Legal Masterclass: *Cybercrime and Electronic Transactions*

Description	This legal masterclass helps you understand and navigate the laws of electronic transactions and cybercrime in South Africa. The aim is for you to conduct electronic transactions lawfully in your organisation—in line with international best practices—and prepare for and avoid cybercrime. The facilitator will present this masterclass from three perspectives: law, commerce, and information technology.
Structure of workshop	**Day 1** **Overview of Electronic Transactions and the Legal Landscape** • Contextualising electronic transactions within the 4IR in Africa • What are electronic transactions? • How do electronic transactions work? • How organisations conduct electronic transactions • The general legal risks associated with electronic transactions • The legal status of electronic transactions **The Legal Framework for Electronic Transactions in South Africa** • Exploring the regulatory framework • Understand the different roles in electronic transactions • Compliance with POPIA, RICA, and ECTA when conducting electronic transactions • The need for ECTA to be updated **Electronic Contracts** • Exploring the regulatory framework • Clickwrap agreements • Browse-wrap agreements • Shrink-wrap agreements • Discussion of best practices for drafting electronic contracts • Dark patterns • Smart contracts **Electronic Signatures** • Why do we sign things? • What is a signature? • Common Law • What is an electronic signature? • Attribution and authentication • Attribution and document integrity • Authentication and verification • Types of authentication (electronic, biometric, cryptographic) • Applicable laws • Role of electronic consent
	Day 2 **Understanding why cybercrime law is important** • Why we need cybercrime law • What is cybercrime? • International perspective • Existing law – Is ECTA effective? • Cybercrimes Act

- Offences
- Penalties
- Jurisdiction
- Investigation
- ECSPs and financial institutions

Stopping your personnel from committing cybercrime

- Cybercrime case studies involving personnel or organisations
- Understanding the offences created by the Act
- Can an employer be vicariously liable?
- The role of your governing body in preventing cybercrime
- Organisational measures to take to prevent personnel from committing cybercrime

Responding to cybercrimes committed against your organisation

- Regulatory frameworks and reporting obligations
- Preserving evidence during a cybercrime investigation
- Supporting those affected by cybercrime
- Risks of cybercrimes

Assisting with investigations into cybercrime

- Gathering evidence
- Drafting an affidavit
- Practical tips
- Opening a criminal case
- What happens next?
- Third-party assistance
- Business continuity
- Not committing additional crimes

Defending your organisation against cybercrime accusations

- The context
- Understanding the accusation
- Strategising your response
- Dealing with SAPS and the prosecution
- Defences

Day 3

AI and Cybercrime

- Understanding why cybercrime law is important
- An overview of the Cybercrimes Act
- Can AI be a criminal?
- Can AI be used to commit a crime?
- Key crimes relevant to AI
- Unlawful interception: RICA and cybercrime
- Assisting with investigations into cybercrime
- Defending accusations of committing cybercrimes

Data protection, information security, and cybercrime

- Who regulates the Cybercrimes Act?
- Cybercrimes vs cybersecurity
- Information security and cybersecurity

- Who falls within the definition of an Electronic Communications Service Provider (ECSPs)?
- Reporting obligations of ECSPs
- Data handling obligations of ECSPs
- An ECSP's obligation to provide technical assistance to authorities
- Balancing your obligations under POPIA and the Cybercrimes Act
- Business email compromise

Developing an organisational cybercrime programme

- Awareness and training
- Setting a cybercrime strategy
- Developing, drafting, and reviewing cybercrime policies, plans, and procedures
- International standards and best practices
- Incident planning, response, and recovery

Mode of Delivery	Online.
Admission requirements	This SLP is open to people working in a legal, business, regulatory, financial environment or any potential student who has completed Grade 12 studies and has a keen interest in many or a specific area of law.
Assessments	There are no assessments.
Masterclass Facilitator	Nathan-Ross Adams is a data and technology attorney at the pan-African ICT law firm, Michalsons. He specialises in data protection, access to information, cybercrime, and information security law regarding emerging technologies—all presented in plain language and legal design. Daily, Nathan-Ross helps Africa's most innovative businesses comply with ICT law. He's also doing his LLD at UJ on "Why and how to regulate artificial intelligence in South Africa to promote sustainable development".