

# HACK TO THE FUTURE

Protecting your Business  
from AI Cyber Threats

*Midland ICT Network*



**Bryan Fitzpatrick**  
Sales Director  
Ekco MSP



# AGENDA

1. The AI Journey
2. Business Benefits & Risks
3. AI- Powered Cyber Attacks
4. Defending Against AI Threats
5. The Role of SOC & SIEM
6. Key Takeaways



# THE AI JOURNEY



## 1. AI Explosion:

The rise of tools like ChatGPT & Copilot – transforming how we work



## 2. Unleashing Benefits:

Boosted productivity, automation & innovation



## 3. Business Risks:

Compliance gaps, misinformation, security threats & loss of control



## 4. Defend & Protect:

Adapting security strategies to safeguard against AI-powered risks



## 5. Strategic AI Advantage:

Leveraging AI to outpace threats & gain a competitive edge

# What is Artificial Intelligence?

## Artificial Intelligence (AI)

- 🔒 Simulates human intelligence in machines.
- 🔒 Includes machine learning, natural language processing & robotics.
- 🔒 Used in Healthcare, Finance, Automotive and more.

## Generative AI

- 🔒 A subset of AI that creates new content like text, images and music.
- 🔒 Learns from large datasets to mimic human-like creativity and communication.



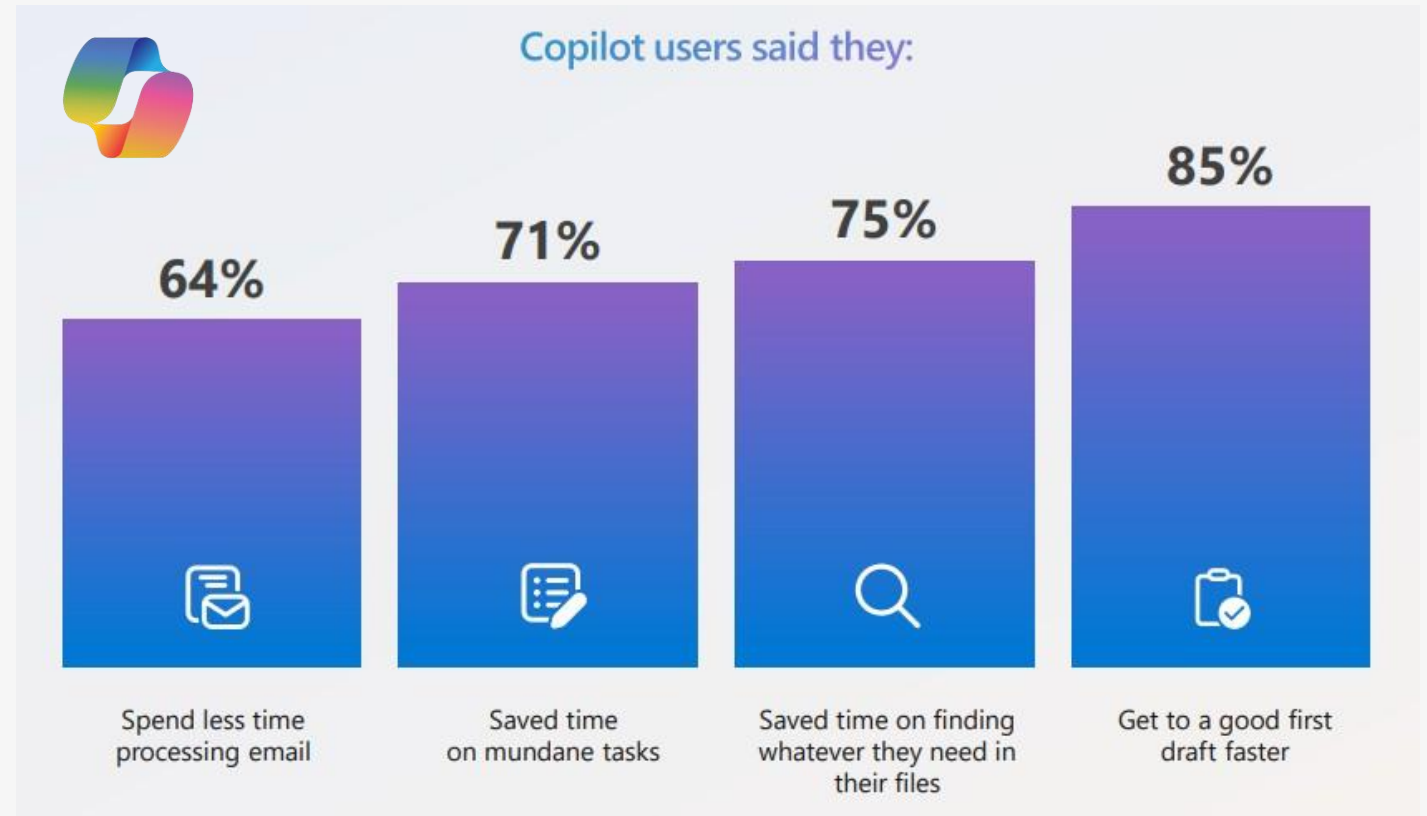
# Business Benefits of AI



# Copilot for Microsoft 365

Transforming Work

---

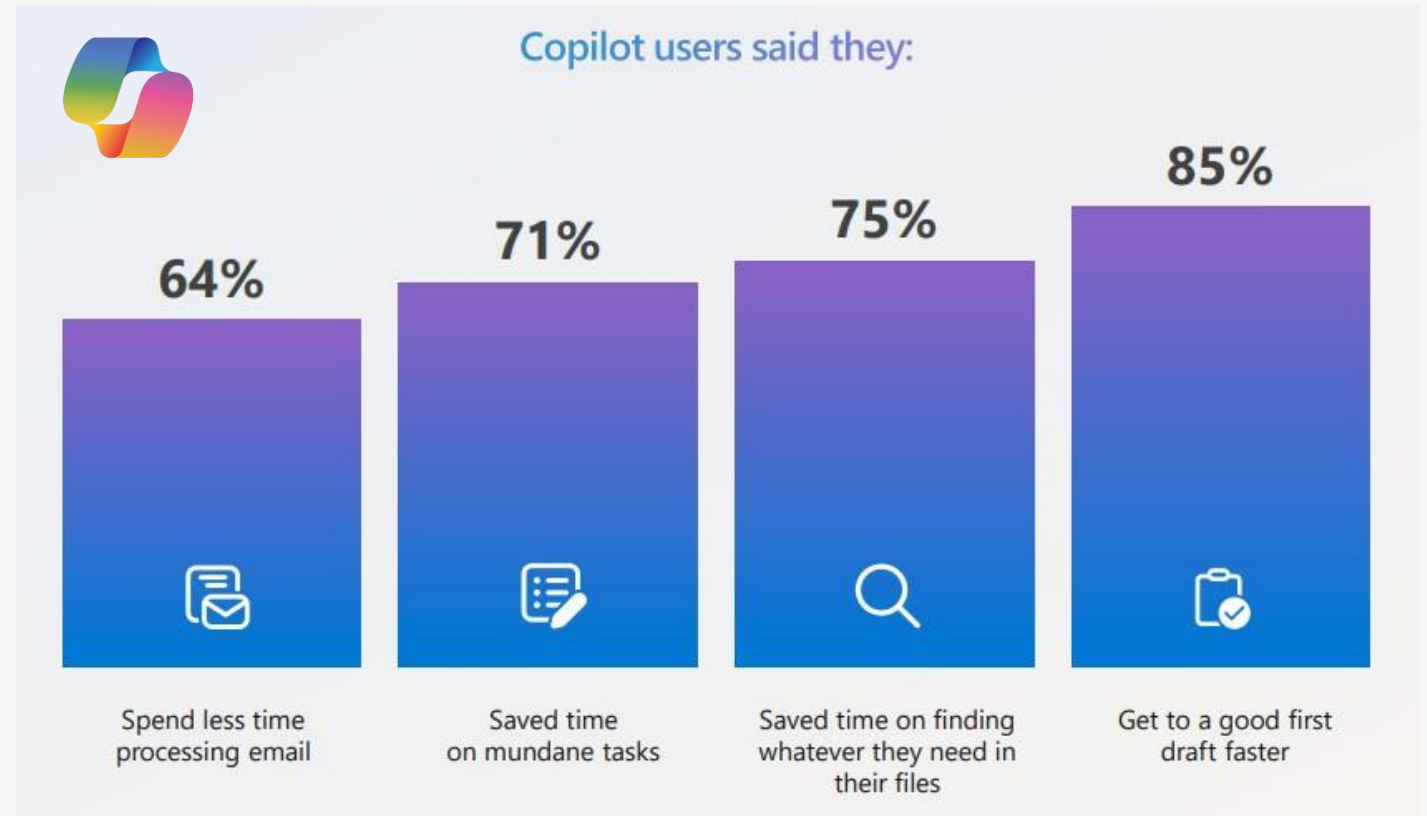




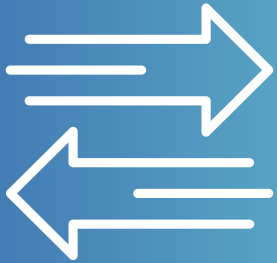
# Copilot for Microsoft 365

Transforming Work

---



# BUSINESS RISKS



EKCC







# AI-Powered Cyber Attacks

# HOW **AI** IS BEING WEAPONISED IN CYBER ATTACKS



## Deepfakes

A deepfake is an AI-generated video, image, or audio file that is meant to deceive people



## Social Engineering

AI-driven social engineering uses algorithms to research, craft, and execute targeted attacks.



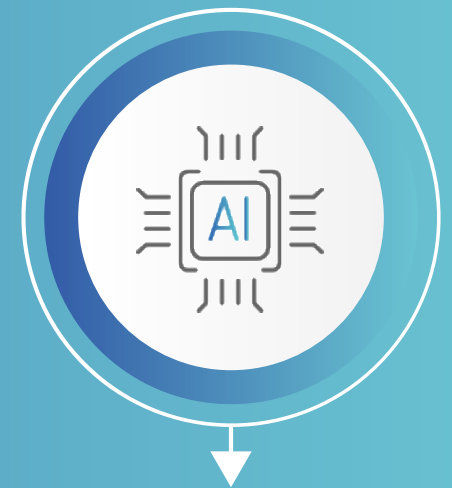
## Phishing Attacks

AI-driven phishing uses generative AI to craft realistic, personalised messages across channels.



## Malware

AI powers advanced malware that learns, adapts, and attacks autonomously.



## Adversarial AI/ML

Adversarial AI targets and disrupts AI/ML systems using manipulation or false data.

# Fake Social Media Accounts

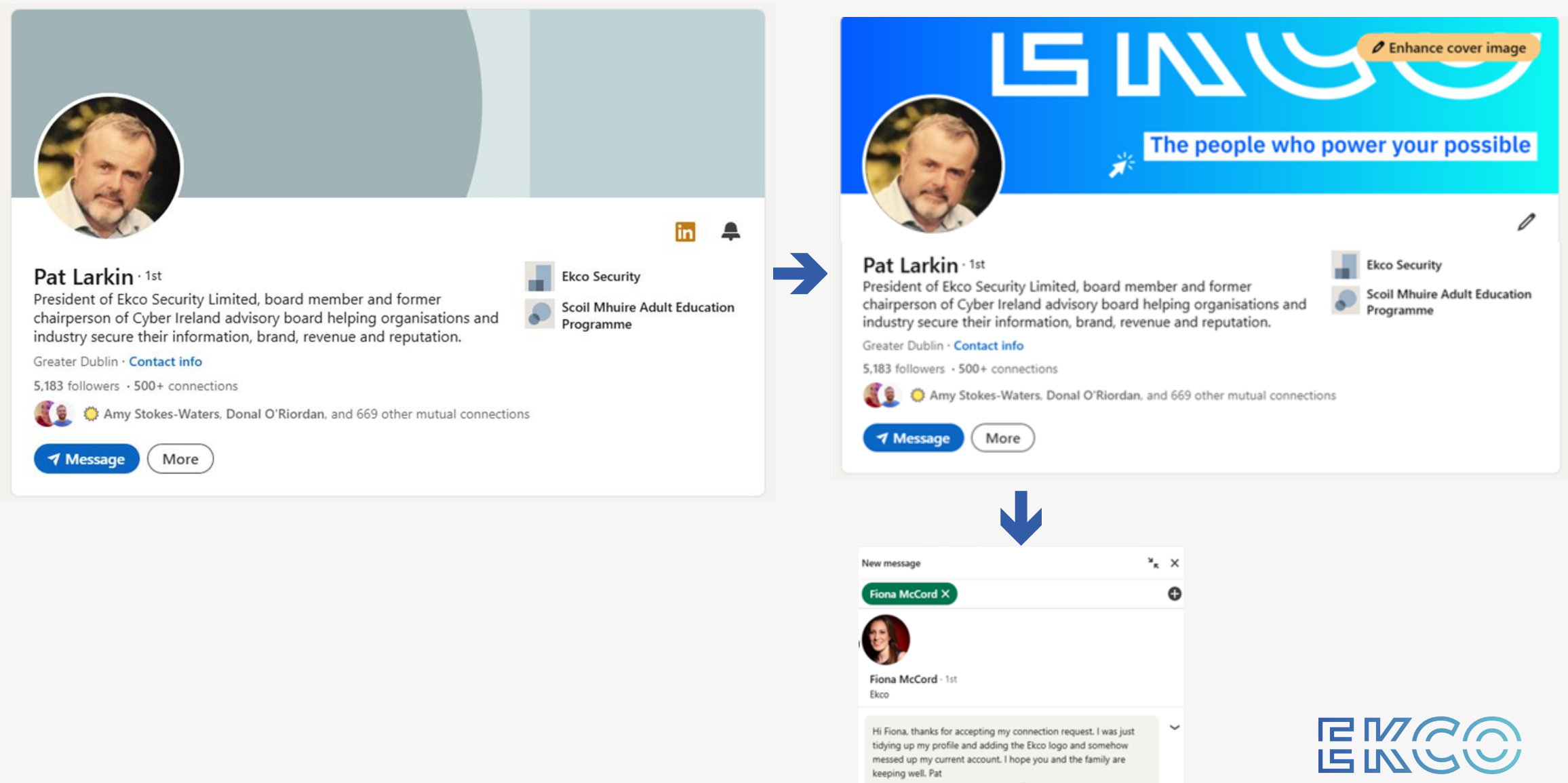
The image displays three screenshots from a social media application, each highlighting a different red flag for identifying fake accounts. The first screenshot shows a 'Requests' tab with two incoming friend requests. The second screenshot shows a conversation with a user named Susan Beck, who has zero followers and posts. The third screenshot shows a conversation with a user named Roger H. Poast, whose handle contains odd characters.

**1 Known Contacts**  
Friend requests from people already connected with you.

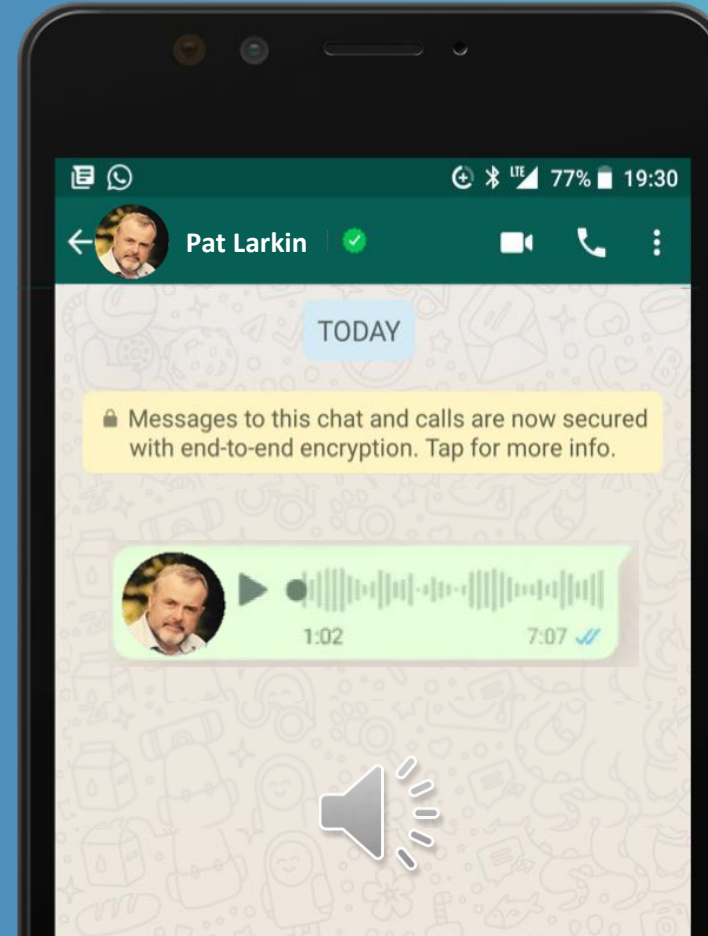
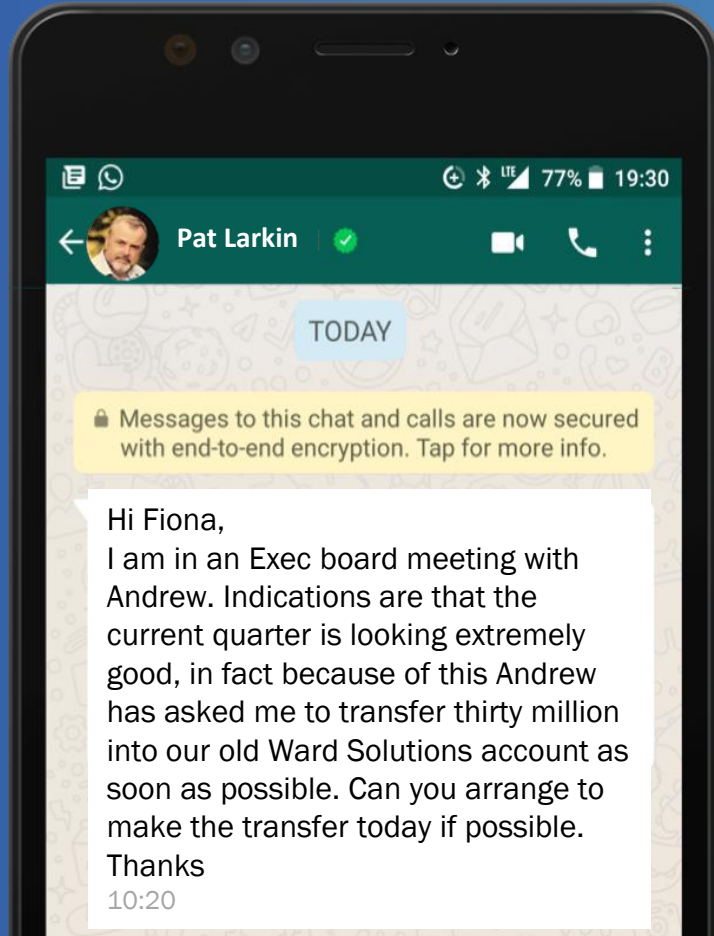
**2 Inactive Following**  
Zero or low followers is a flag especially if you know these people have been active a long time.

**3 Odd Characters in Handle**  
Both use name of the Contact with minor variation to try and avoid notice '.\_.' or '.\_.'

# Deepfakes – Video and Voice



# Deepfakes - Voice - Ekco





# Deepfakes – Video and Voice



Senator Gerard Craughwell- speech from 30 Mar ...

30 MARCH 22  
COMMITTEE ROOM 2

Watch later Share

JOINT COMMITTEE Discussion on cybersecurity and possible hybrid threats following the Russian invasion of Ukraine

TRANSPORT AND COMMUNICATIONS

Pat's opening statement in full

The last time we were here, you asked contributors about the emerging trends we saw in the cyber realm, affecting our clients and what was required to mitigate such threats. This last hearing took place in the ominous shadow of the HSE cyber-attack. Since then cyber-warfare threats have escalated in a manner and in a timeframe, which has blindsided the majority.

On foot of the Ukraine invasion, Ward Solutions notified our clients in our situational security advisories, of what we believe to be significantly increased risks:

Always  
consider your  
**Digital Footprint!**

PERSON  
**Pat Larkin**

Summary

Overview

Number of Founded Organizations 1	CB Rank (Person) 922,546
Primary Job Title Co-Founder and CEO	Primary Organization Ward Solutions
Location Dublin, Dublin, Ireland	Regions European Union (EU), Europe, Middle East, and Africa (EMEA)
Gender Male	
Facebook View on Facebook	LinkedIn View on LinkedIn



# AI Deepfake Fraud Risks

## 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

● [Business live - latest updates](#)



Arup confirmed that fake voices and images were used in the fraud. Photograph: Andrew Brookes/Getty Images/Image Source

The British Engineering company Arup confirmed it was the victim of a Deepfake fraud after an employee was duped into sending HK\$200m (£20m) to criminals by an AI-generated video call.



# Misinformation is a Global Risk



NEWS

## Davos 2025: Misinformation and disinformation are most pressing risks, says World Economic Forum

World leaders, business chiefs and civil society organisations will discuss the risks posed by misinformation, disinformation and artificial intelligence at the World Economic Forum

By  Bill Goodwin, Computer Weekly

Published: 15 Jan 2025 10:00

Misinformation and disinformation pose the greatest risk to countries, businesses and individuals over the next two years.

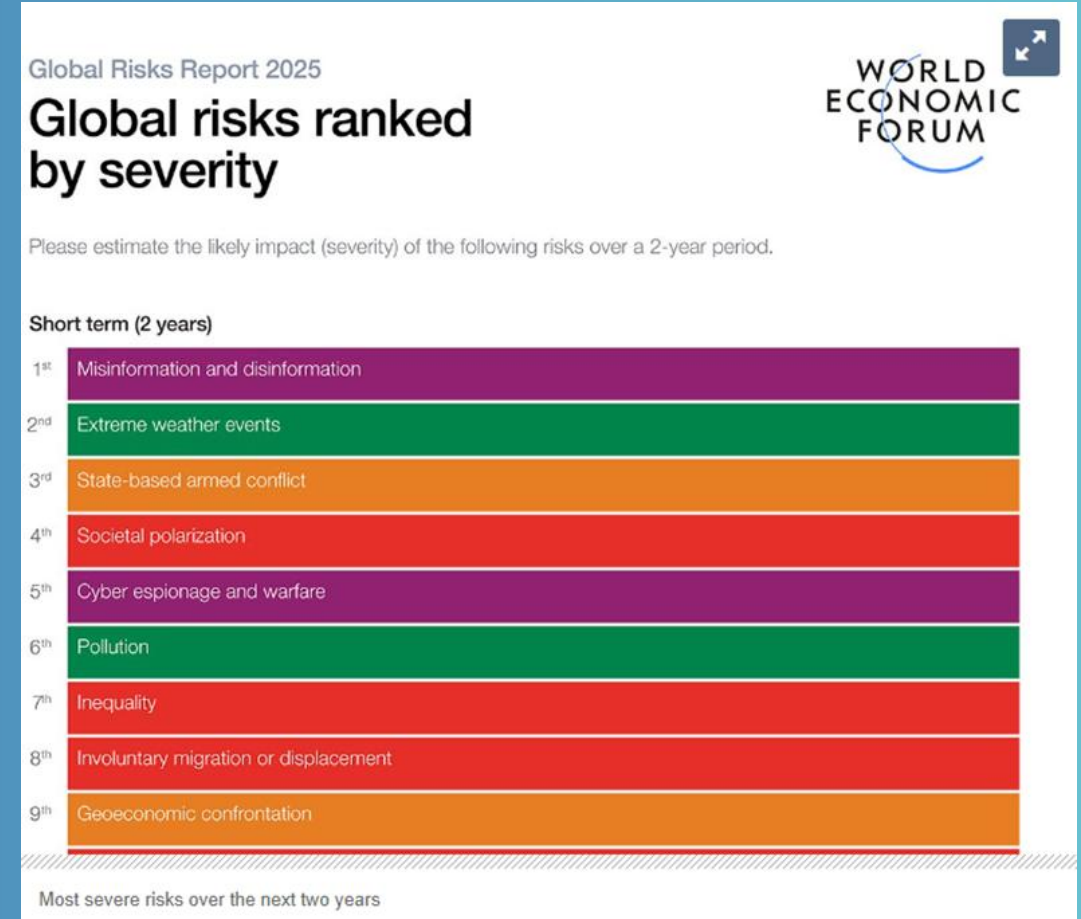
The rise of fake news, the decline of fact checking on social media and the growth of deep fakes generated by artificial intelligence (AI) threaten to erode trust and deepen divisions between countries, the World Economic Forum (WEF) said today.

ADVERTISEMENT

Benchmark your company progress with TechTarget 2024 IT Salary Survey results

[Download Now](#)

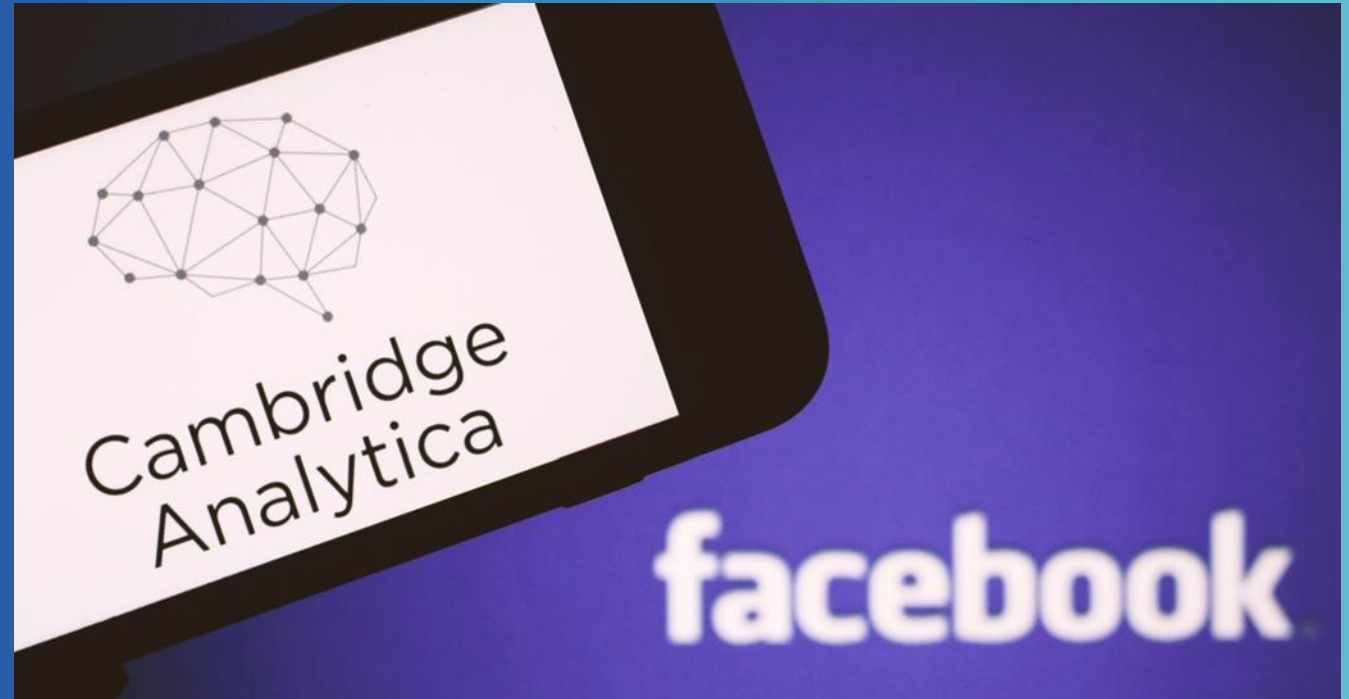
TechTarget Computer Weekly



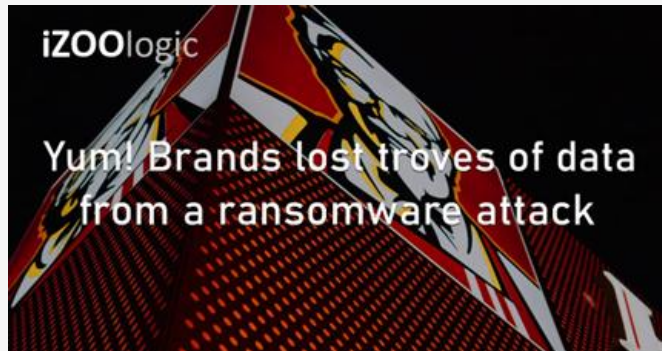
# AI Enabled Misinformation

Personality Quiz on Facebook used to profile users using AI to manipulate their political sentiment using targeted ads.

This **breach** raised significant concerns about data privacy and the ethical use of AI.

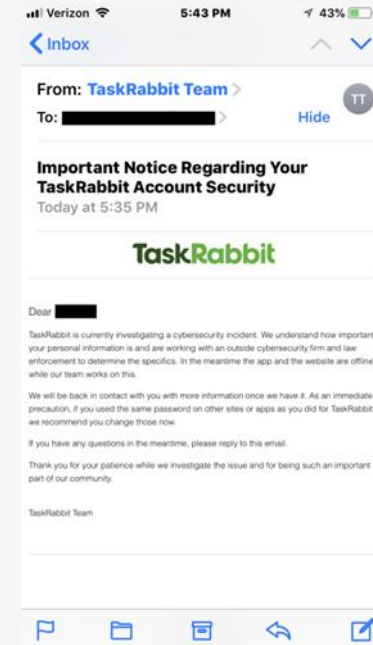


# AI Enabled Breaches & Data Privacy Risks



The attack leveraged AI technology to automate decisions on which data to steal.

*An example of improving the efficiency of traditional breaches using AI.*



3.75 million records. The breach involved the theft of personal information and financial details. The attack utilised an AI-enabled botnet.

*Demonstrating the growing threat of AI-powered cyberattacks.*



AON accused of incorporating biases into its software that discriminated against individuals based on race and disability.

*An example of Data Privacy risks introduced by unethical use of AI.*





# Defending Against AI Driven Cyber Threats

# Today's Threat Landscape

Sophisticated Attacks across **Multiple Domains**



The average number of days to execute a **ransomware attack** fell from 60 days in 2019 to **4** days in 2023

94%

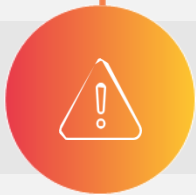
Of organisations fell victim to **phishing attacks**, up from **92%** in the previous year

“What happens when attackers use AI — and your SOC doesn’t?”

# How Threat Actors are Leveraging GenAI Tools to Support & Enhance their Cyber Operations



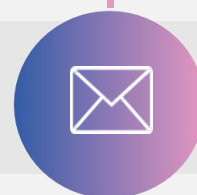
Malware  
Generation



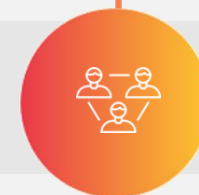
Customising  
Exploits



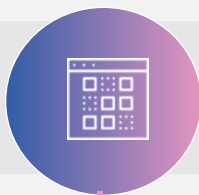
Phishing &  
Social Engineering



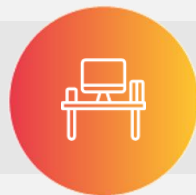
Command & Control  
Communication



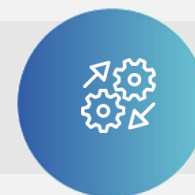
Automated  
Vulnerability Discovery



Password  
Cracking



Disguising  
Malicious Code




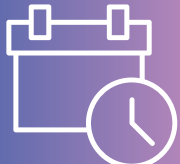


Deepfakes: Data,  
Email, Voice



# Transform SOC Productivity with Generative AI

Respond to cyber threats faster with step-by step guidance, empower any analyst

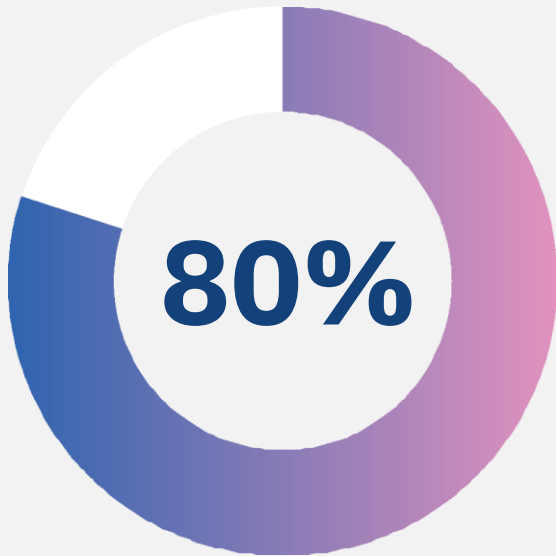
AI in Defensive SOC Services	Anomaly Detection	Automated Response	Threat Hunting with AI
AI-enhanced SIEM/SOAR tools (Ex: Microsoft Sentinel)	UEBA & behavioural analytics to find insider threats & subtle TTPs	SOAR runbooks & GenAI = contextual responses, alert triage & even ticket writing	Natural language queries and autonomous hunting suggestions
			



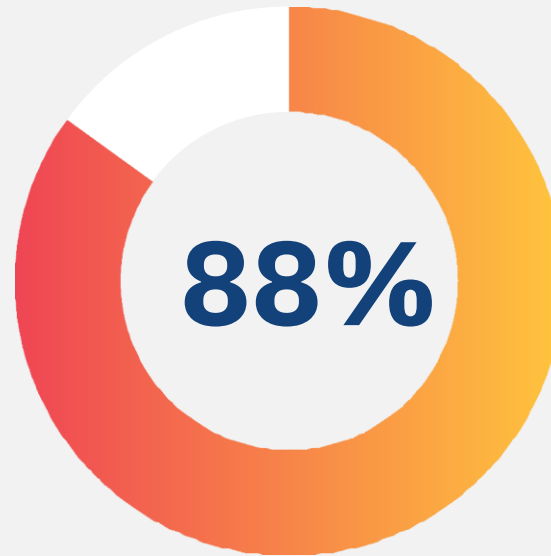
# SOCs Using GenAI are Delivering Real Impact



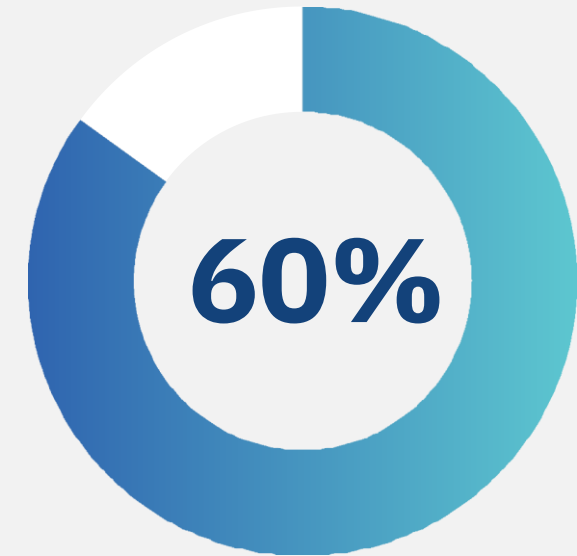
Better, more responsive protection



Possible reduction in incidents <sup>1</sup>



Reduction in threat mitigation <sup>2</sup>



Reduced risk in a material breach <sup>2</sup>

1. Unified SecOps platform preview participants

2. Forrester Consulting, "The Total Economic Impact™ Of Microsoft SIEM And XDR," August 2022, commissioned by Microsoft

# HOW TO DEFEND AGAINST ATTACKS



## 1. Security Assessments



- Continuous Monitoring & Reviews
- Develop Behaviour Baselines
- Detect Abnormal Activity
- Real-Time Analysis of Data

## 2. Incident Response Plan



- Preparation
- Detection & Analysis
- Containment & Eradication
- Recovery

## 3. Security Solutions



- Use AI –Driven Tools to Detect Threats
- SOC & SIEM
- Anomaly Detection Systems
- Behavioural Analytics
- Network Traffic Analysis

## 4. Staff Training



- Train Staff on Evolving AI Threats
- Educate on Data Privacy & Protection
- Promote a 'Zero Trust' Mindset
- Develop AI Security Policies

## 5. Expert Support



- Partner with Security Specialists
- Technology Alignment
- 24/7 Monitoring & Rapid Response
- Real-Time Threat Intelligence
- Ensure Compliance with Regulations

# KEY Takeaways



## Double Edge Sword



AI drives productivity but also increases risk. Success lies in balancing both with the right systems, tools and policies.

## Control, Manage & Harness



AI is here to stay. To stay competitive, businesses must shift their mindset – controlling and managing AI to harness its full potential for productivity and growth.

## Proactive Approach



Protection starts with proactivity. Alignment of IT systems, policies, technologies, and processes will help businesses stay ahead of AI-driven threats.

# Any Questions?

# QR Code / Link for CPD Training



<https://thecpd.group/webinar/portal/512eae82-922b-40b2-aa93-b21ca96c7a75>

# Get in Touch

**Bryan Fitzpatrick**

Sales Director

Ekco MSP

E: [bryan.fitzpatrick@ek.co](mailto:bryan.fitzpatrick@ek.co)

**Visit:** [www.ek.co](http://www.ek.co)

