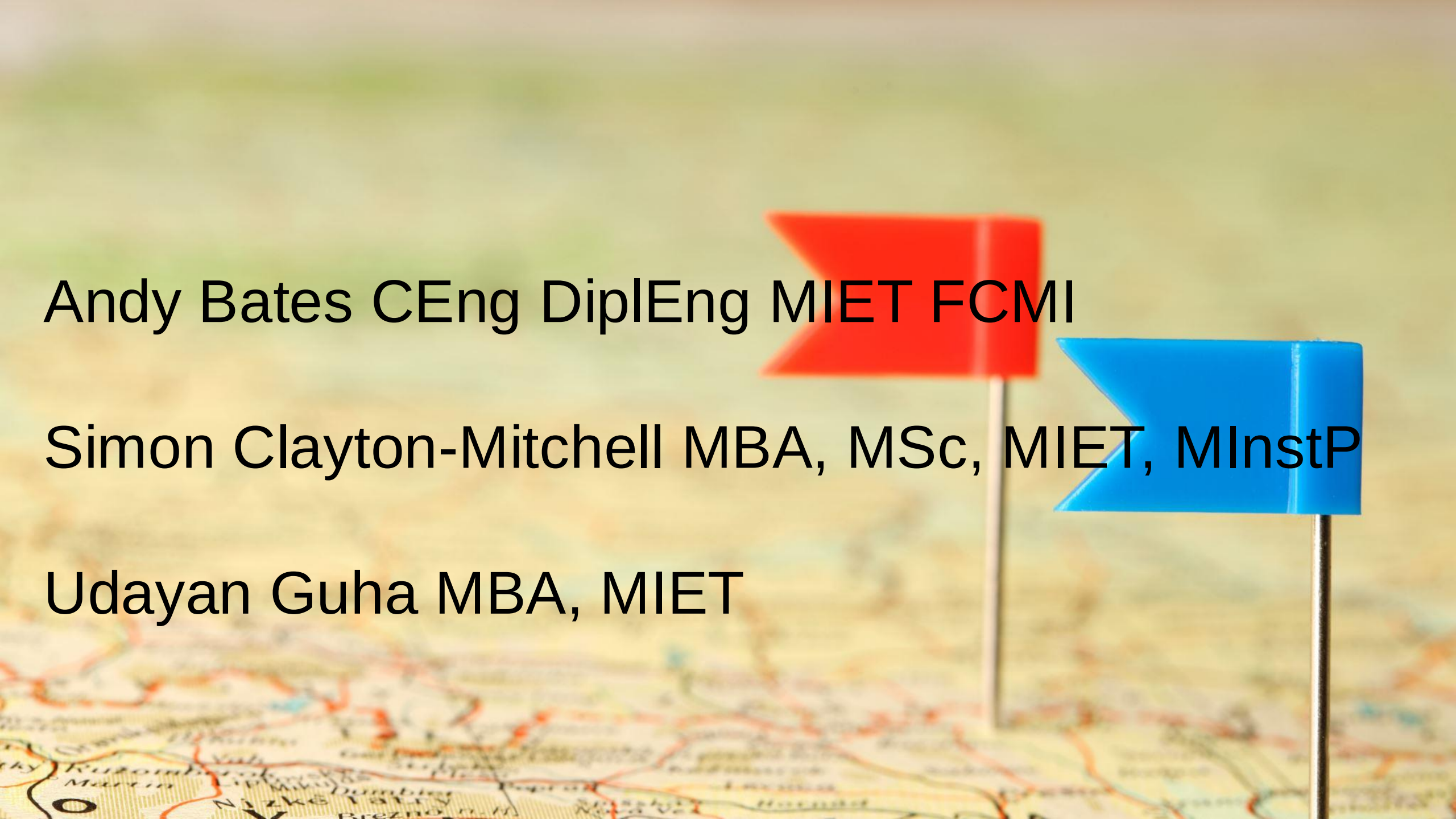
Cyber Threats and Financial Frauds in the Digital Age:

Strengthening Cyber Resilience in Banking, Financial Services, & Insurance Board and beyond



Andy Bates CEng DiplEng MIET FCMI

Simon Clayton-Mitchell MBA, MSc, MIET, MInstP

Udayan Guha MBA, MIET

Cyber Fraud and Cost Implications

1834
France telegraph hack for financial market data

1988
First National Bank of Chicago : $70-million computer theft

2008
Zeus trojan stealing banking information

2020
Marriott hotel chain 5.2m guests information leaked

<1970 | 1970 | 1980 | 1990 | 2000 | 2010 | 2020 | 2030 | >2030

1972
ARPANET: Creeper & Reaper – First worm

1994
Hackers siphoned $10 million from Citibank

2017
Wannacry malware infected >300,000 computers


TOP 10 EMERGING CYBER-SECURITY THREATS FOR 2030
1
Supply chain compromise of software dependencies
2
Advanced disinformation campaigns
3
Rise of digital surveillance authoritarianism/ loss of privacy
4
Human error and exploited legacy systems within cyber-physical ecosystems
enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY
10
Artificial Intelligence Abuse
THREATS 2030
5
Targeted attacks enhanced by smart device data
6
Lack of analysis and control of space-based infrastructure and objects
9
Cross border ICT service providers as a single point of failure
8
Skill shortage
7
Rise of advanced hybrid threats

2030

>2030

Our connected society now means that Cyber risk is a global issue

Economic cost is huge and growing:

- *"..**total cost of all cybercrime** in 2021 ... ~**$6 trillion worldwide**."*

Cyber Crime Magazine

- *" … equivalent to the 3rd largest economy in the world in 2024."*

- ***Global impact in 2025** > GDP of Germany and Japan – combined – at **$10Trn***

Cyber Crime Magazine

Most companies don't know how to respond:

- *"...a lot of the industry operates ... as medieval witchcraft: '**buy my magical amulet and you'll be fine**' "*

UK National Cyber Security Centre's Technical Director

Threat is increasing – things are getting worse:

- *"… **threat is becoming overwhelming** … **existential crisis for the industry**"*

*(*Security Blog on DoublePulsar)

And the problem is increasing

Intensity of attacks is increasing:

- From **clicking on phishing email to** attacker **accessing data is 72 mins**

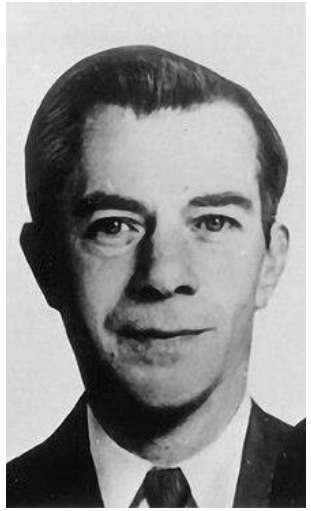
- Password attacks doubled in 2024 compared to 2023
  - 2020: ~**70% of attacks** result of **hacking** into system
  - 2024 - ~**70% of attacks** result of **logging** in with valid credentials

- **74% of larger UK companies** suffered a cyber-attack in 2023

A.I. will lead to more effective attacks:

- Life-like Avatars for social engineering attacks
- Improved phishing emails – email could become unusable
- Virus software that can change its signature
- Analysis of attack surface – find vulnerabilities to exploit

Willie Sutton
(US Bank Robber – 1930s)
"Slick Willy"



"Because that's where the money is"

"You can't rob a bank on charm and personality"

BANK INFO SECURITY

Topics News Training Resources Events Job

TRENDING: In-Person Summit | 2025 Data Security Summit Dallas •

Blockchain & Cryptocurrency , Cryptocurrency Fraud , Cybercrime

Update: Crypto Hackers Exploit Ronin Network for $615 Million

Popular Game Axie Infinity's Blockchain Security Breached Via Hacked Private Keys

Devon Warren-Kachelein (devawarren) · April 14, 2022

The Guardian UK

This article is more than 9 months old

UK engineering firm Arup falls victim to £20m deepfake scam

Hong Kong employee was duped into sending cash to criminals by AI-generated video call

decrypt

NEWS SCENE DEGEN ALLEY LEARN GG EMERGE VIDEOS NEWSLETTERS PODCASTS

XRP $2.20 6.34% BNB $554.19 3.53% SOL $127.77 7.05% USDC $0.

News · Law And Order

What Caused Bybit's $1.4 Billion Ethereum Hack? New Details Revealed

Wallet provider Safe said that a developer's laptop was compromised ahead of the exploit used to swipe $1.4 billion from Bybit.

By Logan Hitchcock

Mar 6, 2025
2 min read

The Indian EXPRESS
JOURNALISM OF COURAGE

TODAY'S PAPER

UPSC SCREEN World India Explained Opinion Politics Business Sports Cities Lifestyle Tech Research Videos

TRENDING Mini Crossword Premium Express Shorts Podcast Health & Wellness

News / Explained / Explained: The story of how North Korea hackers stole $81 million from Bangladesh Bank

Premium

This is an archive article published on June 26, 2021

Explained: The story of how North Korea hackers stole $81 million from Bangladesh Bank

The BBC has published an investigative report detailing how in 2016, North Korean hackers planned a $1 billion raid on Bangladesh's national bank and almost succeeded. Here's how it happened.

You don’t have to be the target to be the victim

MAERSK

Ukraine

$300m lost business
$10m to repair
$0 to criminals

Russia

The Gambia

Addressing the problem is difficult

- **Cyber crime pays:**
  - *2021: CAN Financial, EvilCorp ransomware – $40M*
  - *2023: Caesars Resorts, Scattered Spider ransomware – $15M*

  → *Strong financial incentives*

  → *Sophisticated 'dark' markets for malware*

- **Increasingly easy to conduct attacks:**
  - *Exploit tools available on the dark web*
  - *Exploit brokers*
  - *Nation states, organised crime - and a blurring between the two*

  → *Barriers to entry low - many 'bad actors'*

  → *Don't need massive skills to attack*

  → *"Giving rocket launchers to teenagers"*

- **Attack surface complex, hard to protect:**
  - *Legacy systems* - especially large organisations
  - *Attacker only needs to find one door open*

  → *Utilities, finance companies, CNI…*

  → *Defender has to close every door*

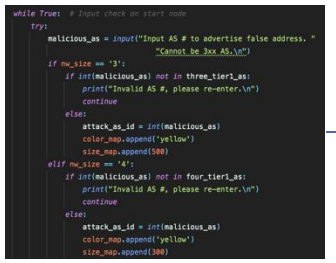
- **Skills are complex, varied:** IT, technical, operations, social engineering → *Complex teams needed – but skills shortage*
- **Industry highly fragmented:** '000s of companies offering 'remedies' → *Complex to construct effective solutions*

“The largest and most sophisticated attack the world has ever seen”

Product - Orion:

- Network Monitoring
- Network Security

solarwinds



Compiler

100110010100110010011010001101110001101011000011101001101010011

Software Update

Air Force

Coast Guard

Navy

Army

Marines

NASA

Microsoft

intel

FORTUNE 500

“The largest and most sophisticated attack the world has ever seen”

Product - Orion:

- Network Monitoring
- Network Security

solarwinds

```
while True:  # Input check on start node
    try:
        malicious_as = input("Input AS # to advertise false address. "
                             "Cannot be 3xx AS.\n")
        if nw_size == '3':
            if int(malicious_as) not in three_tier1_as:
                print("Invalid AS #, please re-enter.\n")
                continue
            else:
                attack_as_id = int(malicious_as)
                color_map.append('yellow')
                size_map.append(500)
        elif nw_size == '4':
            if int(malicious_as) not in four_tier1_as:
                print("Invalid AS #, please re-enter.\n")
                continue
            else:
                attack_as_id = int(malicious_as)
                color_map.append('yellow')
                size_map.append(300)
```

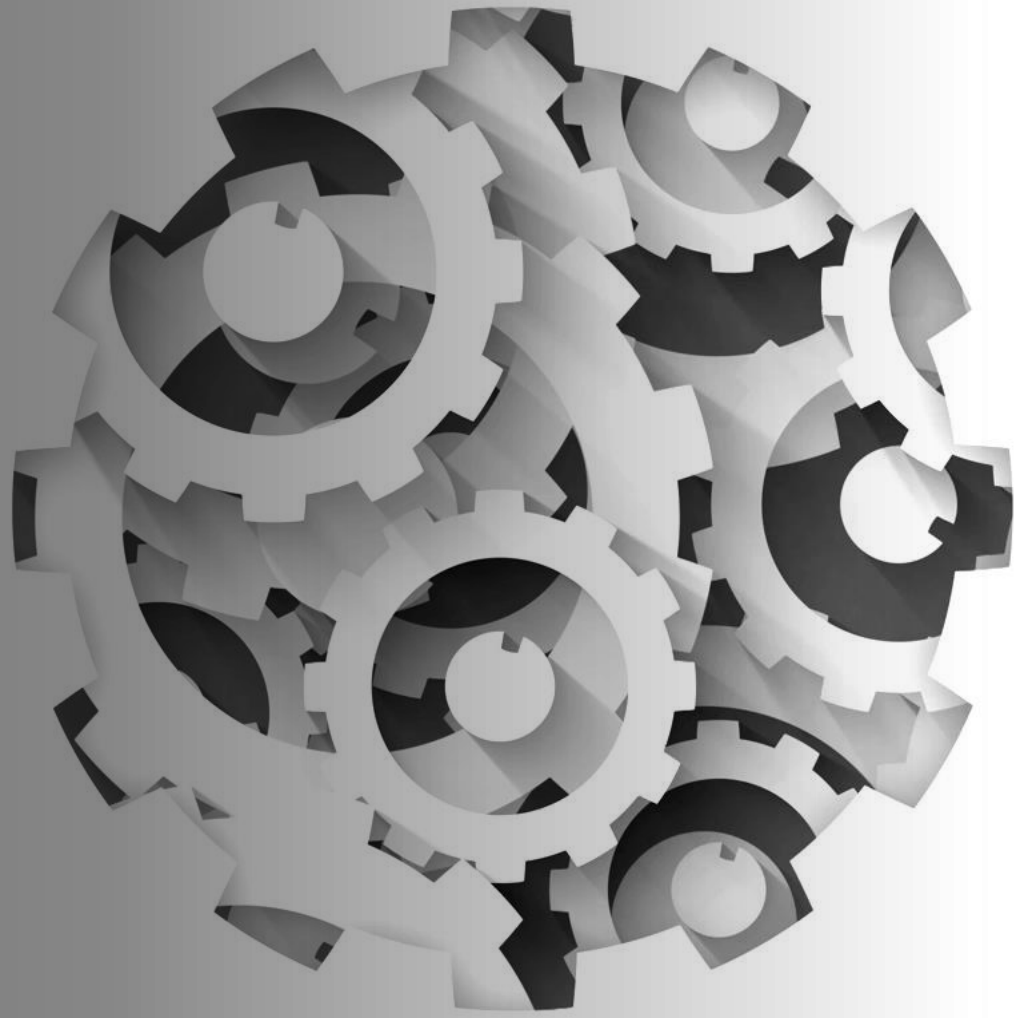
Compiler

```
10011001010011
00100110100011
0100111100011101
01100001110100
11010011
```

Software Update

Password: “solarwinds123”

Cyber Risk Management



EU has introduced regulations to address risk - DORA

European Insurance and Occupational Pensions Authority

Digital Operational Resilience Act (DORA)

What does it cover?

ICT risk management

Principles and requirements on ICT risk management framework

ICT third-party risk management

Monitoring third-party risk providers

Key contractual provisions

Digital operational resilience testing

Basic and advanced testing

ICT-related incidents

General requirements

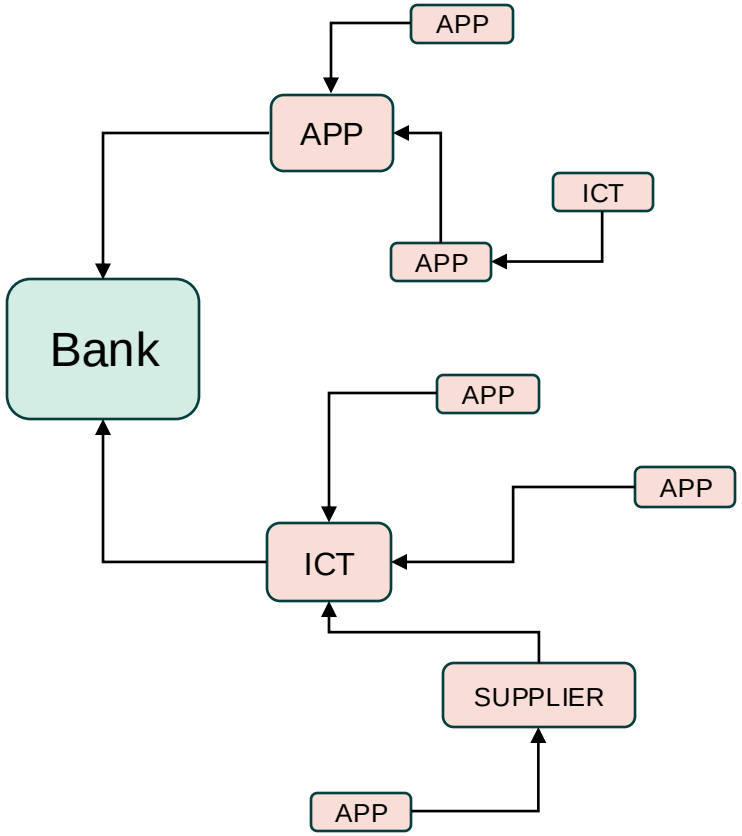
Reporting of major ICT-related incidents to competent authorities

Information sharing

Exchange of information and intelligence on cyber threats

Oversight of critical third-party providers

Oversight framework for critical ICT third-party providers



Ensuring security across the supply chain improves security for society

Digital Operational Resilience Act (DORA)

What does it cover?

ICT risk management

Principles and requirements on ICT risk management framework

ICT third-party risk management

Monitoring third-party risk providers

Key contractual provisions

Digital operational resilience testing

Basic and advanced testing

ICT-related incidents

General requirements

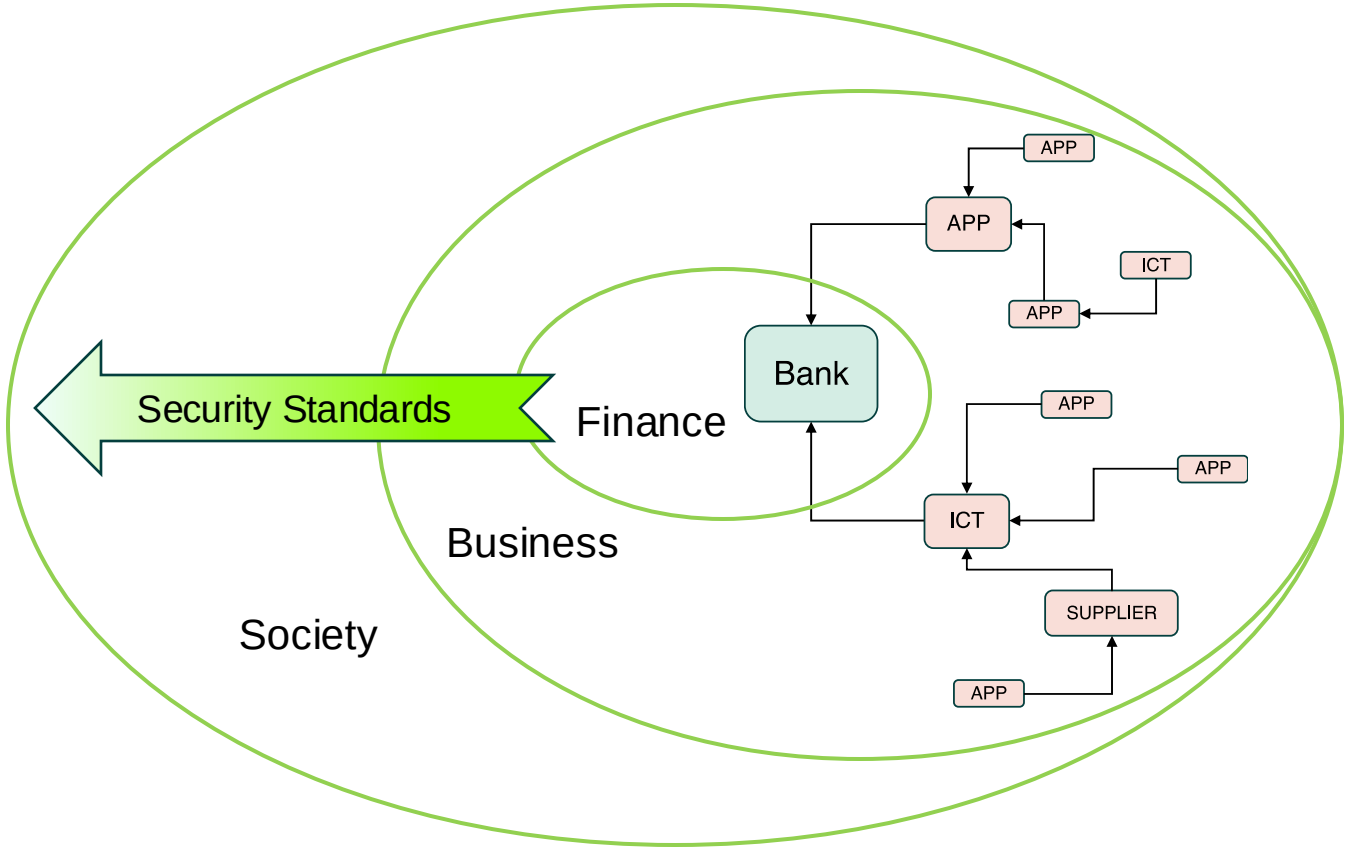
Reporting of major ICT-related incidents to competent authorities

Information sharing

Exchange of information and intelligence on cyber threats

Oversight of critical third-party providers

Oversight framework for critical ICT third-party providers



Effective governance starts with understanding assets and owners

Data & Systems

- Identify internal attack surface
  - Software
  - Hardware
  - Firmware
  - Devices
- Understand external supply chain

Ownership

Accountability

- Legally
- Operationally
- Technically
- Security

Effective governance arises from understanding assets and owners

Effective governance starts with understanding assets and owners

Data & Systems

- Identify internal attack surface
  - Software
  - Hardware
  - Firmware
  - Devices
- Understand external supply chain

Ownership

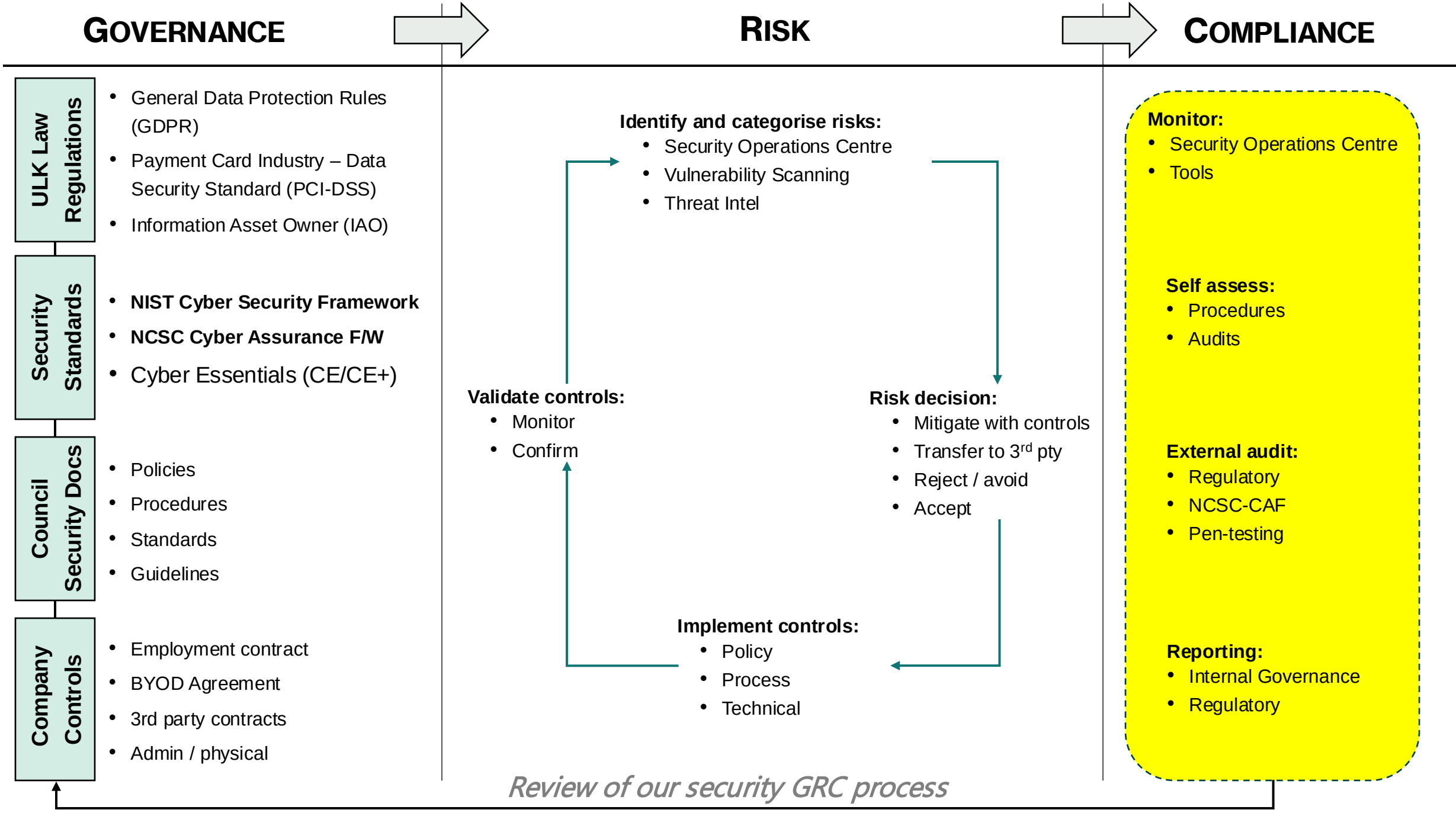
Accountability

- Legally
- Operationally
- Technically
- Security

Governance

- Legal requirements (e.g., GDPR)
- Defining policies, procedures, standards. etc.
- Security implementation: technical, operational
- Security assurance – *"how do I know..."*

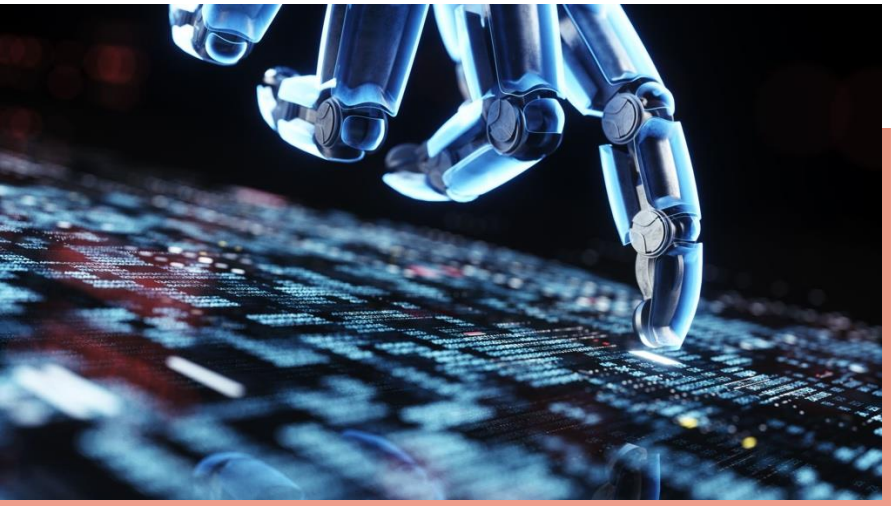
Assurance process

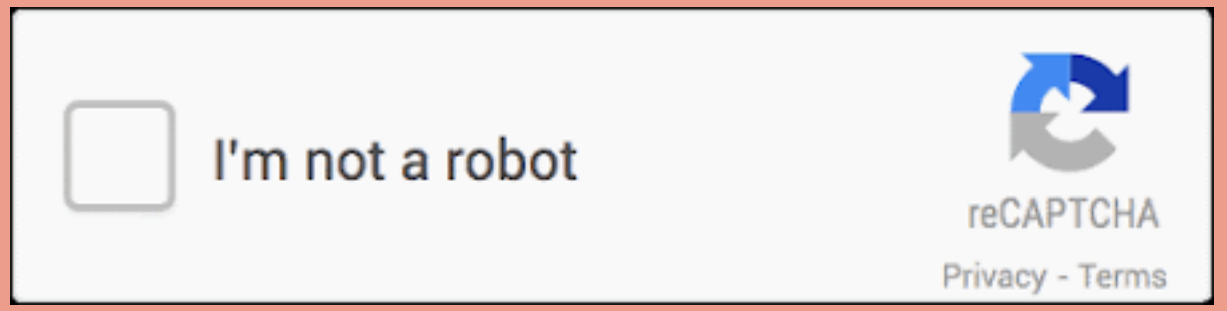

GOVERNANCE
RISK
COMPLIANCE
ULK Law Regulations
General Data Protection Rules (GDPR)
Payment Card Industry – Data Security Standard (PCI-DSS)
Information Asset Owner (IAO)
Security Standards
NIST Cyber Security Framework
NCSC Cyber Assurance F/W
Cyber Essentials (CE/CE+)
Council Security Docs
Policies
Procedures
Standards
Guidelines
Company Controls
Employment contract
BYOD Agreement
3rd party contracts
Admin / physical
Identify and categorise risks:
Security Operations Centre
Vulnerability Scanning
Threat Intel
Risk decision:
Mitigate with controls
Transfer to 3rd pty
Reject / avoid
Accept
Implement controls:
Policy
Process
Technical
Validate controls:
Monitor
Confirm
Monitor:
Security Operations Centre
Tools
Self assess:
Procedures
Audits
External audit:
Regulatory
NCSC-CAF
Pen-testing
Reporting:
Internal Governance
Regulatory
Review of our security GRC process

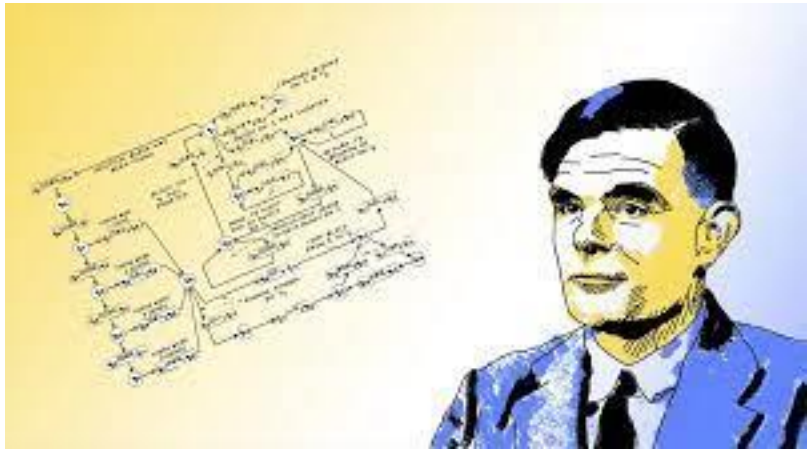
Leveraging A.I.


AI

Is AI New?

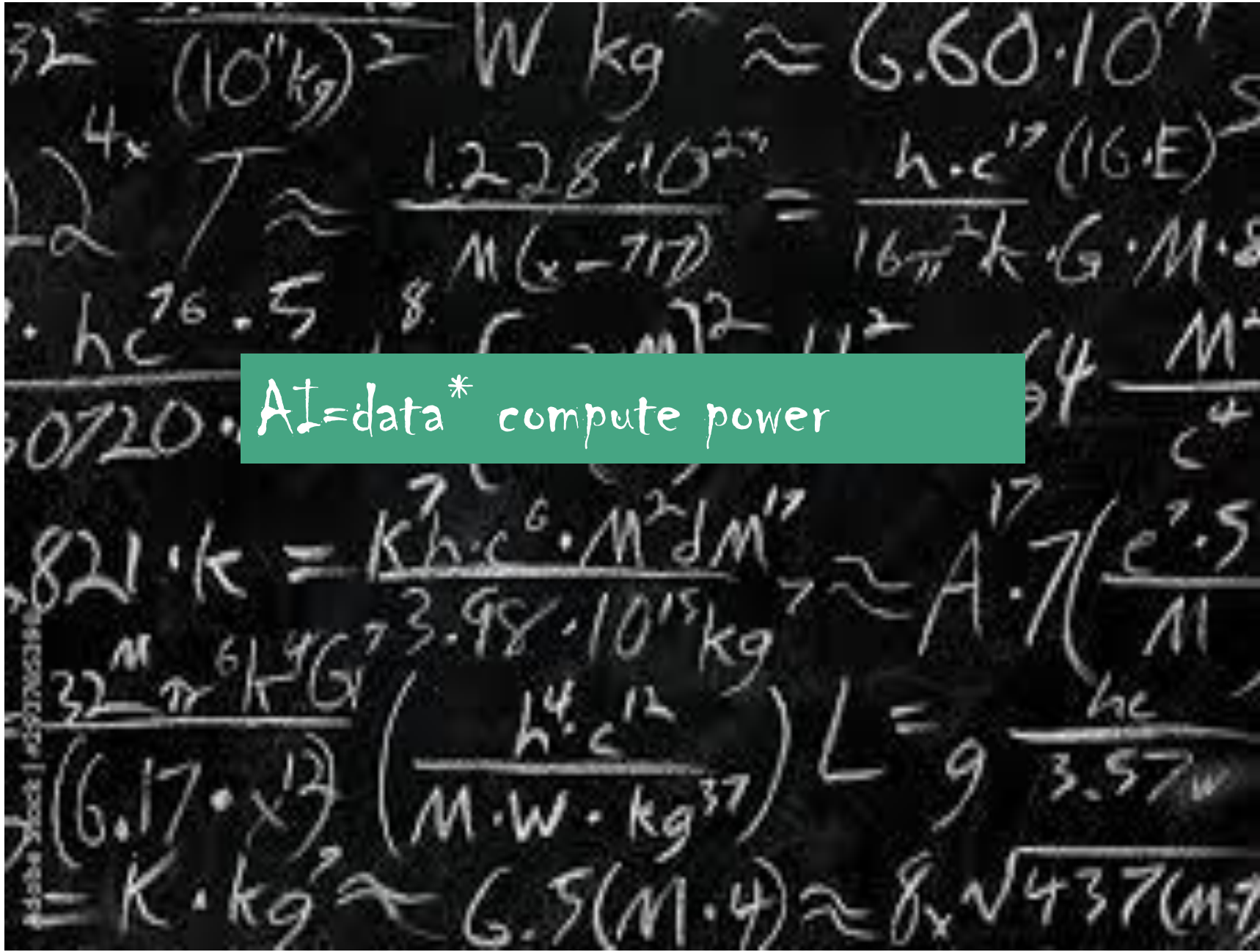







10
20 years ago, we were using AI (!!!) in cyber (well ML)

Why is AI in the news now?

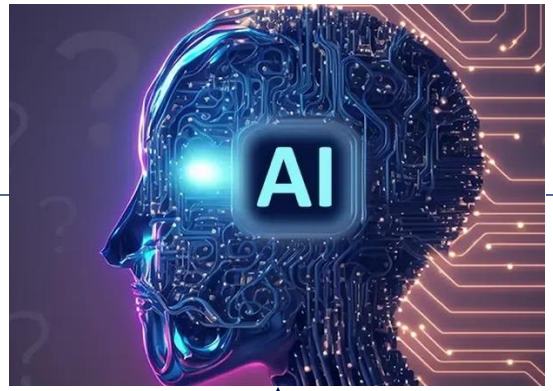


Challenges with current level of AI

Limitation	Result	Consequence
A.I. is NOT intelligent	*No understanding of context*	*Inaccurate or mis-leading information*
A.I. optimises for 'norms' - not outliers	*May actually exclude outliers as part of design*	*Exacerbates biases, eliminate important data*
LLMs designed to get "close" in answer	*"Close" not good enough in many cases*	*Misuse by operators – assume AI correct*
A.I. operates as a black box – no understanding of algorithms	*No transparency on decision making process*	*Inaccurate or mis-leading information, "hallucinations"*

Our assumptions about how AI is thinking can be wrong!

"AI CAN DIFFERENTIATE A WOLF FROM A HUSKY



"It's a Husky"

"It's a Wolf"

ALGORITHM

```
IF background = SNOW
        THEN
                dog = HUSKY
        ELSE
                dog = WOLF
```

This raises serious questions about how AI is used in organisations

Assume results are intelligently derived – no human validation

- Incorrect or invalid results from AI (e.g. hiring decisions)
- Results in deterioration of business intelligence
- Leads to poor decision making - *"AI told us to do this!"*

Replace intelligent decision making – *"AI says No!"*

- Staff overly-rely on AI to do their jobs
- No human validation of what AI is telling staff
- Leads to uninformed decision making - *"AI says No!"*

Input data to public AI – loss of confidentiality

- Data input to public AI now part of AI training data
- Data in public domain – cannot be forgotten
- Loss of confidentiality of sensitive data – *"AI has our data"*

In Summary

Economic cost is huge and growing:

$10Trn in 2025 > GDP of Germany and Japan – combined

Most companies don't know how to respond:

Limited understanding of problem at the management level

Solutions complex to implement, skills shortage

Not just an IT issue – involves whole organisation

Cyber is a Management Issue:

Increase understanding, develop proper governance and risk management processes

>90% of attacks can be stopped by good cyber / IT hygiene (passwords, backups, MFA)