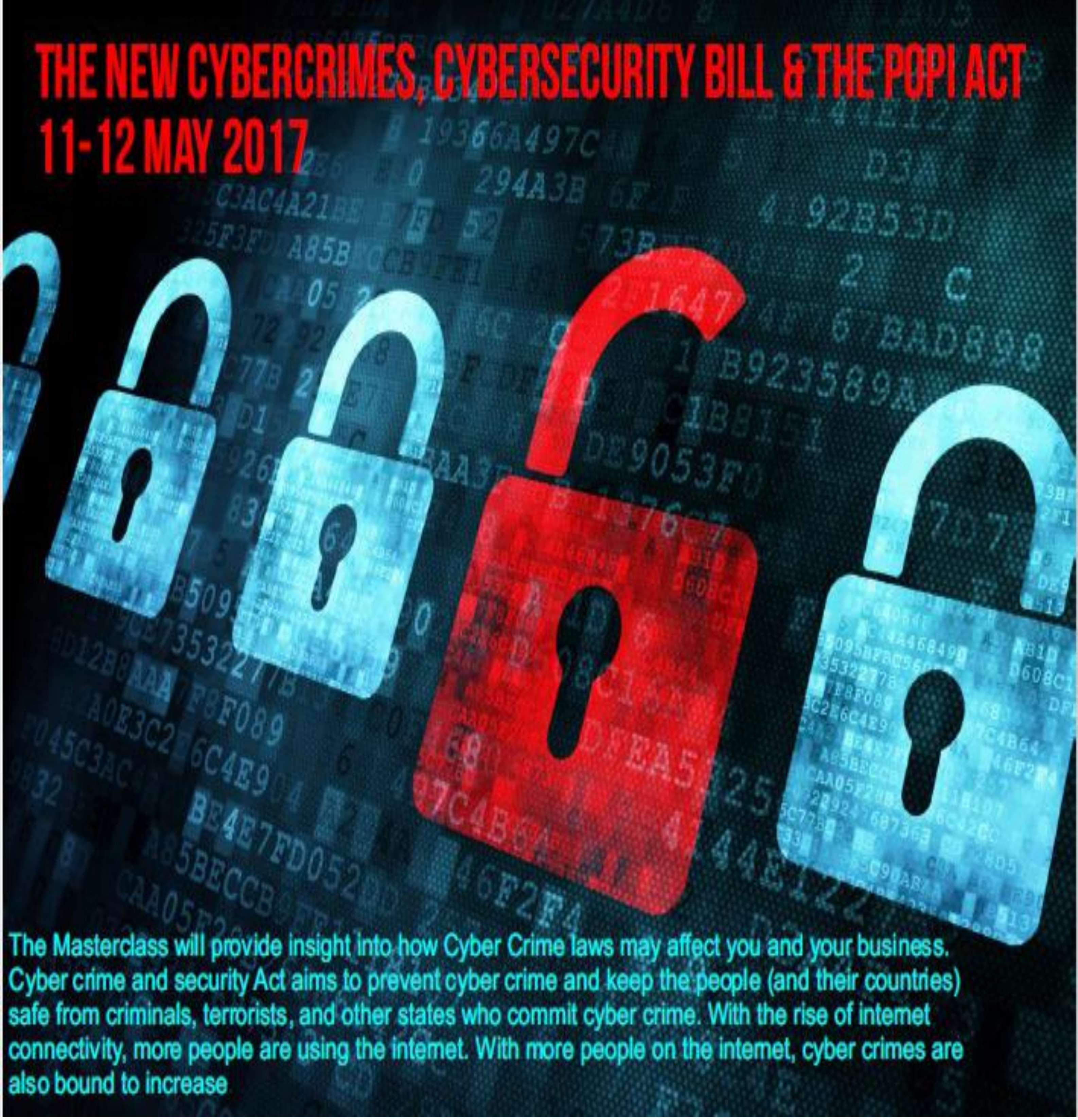

THE NEW CYBERCRIMES, CYBERSECURITY BILL & THE POPI ACT

11-12 MAY 2017

The Masterclass will provide insight into how Cyber Crime laws may affect you and your business. Cyber crime and security Act aims to prevent cyber crime and keep the people (and their countries) safe from criminals, terrorists, and other states who commit cyber crime. With the rise of internet connectivity, more people are using the internet. With more people on the internet, cyber crimes are also bound to increase

AFTER COMPLETING THIS COURSE YOU'LL BE CONFIDENT IN YOUR ABILITY TO

> Evaluate cyber security threats and policies in terms of current legislation and regulations
> Ensure your business or organisation on is taking the necessary protect on measures
>Recommend so ware and hardware products within cyber security categories for a given
> Environment or project
> Develop a cyber security compliance plan and incident response plan for your specific organisation
>Take steps towards creating a cyber security culture within an organisation

Sardonix Training

These courses are provided by Sardonix Training in collaboration with (IITA) accreditation No:4027 under the SETA, in conjunction with SBS registered with the department of high education & training as a private higher education institution under the higher education act, 1997. Registration certificate No:2002/HE07/015

The new enemies of our World, Cyber criminals and terrorists

Why does your staff need Cyber Security Education & Awareness training?
Cyber Criminals target the weakest link in security. “The human. Your staff.”
Technical defences are not stopping incidents from happening because of user behaviour.
23% of phishing emails are opened by staff with 11%opening attachments or clicking on links
Ransomware attacks continue to rise and will cause your data to be encrypted owing to user actions
Traditional training is not fit for purpose and is annual “compliance” tick the box exercise that does not change user behaviour long term.

The Cyber Bill also places obligations on financial institutions, ECSPs (or electronic communications service providers) and those who have a Critical Information Infrastructure (CII). These are defined broadly and you may well be an ECSP or have a CII without realising it. It also has serious implications for all internet users. Find out if you do and what it means for you. Organisations that should attend?

- Service Providers – anyone who may have critical data or infrastructure, or be an ECSP
- Electronic Communications Providers – to understand their responsibilities
- ISPs – anyone who could be an electronic communications service provider
- Financial Institutions (including banks) – because they may be an ECSP or have a CII
- Insurance providers – because they may be an ECSP or have a CII
- Law enforcement agencies – to enforce the Cyber Bill
- The Judiciary – to understand the new law
- Media groups – to assess the impact Cyber the Bill has on freedom of speech and journalism
- Civil Rights Groups – to understand the impact on civil rights, like privacy and freedom of expression

Those who should attend & why?

- Compliance officers – to effectively comply with the Cyber Bill.
- Legal advisers – (corporate lawyers or in-house lawyers) – to provide good legal advice on cybercrime issues.
- Anyone tasked with cyber security or crime – to perform your role effectively.
- Information Security officers – to secure the organisation's information.
- Forensic Investigators – to lawfully gather evidence and assist with the prosecution of cybercrime.
- Magistrates, judges and prosecutors – to deal with cybercrimes.
- Members of law enforcement and investigators – to enforce the Cybercrimes Bill.
- Risk Officers and Managers – to manage cyber-related risks.
- Journalists – to avoid committing cybercrimes.
- IT Governance officers – to ensure governance is in line with the offences.
- IT professionals – to ensure they lawfully deal with various software and hardware tools.
- IT vendors – to ensure they are not selling tools that can be used to commit offences.
- People involved with IT (or POPI) regulatory compliance.
- All Electronic Communications Service Providers (ECSPs).
- Financial institutions.
- Representatives from various government Departments.
- Cyber criminals and terrorists.
- Providers or vendors of software or hardware tools that could be used to commit offences.
- Information Security experts.
- Anyone who owns an Information Infrastructure that Government could declare as critical.
- Everyone who uses a computer or the Internet.
- The Police Service.

Above is those affected by the Cybercrimes, Cybersecurity Bill & POPI Act hence you need this awareness training
Outcomes:

- Know what the Cyber Bill covers
- Understand who could commit a crime, what ECSPs must do, and what it means if you have a CII.
- Apply your knowledge and understanding to influence the legislative process and plan for the commencement of the Bill.

What is covered on this Masterclass?

Day One

- Why is the Cybercrimes Bill important.
- A general overview of the international framework, the Bill and the timeline.
- The overlaps with other laws (like POPI Act and common law crimes).
- The timeline.
- What is the impact on an Electronic Communications Service Provider (ECSP)? Many people do not realise that they are one, and that the Bill places many obligations on them.
- Whether you could have a Critical Information Infrastructure (CII)? What does it mean if you do?
- Access to information and the surveillance of online activities.

- The new offences created by the Cyber Bill.
- Does it limit the freedom of speech? The impact on journalism.
- The impact on the use by IT professionals of legitimate hardware and software tools.
- Who enforces the Cyber Bill? The new structures the Cyber Bill creates.
- The role of the courts and the jurisdiction for the Cyber Bill crimes.
- Admissibility of electronic evidence, information sharing, and agreements with foreign states.
- Our insights and possible actions to take.

Basic principles of cyber security management

- Discuss the evolution and current state of cybersecurity
- Explain the importance of cybersecurity management within an organisation
- Identify the roles and processes in maintaining cybersecurity standards

Risk management

Describe the cyberthreat actors that exist in an organisation and illustrate the different types of threats
Deduce how an organisation can secure itself against cyber attacks
Compare the methods for assessing the cyber security risk

Corporate Governance, Policies and the Regulatory Environment

- Outline the National Cyber security Policy Framework (NCPF)as it is applicable to cybersecurity in South Africa
- Apply the important elements of the Electronic Communications and Transactions Act to a business legislative problem
- Use POPI as a guide to secure information in a business
- Investigate the role of corporate governance in cyber security management in South Africa

Basic Principles of Cyber Security Management

- Discuss the evolution and current state of cyber security
- Explain the importance of cyber security management within an organisation
- Identify the roles and processes in maintaining cyber security standards

Risk Management

- Describe the cyber threat actors that exist in an organisation and illustrate the different types of threats
- Deduce how an organisation can secure itself against cyber attacks
- Compare the methods for assessing the cyber security risk

DAY TWO

Corporate Governance, Policies and The Regulatory Environment

- Outline the National Cyber security Policy Framework (NCPF)as it is applicable to cyber security in South Africa
- Apply the important elements of the Electronic Communications and Transactions Act to a business legislative problem
- Use POPI as a guide to secure information in a business
- Investigate the role of corporate governance in cyber security management in South Africa

Make time to master your skills:

Cyber Security Culture

- Illustrate the impact of social engineering and human weaknesson cybersecurity and compare their differences
- Justify the importance of building a cybersecurity culture
- Develop a proposal for applying a cybersecurity education,training and awareness initiative within an organisation

Cyber Security Architecture

- Summarise the types of IT security principles and methods
- Interpret the concept of secure network design and analyse the threats to a secure network in an organisation
- Deduce a secure software management life cycle in an organisation and recommend a forensic readiness plan

Cyber Security Software and Hardware

- Investigate data protection strategies, including SOC, SIEM and cryptography
- Categorise the types of hardware and software used to protect an organisation's data
- Evaluate a software and hardware product for a specific organisation's cyber security plan

Compliance Management

- Choose a cyber security model that you would use for compliance and management in an organisation
- Differentiate between the NIST cyber security model and the 20 critical controls model
- Correlate the components of a cyber security compliance strategy of an organisation and recommend a compliance management technique

Incident Management

- Relate the elements of incident response in terms of cyber security and identify the incident response process in an organisation
- Distinguish between planning, developing and maintaining an incident response capacity for an organisation
- Recommend statutory reporting requirements to support cyber security incident management in an organisation
- Develop an incident response plan for an organisation

The new enemies of our World, Cyber criminals and terrorists

Sardonix Training

Sardonix Training Academy

THE NEW CYBERCRIMES, CYBERSECURITY BILL & THE POPI ACT

11-12 MAY 2017

PRICE: R 8 999.00

EARLY BIRD R 8 499.00

CONTRACT & REGISTRATION FORM

COMPANY DETAILS:

Company Name: ______________________________

Company Address: ______________________________

Post Code: ______________ Country: ______________

Tel: ______________ Fax: ______________

Authorising Signatory:

Name:(Mr/Mrs/Ms): ______________________________

Designation: ______________________________

Tel: ______________ Fax: ______________

Email: ______________________________

Signature: ______________________________

Please register the following delegates:

Delegate 1:

Name:(Mr/Mrs/Ms): ______________________________

Designation: ______________________________

Tel: ______________ Fax: ______________

Email: ______________________________

Delegate 2:

Name:(Mr/Mrs/Ms): ______________________________

Designation: ______________________________

Tel: ______________ Fax: ______________

Email: ______________________________

Delegate 3:

Name:(Mr/Mrs/Ms): ______________________________

Designation: ______________________________

Tel: ______________ Fax: ______________

Email: ______________________________

Delegate 4:

Name:(Mr/Mrs/Ms): ______________________________

Designation: ______________________________

Tel: ______________ Fax: ______________

Email: ______________________________

Delegate 5:

Name:(Mr/Mrs/Ms): ______________________________

Designation: ______________________________

Tel: ______________ Fax: ______________

Email: ______________________________

CONTACT PERSON:

Vuyisa Zungu
Tel: +27 11 044 7107
Cell: +27 60 680 3847
Fax: 086 263 1693
Email: vuyisa@sardonixy.com / info@sardonixy.com

BANKING DETAILS:

Bank transfers can be made to the following account

Account Holders: Sadonix investments (pty)

Bank	: FNB
Branch	: EDENGLEN
Swift Code	: FIRNZAJJXXX
Branch Code	: 252442
Account Type	: Current
Account Number	: 62554209801

By signing and returning this registration form, the authorizing signatory on behalf of the stated company accepts responsibility for the payment and is subject to the following Terms & Conditions of this contract Delegate Substitutions – Delegate substitutions are welcome at any time. Please notify SARDONIX in writing of any changes.

Delegate Cancellations – All delegates' cancellation must be received in writing and are subject to the following conditions: For any cancellations received 7 working days before the start of a training course will issue a credit voucher for the value paid to be used for up to one year from current events from the date of issue for any future training. Delegate has to choose a future course to attend within 7 working days from receiving the credit voucher and the course year calendar. For any cancellations received less than 7 working days before the date of training course, the full fee will be payable and no refunds or credit voucher will be given if a registered delegate does not cancel or fails to attend the training course, this will be treated as a cancellation and no refund or voucher will be issued

Transfers
Transfer requests must be made in writing 7 days before the start of the event SARDONIX Substitutions. Please note that speakers and topics were confirmed at the time of publishing Training Cancellation and Postponement In the event that SARDONIX cancels an event, delegate's payments at the date of cancellation will be credited to a future SARDONIX event. In the event that SARDONIX postpones an event, delegate payments at the postponement date will be credited towards the rescheduled date. If the delegate is unable to attend the rescheduled event, the delegate will receive a credit voucher representing payments made towards a future SARDONIX event. SARDONIX shall assume no liability whatsoever in the event this conference is cancelled, rescheduled or postponed. For purposes of this clause, a fortuitous event shall include, but not be limited to fire, labour strike, extreme bad weather or other emergency.
Please note that speakers ,venue and topics were confirmed at the time of publishing, however, circumstances beyond the control of the organizers may necessitate substitutions, alterations, change of venue or cancellations of the speakers and, or topics. As such, SARDONIX reserves the right to alter the advertised speakers, venue or course content if necessary. Any substitutions or alterations on the topics ,course content ,or venue will be updated on our web page as soon as possible or given to the delegates before the commencement of the workshop. The content that is altered or substituted shall remain within the same advertised field of training.