

EXECUTIVE SUMMARY

AI has officially overtaken ransomware as the top cybersecurity risk, according to a recent *ITWeb* report. Since most businesses now use AI, whether it's for customer support, automation or data analysis, understanding the risks and knowing how to protect your business has become critical.

AI IS NOW THE BIGGEST CYBERSECURITY RISK – WHAT YOUR BUSINESS SHOULD KNOW

AI's Role In Cyber Threats

Cybercriminals are using AI to send phishing emails, create viruses that change themselves in order to avoid detection and learn and adapt to break into systems. At the same time, businesses use AI to scan for threats, detect unusual activity and respond faster to attacks. Don't think it won't/can't happen to you.

Using AI Safely – A Business Priority

Many risks come from how employees interact with AI. Common issues may include accidentally sharing sensitive data with AI tools, using public or unauthorised AI platforms and misunderstanding what AI systems can and can't do. To prevent problems, we recommend that businesses create clear policies that guide staff on which AI tools are approved, what kind of information can be shared and how to spot and report unusual AI behaviour.

Safeguards

If AI is involved in a cybersecurity incident, you'll want legal safeguards in place. Two key areas to focus on are: (1) Commercial Agreements – make sure your contracts cover responsibility, liability and response when something goes wrong; (2) Internal Policies – set up internal rules that guide how staff use AI (these include safety checks, approval processes and incident reporting steps).

SA's Cyber Laws You Should Know

Legislation	What It Covers
Protection of Personal Information Act, 2013	Protects personal data and how it's used
Electronic Communications and Transactions Act, 2002	Sets rules for online transactions and safety
Cybercrimes Act, 2020	Makes cybercrimes like hacking and data theft illegal
Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002	Governs when and how communications can be monitored

Ensuring that your business implements these laws will go a long way to assist in the event of cybersecurity breaches (and also keep your insurers happy!).

Contact Us

For assistance with cybersecurity agreements, AI policies or legal advice, please contact us at:

Tel : +27 (0)11 884-0792

E-Mail : neil@harty.law or natasha@harty.law

www.harty.law

The eFiles is a periodic newsletter which is distributed free of charge to anyone who wishes to receive articles on legal issues relating to our fields of practice. Please e-mail any comments or suggestions to neil@harty.law.

To subscribe, e-mail efiles@harty.law with "Subscribe" as the subject. To unsubscribe, send an e-mail with "Unsubscribe" as the subject.

This newsletter is for educational purposes only and must not be considered as legal advice. Your individual situation may not fit the generalisations discussed. Only your attorney can evaluate and advise you on your individual situation.

Except as provided below, you may feel free to forward, distribute and copy this eFile as long as you distribute and copy it without any changes, and you include all headers and other identifying information. You may not, however, copy it to a Web site without our prior written consent. If you would like information about obtaining legal services from Harty Rushmere, you can contact Neil Harty at +27(0)11 884-0792 or visit our Web site at www.harty.law. If you would like an attorney from Harty Rushmere to give a presentation on this topic, please call for information.