Part 1: An overview of cybercrime and legal perspective by Quintus van der Merwe of Shepstone & Wylie
A changing e-world
Everything is going digital:

# Telecommunications and informatics (telematics)
# Terminal & other electronic operating systems
# Electronic chart display and information system (ECDIS)
# Electronic data interchange
# GPS and automatic identification system (AIS)
# Access codes and electronic trading (MSC v. Glencore)
# Automated assets…drones, vehicles, ships, trains, plants, warehouses…
Glossary of Terms
http://cybercrime.org.za

Adware, Botnet, Cracking, Crimeware, Cyberbullying, Cyberstalking
Cyberterrorism, Data-Theft, DoS-Attack
Hacking, Hoax-Email, Identity-Theft, Keylogging,
Madware, Malware, Pharming, Phishing, Ransomware,
Scareware, Smishing, Social-Engineering,
Spam, Spyware, Trojan Virus, Vishing,
Website-Defacement, Worm
Targets

IF YOU USE COMPUTERS, YOU ARE A TARGET

Cybercrime broad categories:

• Ransomware / malware / spyware

• Loss of confidential information belonging to you, your employees, shareholders, funders, customers, suppliers or contractors

• Denial of service where you cannot operate because of the attack or diversion of assets

• “Viruses” resulting in business interruption and disruption
Cybercrime a Big Problem

• According to a 2016 survey by PWC, cybercrime is the second most reported type of economic crime and SA high on the list. [definition of cybercrime skews stats and many incidents are not reported]

• The global cost of cybercrime will reach over $1.5 trillion in profits in 2018 & estimated over 2 trillion $ by 2019 and more in the future...

• Of 383 organisations interviewed regarding data breaches in 2016, the average costs of such breach / attack was $4 Million.

• There was a 38% increase in cyber security incidents in 2016 compared to the previous year and figures for 2017 not good.

• Cost of security is huge!
# 2018 at a glance

<table>
<thead>
<tr>
<th>Crime</th>
<th>Annual Revenues</th>
</tr>
</thead>
<tbody>
<tr>
<td>Illegal online markets</td>
<td>$860 Billion</td>
</tr>
<tr>
<td>Trade secret, IP theft</td>
<td>$500 Billion</td>
</tr>
<tr>
<td>Data Trading</td>
<td>$160 Billion</td>
</tr>
<tr>
<td>Crime-ware/CaaS</td>
<td>$1.6 Billion</td>
</tr>
<tr>
<td>Ransomware</td>
<td>$1 Billion</td>
</tr>
</tbody>
</table>
Reasons

• Massive organised crime business

• 48% of security breaches are caused by acts of malicious intent. Human error and system failure account for the rest.

• For commercial reasons many losses are simply not reported.
Maersk - The Petya Cyber attack triggered a crash of Maersk Group’s IT Systems across the world began in Ukraine.

- Spyware
- Crash targeted a complete collapse of e-infrastructure.
- It was a ransom attack calling for payment in return for releasing system and files
- Cost a huge amount – said to possibly hit $300 million.
- Exceptionally sophisticated IT Systems with incredible security protocols allowing tracking of cargoes.
- Affected all business units, container shipping, port and tug ops, oil and gas, drilling services and oil tankers, port operations, APM Terminals
MSC vs Glencore International AG

• Electronic release system targeted – 69 shipments of cargo successfully delivered.
• 70th shipment the carrier sent pin codes against bills of Lading to Glencore’s agent
• 2 of the containers stolen
• MSC held liable for breach of contract, bailment and conversion
• The afore point’s train of causations not broke by cyberattack
• Risk of theft transferred to carrier
• Previous conduct did not give rise to estoppel
• New technologies give rise to new risks and you must provide for them contractually
“Sensitive personal information about nearly 1m people who pay traffic fines online in SA has been leaked publicly, an Australian cyber security researcher Troy Hunt has found. TimesLIVE says the data leak of 934 000 records contains identity numbers, e-mail addresses, full names and passwords. Hunt, along with Tefo Mohapi from iAfrikan, discovered that the 'data was backed up or posted publicly by one of the companies responsible for traffic fines online payments in SA'. The leak does not affect all licensed drivers; only those who have registered to pay traffic fines online using one or more of the sites that provide the service. People who have registered to pay traffic fines online were urged to change their passwords, says the news site. ‘This is yet another reminder of how far our data can spread without our knowledge. In this case, in particular, the presence of plain-text (unencrypted) passwords poses a serious risk because inevitably, those passwords will unlock many of the other accounts victims of the breach use. This one incident has likely already led to multiple other breaches of online accounts due to that reuse,’ said Hunt to iAfrikan. iAfrikan said it had alerted the Hawks and the Information Regulator about the leak.”
What we have seen

• Invoices cloned and beneficiaries altered
• Emails hacked – knowledge of sensitive transactions
• Shipment documents altered
• Banks, SARS, Telkom emails calling for information
• Somali pirates – citadel
• https://haveibeenpwned.com/
Problem Misunderstood

JWC International carried out a survey of high profile company security and IT Heads to determine understanding of the risk

1. What did the company understand about cyber security threats.
2. How would they manage the risk

- 67% Cybersecurity not a serious threat to their company
- 91% Indicated no formal training, knowledge or skills regarding cyber security
- 100% of IT confirmed no cyber security training for staff.
- 53% had a relevant IT Policy to avoid threat
Risks

- Systems crashing, being wiped clean or being incapacitated
- Loss of cargo or assets
- Assets or equipment damaged or destroyed
- Massive claims for business interruption
- Remedial costs can be enormous
Possible liability

• **Contractual:**
  – breach of confidentiality because of theft of confidential information
  – failure to perform because of denial of service attacks
  – becoming a gateway or conduit to cybercrime where your computer system is used to gain access to other people’s computers

• **Delictual:**
  – is there a duty of care in relation to cybercrime?
  – cybercrime is foreseeable, what kind of precautions do you have to take to avoid delictual liability?

• **Statutory:**
  - POPI or General Data Protection Regulation (GDPR)
Cybercrime and delict

• **Is it foreseeable?** - “Cyber crime, already a significant threat, has been described as a wave soon to become a tsunami, and the banks face the challenge of providing a secure platform that will counteract the activities of fraudsters, who seem always to be one step ahead of Joe Public”. Advocate John Myburgh, the chairperson of the board of the Ombudsman for Banking Services

• Delict - “The breach of a legal duty of care, which will ground an action for damages at the suit of any person to whom the duty was owed and who has suffered harm in consequence of the breach”
Cybercrime and contracts

- How to limit or exclude liability in your contracts:
- Draft your confidentiality obligations taking account of the precautions you take relating to cybercrime
- Consider expressly defining cybercrime as an impossibility event excusing non performance (“force majeure”)
- Limit or exclude your liability for cybercrime
- Obtain waivers in relation to claims relating to the information you obtain
- Deal with the precautions you take against cybercrime in relation to service standards and obtain an express agreement by the other party that they are satisfied with that those standards
Cybercrime and contracts

- Deal with responses to cybercrime, who you can and will tell about the attack and how you will deal with the attack
- In a service provider, subcontracting or agency context, set out what precautions you require the service provider/contractor/agent to take, when you can audit their systems (make sure that the audit right doesn’t shift responsibility for ensuring proper cybersecurity to you) and what liability you can pass on to them
- Insurance against cybercrime
- The cost of all these rights and precautions
- Cybercrime related rights cost allocations between the parties
Employment contracts

• The employee’s confidential information

• Potential claims by the employee and limits or exclusions of liability

• Standards applicable to cybercrime and how that impacts on the employee’s job
Cautionary note – the so called ticket cases

• The ticket case rules apply to standard form contracts e.g. tickets that you couldn’t reasonably expect to find the exemption or an exemption of that nature in the contract

• Even in contracts signed by the parties, unusually onerous clauses must be drawn to the attention of the other party if they are to be enforceable
End of Part 1:

"Don't believe everything you see online."
Part 2: Insurance perspective on Cyber Risk & Liability by Carolyn Roach of JLT South Africa
• Jardine Lloyd Thompson (JLT) is one of the world’s leading Global Specialty risk advisors and brokers, providing insurance, reinsurance and employee benefits related advice, brokerage and associated services.

The JLT group of companies was formed when Jardine Insurance Brokers, a company dating back to 1832, merged with Lloyd Thompson in 1997. Today, the JLT International Network comprises of owned, partly owned and non-owned broking and employee benefit consultancy operations in more than 135 countries worldwide.
JLT Group - Where we operate

JLT owns offices in 40 territories with over 10,000 colleagues, supported by the JLT International Network. This enables us to offer risk management and employee benefit solutions in over 135 countries around the world.
JLT South Africa (JLT SA) is a subsidiary of JLT plc, providing corporate and specialist insurance, reinsurance and employee benefits broking services, with offices in Johannesburg, Cape Town and Durban.

At JLT SA, we believe in going beyond the expected for our clients, and always putting our clients first.
Our Risk & Insurance division provides insurance and reinsurance broking and risk management services to clients within a wide range of business sectors.

Our sectors include:

- Aviation
- Communications, Technology & Media
- Construction
- Credit, Political & Security risks
- Financial Lines Group
- Agriculture
- General Property & Casualty
- Guarantees
- Marine Insurance
- Mining & Natural Resources
- Reinsurance
What is Cyber Risk

• Exposures emanating from computer network and the internet

• Business risks
  – Operational
  – Financial
  – Intellectual property
  – Reputational
  – Legal and regulatory

Cyber Insurance
Average Exposure by Country

<table>
<thead>
<tr>
<th>Country</th>
<th>Exposure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finland</td>
<td>2.3</td>
</tr>
<tr>
<td>France</td>
<td>1.5</td>
</tr>
<tr>
<td>South-Africa</td>
<td>1.8</td>
</tr>
<tr>
<td>Sweden</td>
<td>1.6</td>
</tr>
<tr>
<td>Germany</td>
<td>1.3</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>1.1</td>
</tr>
<tr>
<td>Indonesia</td>
<td>0.9</td>
</tr>
<tr>
<td>Malaysia</td>
<td>0.8</td>
</tr>
<tr>
<td>Singapore</td>
<td>0.7</td>
</tr>
<tr>
<td>Australia</td>
<td>0.6</td>
</tr>
<tr>
<td>Hong Kong</td>
<td>0.5</td>
</tr>
</tbody>
</table>

Results 2017

Exposure by Industry in South Africa

- Materials – 21.4%
- Financials – 18.7%
- Industrials – 17.9%
- Consumer Discretionary – 12.7%
- Consumer Staples – 11.5%
- Real Estate – 5.7%
- Information Technology – 5.3%
- Telecommunication Services – 2.7%
- Healthcare – 2.3%
- Energy – 1.5%
- Utilities – 0.3%
“Our general liability policy will cover the loss.”

“I am not a target for hackers.”

“We have top notch security in place.”

“We do not sell goods or services online so we are not exposed to cyber risk”
Biggest risks from a cyber incident

- Reputational
- Operational
- Relationship with suppliers/third parties
- Financial
- Future business prospects
**Financial Impact**

Cost of a data breach
- Average total cost $ 3.62m
- Average cost of lost/stolen record $141
- Organisations in South Africa are the most likely to experience a material data breach involving 10 000 or more records in the next 24 months

Regulatory Fines and Penalties
- POPI
- GDPR (General Data Protection Rules)

On average takes 191 days to identify breach 66 days to contain breach

Global average per record: **$141**
- Health Care Organizations: **$280**
- Financial Services: **$245**
- Research: **$101**
Cyber Risks

Principally 1st Party

- Denial of Service
- Fines & Penalties
- Hardware & Software failure

Principally 3rd Party

- Infringement of IP
- Transmission of Virus

Reputation

Security

Liability

Privacy

- Extortion
- Hacking
- Theft of IP

- Privacy Breach
- Loss of Data
1st Party Risk

• Hacking & Hacktivism
• Loss of Data
  - Causes
• Cyber Extortion
  - Many variations of the theme;
    o Threat of attack – denial of service
    o Data held hostage – network infected, encrypting data or blocking access
    o Threat of release of sensitive data
• Theft of Intellectual Property
  - Disgruntled employee
  - Occurrence of espionage
• Hardware & Software Failure
  - Unavailability of online trading
  - Loss of presence of the web
  - Loss of data
3rd Party Risk

- Transmission of computer virus
  - 25,000 new computer virus detected daily
  - Computer Virus is an exclusion under majority of standard Asset & General Liability insurance policies
- Disparagement, Plagiarism and Infringement
  - Breach of Copyright, Trademark, Trade Secret, Domain Name, Broadcasting rights
  - Libel and Slander
  - Defamation
- Breach of Privacy
Cyber Markets

- 6 local markets up to R700m capacity
- International market +25 Lloyds with $300-$350m capacity
Response Management

Incident

Breach Response Team

- Computer Forensics
- Public Relations
- Attorneys
- Credit Monitoring
Future of Cyber

• Bodily Injury and Property Damage
• Crypto currencies and Blockchain
Questions??
Whilst all reasonable care has been taken in the preparation of this presentation no liability is accepted under any circumstances by Jardine Lloyd Thompson for any loss or damage occurring as a result of reliance on any statement, opinion, or any error or omission contained herein. Any statement or opinion unless otherwise stated should not be construed as independent research and reflects our understanding of current or proposed legislation and regulation which may change without notice. The content of this document should not be regarded as specific advice in relation to the matters addressed.
Quintus van der Merwe | Partner

SHEPSTONE & WYLIE

Shipping & Logistics (including Customs @ Wylie)

24 Richefond Circle, Ridgeside Office Park, Umhlanga Rocks, 4319, South Africa

Direct Telephone: +27 (0) 31 575 7306

Mobile: +27 (0) 82 466 5062

E-Mail: qvdm@wylie.co.za

Other Offices: Johannesburg, Cape Town, Richards Bay & Pietermaritzburg

www.wylie.co.za