nccgroup

People powered, tech-enabled cyber security

Quantifying Cyber Risk & Managing Hidden Threats

Nigel Gibbons - Senior Advisor & Director of Global Cloud Security Services

21 November 2024

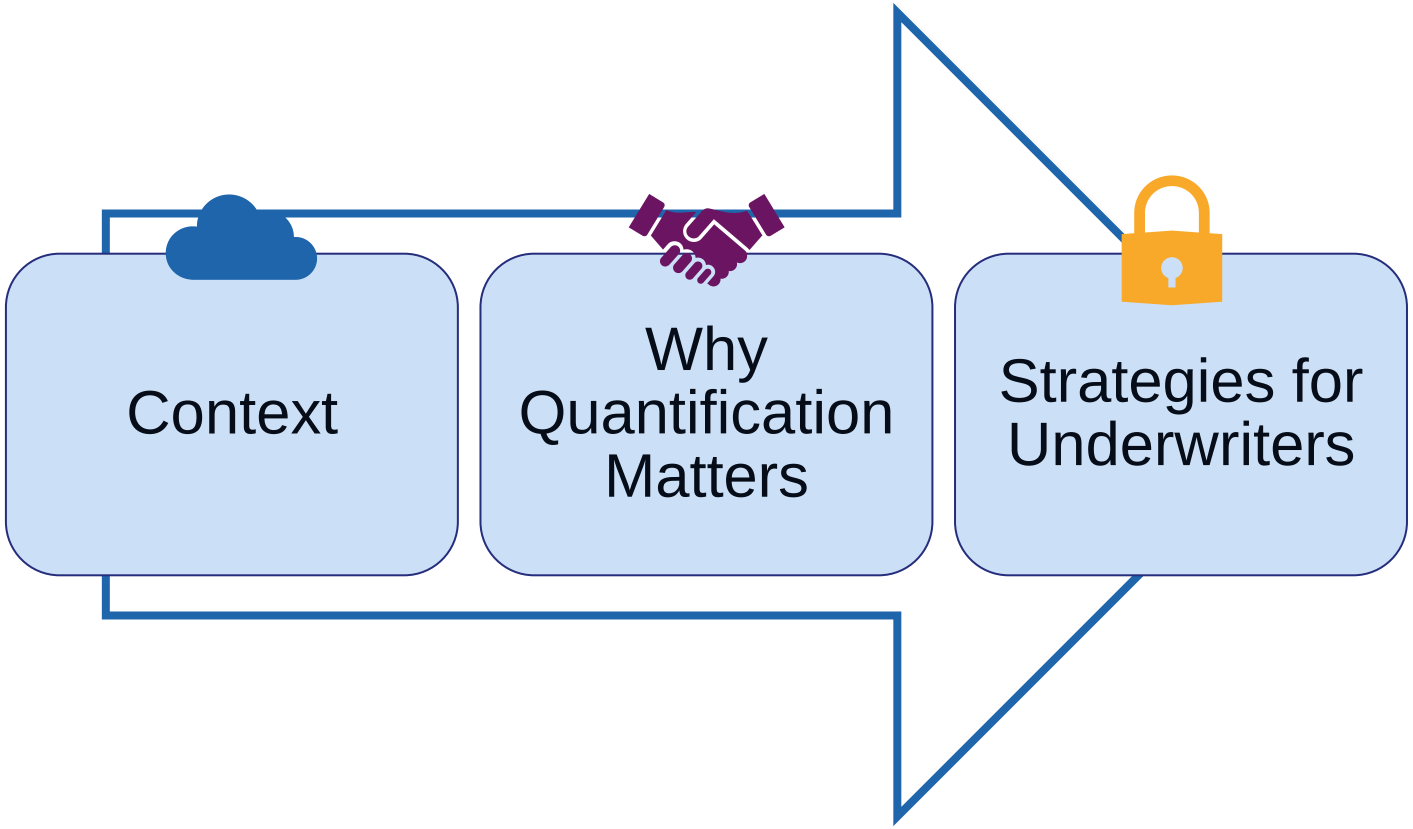
People powered, tech-enabled cyber security

Cyber Security for Digital Transformation

Regulatory Compliance

Enterprise Cyber Resilience

Today’s Journey



Context

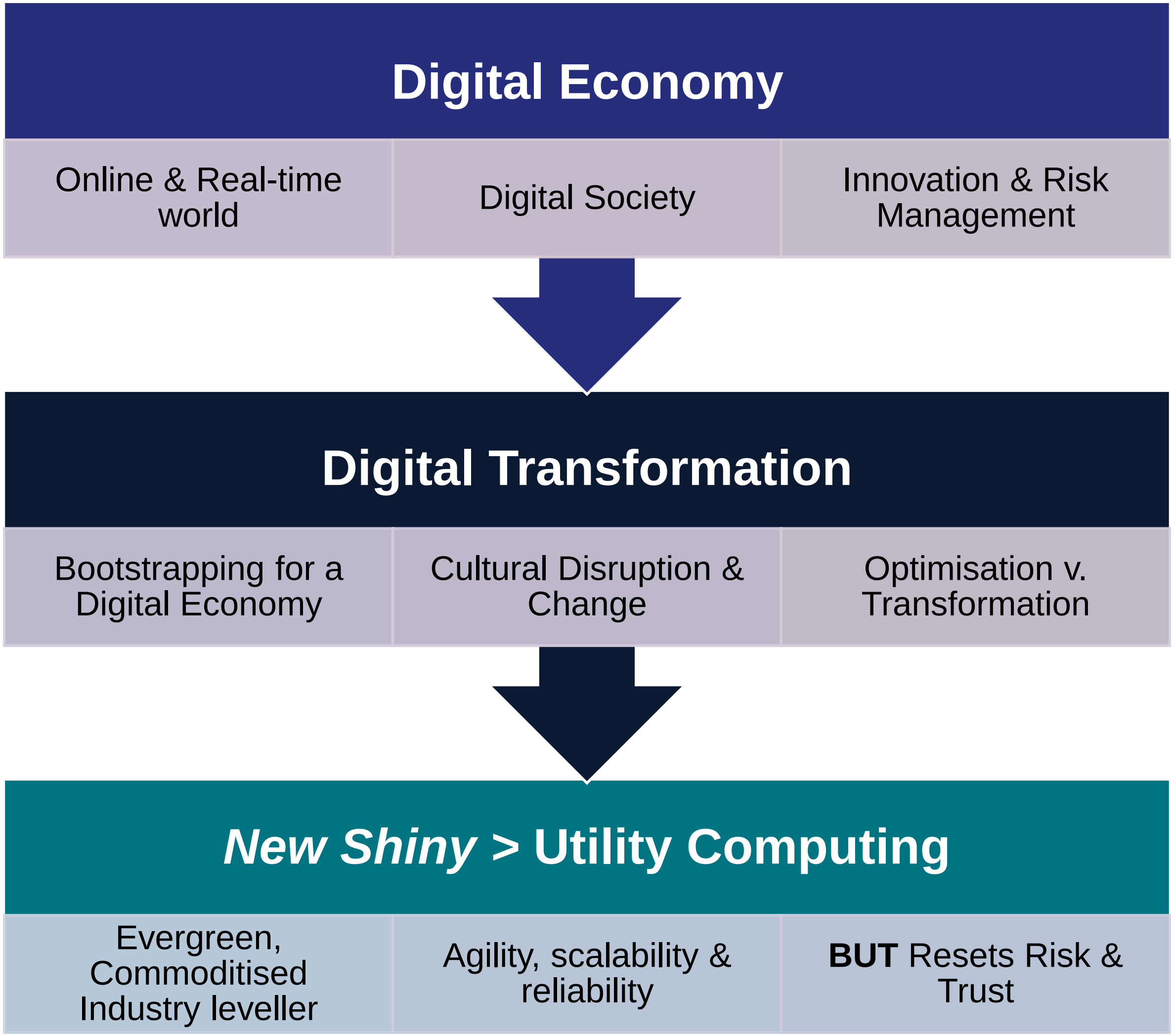
Why Quantification Matters

Strategies for Underwriters

Context

Cyber Risk In Context

It’s the Digital Economy ….



Digital Economy

Online & Real-time world

Digital Society

Innovation & Risk Management

Digital Transformation

Bootstrapping for a Digital Economy

Cultural Disruption & Change

Optimisation v. Transformation

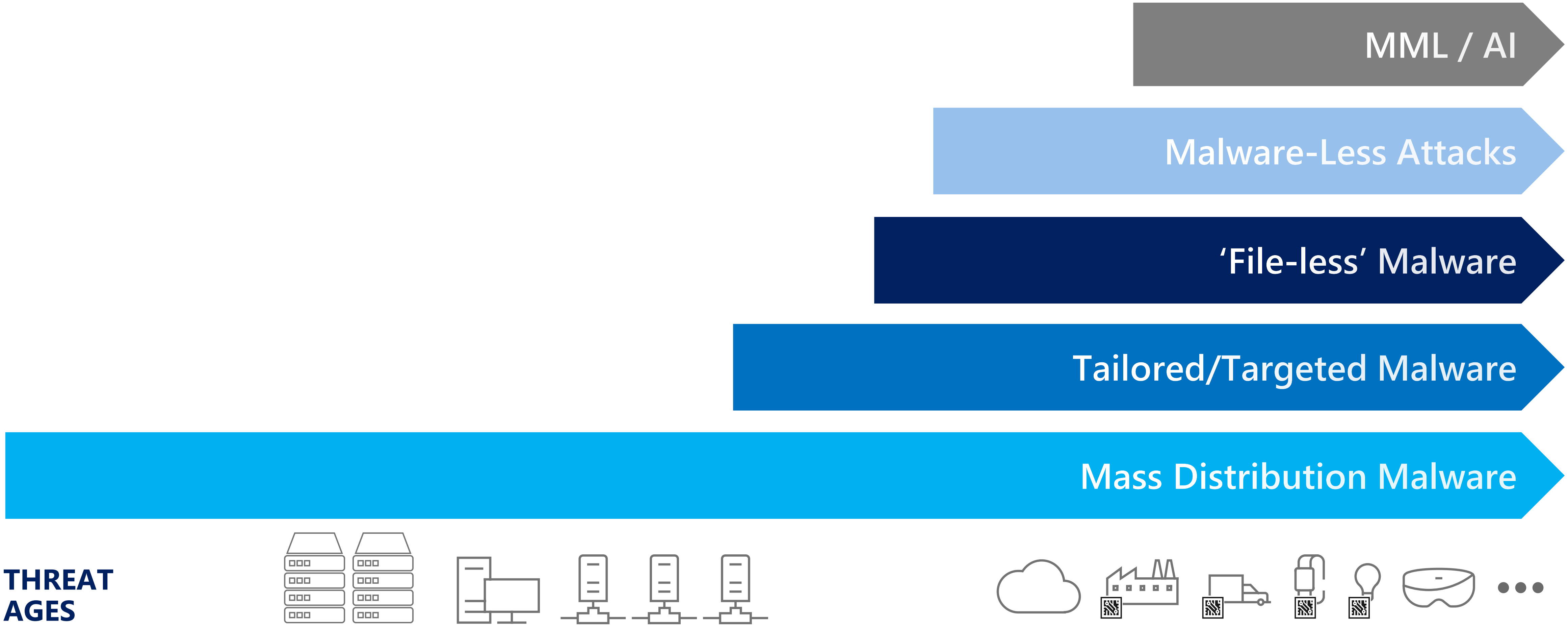
***New Shiny* > Utility Computing**

Evergreen, Commoditised Industry leveller

Agility, scalability & reliability

BUT Resets Risk & Trust

Threat Intelligence Is Accelerating



MML / AI

Malware-Less Attacks

'File-less' Malware

Tailored/Targeted Malware

Mass Distribution Malware

THREAT AGES

Malware and Infrastructure

Identity, Apps & Supply Chain

LMF Cyber Summit

1st Takeaway

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

nccgroup

Poll 1

Generative AI, Quantum Computing and Embedded Systems / IoT are among the most prominent emerging risks we are currently seeing.

Which of these emerging risks are currently a priority for you to deal with?

A. Generative AI

B. Quantum Computing

C. Embedded Systems/IoT

D. Other

LMF Cyber Summit

Why Quantification?

Why Quantification Matters

Despite challenges, quantifying cyber risk is essential. It enables organisations to:

Assess Exposure Accurately - By assigning measurable values to potential risks, to better understand an organization's exposure and set appropriate premiums.

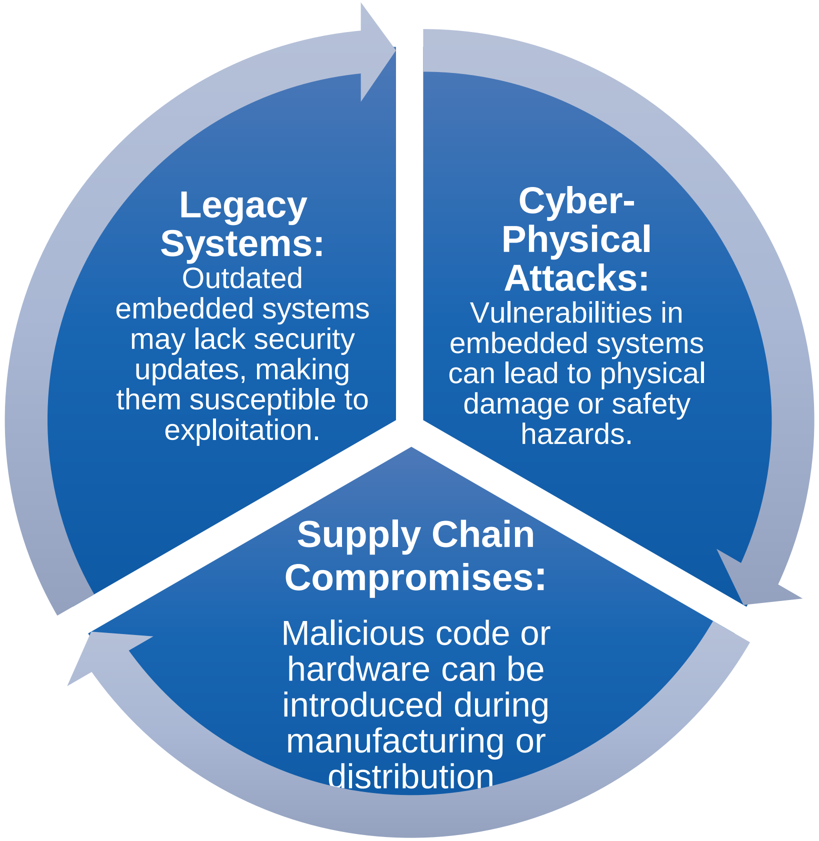
Enhance Decision-Making - Quantification provides a data-driven foundation for underwriting decisions, risk selection and portfolio management.

Facilitate Communication - Clear metrics help convey risk levels to stakeholders (underwriters), clients and regulators in a comprehensible way.

LMF Cyber Summit

Managing Hidden Threats - The Case of Embedded Systems

Embedded systems are integral to a wide range of devices and infrastructure, from industrial control systems to consumer electronics. The risks they pose include:



Legacy Systems: Outdated embedded systems may lack security updates, making them susceptible to exploitation.

Cyber-Physical Attacks: Vulnerabilities in embedded systems can lead to physical damage or safety hazards.

Supply Chain Compromises: Malicious code or hardware can be introduced during manufacturing or distribution

Underestimation of Threats - Embedded systems are often perceived as benign or low-risk due to their specialized functions.

Lack of Visibility - These systems may not be included in regular IT security assessments.

Complexity in Assessment - Evaluating the security of embedded systems requires specialized knowledge and

Forensic Limitations in the Cloud

Access to Physical Hardware - Forensic investigations often require access to physical hardware; however, in cloud environments, this hardware is managed by service providers, limiting forensic activities.

Chain of Custody - Establishing and maintaining a clear chain of custody for digital evidence in the cloud is problematic because of the virtual and distributed nature of the infrastructure.

Tool Effectiveness - Forensic tools that were originally designed for on-premises environments may not be effective or applicable in cloud environments, necessitating the development of new methodologies and tools.

Data Collection - Collecting relevant data for forensic analysis is more complex in a cloud setting due to the dynamic provisioning and de-provisioning of resources.

Legal and Compliance Issues - There are jurisdictional challenges and compliance issues related to data location and access, as data stored in the cloud can reside in multiple countries, each with its own set of laws and regulations.

API & Integration Exposure - Many cloud services operate with extensive use of APIs, which, if compromised, can give incidents ie: ransomware an additional propagation vector across systems and services.

LMF Cyber Summit

Evolutionary Risk – A new ‘Panacea’ on the Block?

AI BENEFITS

✓ **Enhanced Detection Capabilities**

- Real-time Threat Detection - AI can process vast amounts of data at speed.
- Anomaly Detection - AI models are particularly adept at identifying deviations from normal behaviour.

✓ **Predictive Capabilities**

- Threat Anticipation - Through predictive analytics by analysing trends and patterns.
- Risk Assessment - AI can automate the risk assessment process.

✓ **Automation of Routine Tasks**

- Incident Response - AI can automate responses to common threats and reduces human error.
- Log Analysis - AI can automate the analysis of vast logs.

✓ **Improved Investigation Efficiency**

- Root Cause Analysis: AI can assist in quickly determining the cause of a breach.
- Forensics: AI tools can sift through massive datasets to identify relevant evidence.

AI CHALLANGES

X **Complexity of Integration**

- Data Silos - Integrating AI across diverse and distributed cloud services.
- Compatibility Issues - Existing security infrastructure might not seamlessly integrate with AI tools.

X **Reliance on Quality Data**

- Data Dependence - The effectiveness of AI is highly dependent on the quality of the data it is trained on.
- Bias in Data - AI systems can inherit biases.

X **Skill Gap**

- Expertise Requirements - Deploying and managing AI-based security solutions require specialized skills.
- Continuous Learning Need - AI systems require ongoing training and fine-tuning.

X **Security of AI Systems Themselves**

- Vulnerability to Manipulation - AI systems can be targeted by attackers aiming to manipulate their LLM’s.
- Transparency Issues - The "black box" nature of AI.

nccgroup

Strategies

The Digital Edge

Cyber Security – Qualifying Risk

Is fundamental to making a business model operational in the digital economy.

Risk > Resilience > Reward

Consider the risk of moving too slowly, challenger Org's are …

All organisations make decisions based on risk –
and smart organisations will consider the risk of moving too slowly -
defining the upper boundary of acceptable risk builds resilience

Strategies for Underwriters

Integrate Multidisciplinary Approaches

Combine insights from cybersecurity experts, engineers and risk analysts to create a holistic view of the risk landscape.

Enhance Data Collection

Encourage clients to maintain detailed records of cyber incidents and share anonymized data to build a more robust industry dataset.

Adopt Standard Frameworks

Utilize standardized risk assessment frameworks to ensure consistency and comparability in evaluations.

Educate Clients on Hidden Risks

Raise awareness about the importance of securing embedded systems and the potential impact on their operations and insurance coverage.

Stay Informed of Emerging Threats

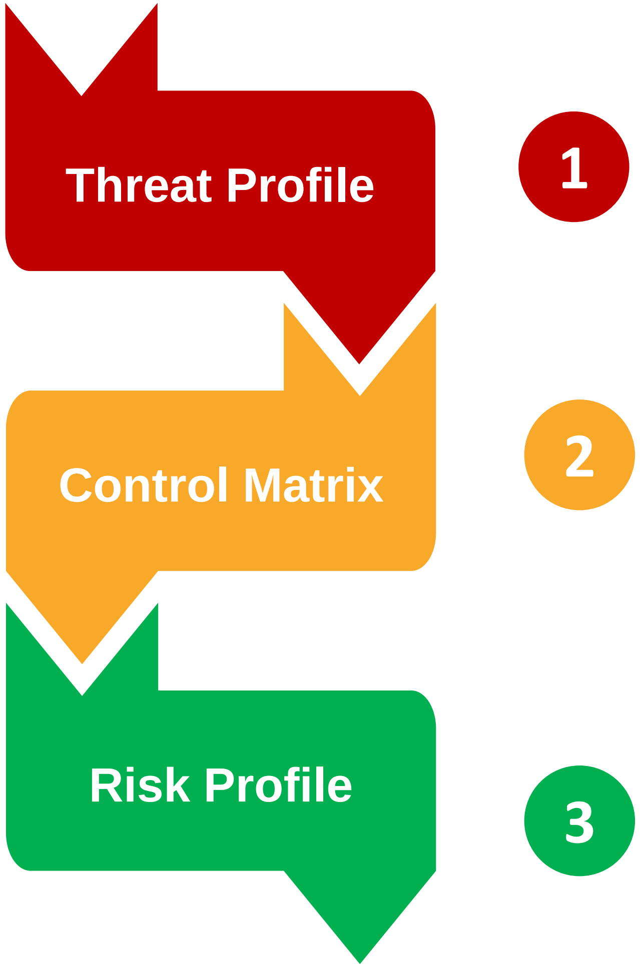
Regularly update your knowledge base with the latest developments in cyber threats and mitigation techniques.

2nd Takeaway

Risk is your wingman –
The better an organisation understands its risk landscape, the more effectively it can build resilience and the easier to underwrite!

As your clients … *How close can you fly to your organisations digital risk envelope?*

Risk Management Foundations – 1. Gain Threat & Risk Visibility



Define the organization unique Threat profile that the rest of the process is built on:

- Threat profiling / scenario workshops
- Attack tree exercises
- Resilience (response) exercises

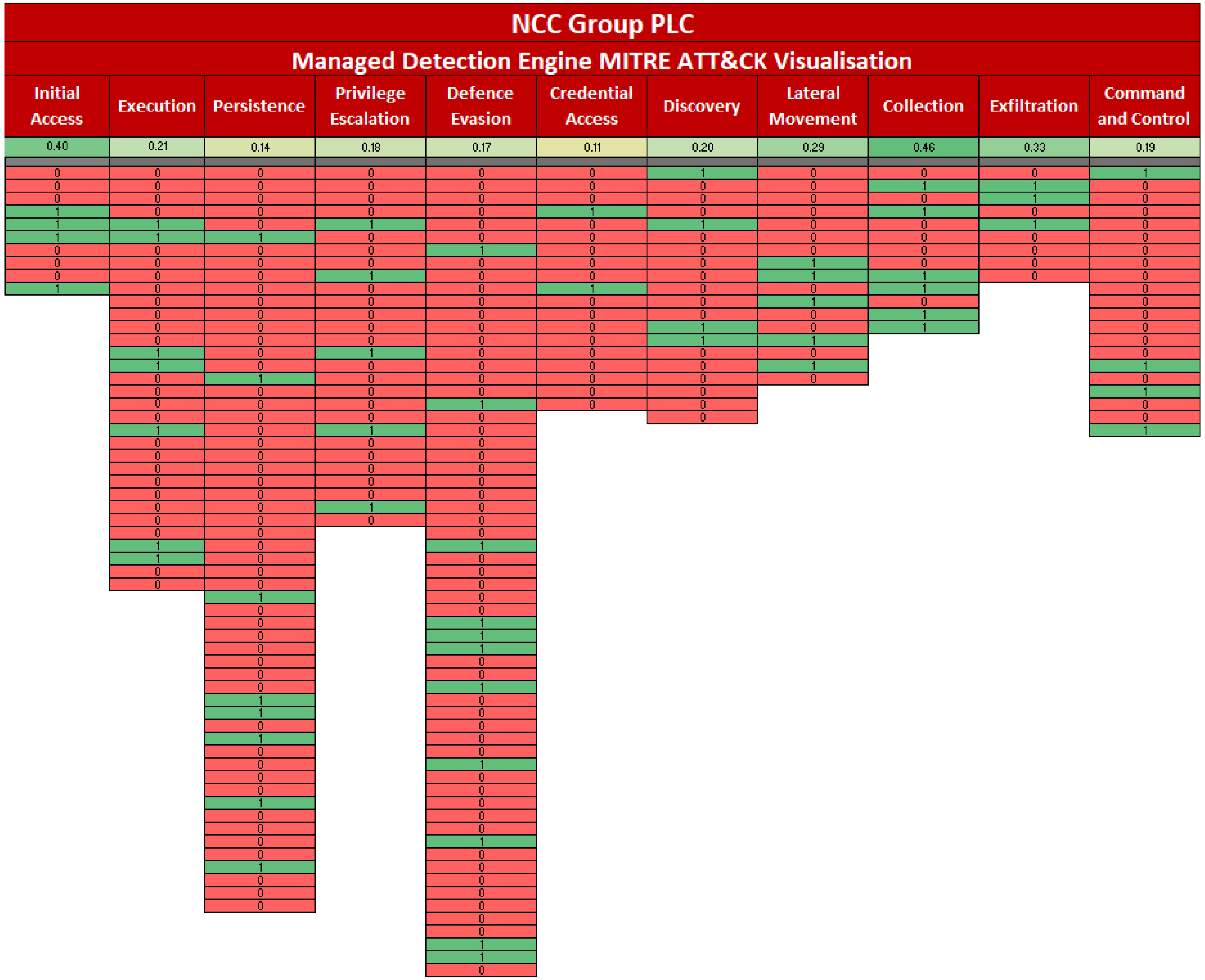
Using the Cyber Kill Chain, the Miter Att&cK framework with NCC red team experience against regulatory frameworks, to produce a unique ‘*Cyber Fingerprint*’:

- Map threats to the Miter Att&ck framework
- Overlay existing controls (standards based ie:NIST, CIS-18 etc) - technical, people & process.

Consolidated into business specific impacting risk events to apportion monetary loss against, to produce a Cyber balance sheet.

- Business & InfoSec Workshop
- Risk Impact Report
- Illustrated with 5x5 Risk Matrix and Spider diagram gap analysis/exposure
- Mapping to actual business service line cost of impact

MITRE Att&ck Illustration – 2. Visibility of Your Unique Cloud Cyber Fingerprint



NCC Group PLC

Managed Detection Engine MITRE ATT&CK Visualisation

Initial Access	Execution	Persistence	Privilege Escalation	Defence Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
0.40	0.21	0.14	0.18	0.17	0.11	0.20	0.29	0.46	0.33	0.19
0	0	0	0	0	0	1	0	0	0	1
0	0	0	0	0	0	0	0	1	1	0
0	0	0	0	0	0	0	0	0	1	0
1	0	0	0	0	1	0	0	1	0	0
1	1	0	1	0	0	1	0	0	1	0
1	1	1	0	0	0	0	0	0	0	0
0	0	0	0	1	0	0	0	0	0	0
0	0	0	0	0	0	0	1	0	0	0
0	0	0	1	0	0	0	1	1	0	0
1	0	0	0	0	1	0	0	1		0
	0	0	0	0	0	0	1	0		0
	0	0	0	0	0	0	0	1		0
	0	0	0	0	0	1	0	1		0
	0	0	0	0	0	1	1			0
	1	0	1	0	0	0	0			0
	1	0	0	0	0	0	1			1
	0	1	0	0	0	0	0			0
	0	0	0	0	0	0				1
	0	0	0	1	0	0				0
	0	0	0	0		0				0
	1	0	1	0						1
	0	0	0	0						
	0	0	0	0						
	0	0	0	0						
	0	0	0	0						
	0	0	0	0						
	0	0	1	0						
	0	0	0	0						
	0	0		0						
	1	0		1						
	1	0		0						
	0	0		0						
	0	0		0						
		1		0						
		0		0						
		0		1						
		0		1						
		0		1						
		0		0						
		0		0						
		0		1						
		1		0						
		1		0						
		0		0						
		1		0						
		0		0						
		0		1						
		0		0						
		0		0						
		1		0						
		0		0						
		0		0						
		0		1						
		0		0						
		1		0						
		0		0						
		0		0						
		0		0						
				0						
				0						
				1						
				1						
				0						

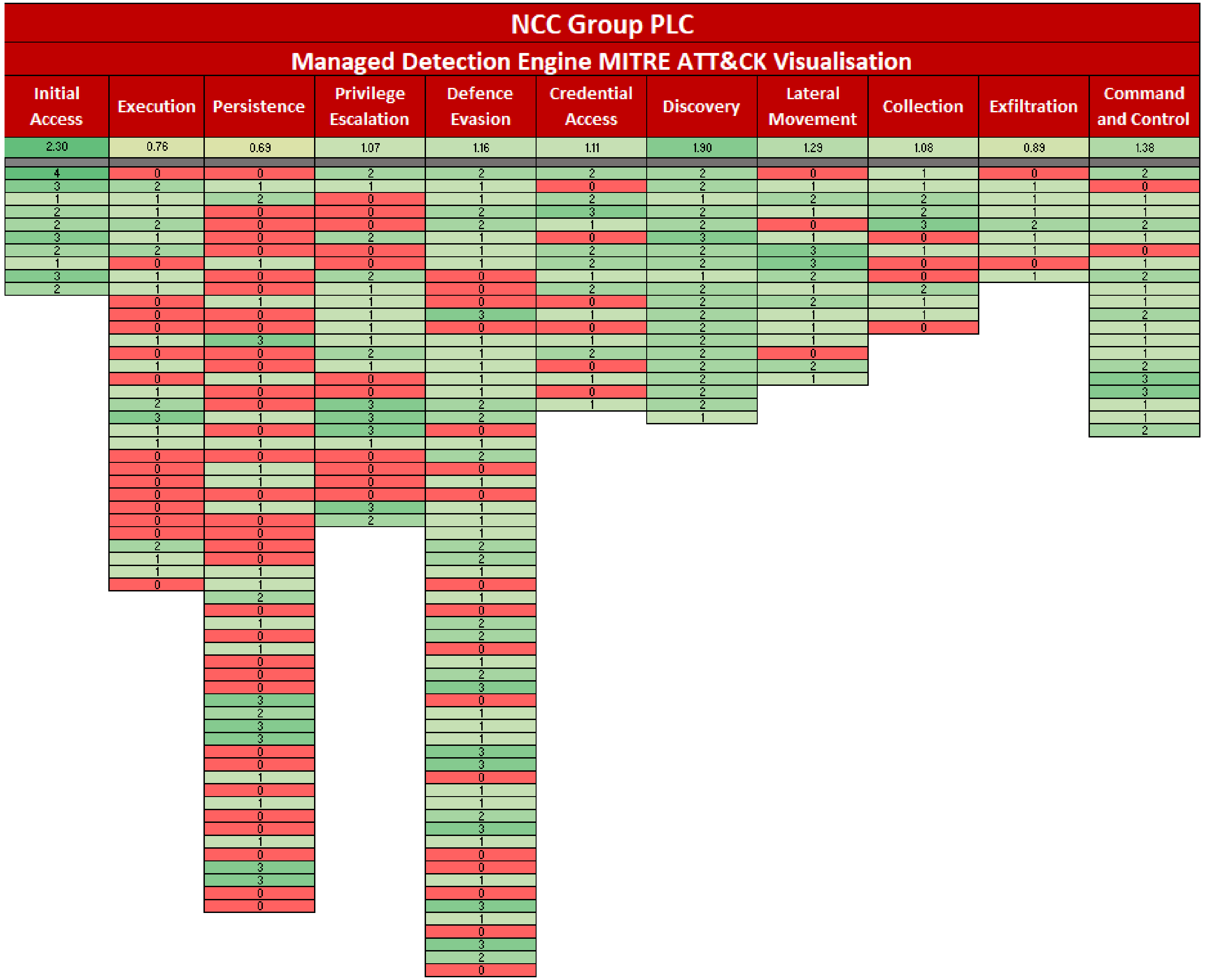
Example visualisation, Cloud Controls Threat Intelligence Coverage

Perspective 1 – Illustration of an organisations Threat Profile.

LMF Cyber Summit

nccgroup

MITRE Att&ck Illustration – 2. Visibility of Your Unique Cloud Cyber Fingerprint



NCC Group PLC

Managed Detection Engine MITRE ATT&CK Visualisation

Initial Access	Execution	Persistence	Privilege Escalation	Defence Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
2.30	0.76	0.69	1.07	1.16	1.11	1.90	1.29	1.08	0.89	1.38
4	0	0	2	2	2	2	0	1	0	2
3	2	1	1	1	0	2	1	1	1	0
1	1	2	0	1	2	1	2	2	1	1
2	1	0	0	2	3	2	1	2	1	1
2	2	0	0	2	1	2	0	3	2	2
3	1	0	2	1	0	3	1	0	1	1
2	2	0	0	1	2	2	3	1	1	0
1	0	1	0	1	2	2	3	0	0	1
3	1	0	2	0	1	1	2	0	1	2
2	1	0	1	0	2	2	1	2		1
	0	1	1	0	0	2	2	1		1
	0	0	1	3	1	2	1	1		2
	0	0	1	0	0	2	1	0		1
	1	3	1	1	1	2	1			1
	0	0	2	1	2	2	0			1
	1	0	1	1	0	2	2			2
	0	1	0	1	1	2	1			3
	1	0	0	1	0	2				3
	2	0	3	2	1	2				1
	3	1	3	2		1				1
	1	0	3	0						2
	1	1	1	1						
	0	0	0	2						
	0	1	0	0						
	0	1	0	1						
	0	0	0	0						
	0	1	3	1						
	0	0	2	1						
	0	0		1						
	2	0		2						
	1	0		2						
	1	1		1						
	0	1		0						
		2		1						
		0		0						
		1		2						
		0		2						
		1		0						
		0		1						
		0		2						
		0		3						
		3		0						
		2		1						
		3		1						
		3		1						
		0		3						
		0		3						
		1		0						
		0		1						
		1		1						
		0		2						
		0		3						
		1		1						
		0		0						
		3		0						
		3		1						
		0		0						
		0		3						
				1						
				0						
				3						
				2						
				0						

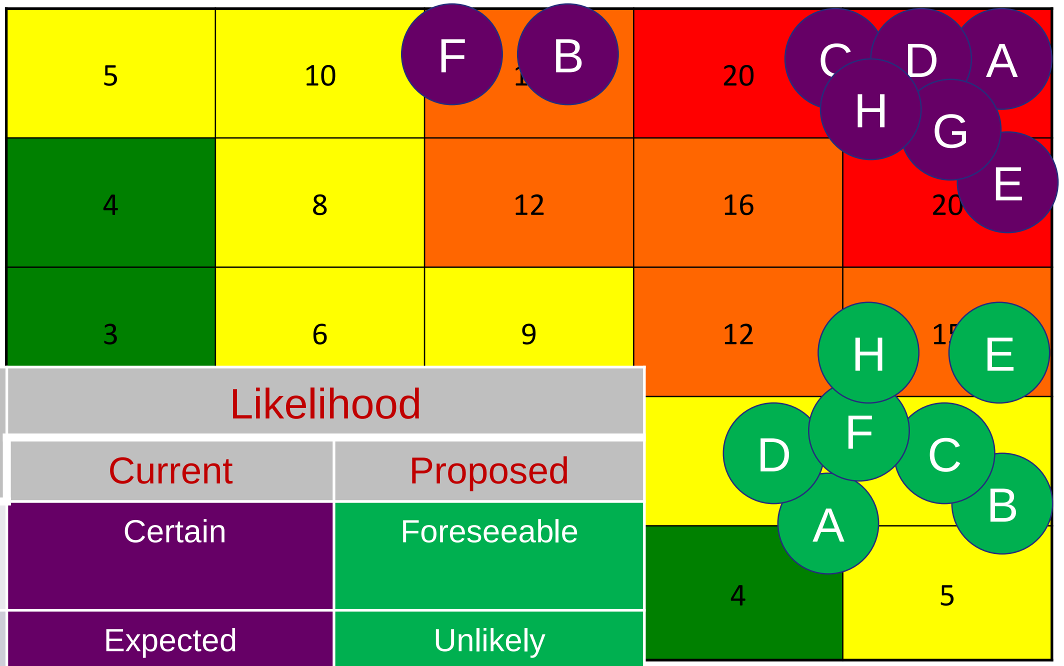
Example visualisation, Cloud Controls Threat Intelligence Coverage

Perspective 2 – Overlay existing controls to see where the gaps are, and where investment needs to be focused (or reprioritised)

LMF Cyber Summit

Illustration – 3. Visibility of Actual Risk of Breach Exposure

Current v. Mitigated
Risk Scores



Ref	Risks that could lead to a breach	Impact	Likelihood	
			Current	Proposed
A	No monitoring & alerting capabilities across the cloud estate	Very High	Certain	Foreseeable
B	Uncontrolled use of 3rd party applications – Drop Box / Slack etc.	Very High	Expected	Unlikely
C	Lack of Privileged Account Protection & MFA	Very High	Certain	Foreseeable
D	Lack of object level JML controls	Very High	Expected	Foreseeable
E	Lack of data exfiltration controls	Very High	Foreseeable	Unlikely
F	Limited control & use of BYOD	Very High	Certain	Unlikely
G	Cannot ensure protection of Personal Information	Very High	Certain	Unlikely
H	Underutilised technology investments that can mitigate risk	Very High	Expected	Unlikely

LMF Cyber Summit

Poll 2

What is the main challenge that you experience when trying to accurately quantify risk?

A. Full visibility of the risk landscape

B. Understanding, quantifying, and accounting for emerging threats

C. Accuracy of data used

D. Difficulty understanding a firm’s risk appetite, training, and governance

Now it's your turn – Tabletop Exercise …

These exercises are designed to engage you in assessing and quantifying cyber risks associated with specific incident scenarios.

Each group will act as an underwriting team tasked with evaluating the presented scenarios.

Objective:

- Simulate the complexities of underwriting cyber risks in various industries.
- Enhance your ability to quantify complex cyber risks.
- Develop comprehensive underwriting strategies that reflect accurate risk assessments.
- Share insights and approaches with other groups to foster collaborative learning.

DON’T PANIC when you see the details, this is a time bound exercise (@20mins) so the level of response should be proportional, so avoid getting into the weeds. You will have the benefit of taking ALL the scenarios away with you for post event rumination By engaging with these scenarios, you will sharpen your analytical skills, enhance your understanding of emerging cyber threats, and refine your approach to quantifying and managing cyber risk effectively.

Quantification Solution

LMF Cyber Summit

NCC Group Cyber Risk Quantification Workshop

Discover the power of Cyber Risk Quantification (CRQ) with NCC group’s complimentary, consultant-led workshop designed to help organisations make informed decisions about managing cyber risk.

Gain insights into CRQ and the Factor Analysis of Information Risk (FAIR™) methodology and their role in modern cyber risk management. Explore how CRQ allows you to:

- Better understand and prepare for cyber risks.
- Establish a common language between practitioners, risk owners and Senior Leadership.
- Demonstrate the effectiveness of a security program.
- Align cyber risk with other business risks.

Please reach out with any queries using the form at this link:

https://www.nccgroup.com/us/campaign/cyber-risk-quantification-workshop

Duration: 90 minutes

Format: Structured consultation

Cost: Free to attend

Location: Virtual

Most suitable for:

- CISOs,
- Chief Risk Officers,
- Heads of Governance, Risk and Compliance
- Cyber Security teams accountable for tracking and managing cyber risk across medium to large enterprises.

Q&A

Quantifying Cyber Risk & Managing Hidden Threats

Nigel Gibbons - Senior Advisor & Director of Global Cloud Security Services

21 November 2024