UAE Internal Auditors Association
JOIN, LEARN & SHARE

The 11th Conference

The Future of Cybersecurity and What Controls The CAE Should Test For

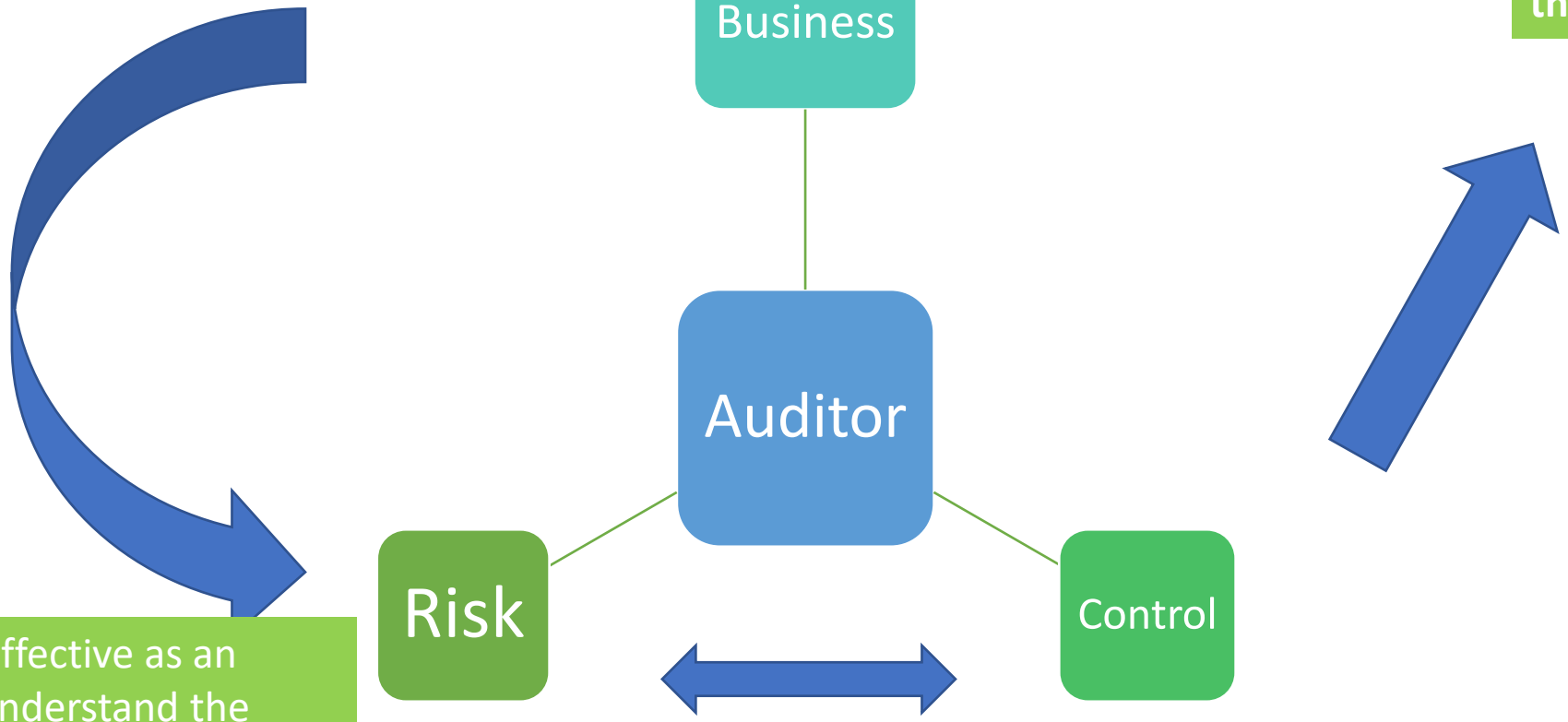
Dr. Fene Osakwe
Global Cybersecurity Advisor

CISM,CISA,OCP,ISO270001,ISO27005,C|CISO, COBIT5, CEH,CRISC

OUTLINE

- Introduction
- Why Cybersecurity is important for the CAE
- **The Past** - Where we are coming from
- **The present** - Where we are
- **The future** - Where we are heading
- What should be the Auditor's control response
- Conclusion

INTRODUCTION - Audit - The Touch points



Oversight of the Business

It is impossible to be effective as an auditor, if we do not understand the business objectives and cannot articulate and stay abreast of business risk that could impede such objective

Why should we care

The most important global business risks for 2022

1
↑ 44%
2021: 3 (42%)

Cyber incidents
(e.g. cyber crime, IT failure/ outage, data breaches, fines and penalties)

2
↓ 42%
2021: 1 (41%)

Business interruption
(incl. supply chain disruption)

Watch our short film about the top 10 risks for 2022

View the full Allianz Risk Barometer 2022 rankings here

3
↑ 25%
2021: 6 (17%)

Natural catastrophes
(e.g. storm, flood, earthquake, wildfire, weather events)

Key

- ↑ Risk higher than in 2021
- ↓ Risk lower than in 2021
- → No change from 2021
- (5%) 2021 risk ranking %

Figures represent the number of risks selected as a percentage of all survey responses from 2,650 respondents.

All respondents could select up to three risks per industry, which is why the figures do not add up to 100%.

4
↓ 22%
2021: 2 (40%)

Pandemic outbreak
(e.g. health and workforce issues, restrictions on movement)

5
→ 19%
2021: 5 (19%)

Changes in legislation and regulation
(e.g. trade wars and tariffs, economic sanctions, protectionism, Brexit, Euro-zone disintegration)

6
↑ 17%
2021: 9 (13%)

Climate change
(e.g. physical, operational, financial and reputational risks as a result of global warming)

7
→ 17%
2021: 7 (16%)

Fire, explosion

8
↓ 15%
2021: 4 (19%)

Market developments
(e.g. volatility, intensified competition/new entrants, M&A, market stagnation, market fluctuation)

9
↑ 13%
2021: 13 (8%)

Shortage of skilled workforce

10
↓ 11%
2021: 8 (13%)

Macroeconomic developments
(e.g. monetary policies, austerity programs, commodity price increase, deflation, inflation)

Why this surge?

- In 2022, the average cost of a data breach has reached a record high of US$4.35 million, according to the 2022 cost of a data breach report by IBM and the Ponemon institute.
- Its findings are based on 550 breaches across 17 countries and 17 industries with data gathered from over 3,600 interviews
- In MENA, Kaspersky reported 17% increase in malware attacks in the middle east
- Denial of Service (DOS) attacks in UAE, increased by 183% in 2021 (https://internationalsecurityjournal.com/cyber-attacks-middle-east/)
- World Economic Forum says that Africa is loosing 4 Billion annually to cyber crime. (https://www.weforum.org/agenda/2022/08/africa-must-act-to-address-cybersecurity-threats/)

Why should we care

- If globally, Cyber risk is becoming one of the biggest threat to business, It is important for the CAE to have an overview of what it is, what are the drivers and how to mitigate it

- We have answered “the what” and “the why”. Now, lets talk about “the how”. How did cyber risk crip up on us and become one of our major Business Risk

The Past – Where are we coming from

- Less Technology was used to enable businesses
- Focus of audit was on what IT Systems support Financial Statement that could probably lead to material misstatements
- Data centers were “on premise”. So data was largely within your control in your data center
- Traditional borders existed – So you didn’t worry to much about what was happening outside your region
- No regulation

- No access to hacking tools
- Skillset to execute a hack was not easily available
- Breaches were not monetized.

- **Cyber risk = IT Problem**

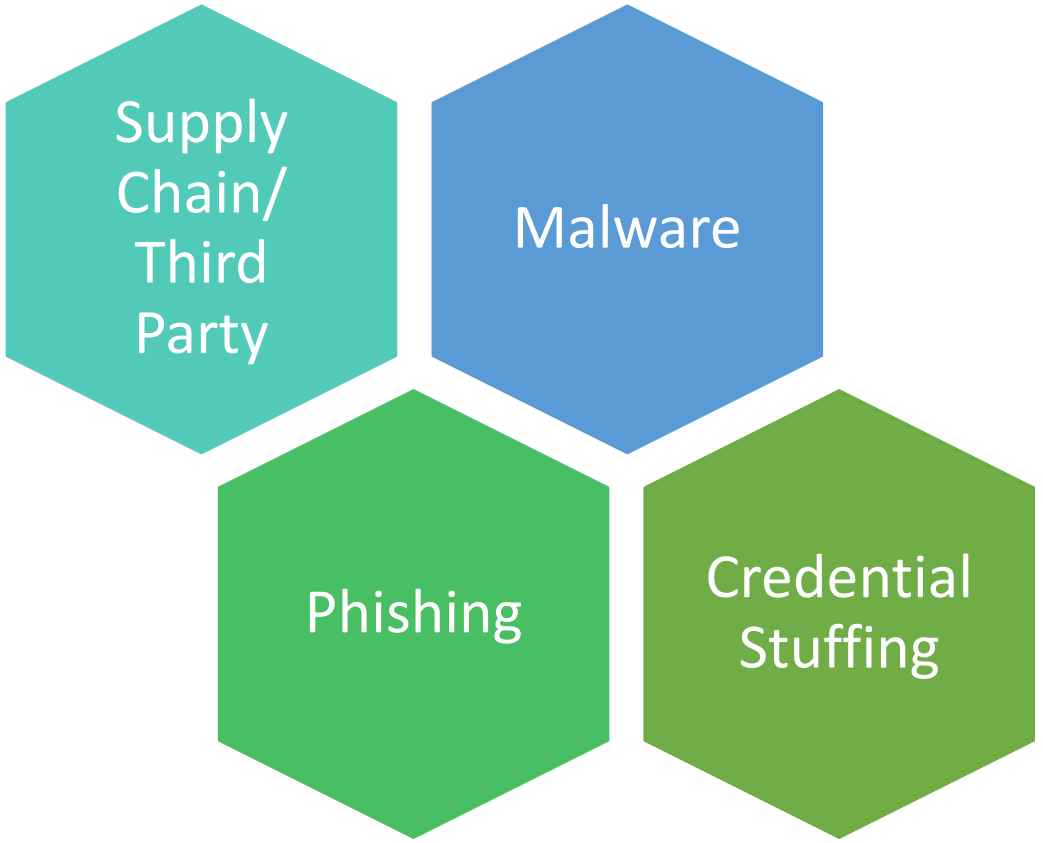
The Present

- Businesses now heavily reliant on technology
- Remote working
- Mobile
- Technology
  - Cloud computing
  - Digital transformation
- Regulation has been introduced (partially)
  - Data privacy laws

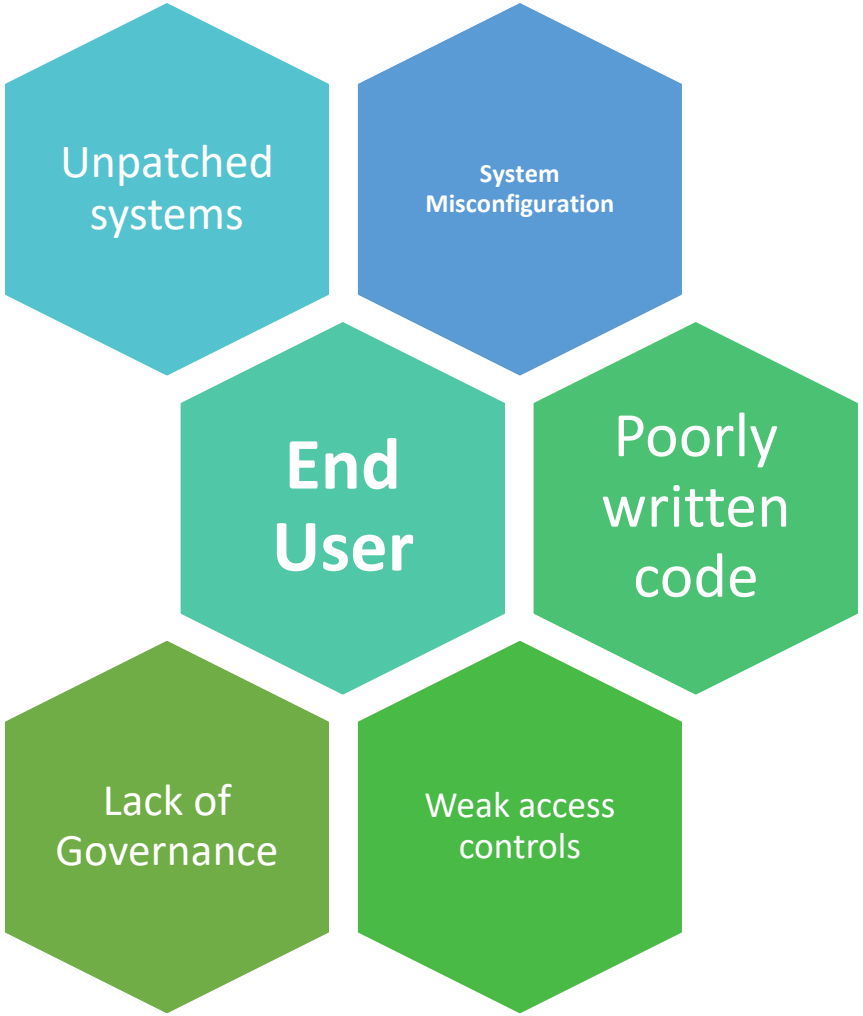
- Easy access to hacking tools for free
- Breaches are now being monetized(ransomware)
- Nation state sponsored

- **Cyber risk = CISO Problem**

The Present - Major Threat



The Present – What do these threats take advantage of



The Future

- Businesses will be fully in the cloud & Digital
- Remote/ hybrid working
- Targeted attacks
- Supply chain attacks will be on the increase
- Credential stuffing attacks will increase
- Multi actor Authentication will not be enough
- Heavy fines for Data breaches
- Regulation for all sectors
- Cyber security experience will be required at the Board.
- Cybersecurity will evolve to Cyber resilience

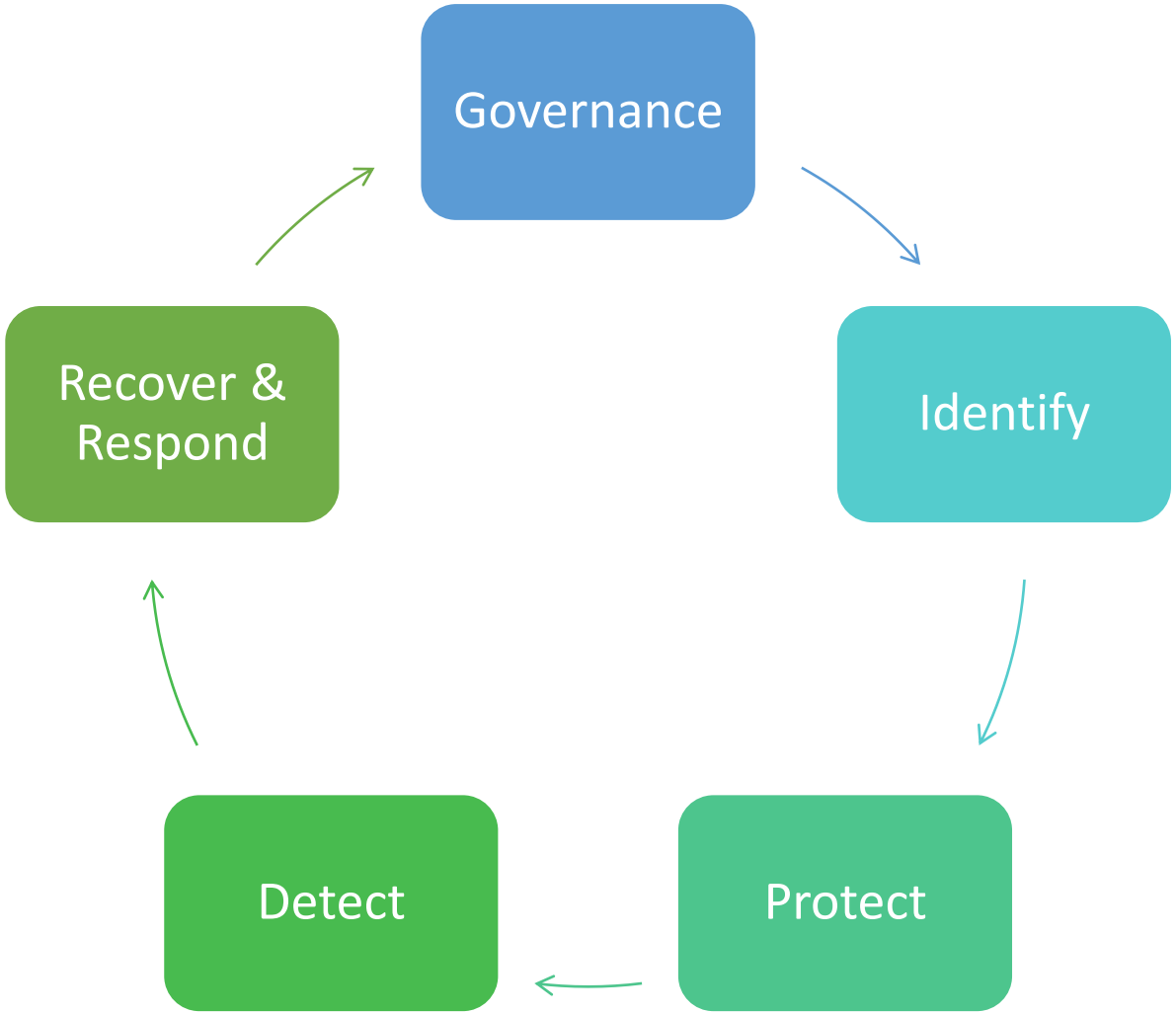
- Hacking as a service, phishing and a service, malware as a service.

- **Cyber risk = CEO/ Board Problem**

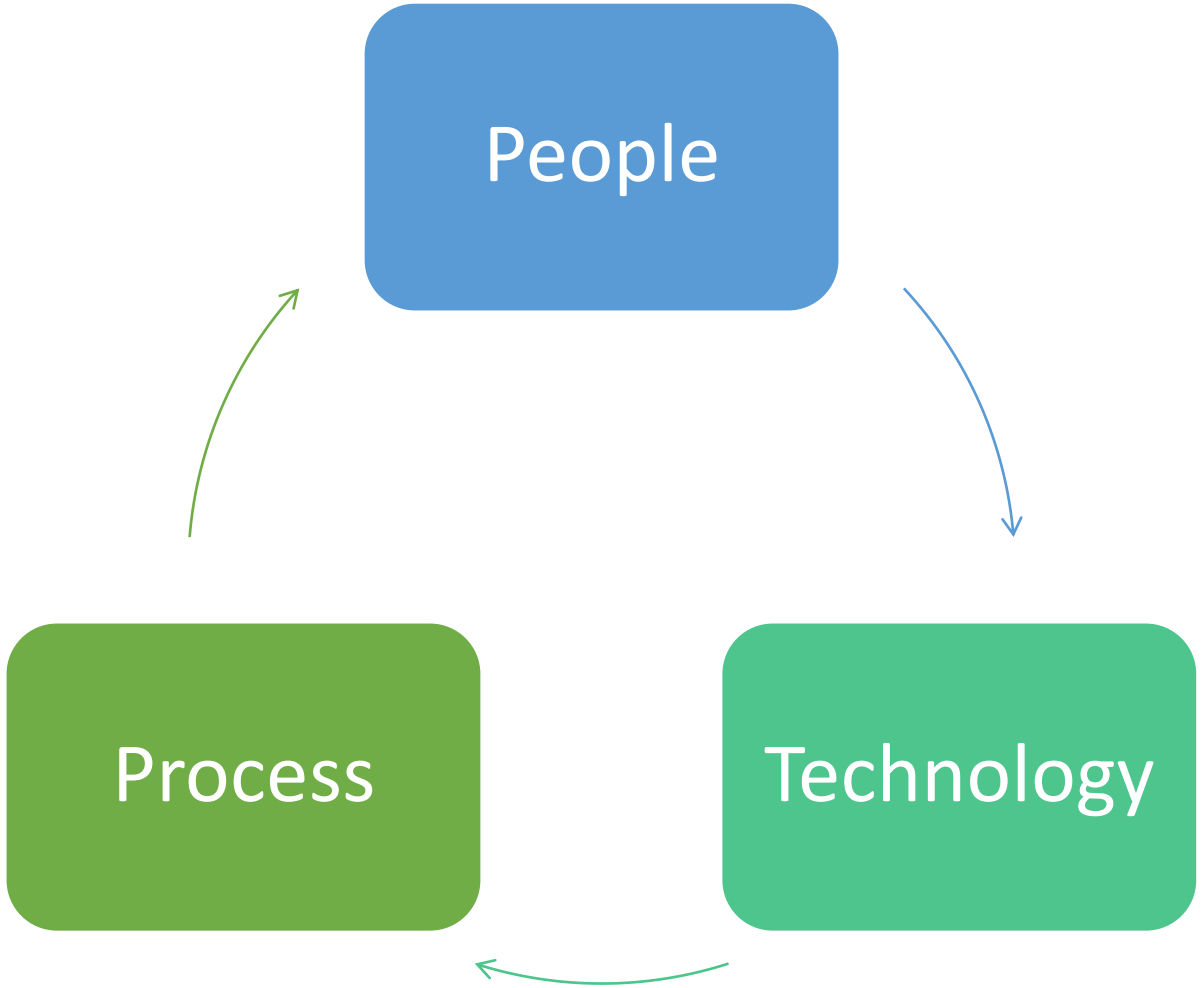
What should be the response of the CAE

- Understand the trend
- Understand the risk
- Ensure controls are designed to address the main cyber domains

Our Audit programs have to test



What areas should these control cover



In conclusion

- The auditor is not being called upon now, when a breach happens, just the CISO. The CAE will soon be in the eye of the storm for what will become the biggest business risk
- We should proactively start getting our teams ready to audit, and recommend appropriate controls to ensure that our business are able to survive cyber threats and keep afloat.
- We may need to design a work program around Cybersecurity and do an assessment of where our organizations are. And start building from there.
- Happy to connect with you
- https://www.feneosakwe.com/ https://www.linkedin.com/in/dr-h-c-fene-osakwe-1617b585/ feneosakwe@gmail.com

UAE Internal Auditors Association
JOIN, LEARN & SHARE

The 11th Conference

THANK YOU

feneosakwe@gmail.com