Innovation and Cybersecurity **Conference**

2018

28–30 August 2018

Coordinating efforts, **establishing response** structures, and **creating** regulatory certainty in a **disruptive environment** where **innovation** and cyber converge

South African Reserve Bank

Cyber Insurance

Cyber Risk and Insurance

Cyber

Cyber is a broad risk that organisations face by virtue of their reliance on information technology, connectivity and automated processes. In an increasingly punitive legal and regulatory environment, and with more frequent contractual requirements for cyber liability insurance, forward thinking companies are taking proactive steps to explore and transfer cyber risk.

Cyber Attacks

Cyber attacks can be defined as any attempt to damage, disrupt or gain unauthorized access to an electronic communications network, computer or computer system; including but not limited to Mobile banking exploitation, Network and online banking disruption, Social engineering, Malware and Ransomware attacks, Intentional acts committed by rogue employees, Securities and market trading manipulation, ATM skimming, Insider access

Cyber Insurance

Cyber Insurance is designed to cover any risk of financial loss, disruption or damage to the reputation of an organization from an intrusion into its technology systems.

South African Reserve Bank

Cyber as a balance sheet risk

Business Disruption

Financial statement impact of breaches shift to business disruption

- Denial of service & ransomware attacks can be more severe than data breaches
- 2017 WannaCry & NotPetya ransomware attacks resulted in extended business disruption

D&O Claims

D&O follow on claims represent an increasing exposure

- Wendy's derivative suit arising from a data security breach was settled for cybersecurity changes, corporate governance therapeutics, and $950,000 in plaintiffs' attorneys' fees (May 2018)
- Yahoo!'s breach-related securities class action claim settlement of $80M is the first substantial data breach-related shareholder lawsuit recovery (March 2018)
- Home Depot follow-on claim appeal settled for $1M+ corporate governance changes (May 2017)
- Pending Equifax follow-on directors and officers claim arising out of a network security breach
- Wyndham follow-on directors and officers claim: road map to effective litigation defenses

South African Reserve Bank

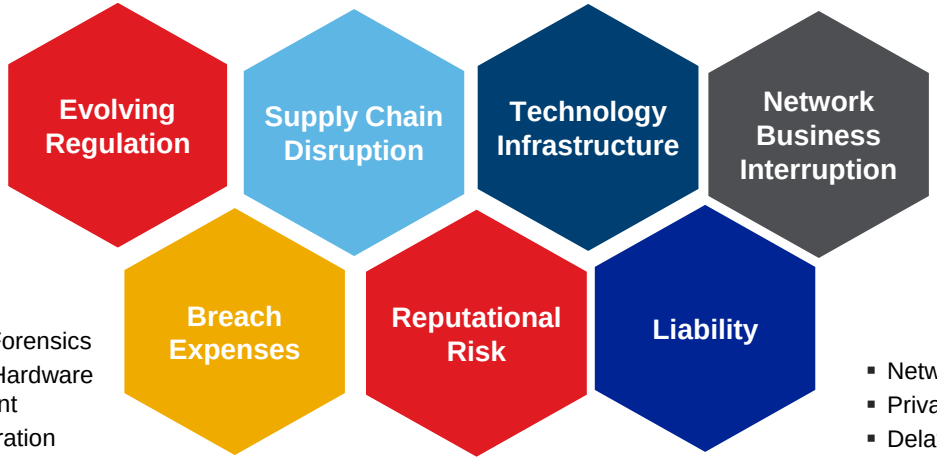
Cyber Risk Considerations – Q2 2018

- "Big data" as a liability
- Evolving Cybersecurity Requirements – NY Dept. of Financial Services
- EU General Data Protection Regulation effective May 25, 2018

- Dependent & Contingent Businesses
- Technology Dependencies

- Information Technology Platform
- IoT / Cloud / SaaS solutions
- Operational Technology

- Technology Failures
- Extended Outages caused by malicious code
- Logistics
- Net Income Loss + Extra Expense



- Computer Forensics
- Software / Hardware Replacement
- Data Restoration
- Notification / Credit Monitoring

- Customer Erosion
- Public Relations Costs

- Network Security Liability
- Privacy Liability
- Delay in Delivery
- Return or Offset in Fees
- Contractual Liability / Liquidated Damages

South African Reserve Bank

Common Gaps in Standard Policies

Property Insurance:

Malware and Denial-of-Service attacks do not constitute '**physical perils**' and do not damage '**tangible property**'

Malpractice/E&O/PI:

- Unauthorized access **exclusions**.

- Requires **negligence** in provision of defined business activities.

no cover for information
ner **regulatory actions**

Common Hurdles:

- Intentional acts and **insured vs. insured** issues.

-No coverage for **expensive crisis expenses** required by law or to protect **reputation.**

General Liability Insurance

CGL Privacy coverage limited to '**publication or utterance**' resulting in one of traditional privacy torts.

Crime Coverage

Crime policies require **intent… theft** of money, securities, or tangible property.

South African Reserve Bank

Silent Cyber

Silent CYBER

Products Liability

- Remote hacking of Jeep resulted in Chrysler recalling 1.4M vehicles
- Internet of Things ("IoT") creates additional products exposure

Casualty

- Zurich Insurance Co. v. Sony Corp. of America - ISO Exclusion – Access Or Disclosure of Confidential or Personal Information and Data-Related Liability
- AIG announces that they will affirmatively cover Cyber bodily injury subject to AP and additional underwriting

Property

- Potential overlap with Business Interruption ("BI"), Dependent BI and Data Restoration coverage
- FM Global Cyber solution – cutting back on capacity, AP
- Malware / DDOS attacks do not constitute "physical perils" and do not damage "tangible property"

Crime

- Social Engineering Losses – Cyber policies exclude loss of monies
- Crime policies require intent – theft of money, securities or tangible property

Kidnap & Ransom

- Cyber extortion claims filed under K&R policies → Guaranteed Cost, though scramble for access to experienced vendors
- As multi-year K&R policies expire, carriers are affirmatively excluding cyber

Directors & Officers

Home Depot data breach-related derivative lawsuit – settlement required HD to adopt certain cyber-security related corporate governance reforms (and pay up to $1.125M in plaintiff's attorneys' fees)
Equifax follow-on D&O claims arising out of a network security breach

Cyber Insurance Coverage

Policy Triggers

Cyber Policies are designed to cover first party and third party loss following from an actual or suspected **Breach of Personal and/or Corporate Information,** a **System (Operational) Failure** or a **Network Security Failure**

Breach of Information

Unauthorised disclosure or transmission of Personal and/or Corporate information for which the company is responsible either as a Data Processor or a Data Controller (Responsible Party / Data Custodian)

Operational Failure

Any negligent act or negligent failure by an employee whilst operating, maintaining or upgrading the computer system

South African Reserve Bank

Cyber Insurance Coverage

Network Security Failure

Any intrusion due to the failure of the security of the Company's Computer System, including that which results in or fails to mitigate any unauthorised access, unauthorised use, denial of service attack or denial of access or receipt or transmission of a malicious code, malicious software or virus which causes destruction, modification, corruption, damage or deletion of Third Party Data stored on the Company's Computer Systems

The disclosure of data:

- Due to the physical theft or loss of hardware
- By an employee

Theft of passwords or network access code from:

- The companies premises
- Company computer systems
- Any officer, director or employee of the company

South African Reserve Bank

Cyber Insurance Coverage

Company's Computer System

Any computer hardware, software or any components that are linked together through a network of two or more devices accessible through the internet or internal network or that are connected through data storage or other peripheral devices which are owned or operated by the company

Any third party computer or electronic device (including mobile phones, tablets or computers owned or controlled by an employee of the company) used to access the company's computer system or data contained therein

Any cloud service used by the bank (any on-demand access to hosted computer infrastructure or computing platforms, including cloud computing services provided on an Infrastructure as Services (Iaas) or Platform as a Services (Paas) model), provided by any natural person or entity not owned, operated or controlled by the company

South African Reserve Bank

Cyber Insurance – 1st Party Cover

First Response Costs

First Response Costs following an alleged or actual breach of information, security failure or operational failure:

Reasonable fees and expenses of a:

- Response Advisor for Legal Services,
- IT specialist in providing the First Response IT Services
- Crisis Consultant

In respect of an actual or suspected **Breach of Personal Information**, **Security Failure** or **System Failure.**

Such fees & expenses are only paid for a period of 72 hours from the initial report to the Response Advisor (by contacting the Emergency Number)

No excess applies to this insuring clause

South African Reserve Bank

Cyber Insurance – 1st Party Cover

Event Management Expenses

Event Management Expenses following an alleged or actual breach of information, security failure or system failure:

Reasonable fees, costs and expenses for:

Response advisor to provide **legal advice** in respect of the requirement to notify data subjects and/or relevant regulator

IT Specialist to investigate a security or system failure to establish:
Whether a failure has occurred, how it occurred and if it is still occurring
Identify whether the failure has resulted in a breach of information and the extent thereof
Containing the attack including a denial of service attack
Resolving a denial of service attack and removing any malicious software, code or virus from the system and identifying any compromised Data
Examining the system to determine the remedial actions required to comply with an enforcement notice

South African Reserve Bank

Cyber Insurance – 1st Party Cover

Event Management Expenses

Data restoration costs to determine if the data can or cannot be restored or recreated; and reload customise licenced software

Crisis consultant to mitigate or prevent the potential adverse effect, or reputational harm, of a newsworthy cyber event including the design and management of a communications strategy

Notification costs for preparation for and notification to data subjects and any regulator of a breach of personal and corporate information (POPI) including the costs of a call centre

Credit and ID monitoring including the costs of identity theft insurance (POPI)

Data Protection Obligations: (POPI)
Defence costs in respect of a regulatory investigation
Data protection fines that the company is legally liable to pay in respect of a regulatory investigation

South African Reserve Bank

Cyber Insurance – 1st Party Cover

Extortion Loss

The **Insurer** will pay all **Extortion Loss** that an **Insured** incurs solely as a result of an **Extortion Threat**

Extortion Loss means:

- **Ransom Monies**;
- Reasonable and necessary fees, costs and expenses of the **Cyber Extortion Advisor** to conduct an investigation to determine the cause of and to end an **Extortion Threat**

Network Interruption

Network business interruption: loss of income and extra expense due to network security failure

South African Reserve Bank

Cyber Insurance – 3rd Party Cover

Liability Coverage

Damages and defence costs from any claim made against the insured arising from an actual or alleged:

- Breach of personal and/or corporate information
- Security failure to guard against threats such as hackers, viruses, worms, trojan horses and denial of service attacks whether or not resulting from the provision of professional services
- Failure to notify a data subject and/or any regulator of a breach of information in line with the requirements of Data Protection Legislation
- Breach of duty in respect of the processing of personal and/or corporate information (Outsource Service Providers)
- Digital Medial Liability

South African Reserve Bank

Cyber Insurance – 1st Party Cover

OSP Extension

Reasonable fees, costs and expenses incurred by the insured for event management expenses in connection with a breach of personal information, corporate information, security failure or system failure including:

- Response advisor
- IT Specialists
- Data restoration costs
- Network business interruption: loss of income and extra expense due to network security failure

South African Reserve Bank

Cyber Insurance - Exclusions

Exclusions

- Anti-Trust
- Bodily injury and Property Damage
- Contractual Liability
- Conduct
- Intellectual Property:
- Licensing Fee:
- Prior Claims and Circumstances
- Securities Claims
- Terrorism/ War (with a carve-back for cyber terrorism)
- Monetary Value
- Over Redemption
- Uninsurable Loss: any matters which the Insurer is prohibited from paying by the law of this Policy or the jurisdiction where a Claim is made or where an Insured Event first arises.

South African Reserve Bank

Cyber Insurance - Exclusions

Exclusions

- Pollution
- Systems
- Failure to Put Right
- Rectifying Deficiencies
- Wrongful Collection
- Employment Practices Violation
- Insured’s Fees, Compensation or Costs of Providing Services
- Tax

South African Reserve Bank

Cyber Claims Process

Claims Process

Cyber policies are activated by dialling the toll-free number stated in the schedule of the policy.

Information to be provided when activating the hotline:

- Name of Insured
- Policy Number
- Brief details of the incident

What to expect once dialling the hotline:

- Immediate response within one hour from claims and breach counsel
- Expert IT Forensics: what's been affected and how can it be contained, repaired or resolved
- Payment of ransom if an extortion attack which cannot be resolved by forensics
- Expert legal advise and PR consultancy to contain reputational damage
- Costs of notifying data subjects who may be affected and credit & identity monitoring to prevent further losses
- Professional preparation for any investigation, insurable fines and penalties by a data protection regulator
- Defence costs and damages for and resultant liabilities
- Business Interruption claim calculated

South African Reserve Bank

AIG – Claim Example

12th February 2017

Buffalo Limited (Buffalo), a private bank in South Africa, servicing international clientele, was acquired by the globally renowned financial institution, Rhino Limited (Rhino) on the 1st January 2016. The integration was running smoothly when Rhino began receiving queries from clients who had received "spoof" phishing emails claiming to be from Rhino. Rhino began conducting a preliminary investigation into the incident. This revealed that three employees of Buffalo first clicked on a link contained in the phishing email on the 10th March 2016, thereby exposing their mailboxes to the perpetrators.

13th February 2017

It soon became apparent that the perpetrators obtained contact information for Buffalo's clients by gaining access to the three employees' inboxes and that it was them sending the "spoof" phishing emails.

These emails, like the one originally received by the employees, prompted the client to click on a false link where they were asked to provide login credentials. 93 of the 101 client who have reported receipt of this phishing e-mail were listed on a spreadsheet found in one of the employee's mail boxes. This spreadsheet was a master list of email addresses for approximately 21,000 clients.

South African Reserve Bank

AIG – Claim Example

14th February 2017

Rhino commenced a forensic analysis but before the day was out the CEO received an email from the perpetrators stating that Rhino needed to provide R50 million in cash within a week or they will release the personal details pf Buffalo's clients. Rhino's main payment system then goes offline.

15th February 2017

Business Interruption procedures commence but Rhino is overwhelmed with angry clients. Rhino begins remediation measures. News is provided that early forensic results indicate personal information has been taken by the perpetrators in relation to clients all over the world. An early notification goes out via email to warn 21,000 clients of the current phishing scam but it does not contain details about any potential breach of Rhino's systems or personal information.

20th February 2017

Forensics notify Rhino that an in depth analysis of data and duplication of records narrowed the compromised records to C.1200. In response to this Rhino pays the extortion payment. Within hours their payment system is back online. Rhino begins reviewing the jurisdictional notification requirements for the clients which have been affected and find that about half require mandatory notification of this loss. They begin providing notification to these clients.

South African Reserve Bank

AIG – Claim Example

10th March 2017

Media attention has begun to focus on this event as Rhino reaches out to clients who were impacted, the attention is negative and Rhino begins to get a lot of concerned calls from clients. Following this the Information Regulator contacts Rhino saying they would like to discuss this event with them as there appears to be a breach of the Protection of Personal Information Act.

20th June 2017

The company is ultimately fined by the Information Regulator and Rhino is worried the Regulator may take an interest in interviewing their CEO and CFO.

10th December 2017

Six months has passed since Rhino paid a significant fine to the Information Regulator. As a result of the breach and all the negative press, clients have been leaving the bank in droves and the share price has fallen by 30%. There are reports that shareholders are looking to bring a derivative action against the bank as they believe the Directors should have conducted better due diligence before purchasing Buffalo.

South African Reserve Bank

Q2 2018 EMEA Cyber Market Snapshot

Capacity is continuing to grow across geographies

- Over 75 unique insurers E&O / Cyber Liability capacity
- Capacity is available locally (primary and excess), London (primary and excess) and Bermuda (excess only, generally excess of $50M)
- Growing number of Insurers developing appetites for large, complex risks
- There is over $700M in theoretical capacity available in the E&O/Cyber market

Coverage continues to evolve and become more valuable for insureds

- Coverage breadth continues to expand
- Insurers continue to differentiate their offerings with new or enhanced coverage components
- Emphasis on pre-arranged vendors
- Broadening systems failure and contingent business interruption coverage solutions

Stronger Data is being gathered as more breaches are reported

- Increased ransomware activity and business interruption concerns
- Complexity of breaches has driven an increase in incident response expenses incurred by Insureds
- Claims and loss data has expanded coverage offerings and improved actuarial data for loss modelling purposes
- Increasingly punitive legal and regulatory environment

Q2 2018 EMEA Cyber Market Snapshot

Retentions are being reviewed since WannaCryb, NotPetya and Equifax Incidents

- Retentions of all levels are available in the market, but can vary greatly based on industry class, size and unique exposures
- Adjusting retentions can lead to increased coverage and/or pricing flexibility

Pricing trends are competitive, but increasing for some industries

- Average premium rates reflect a decline – however dependent on industry, claims history and scope of coverage
- Excess rate environment continues to be competitive
- Some Insureds have secured significant coverage improvements as a result of paying higher premiums

South African Reserve Bank

Q2 2018 South Africa Cyber Market Snapshot

Législation

- SA lags behind the USA, Europe and the UK from a legal perspective as we still await the enactment of the sanctions section of POPI
- Other applicable legislation incudes: Electronic Communications and Transactions Act, Consumer Protection Act, Promotion of Access to information, Draft Cyber Crimes & Cyber Securities Act, King 4 Report on Corporate Governance and so forth
- GDPR's affect on SA companies

Market Overview

- There are currently six local insurers in SA offering cyber insurance, namely AIG, Allianz, Camargue, Chubb, ITOO and SHA
- We can access local capacity of R850 million before approaching the Lloyd's markets
- Client's must complete a proposal form prior to obtaining a quotation
- Pricing is based on each individual clients business profile, revenue, number of records held, categories of records held, IT Security in place and IT governance

South African Reserve Bank

2018 Purchasing Trends by Industry

Limit increases at Renewal

- Companies in a number of industries, including financial institutions, hospitality, healthcare, retail, manufacturing, technology, media and transportation, are **seeking higher limits options**
- For other industries, many organisations are still evaluating the purchase of cyber insurance or use of their captive to provide cyber cover due to regulatory, contract, D&O, benchmarking / loss information and financial statement pressures, among other reasons

More new Buyers

- Manufacturing, critical infrastructure, pharmaceutical / life sciences, industrials & materials / automotive, public sector, energy / power and utilities, higher education, real estate / construction, agribusiness and transportation / logistics industries saw the biggest uptick in new cyber insurance purchases in 2018
- Major concern in these industries is business interruption loss and reliance on technology

Shifting focus on cyber risk exposures

- In prior years, organisations' primary cyber concern was related to privacy breaches
- In 2018, more clients across all industries have focused on business interruption coverage, including system failure cover, cyber extortion and digital asset restoration
- Cyber insurance cases where courts upheld denial of coverage demonstrate the critical importance of matching customized policy wording to specific insured cyber exposures

South African Reserve Bank

Contact Details

Kerry Curtin

Business Unit Manager & Cyber Champion
Aon South Africa (Pty) Limited – Financial Institutions Business Unit
+27 (0) 11 944 7838
kerry.curtin@aon.co.za

South African Reserve Bank