ENSafrica
light at the end of the cybercrime tunnel

thank you for joining
we will be starting soon
Agenda

• mitigating the risk | **Roy Gillespie**
• the latest trends in cybercrime | **Ulrich Kruger**
• developments in the law, in particular the Cybercrimes Act | **Suad Jacobs**
• data breach implications and how to mitigate your risks as a company | **Nicole Gabryk**
cybercrimes webinar | mitigating the risk

Roy Gillespie
25 NOV 2020
Organisations are increasingly looking to protect themselves

Various cyber security standards ISO Global Standards (27001, 27005, 27032), NERC, NIST, ANSI/ISA, IEC 62443 etc. which provide information security risk management and cybersecurity guidelines

Earlier this year the SEC issued a report on Cybersecurity and Resiliency Practices applicable to public companies across a range of industries at a time when cybersecurity threats continue to touch every region of the world and virtually every sector of the economy.

Governance and risk management — establishing board and senior leadership oversight of cybersecurity and resiliency programs, conducting risk assessments, creating written policies and procedures that address cybersecurity issues, testing and monitoring of relevant policies, updating policies and procedures to address any gaps or weaknesses and developing methods of communicating internally and externally regarding cybersecurity issues.

Access rights and controls — understanding, managing and monitoring user access to data and systems.

Data loss prevention — developing a vulnerability management program to conduct routine scans, implementing security measures to intercept threats and block access to personal email or other insecure platforms, implementing security measures to detect threats at endpoints, using a patch management program, keeping an inventory of hardware and software assets, using encryption and network segmentation, monitoring insider threats and securing legacy systems and equipment.
cyber security | risk mitigation cont.

• **Mobile security** — creating policies and procedures relating to the use of mobile devices, managing use of mobile devices, mandating the use of multi-factor authentication and training employees on relevant policies and procedures.

• **Incident response** — establishing a risk-assessed incident response protocol, complying with applicable reporting requirements, designating responsibilities for specific employees in the event of a cyber-related incident and testing the incident response protocol.

• **Resiliency** — keeping inventory of core business systems and processes, creating an operational resiliency strategy that assesses risk tolerance and contemplating other safeguards such as storing back-up data offline or on another network.

• **Vendor management** — establishing a vendor management program to ensure that security measures and other safeguards are followed, understanding the specific terms of any agreements with vendors and monitoring and testing the vendor relationship for potential issues.

• **Training and awareness** — training employees on cybersecurity policies and procedures, providing employees with specific examples and exercises during training and monitoring the effectiveness of training.
cybercrimes webinar | the latest legal developments

Suad Jacobs
25 November 2020
who is impacted by the Bill

- It impacts all of us who process data or use a computer
- People involved with IT (or data protection) regulatory compliance
- All Electronic Communications Service Providers (ECSPs)
- Financial institutions
- Representatives from various government departments
- Cybercriminals
- Vendors of software or hardware tools that could be used to commit cybercrime
- Information security experts
- Everyone who uses a computer or the internet
offences

- The Cybercrime Bill creates many new offences. Some are related to data, messages, computers, and networks
  - hacking
  - unlawful interception of data
  - ransomware
  - cyber forgery and uttering
  - cyber extortion
- Penalties include a fine, imprisonment, or both
- The Bill empowers law enforcement with extensive powers to investigate, search, access and seize just about anything (like a computer, database or network)
- To deal with cybercrime, the minister of police must establish and maintain:
  - a point of contact for cyber crimes
  - the capacity to detect, prevent and investigate cybercrimes
chapter 4 – duty to report

- Section 54 (1) of the Bill creates a duty to report for ECSPs and financial institutions
  - report offences to the police no later than 72 hours
  - preserve any information that relates to it
- If an ECSP or a financial institution does not report an incident it could be liable on conviction to a fine (maximum of R50 000)
- This Bill does not place a duty on ECSPs or financial institutions to
  - monitor the data they transmit or store on their systems, or
  - to actively look for situations that indicate unlawful activity
- The Bill empowers the President to enter into agreements with other states considering this is a global issue
cybercrimes webinar | data breach implications and how to mitigate your risks as a company

Nicole Gabryk
25 NOV 2020
security compromises POPIA

- Section 22 of POPIA imposes a mandatory security compromise notification obligation:

  “Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the responsible party must notify...”

- regulator & data subjects

- comprehensive notification

- quick turnaround
alleged criminal behaviour - “special personal information”

POPIA

Personal information concerning-

- The criminal behaviour of a data subject to the extent that such information relates to:
  - The alleged commission by a data subject of any offence;
  - Any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings
  - NB: obtain consent to process Special Personal Information, including biometric information, images, photos, fingerprints, CCTV footage and/or access points to premises for identification and criminal checks
Do document the processes and findings of the response team. These are useful in strengthening cyber security, in addressing regulatory and legal requirements, as well as managing the concerns of staff and customers.

Do take steps to prevent future attacks and consider using cyber-security specialists.

Do consider obtaining appropriate insurance cover to mitigate losses to your organisation following a cyber-event.

**TOP TIPS**

Don’t only react cyber events - plan for them in a comprehensive incident response plan to avoid panic, ensure effective crisis management and to mitigate losses.

Don’t become so preoccupied with the breach that you overlook the legal consequences, including mandatory breach notifications, and consider seeking help from specialist data-protection attorneys.
thank you for joining us

Africa’s largest law firm
ENSafrica.com