THE INSURANCE AND PENSIONS COMMISSION (IPEC)

Rethink Cyber Security: A Regulatory Perspective

Presenter Sibongile Siwela

What is cybersecurity?

The protection of internet connected systems, including hardware, software and data from cyber crime;

Why the need for a re-think of cybersecurity

- □ Innovative global technologies (e.g. mobile, digital, payment platforms) disrupting the traditional infrastructure of the insurance industry;

- ▪ Fast developments, accelerating rapidly, new business models to enable stronger customer-centric focus;

- ▪ New models driving growth expansively across geographical, operational and technical platforms to meet customer evolving needs;

- ▪ These will require new capabilities; governance and cyber risk, and a shift in oversight and responsibility across the corporate organisation.

Examples of recent major cyber incidents in the insurance industry

- A US health insurer suffered cyber attack in July 2016,
- compromising two separate data systems
- exposed the confidential information of 3.7 million customers and health care providers.
- Accessed both personal identifiable information (social security numbers, claims and health insurance information) and
- payment data, including cardholder names, card numbers and expiration dates.

Examples of recent major cyber incidents in the insurance industry

- In 2015, one insurer in the US experienced a cyber attack;
- compromised the addresses, employment information and income data of more than 78 million policyholders.

Examples of recent major cyber incidents in the insurance industry

- Another major US insurer announced a data breach of their IT systems in 2015;

- affecting 1.1 million members.
- Cyber attackers acquired the members' usernames to access personal information such as names, birth dates and email addresses;
- The insurer notified each member impacted by the breach, and offered free credit monitoring and identify theft protection.

CYBER CRIME IN ZIMBABWE

- In Zimbabwe, cyber crime is currently dealt with using the Constitution and Criminal Law (Codification and Reform) Act [*Chapter 9:23*];

- To regulate cyber space, the Government gazetted the **Cyber Security and Data Protection Bill** on 15 May 2020;
- The Bill seeks to:
  - Introduce general rules on the processing of personal data and outline the duties of data controllers and processors; and
  - Increase cybersecurity in order to build confidence and trust in the use of information and communication technologies in Zimbabwe.

Compliance Issues:

- Governments and regulatory bodies are driving cyber-related governance practices around the collection, storage and use of data;
- Compliance with data protection laws, pro-privacy bills, cybersecurity and information sharing will require significant investment;
- Insurers will need to adopt written cybersecurity policies and procedures on customer data privacy, service providers and network security;
- Non-compliance with cybersecurity laws attracting fines across different jurisdictions.

Rationale for Regulating Cyber Space

- Of particular concern to policymakers and enforcement authorities the world over are business practices that may contribute to security incidents;

- Given that the insurance industry is not immune from cyber crime, regulators across the globe are imposing business practice requirements intended to enhance cybersecurity for the protection of national cyber space and policyholder personal information;

- Regulators, however, need to avoid the enactment of conflicting requirements that might make compliance materially burdensome and complicated for entities;

Role of Insurance Industry Entities in Cyber Security……

- Periodic cybersecurity risk assessments to establish risks and vulnerabilities;
- These will inform the development and implementation of policies, procedures, and safeguards based on identified risks;
- Given this important role, insurers with multi-state operations need to be vigilant particularly in light of active state legislative and cybersecurity enforcement.

Role of Insurance Industry Entities in Cyber Security……

- **Develop, implement, and maintain comprehensive, risk-based information security programmes**:
  - Programmes must encompass administrative, technical, and physical safeguards to protect non-public policyholder personal information and the licensee's information systems.
  - Chosen safeguards should be commensurate with the size and complexity of the insurance business, as well as responsive to the risks identified during regular risk assessments.

Role of Insurance Industry Entities in Cyber Security….

- **Implement appropriate security measures**:
  - Appropriate security measures are encouraged to include:
    - Access limitations;
    - Multi-factor authentication;
    - Encryption of non-public information during transit and on portable devices,;
    - Intrusion detection mechanisms;
    - Audit trails;
    - Data retention and disposal practices; and
    - Disaster recovery and business continuity plans.

Role of Insurance Industry Entities in Cyber Security

- **Institute an incident response plan**:
  - Each licensee is encouraged to formulate **an incident response plan** designed to promptly respond to and mitigate any cybersecurity incidents.
  - Model response plans should ordinarily contain:
    - Specific plan requirements, such as internal response processes;
    - Clearly defined roles and decision-making processes;
    - Managed internal and external communications;
    - Incident documentation procedures, and mechanisms for post-incident revision and remediation.

Role of Insurance Industry Entities in Cyber Security

- **Report cybersecurity events**:
  - Regulated entities are encouraged to notify the Regulator 'cybersecurity events.'
  - An event must be reported even if it happens to any one of the insurer`s group entities domiciled offshore;
  - These include any compromise of non-public information and if it creates a reasonable likelihood of material harm to a consumer or business operations;
  - Reporting must occur within a reasonable timeframe after discovering the event;
  - Licensees must retain all records concerning a cyber event for a reasonable timeframe and must make those records available to the Commissioner upon request.

Role of Insurance Industry Entities in Cyber Security

- **Train employees**:
  - Each licensee is expected to provide security awareness training to all employees in addition to training its c-suite;
  - Licensees are also responsible for tracking legal and threat developments in the cybersecurity ecosystem and for upgrading their respective training programmes including security safeguards to reflect such developments;
  - Failure to develop and upgrade training programmes will result in security breaches thereby compromising policyholder and corporate information.

Role of Insurance Industry Entities in Cyber Security

- **Involve the board**:
  - Given that Boards of Directors are ultimately responsible for overseeing the ultimate information security programmes, licensees are encouraged to involve their boards.
  - The board must receive an annual report on the overall status of the security programme.

Role of Insurance Industry Entities in Cyber Security

- **Conduct planned security assessments:**
  - A key consideration for entities is periodic assessment of the effectiveness safeguards' key controls, systems, and procedures.'
- **Oversee vendors**:
  - Licensees must exercise due diligence by vetting vendors prior to on-boarding and contractually require vendors to implement appropriate safeguards to protect non-public consumer information and information systems;
  - Carry out an investigation to gather information in the cyber event occurring within a vendor's systems.

Conclusion

Key considerations in developing a Cybersecurity System:

- Weaknesses and sources of disruption in the operating model, particularly with respect to third parties?
- Risk appetite and risk culture needed to protect the corporate brand?
- Impact on organisation, including changes to behaviour and responsibilities of the C-suite?
- Compliance agenda and response to regulatory requirements? and
- Optimising a framework to respond to technological opportunities, risks and disruption to protect brand and reputation and enhance investor confidence and prepare insurers for the challenges of tomorrow.

Thank you