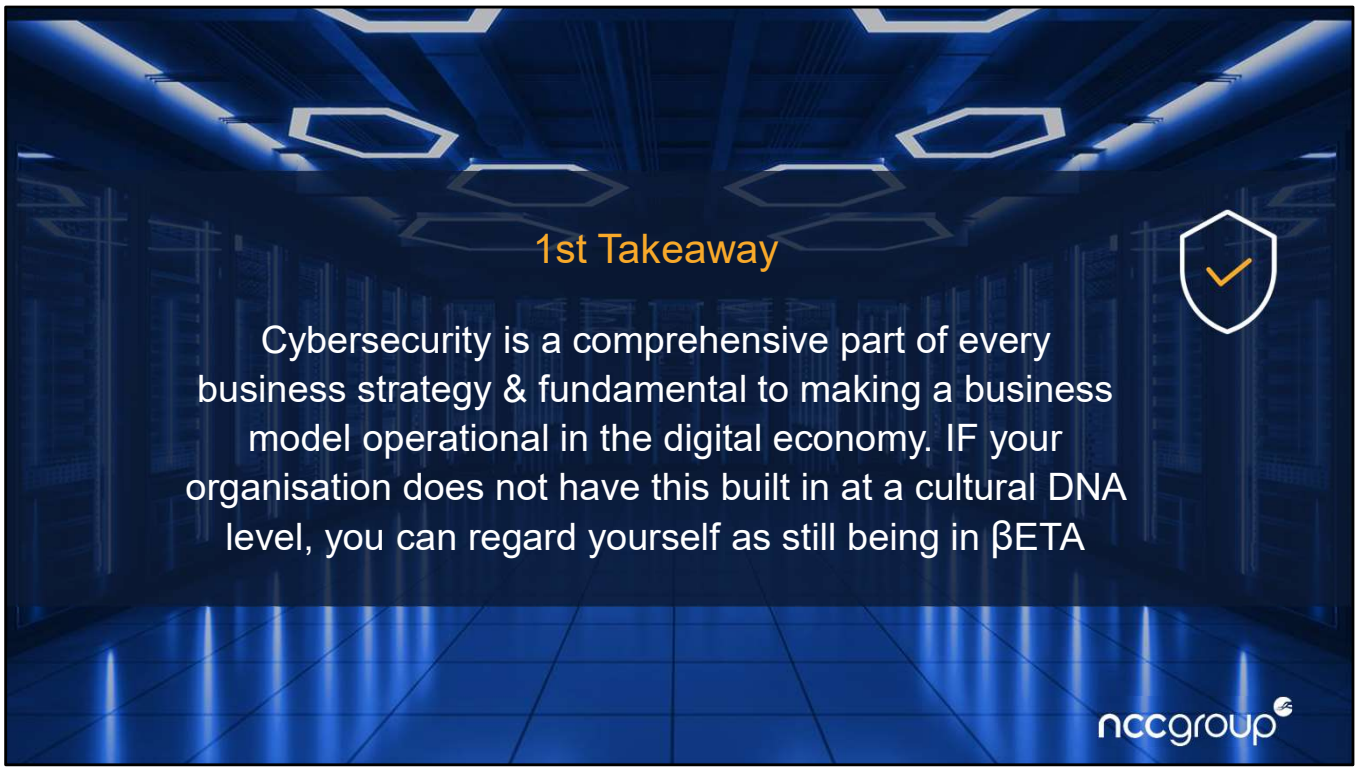
Please visit our stand out in the lobby area to meet me and my NCC Group colleagues – we can share examples of how we're securing our global FS client base.

Financial Services is experiencing the most intense disruption and evolution of all industries, and this has accelerated as a result of the global pandemic. NCC Group's Senior Adviser and Global Cloud Security Practice Lead, Nigel Gibbons, will touch on the sector's hot topics such as growing automation, the rise of fintech and a deep shift in the ways consumers expect to access services. While dealing with these growth opportunities, banks, insurance companies, asset managers and private equity firms need to maintain trust and reputation with their stakeholders.

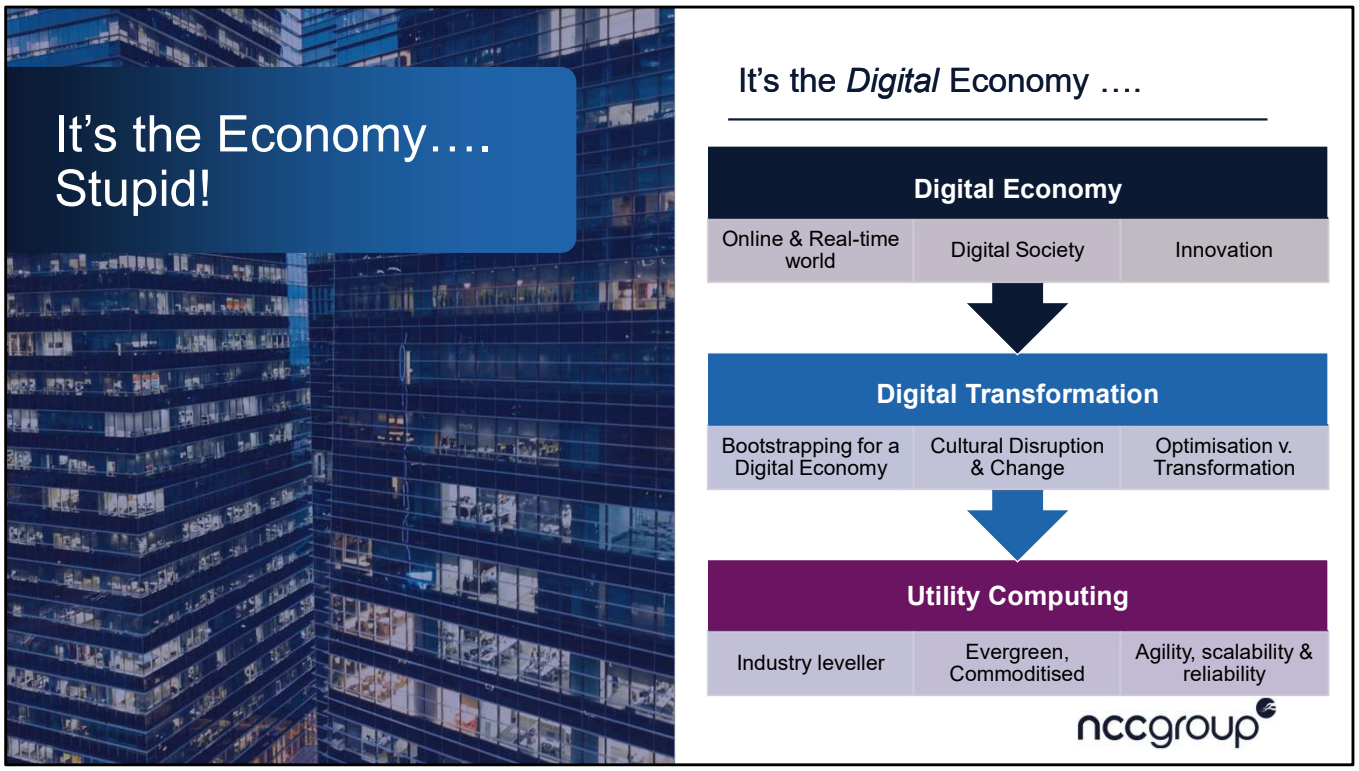
Nigel will share examples of how NCC Group is helping executive boards establish an end-to-end cyber security risk management approach that also incorporates the latest threat intelligence, issues arising from geopolitical instability and keep on top of the increasingly complex compliance and regulatory landscape.

If there are two things and two things only you take away form today let them be:



1st - Cybersecurity is a comprehensive part of every business strategy & fundamental to making a business model operational in the digital economy. IF your organisation does not have this built in at a cultural DNA level, you can regard yourself as still being in BETA

Cybersecurity is a fundamental enabler of the digital economy and is already influencing the success and failure of business and national stability.



We live in a digital society, doing business in a digital economy, increasingly reliant on digital systems to keep balance across our lives, environment, and material conveniences.

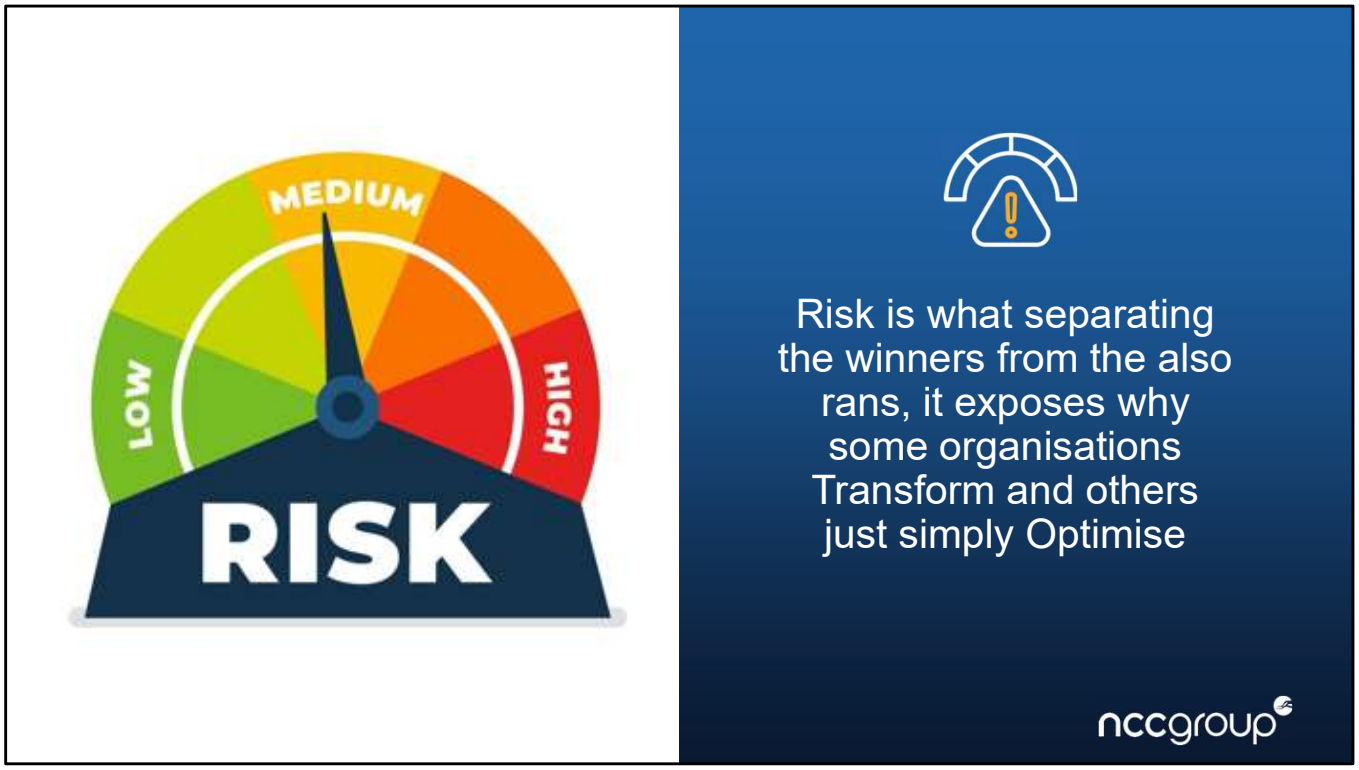
Cybersecurity has become a crucial component of modern business strategy due to the increasing frequency and sophistication of cyber-attacks. Implementing strong cybersecurity measures can help protect a company's assets, reputation, and customer trust, as well as the increase demands from compliance with regulations.

We see all around us and you will no doubt have experienced it first-hand the transformational movement that promises to pave the road for our smooth ride into a rosy digital future.

So if the formulae is so simple WHY are organisations failing to realise their full potential and feel unincumbered to press that virtual accelerator of business growth to the floor?

With digital transformation in some form taking place in 96% of organisations and 90% of those using cloud, the inevitable complexity of those environments become a barrier to implementing proper data security measures. But we don't have time to get into the

weeds of the many why's because upstream there is an all-encompassing rationale.



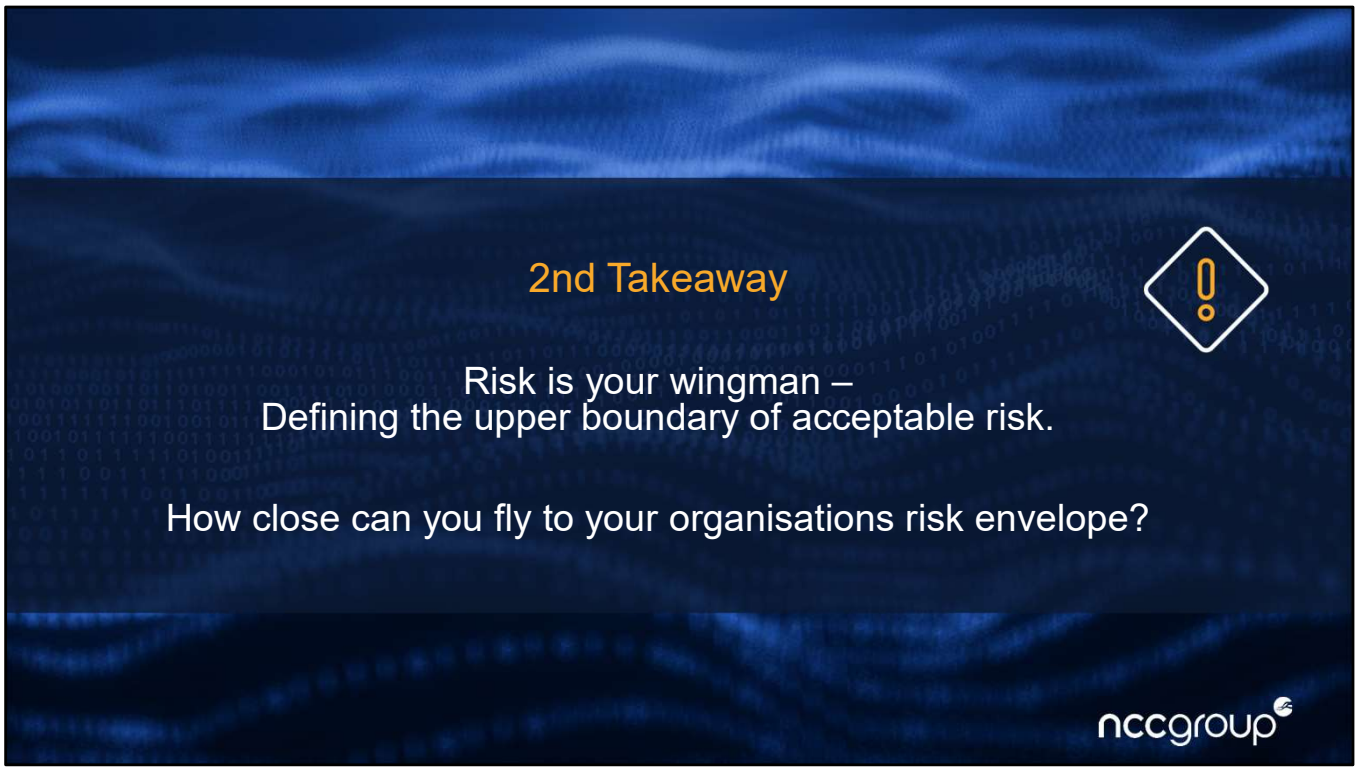
Risk is what separating the winners from the also rans, it lies behind why some organisations Transform and others just simply Optimise. Every decision an organisation makes has the potential to introduce risk, one of the biggest can be technology or digital solution choices. Technology evolution and dynamics is changing so fast that relying on technology for Risk Management itself becomes its own risk surface.

With regulation beginning to set benchmarks for digital resilience in the financial industry, heralds a future that will mandate that Cyber security risk be integrated into the overall organisational approach to risk management at all levels.

A current trend of dealing with cyber security risk as a standalone topic will make it hard to recognise its wider implications. Conversely the trait we also see of collapsing it into 'IT Risk' is an oversimplification and perhaps the biggest risk of all!

All risk professionals recognise that accurate quantification is only as good as the data going in. Cyber risk is no different but there is a lack of accurate and consistent inputs which of all sectors the Financial alongside the Insurance Services sectors should be ahead of the curve on.

Why! - Remember I said there were 2 takeaways … here comes number 2.



Identify and quantify the level of risk you are willing to accept in pursuit of your objectives and to establish appropriate risk management strategies and controls to manage and mitigate those risks.

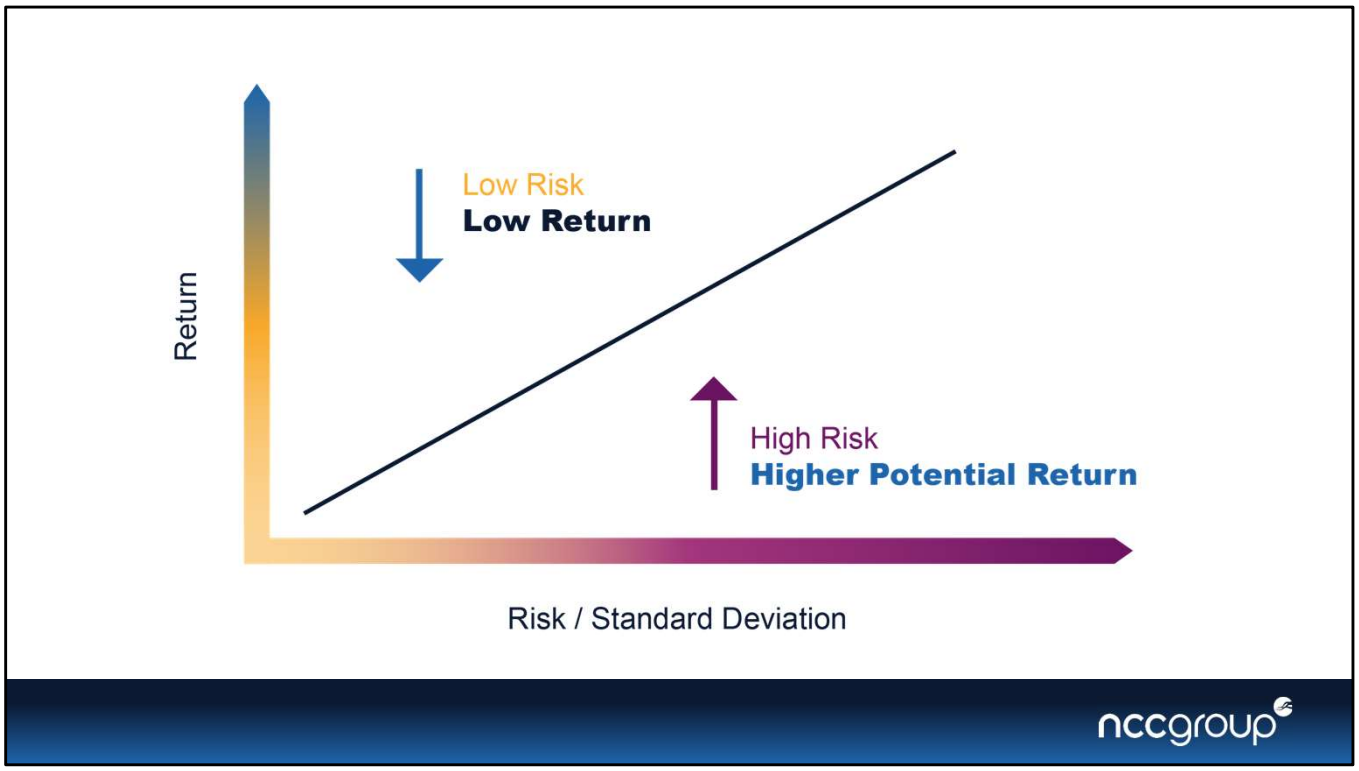
The digital transformation has accelerated significantly in recent years. The pandemic has opened up financial services markets to new providers, both fintech and, more recently, large technology companies who are searching for ways to boost their revenues.

The intense competition from digital native organizations brings new competitive dynamics to the market, and for many legacy organizations, it's becoming more challenging than ever to catch up.

The adoption of technology has been progressing in layers, with newer technology being built on top of existing solutions. As a result, the amount of legacy technology and code that these organizations need to maintain staggers the further digital transformation. As old technologies are often incompatible with new digital standards, such as UX, mobile-friendliness, and multi-channel capabilities, organizations often need to find workarounds that enable them to take advantage of the legacy technology they already have in the new world.

The key to success is to kill everything in your backlog that isn't aligned with your company's strategic priorities. The initiatives that pass this test must be reexamined and realigned in order to realign the entire organization on delivering the best possible service to end customers as a matter of policy.

Today, technology skills are no longer highly centered in IT; they need to be present across organizational functions and coupled with soft skills to achieve transformation success.



The risk envelope is determined by various factors, such as the organization's risk tolerance, risk appetite, and risk capacity, as well as regulatory requirements and other external factors. It helps organizations to identify and quantify the level of risk they are willing to accept in pursuit of their objectives, and to establish appropriate risk management strategies and controls to manage and mitigate those risks.

The risk envelope can be visualized as a boundary or boundary conditions that define the range of risks that an organization is willing to accept. It can be represented graphically as a curve that shows the relationship between risk and reward, with the risk envelope defining the upper boundary of acceptable risk.

Financial org.s and Banks for example will inevitably move their core functions to the cloud whether that happens in a few months or a few years. Few Banks that have not begun their cloud journey and Accenture research suggests that 82% of them plan to have at least half of their mainframe workloads in the cloud 10 years from now, and 31% of them have already reached that stage.

Financial orgs. are facing increasing competitive pressures from new entrants, including both digital-first banks and non-bank providers moving into the financial services arena. These tech-focused companies are embracing the full functionality of cloud and raising the bar with their products, creating higher customer expectations. Banks will need to harness the power of their cloud transition, including their core, to meet those expectations in terms of speed and responsiveness.

With digital transformation in some form taking place in 96% of organisations and 90% of those using cloud, the inevitable complexity of those environments become a barrier to implementing proper data security measures.

Why are organizations failing to meet their digital transformation security goals?
They are NOT all executing properly or optimizing the allocation and use of resources in managing digital economy cyber-related risks.

Action – Achieve a greater level of integration between security functions and the business (Investment in better internal and external partnerships)

Goal – To realise their business outcomes faster and more securely, in real-time

Digital transformation is not simply the adoption of new technology; it requires significant structural and process changes. However, traditional financial services enterprises often already have a very strong organizational culture. The old culture is often resistant to change or implementing new workflows, hindering new digital initiatives.


People led knowledge and capability is at our core
nccgroup
www.nccgroup.com
Twitter: @NCCGroupplc @NCCGroupInfoSec