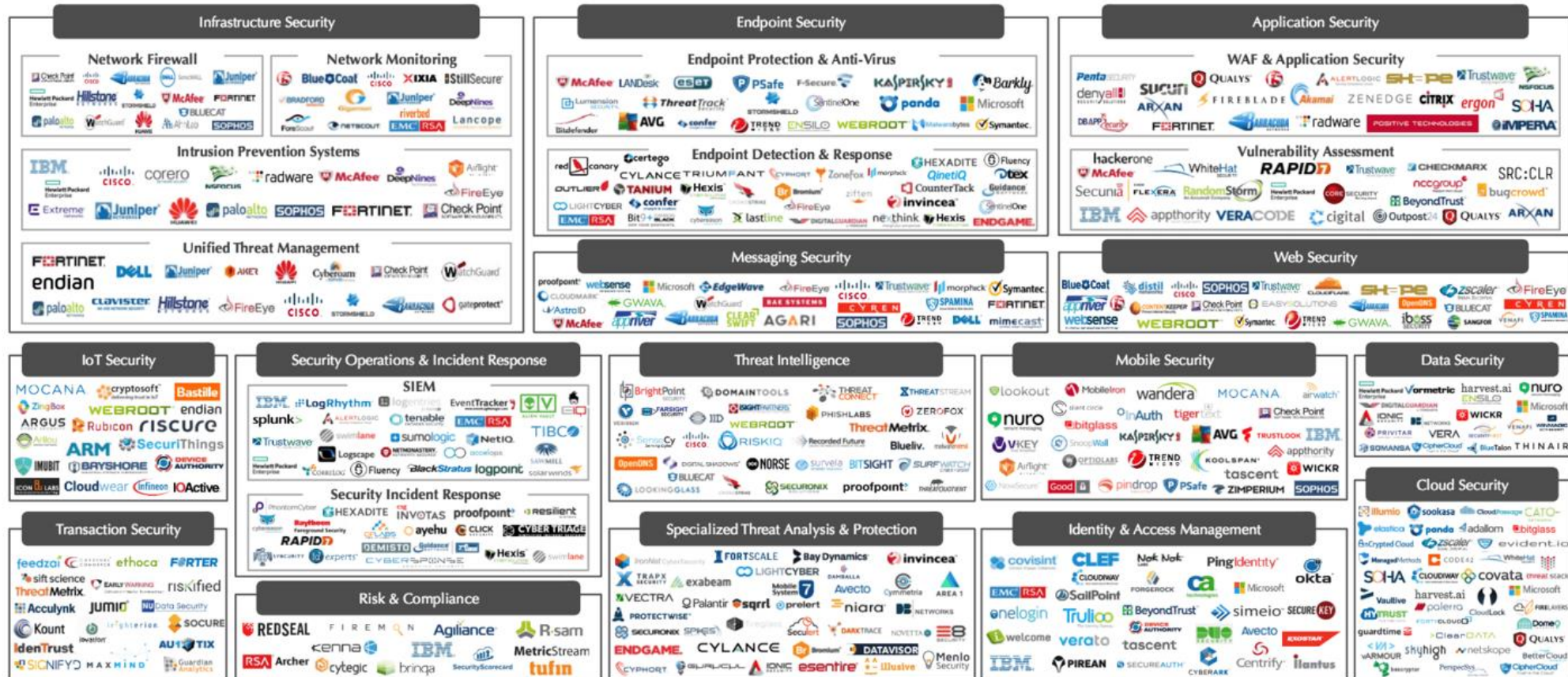


Here, there and everywhere:

Little or nothing on our premises:

- Some on prem... some in cloud (yours, mine and theirs)
- Complex relationships for who can access your data
 - your staff, third parties
- Motivated, capable and well-resourced attackers

Of course, vendors are here to help and make things simple...



With complexity, comes even more complexity....

As the IT landscape has become more complex and the bad guys have become more capable and well resourced, a new industry relating to cyber security tooling sprung up – this industry was valued at **USD \$139.77 billion in 2021**

Their hearts might be in the right place (???) but there is no single solution to our problems – my call out to the vendors is work with us to understand our business and our issues – don't tell us your widget will solve the problems without engaging with us and building understanding... <END RANT>.

Today's Session

1

A brief history

A whirlwind tour of the history of the security discipline and how it has sort of evolved...

2

How did we defend?

The way we have defended these threats has evolved. Let's look at then vs now...

3

Starting again...

If we had the ability to stop time and step back and think again, what would we consider...

4

What about the future?

We know what we know but the great challenge for all of us is the future – how do we set ourselves up for success and what do we need?

Starting again – Greenfields vs scorched earth??



Greenfields Opportunity?

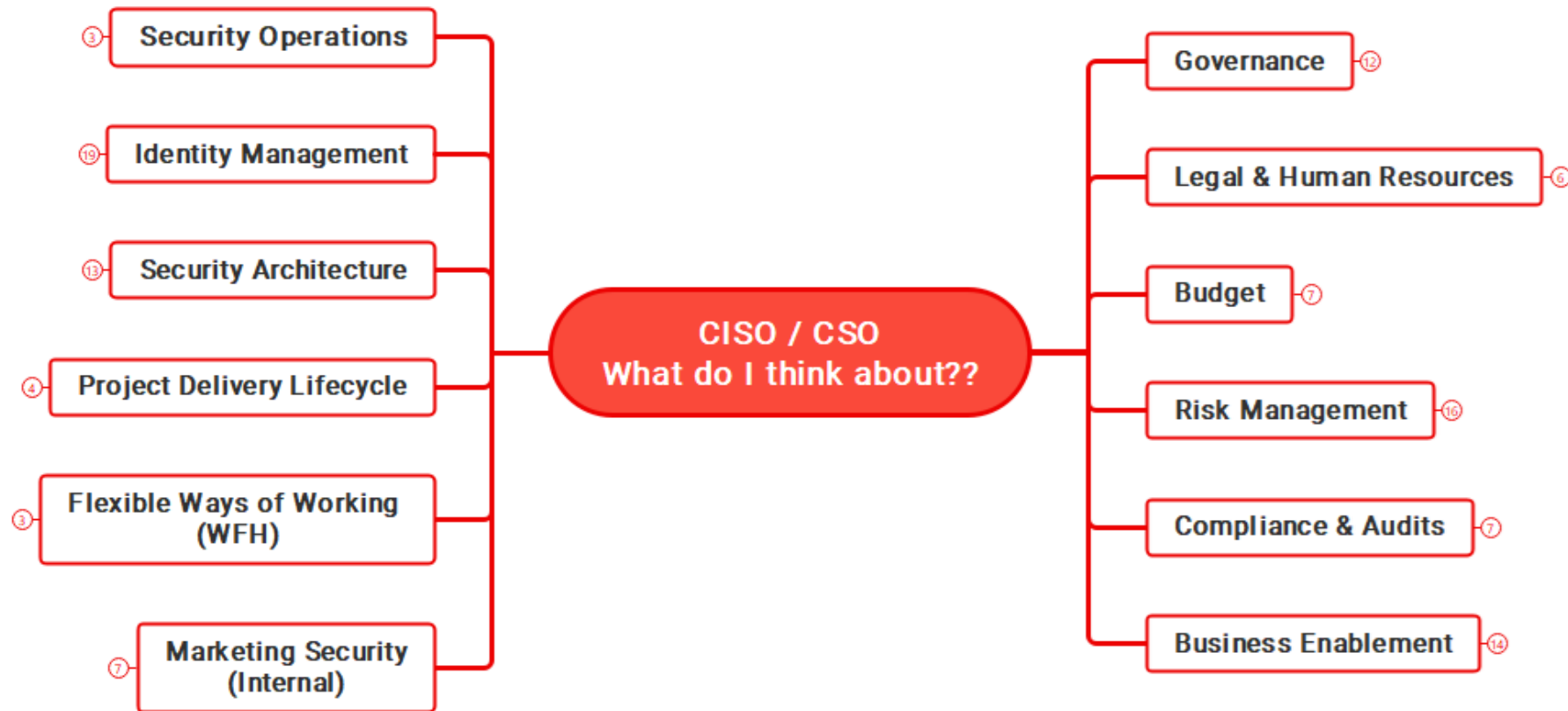
- If we were to take a step back and start again, is it an opportunity for us to build a new way to: prevent attacks, detect and investigate attempts, resolve incidents and recover from them and ultimately learn from these incidents and create better defences in the future?

Scorched Earth

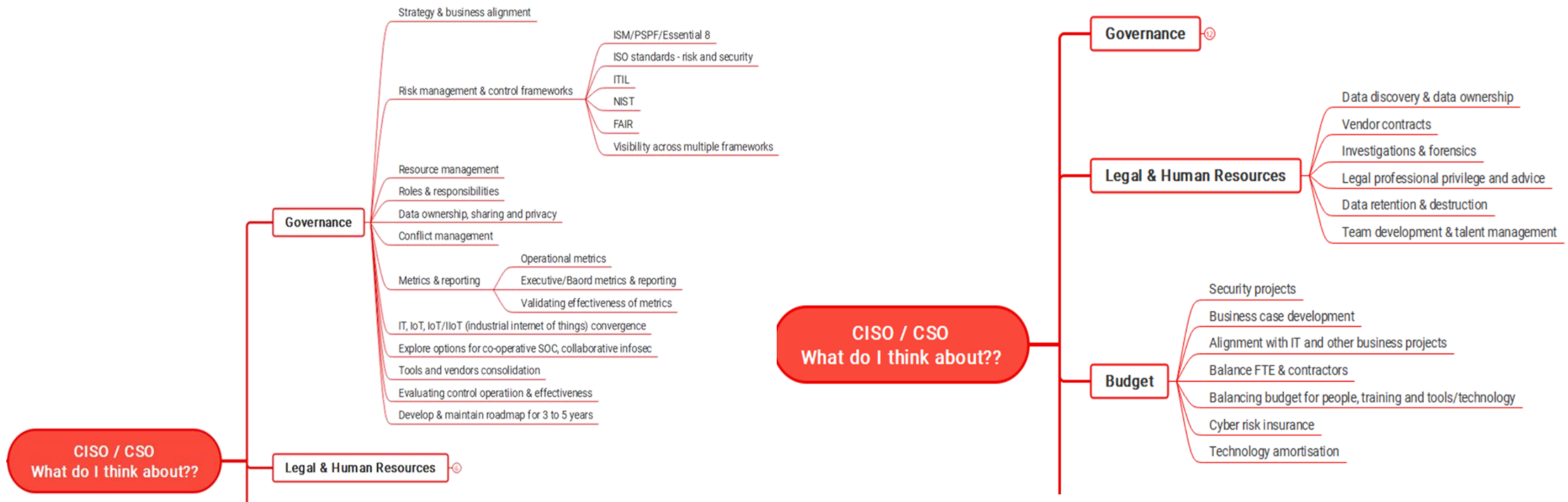
- If we were to take a step back and start again, is it too far gone?
- Would we be presented with a broken and impossible system where we are so far behind the bad guys that if we take our foot off the pedal for even a moment, we will ultimately be consumed and overrun?



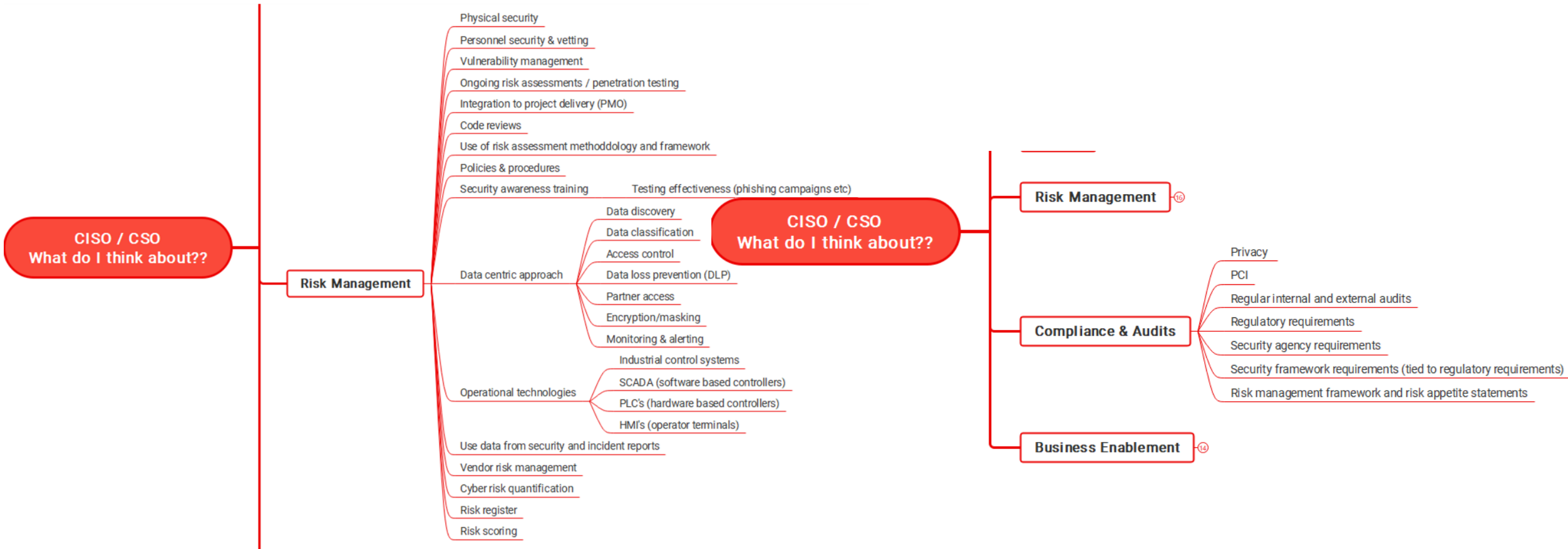
Starting again – What do we need to consider?



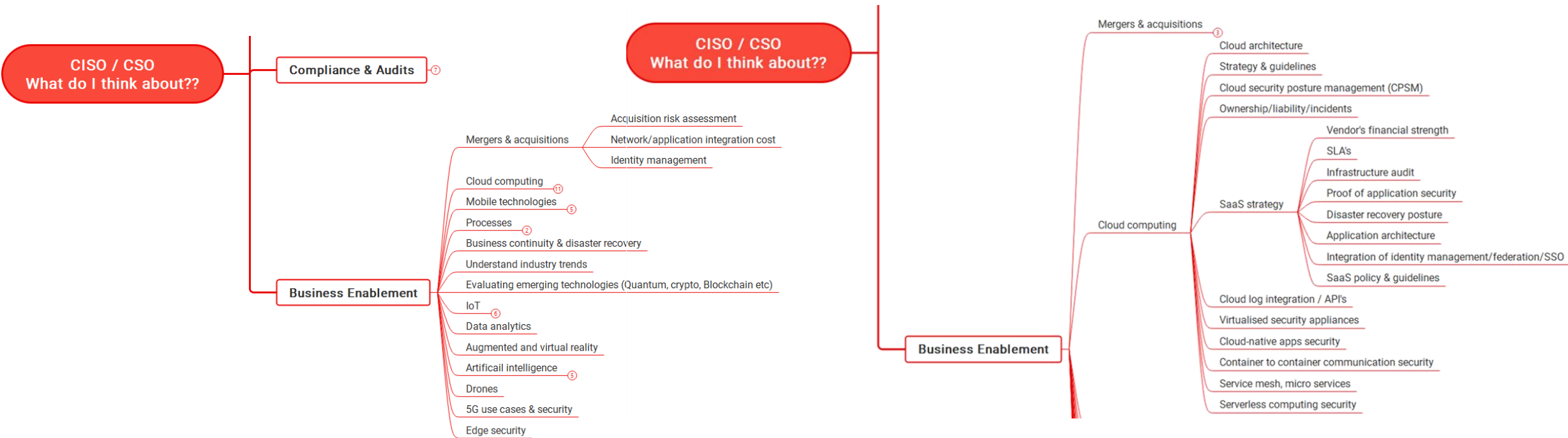
Starting again – What do we need to consider?



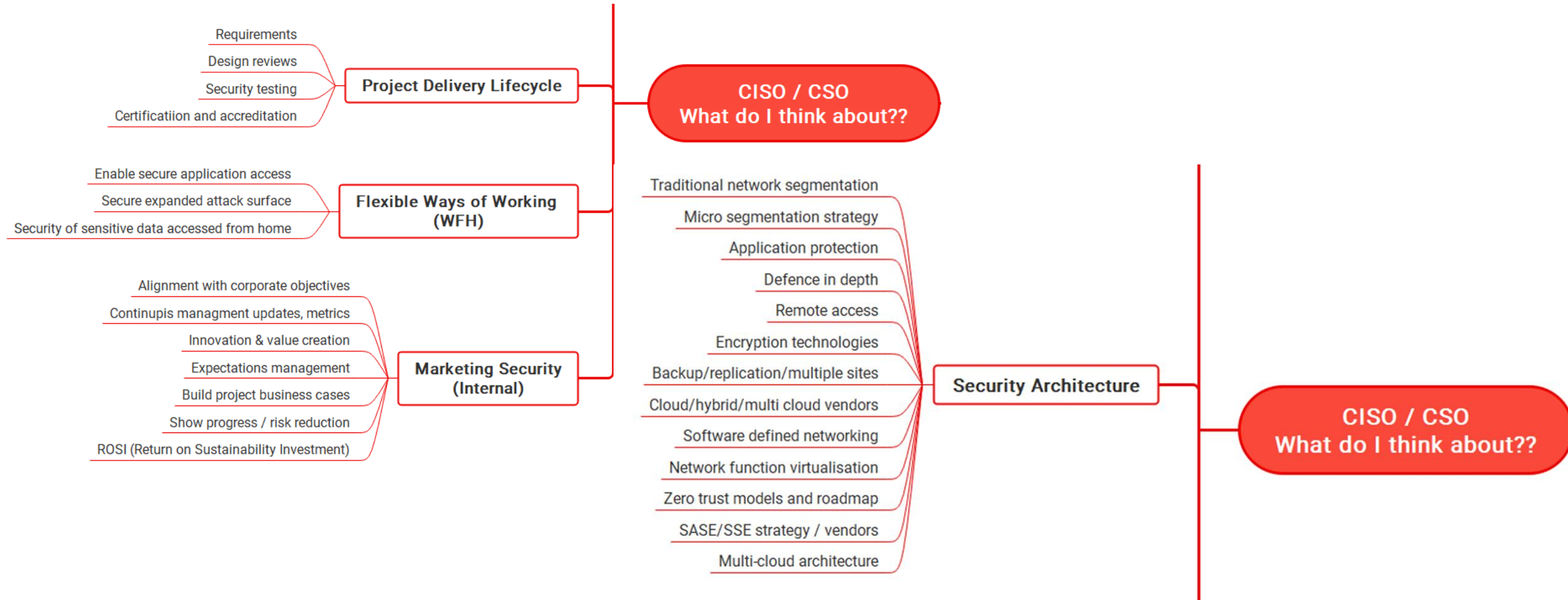
Starting again – What do we need to consider?



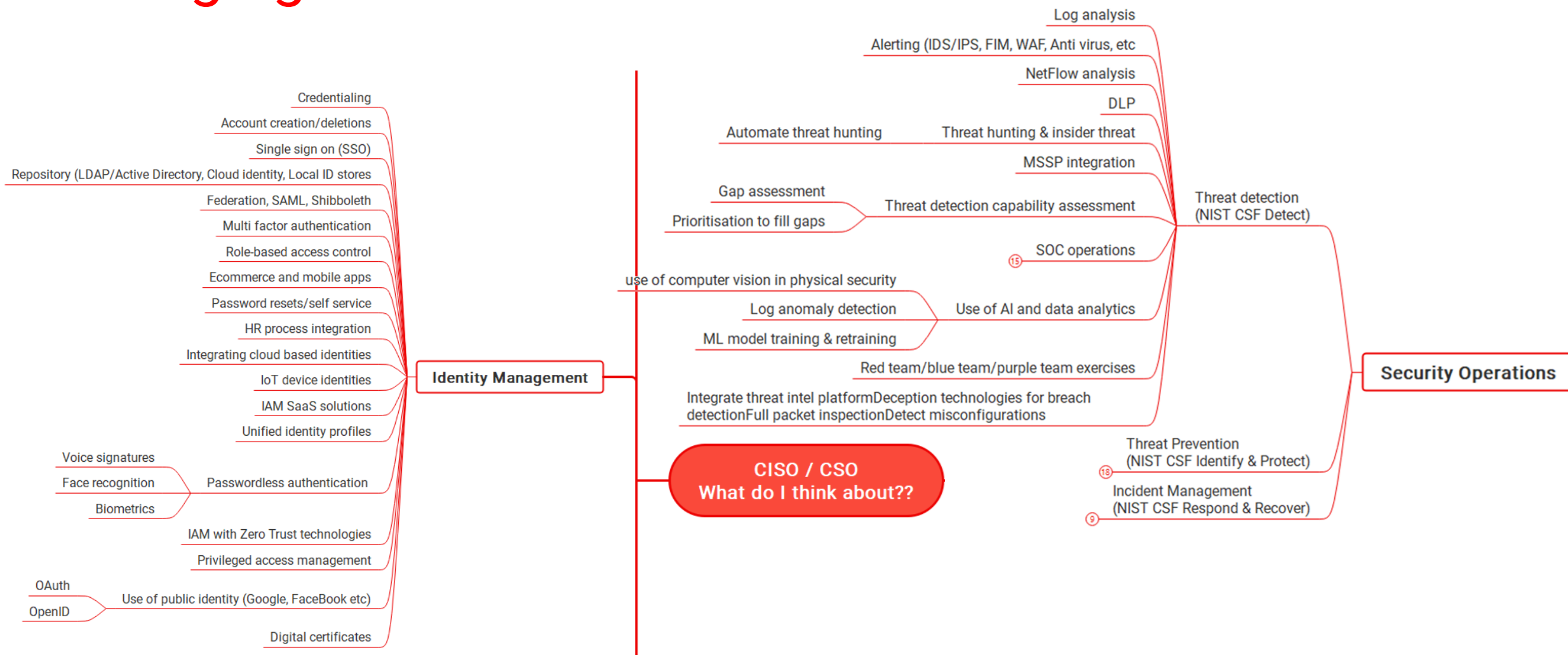
Starting again – What do we need to consider?



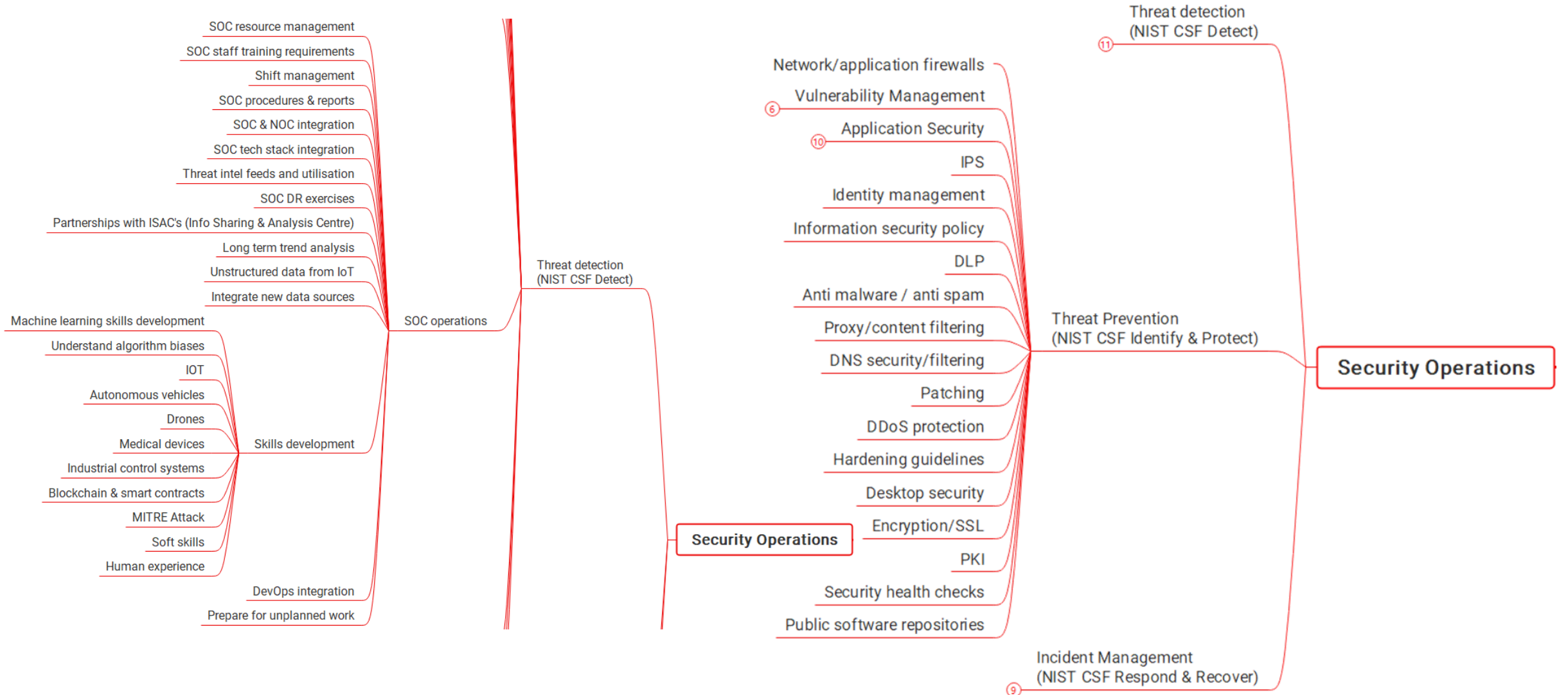
Starting again – What do we need to consider?



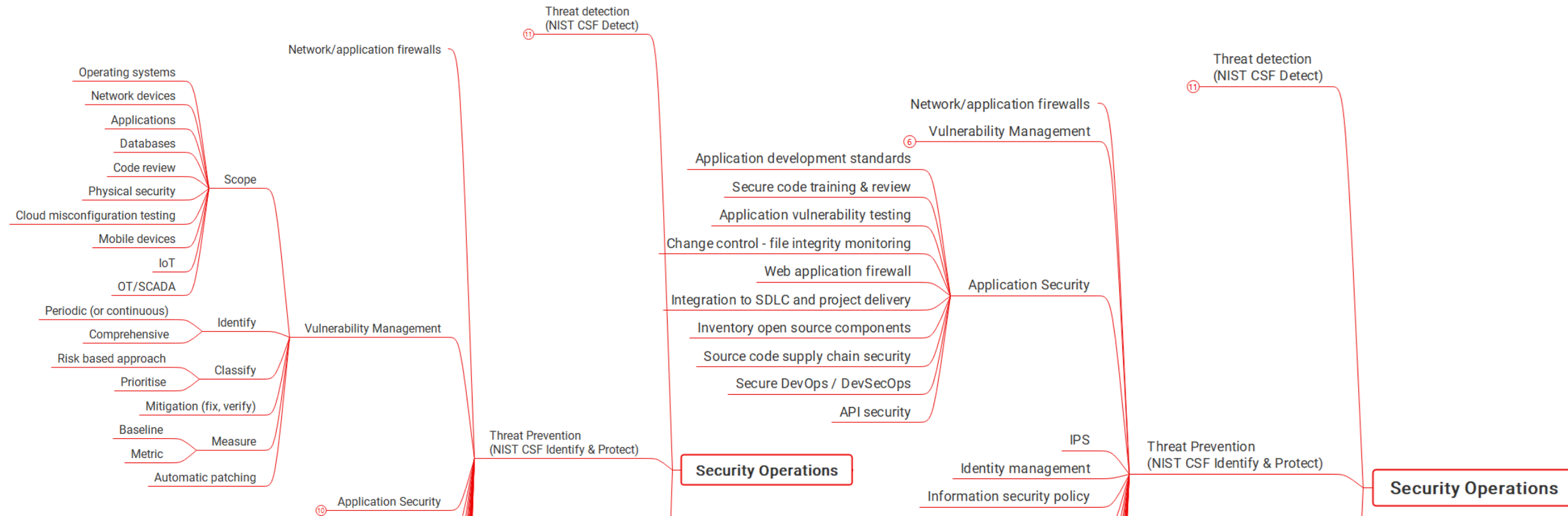
Starting again – What do we need to consider?



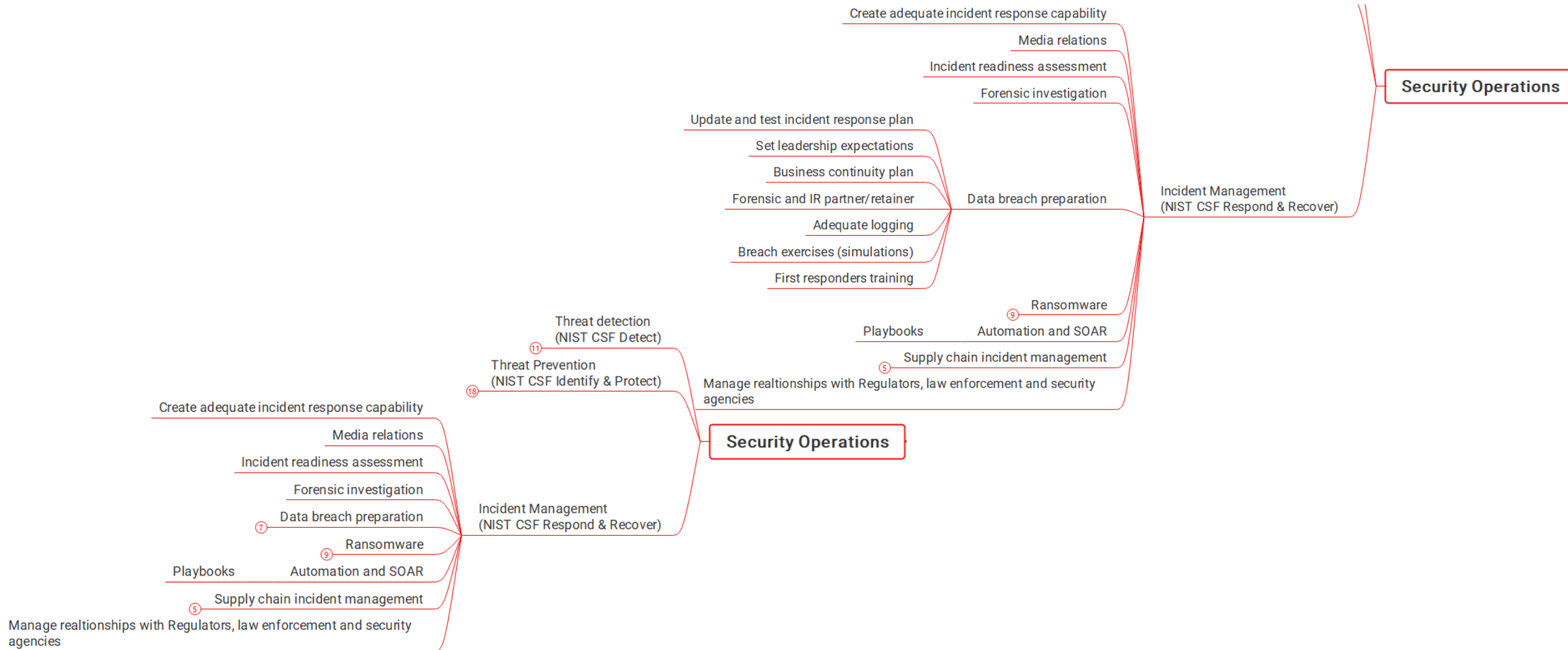
Starting again – What do we need to consider?



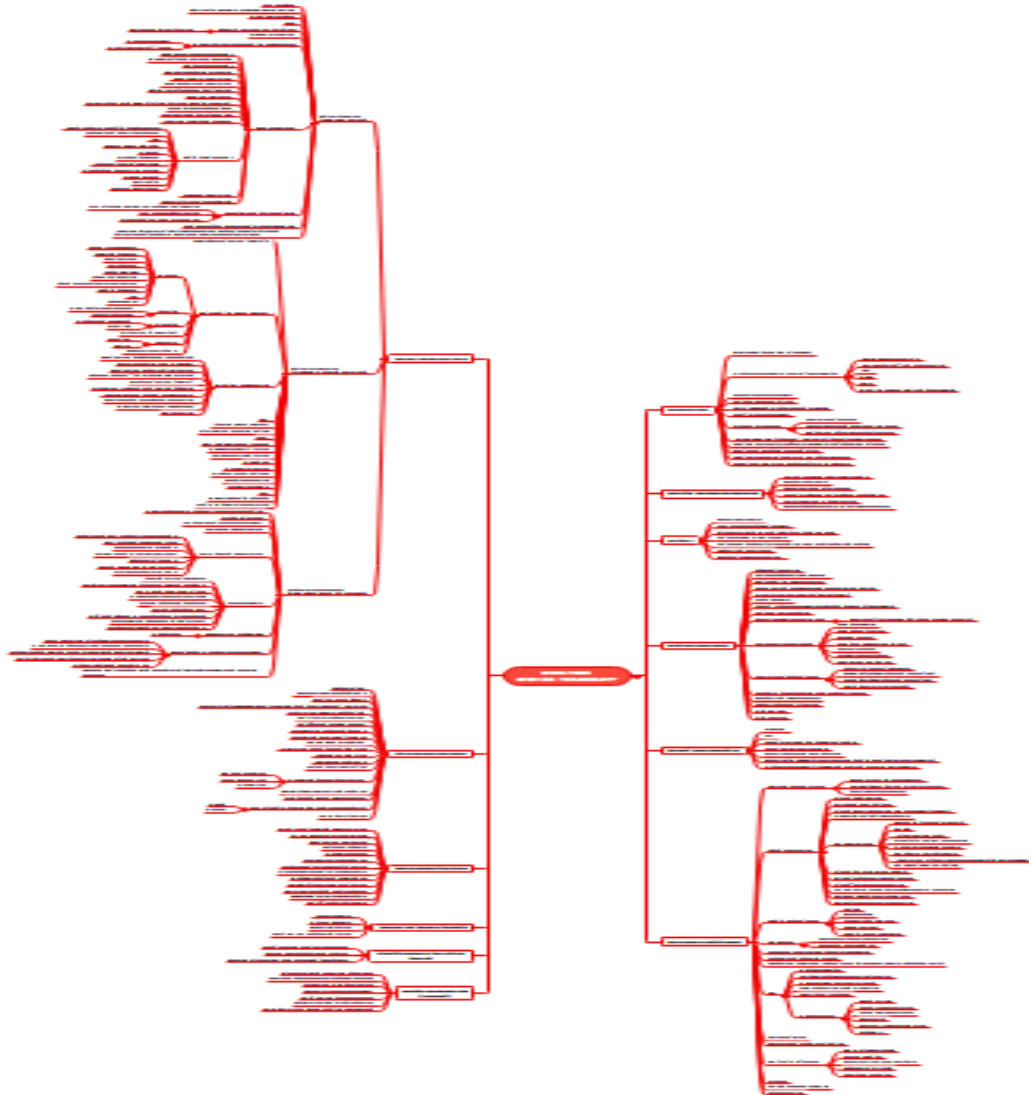
Starting again – What do we need to consider?



Starting again – What do we need to consider?




Starting again – What do we need to consider?



MIND BLOWN!!!


Starting again – What do we need to consider?

Regulatory environment



Security of Critical Infrastructure Act 2018
No. 29, 2018

An Act to create a framework for managing critical infrastructure, and for related purposes




GUIDELINES TO
COUNTER FOREIGN
INTERFERENCE IN
THE AUSTRALIAN
UNIVERSITY SECTOR








University Foreign
Interference Taskforce

Slide 23


Risk Management




NIST Cyber Security Framework

ACSC Essential Eight			
 Application Control <small>To prevent the execution of unapproved applications</small>	 Configure Microsoft Office Macro Settings <small>To block untrusted macros</small>	 Patch Applications <small>To mitigate security vulnerabilities within 48 hours</small>	 User Application Hardening <small>To disable unneeded vulnerable features in Microsoft Office</small>
 Multi-Factor Authentication <small>To reduce risky access to systems</small>	 Restrict Administrative Privileges <small>To limit powerful access to systems</small>	 Patch Operating Systems <small>To mitigate security vulnerabilities within 48 hours</small>	 Daily Backups <small>To keep critical data in record for timely access</small>

Privasec




RISK APPETITE




The 3 Lines of Defense Model


Controls and standards




Security Controls Library




Suite of Security Standards




Consulting & advisory



Education & awareness



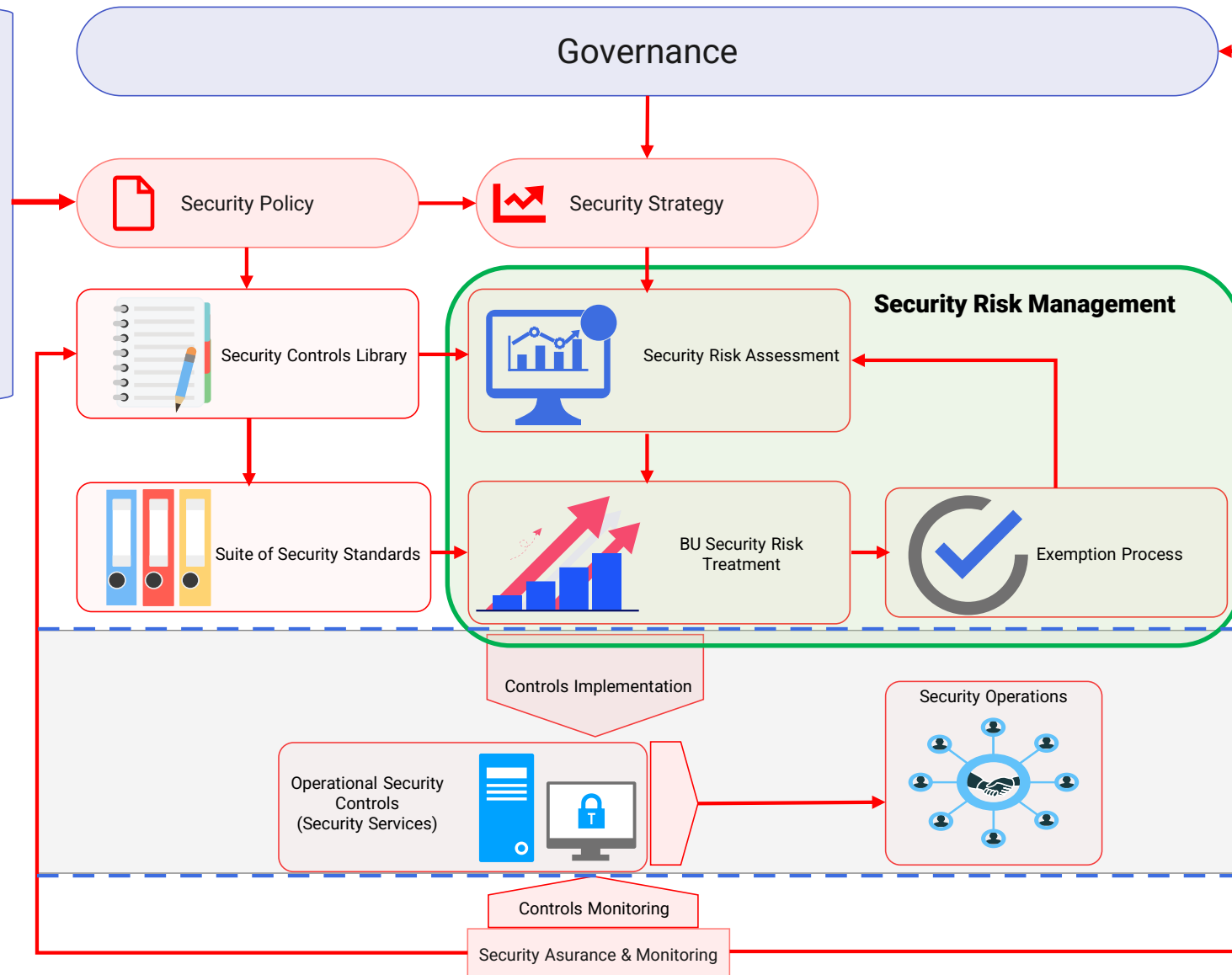
Assurance Review



Good enough security

Starting again – What do we need to consider?

- Business Strategy,
- Business requirements,
- Objectives,
- Technology drivers,
- External drivers such as regulatory requirements
- Organisational risk appetite
- Threat environment



Advisory functions such as policy, strategy, risk assessment, controls and standards advice, governance controls monitoring, and assurance form the backbone of a holistic approach to security

A much smaller operations function that gives effect to the security controls through functions such as vulnerability management, a SOC etc

ADVISORY

Starting again – What do we need to consider?

Visibility

The adage is that you can't protect what you can't see. Make sure you know what your assets are, where they are and who owns them.

The new paradigm

Embrace the new paradigm – cloud, on prem, identity as the perimeter, zero trust, remote working. Don't forget the basics either such as backups, vuln mgt, network segmentation, IAM etc.

Tooling

Invest in the tools that will make a difference and give you the greatest visibility and defences. Defence in Depth is a must – multiple layers of defence to ensure that people, assets and reputation are secured.



Risk

At the end of the day – security is all about risk. You can't do everything so make sure effort and resource is pointed at the things you care about

Education & Awareness

Security is a people issue. Think about things like recommending home network security for employees – it makes a difference to security posture overall.

Buy in & Support

Spend a lot of time making sure that you have the buy in and support you need from the IT business and the rest of the business to make sure your program can work. Remember senior execs and Board.

Today's Session

1

A brief history

A whirlwind tour of the history of the security discipline and how it has sort of evolved...

2

How did we defend?

The way we have defended these threats has evolved. Let's look at then vs now...

3

Starting again...

If we had the ability to stop time and step back and think again, what would we consider...

4

What about the future?

We know what we know but the great challenge for all of us is the future – how do we set ourselves up for success and what do we need?

What about the future???

- Privacy Rights - To cover 5 Billion citizens and 70% of global GDP (2023)
- Consolidation - 80% will unify web and cloud services from a single SSE platform (2025)
- Zero Trust – 60% will fail to realise benefit (2025)
- Third Party – 60% will use cybersecurity risk as a primary determinant for business transactions (2025)
- Ransomware Threat – 30% of nations to pass legislation on ransomware (2025)
- Weaponised OT – will result in human casualties (2025)
- Resilience – 70% of CEOs to mandate a culture of organisational resilience
- Board Governance – 40% to have dedicated cyber committees and 50% to have performance requirements for C-Level



**Thanks for watching
and Best of luck!!**

