100 YEARS

MOORE Kingston Smith

Moore Kingston Smith

Top for Charity Expertise

★★★★★

2022/23 Charity Finance Audit Survey

Cyber security and risk

How likely is an attack?

MOORE ClearComm

RANKED 2022

#3 MOORE Kingston Smith

AccountancyAge Mid-Tier Power Index 2022

#MTPI

Agenda

- Latest cyber crime data and trends
- Cyber attack likelihood
- Risk psychology
- Leadership and risk management
- Digital cyber risk report

- Maritz Cloete and Rich Jackson (Moore ClearComm)
- Mike Clarke (Empowered People Thrive)

"Our psychology is a significant obstacle to appropriate risk preparation."

End Times: A Brief Guide to the End of the World

Bryan Walsh

MOORE ClearComm

LATEST CYBER ATTACK DATA

Latest cyber attack data

- World Economic Forum 2018 Global Risks Report:

"The top three risks to global stability over the next five years are natural disasters, extreme weather and cyber attacks."

- We can "see" and "feel" natural disasters and extreme weather, they impact society as a whole and are accepted as a global issue
- The threat of cyber attacks is less tangible
- This probably makes cybercrime a greater threat than society realises

"Prediction is very difficult, especially if it's about the future."

Niels Bohr

(Father of the atomic model, Nobel Laureate)

Latest cyber attack data

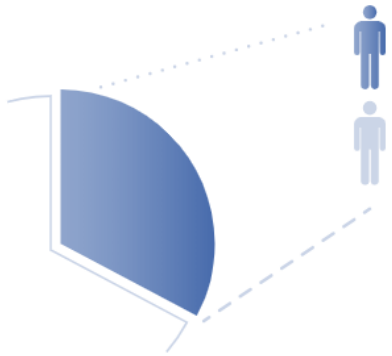
- 70-75 million people are victims of cyber crime, each year
- Cybercrime rose by 600% at the peak of the COVID-19 Pandemic
- Every company is a reachable target, and has operations, brand, reputation, and revenue pipelines that are at risk from a cyber attack
- In 2022, 34.5% of company executives confirmed that their organizations accounting / financial data was targeted by cyber criminals
- International Data Corporation (IDC) says that “AI in the cybersecurity market is growing at a CAGR of 23.6% and will reach a market value of $46.3 billion by 2027” *(Forbes)*
- The cost of cybercrime is predicted to hit $8 trillion in 2023 and will grow to $10.5 trillion by 2025 *(Cybersecurity Ventures)*

Latest cyber attack data cont.

1 in 3

users click on harmful content in phishing emails, and out of these

1 in 2



proceed to enter sensitive information

(16.5% of recipients)

Digital Natives* are

↗ 65%

more likely to click on phishing emails than older users

*a person who grew up with the presence of digital technology or in the information age - digital natives are typically comfortable with and fluent in technology

MOORE ClearComm

Emerging threats and trends

- Ransomware: more refined and intelligent
- Phishing / Vishing: enabled by AI
- Supply chain targeting
- Insider threats on the increase
- Internet of Things (IoT)
- Business Email Compromise attacks continue to increase
- MOVEit hack 2023

QUESTION

Why aren’t more organisations reacting to the obvious and immediate threat of cyber crime?

QUESTION

What are the basic first steps we should recommend any business (or leader) takes, to reduce their cyber risk?

CYBER ATTACK LIKELIHOOD

Cyber-attack likelihood

- 39% chance your business will suffer a cyber-attack this year (based on 2022 global average)
- 75% of security professionals say cyber risk has increased due to geopolitics, AI, and remote work
- Only 14% of SMES rate their ability to mitigate cyber threats as “highly effective”
- Of those businesses reporting an attack, 27% say they are attacked every week

Cyber-attack likelihood

- Most common attack method is phishing (83%), a human-based attack strategy (social engineering)
- Supply chain attacks are increasing, vastly widening the payload of a successful cyber incident
- 37% year-over-year increase of supply chain attacks, between 2021 and 2022
- Every organisation is part of a supply chain, very few assess or consider the risks posed by suppliers

RISK PSYCHOLOGY

Risk psychology

Risk defined:

- Probability or threat of damage, injury, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through preemptive action

Risk Management:

- Identification, evaluation, and prioritization of risks (defined in ISO 31000 as the “effect of uncertainty on objectives”) followed by
- Application of resources to minimize, monitor, and control the probability or impact of unfortunate events, or to
- Maximize the realisation of opportunities

Risk psychology cont.

Example of risk apathy in cyber security:

- 91% of people know that password recycling poses huge security risks, yet
- 59% still use the same password - everywhere
- This means that 6 in 10 people knowingly take (and accept) a risk with their cyber security
- They are your employees and colleagues, and carry this mentality into the business environment

Risk psychology cont.

QUESTION

What is the human psychology of risk – and why do human beings carry out actions even when they know it's a dangerous thing to do?

QUESTION

Are some people instinctively more likely to accept risks where others may not – and if so, why?

LEADERSHIP & RISK MANAGEMENT

Leadership and risk management

- 82% of boards or senior management within UK businesses rate cyber security as a ‘very high’ or ‘fairly high’ priority
- 54% act to identify or assess their cyber risk
- 13% of businesses assess risks posed by suppliers
- 61% of large businesses invest in staff training
- Compared to 17% of businesses overall

“Board members have a pivotal role in improving their organisation’s cyber resilience and exploiting the opportunities that technology brings.”

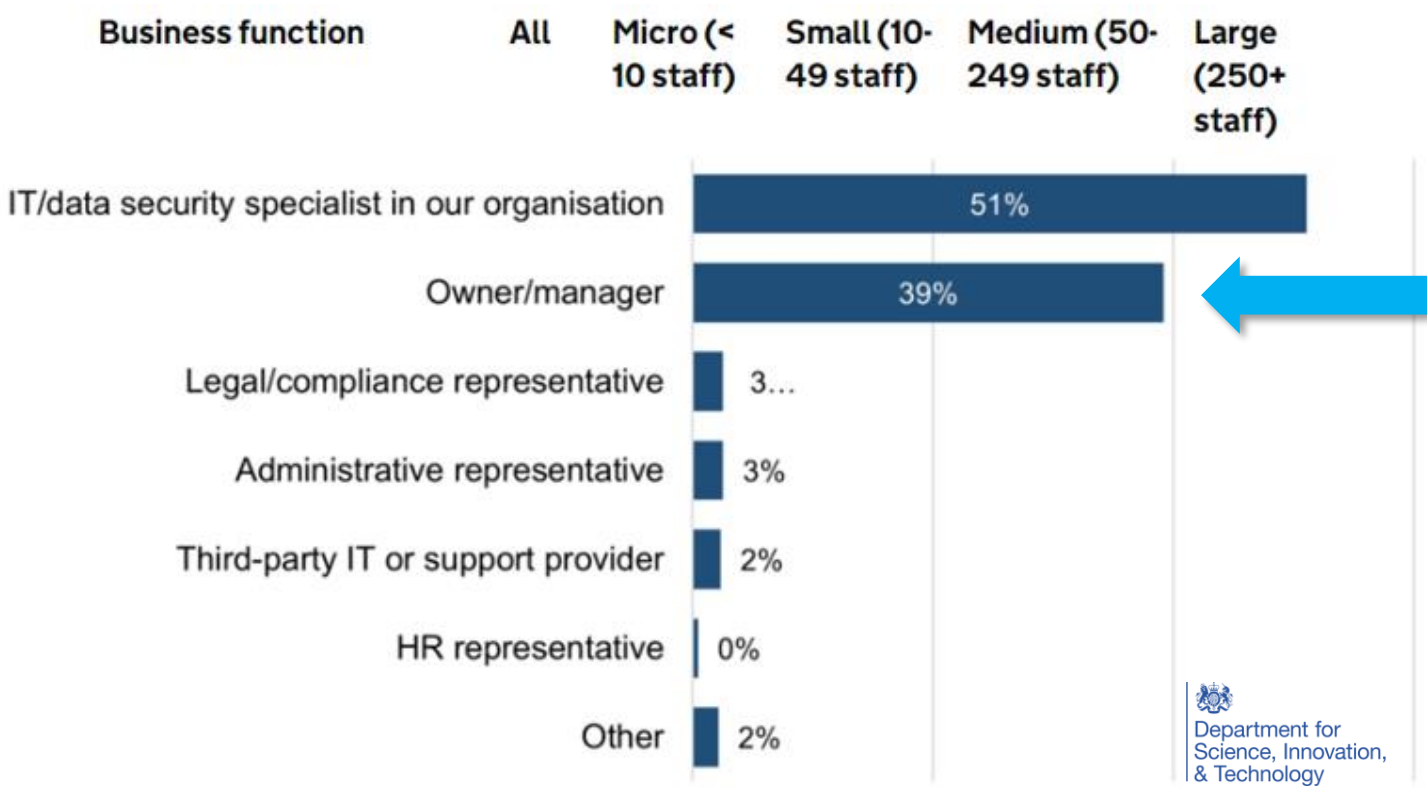
Lindy Cameron

Chief Executive Officer, NCSC

Cyber Security investment and culture, must be led from the top

Leadership and risk management cont.

Main decision maker when investing in cyber security improvements:



5.5 million businesses in the UK

99.9% are SME

MOORE ClearComm

Leadership and risk management cont.

Why businesses invest in improved cyber security measures:

Good cyber security provides a competitive advantage, as well as protecting an organisation, its customers, suppliers and employees.

QUESTION

What drives a leader to decide that investing in (or developing) a cyber security culture is the right thing to do or (conversely) to ignore the risk?

QUESTION

Do leaders or business owners convince themselves that “it won`t happen to us” and where does that psychology come from?

DIGITAL CYBER REPORT

Free Digital Cyber Report

- Digital cyber risk report, provides a hacker's eye view of your organisation
- Using your domain as a starting point, we can identify the vulnerabilities that could be exploited by attackers
- Your report will uncover any data breaches, stolen credentials, shared servers, missing security certificates and more

Digital Cyber Risk Report includes:		
Breached Email Addresses	Hosts Sharing Nameservers	HTTP Security
Blacklisted Domains	Permutations	DNS Security

MOORE ClearComm

Contact: richard.jackson@mooreclear.com

QUESTIONS

Our next event

Creating a culture of privacy

Date: Thursday 9 November 2023
Time: 10.00am-11.00am

Speakers:

- Rich Jackson, Strategic Business Manager, Moore ClearComm
- Meagan Mirza, Data Protection Officer, Moore ClearComm

Booking link: Webinar invitation: Creating a culture of privacy

Location: Zoom

MOORE ClearComm

Moore ClearComm
9 Appold Street
London
EC2A 2AP
t: +44 (0)20 4582 1983

www.mooreclear.com

MOORE ClearComm