Audit Committee Insight

Technology Risk Update

October 2023

Technology Risk Update

1. Introduction & Background

The risks posed by technology are ever changing and their potential impact wide ranging.

Audit Committees need to ensure they are aware of key technology risks and how their organisation is managing them.

This briefing provides and update on some key technology risks for Audit Committees to consider.

2. AI Chatbots and LLMs

An Artificial Intelligence (AI) chatbot is a system capable of maintaining a conversation with a user in a natural language. An example is ChatGPT. It produces human-like text and is underpinned by LLM technology.

LLMs are large language models. An algorithm is trained using large quantities of text-based data, from a wide array of sources. Due to the volume of data consumed, it is not possible to filter / verify all data within the model. A model can be "trained" and released and / or "fine-tuned" using additional data, however, the model is reflective of the data set / training applied.

ChatGPT was released in late 2022 and is one the fastest growing consumer applications. Other variants being produced / under development include Google's Bard and Meta's LLaMA (for science papers). There is also a malware variant WormGPT.

Emerging threats and opportunities are being tracked. For further guidance see National Cyber Security Centre's (NCSC) blog: https://www.ncsc.gov.uk/blog-post/chatgpt-and-large-language-models-whats-the-risk?ref=axbom.se

3. Deepfake and Shallowfake

A deepfake video is deceptively realistic. The term typically refers to video that has been digitally manipulated to replace one person's likeness (face and / or voice) with that of another. They can also create images of fake events.

Whereas a shallowfake may be video that is presented out of context or altered using simple editing tools.

They are used to entertain or spread misinformation / deceive.

The AI firm Deeptrace reported finding 15,000 deepfake videos online in September 2019 – a near doubling over 9 months. This number continues to grow (https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them)

A recent example of a deepfake scam was the Martin Lewis / Elon Musk deepfake video: https://www.bbc.co.uk/news/uk-66130785.

4. Messaging Solutions

There are a variety of messaging solutions available. These can be used in the corporate environment for communications, etc.

Messaging solutions are used for messaging and voice calling, video and telephone calls and / or to send photos and videos to contacts. They allow communication between a range of different devices, supporting one-on-one or group communication.

Organisations need to consider whether to permit solutions in their corporate environment as some government agencies have banned solutions due to risks. Organisations should ensure that messaging solutions are being corporately managed. For instance, that there are appropriate policies in place to risk assess, configure, manage, maintain and assure these solutions.

Users should also enable 2-step verification to protect their accounts and

be aware of who has access to corporate / personal information.

Training and Awareness

Organisations should continue to brief staff on the use social media and about potential threats, for instance from fake accounts, phishing and cold calls, etc.

There have been recent reports of a WhatsApp Pink (pink icon in app store) scam. The application is believed to contain malicious code.

In 2023 the UK Security minister asked NCSC to review TikTok over security and data privacy concerns, such as its ability to capture biometric data and access / store / secure data collected. It has been fined by ICO for not safeguarding children's data and is currently banned on government phones in the US, Canada and EU.

Further guidance is available via NCSC:
https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely
https://www.ncsc.gov.uk/guidance/social-media-protect-what-you-publish
https://www.ncsc.gov.uk/collection/device-security-guidance/policies-and-settings/choosing-an-enterprise-instant-messaging-solution
https://www.bbc.co.uk/news/uk-politics-64950157

We have listed below what we view to be key questions for Audit Committee members to consider:

1. Which Large Language Models does the organisation permit in its corporate environment?
2. Which platforms / messaging solutions should the organisation permit in the corporate environment?
3. Are these solutions being corporately managed? For instance, are appropriate policies in place to risk assess, configure, manage, maintain and assure these solutions?
4. Is 2-step verification enabled to protect social media accounts?
5. How is video content corporately managed?
6. Are staff being briefed about potential deep and shallow fake video content?
7. Is the organisation continuing to brief staff on the use social media, and potential threats, for instance from fake accounts, phishing and cold calls, etc.?
8. How are emerging technology opportunities and threats being tracked?

Find out more: If you have any queries or feedback on this briefing, please contact: Paula Fagan, Head of Technology Risk at MIAA (M: 07825 592 866; E: paula.fagan@miaa.nhs.uk