Cyber risks in a world of AI

Written by David Fleming, Chief Technology Officer at Mitigo

AI is a hot topic. Many professional service firms are already using AI or exploring its potential to revolutionise the way they deliver their services. But it's not all good news. Cybercriminals are also interested in the benefits of AI and how it can make their activities more profitable. Here, we discuss the potential impact of AI from a cybercrime perspective, and provide some tips on how to mitigate the risk AI presents.

Here are three aspects to consider.

Local unauthorised use of AI tools.

Staff members may already be using ChatGPT and other AI to make their work more effective. In our cybersecurity assessments, we often see a significant footprint of AI tools that are being used locally on the employee's computer. This is largely invisible to the business and the person who is responsible for IT or cybersecurity.

The issues here are:

- Downloading of applications that aren't subject to the appropriate level of due diligence.
- Uploading business information and data into hosted AI engines where control is lost.
- Loss of effectiveness of existing controls e.g. Anti-Virus will be blind to these new processes.

Take away actions:

1. Start with a policy that defines legitimate use and make sure it is published and understood.
2. Create a process to assess and approve/decline existing use cases.
3. Ensure local admin rights and AV settings prevent the download of applications to devices.
4. Toughen browser and AV settings to flag use of AI websites or websites with low trust scores.

Poor development and implementation of AI.

The core focus of development and implementation of AI will be the benefit it can bring to a business e.g. by reducing costs or increasing efficiencies. Therefore, at the design stage, security elements can often be overlooked, which in turn can lead to vulnerabilities.

The issues here are:

- The development process will require you to experiment with different services and providers. This has an inherent risk as cybercriminals will move fast to insert malicious code into services (this is already happening).

- You are introducing a new supplier and processes into your supply chain and these need to be controlled.
- The attack surface of your organisation has changed and potentially grown. You need to ensure you design appropriate controls and security.

Take away actions:

1. A separate environment should be created for the development/experimentation process to reduce the risk of a malicious actor connecting to your business-as-usual network.
2. A due diligence process should be designed and carried out on new suppliers.
3. Existing policy needs to be updated to include the new technology and processes. For example, how are software patches identified and updated.
4. Your control framework needs to be updated. What controls, monitoring and alerts need to be created to secure the new business process.

Increased sophistication of cyber-attacks powered by AI.

The adoption of AI by cybercriminals to launch attacks and exploit vulnerabilities is arguably the biggest threat to a business. This includes enhanced ability to get round cyber training and control measures.

Some examples:

- Spotting flaws in emails and websites has long been a protection against cybercrime. AI will enable greater sophistication. Social engineering can be taken to a new level as multiple approaches can be coordinated to entrap a victim.
- Impersonation is often a key part of attacks. Imagine deep fakes of images and voices, and think about what the criminals could do with that.
- Speed of development will increase. Every time a control stops a malicious bit of code, AI will have the ability to instantly analyse and code a solution for the criminals.

Take away actions:

1. Simulated attacks on staff need to be more frequent and mimic the new approaches.
2. Authentication and conditional access need to be improved to make the stealing of credentials ever more difficult for the criminals.
3. Layers of defence will be essential. If a human gets duped, ensure that there is sufficient control and alerting to stop the progression of an attack.
4. Assessment and assurance will become increasingly important. Frequent assessment by experts will be required to keep you hardened against the increasing sophistication and scale of attack.