WEBINAR

Enemy at the Gates:
The practicalities and difficulties of data breaches
19 May 2022

CDH
CLIFFE DEKKER HOFMEYR

INCORPORATING
KIETI LAW LLP, KENYA

Cyanre™ the digital forensic lab

THE LEGALS – PRACTICALLY SPEAKING

CDH
CLIFFE DEKKER HOFMEYR
INCORPORATING
KIETI LAW LLP, KENYA

By Preeta Bhagattjee

WHAT HAPPENS IF THIS HAPPENS TO YOU?

MANAGING A DATA BREACH INCIDENT

CLIFFE DEKKER HOFMEYR

- Reporting obligations = POPIA, Cybercrimes Act, If paying a ransom
- Managing reputational risk
- Managing system and technology risks
- Ensuring business continuity
- Possible damages, costs, fines & penalties
- Need an effective risk mitigation plan

BEING PROPERLY PREPARED……

CLIFFE DEKKER HOFMEYR

- Effective Compliance Universe
- Policies and procedures
- Mature data processing compliance practices
  - Data breach response plans (incident management)
  - Data processing records
  - Data Minimisation
  - Effective Retention and Disposal Procedures
  - De-identification /anonymisation practices
  - Staff training and awareness
  - Third party management
- Managing via contracting
  - Operator Agreements
  - Data Sharing agreement
  - Cross border data transfer agreements
- Updating protocols in line with risks (POPIA sections 19.2 and 19.3 obligations)
- Don’t forget about the paper……..

REPORTING OBLIGATIONS UNDER POPIA

CLIFFE DEKKER HOFMEYR

- Trigger for reporting = a qualifying breach
- Responsible party reports – determine your role under POPIA; Operator must notify the responsible party immediately
- Reporting does not amount to non-compliance or a breach of the provisions of POPIA

SECTION 22 OF POPIA –

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—

- ***the Regulator; and***
- ***the data subject, unless the identity of such data subject cannot be established.***

UNPACKING POPIA NOTIFICATION FURTHER

CLIFFE DEKKER HOFMEYR

- Who to notify and why?

  INFORMATION REGULATOR + DATA SUBJECTS = COMPLIANT NOTIFICATION

- Identifying the impacted data subjects
- Timelines for notification

  “as soon as reasonably possible after the discovery of the compromise”

NOTIFICATION continued

CLIFFE DEKKER HOFMEYR

- How to make notification?
- What to disclose to data subjects?
  - Describe the possible consequences of the breach
  - Provide sufficient information to enable data subjects to take protective measures
- What happens if it’s a small or insignificant breach?
- Operator must notify the responsible party immediately

THIRD PARTY RISKS

CLIFFE DEKKER HOFMEYR

Third party access = unseen risks

who has access to your data, your systems, your premises,

document storage facilities, equipment?

- POPIA requires an operator agreement (confidentiality and safeguards)
- As a responsible party, this is the best legal mechanism to manage your risks, including in respect of damages or fines and penalties
- Responsible party-responsible party data processing agreements

Enemy at the Gates: The practicalities and difficulties of data breaches

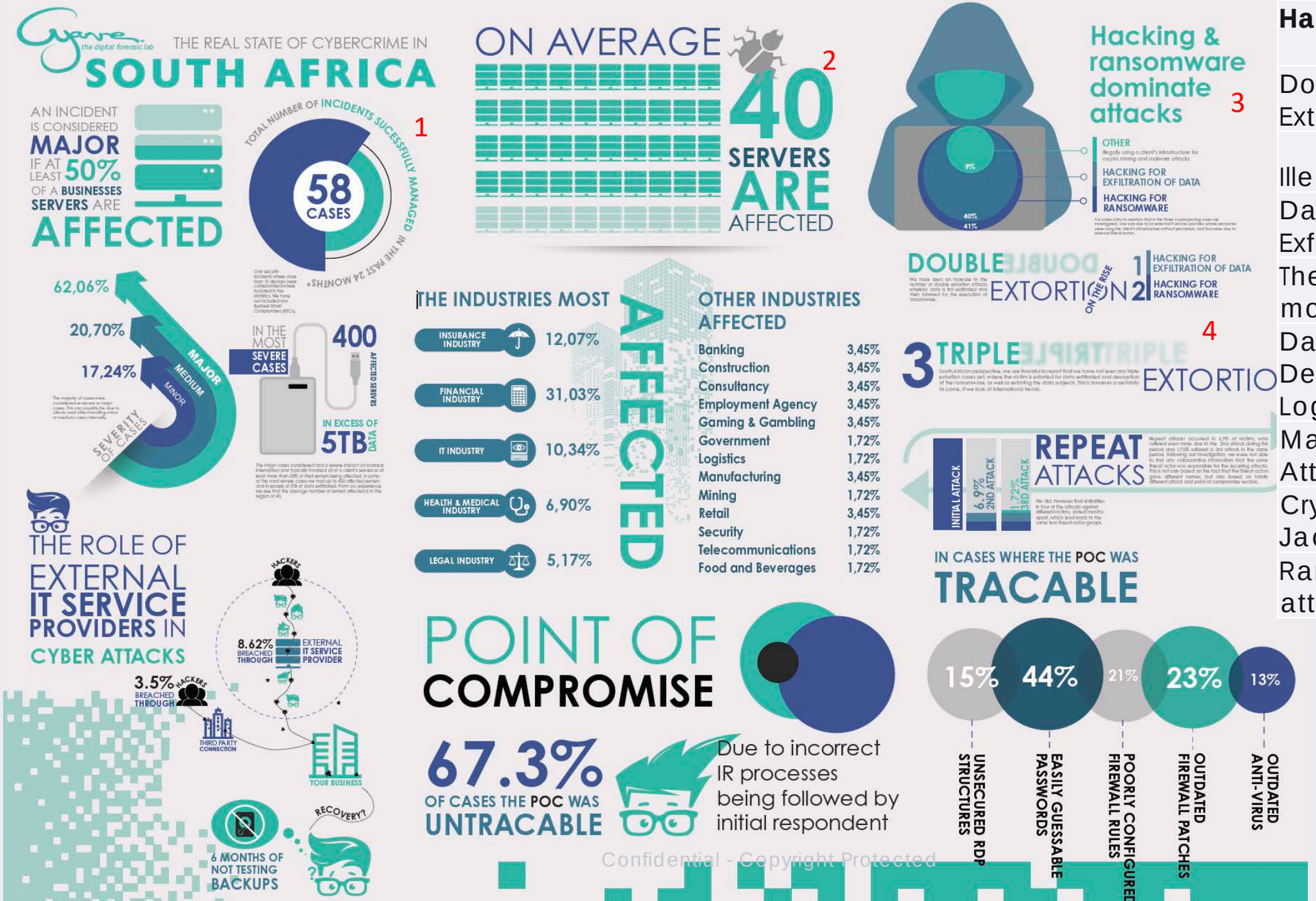
TOP CYBER THREATS IN SA

$300m

40%

41%

Double Extortion
Triple Extortion



Hacking Objectives	
Double Extortion	6,90%
Illegal Access	13,79%
Data Exfiltration	13,79%
Theft of money	6,90%
Data Destruction - Logic Bomb	3,45%
Malware Attack	8,62%
Crypto Jacking	5,17%
Ransomware attack	41,38%

HOW DOES THREAT ACTORS SELECT A TARGET

Gyanre™ the digital forensic lab

Drive by Shooting/ Shotgun Approach

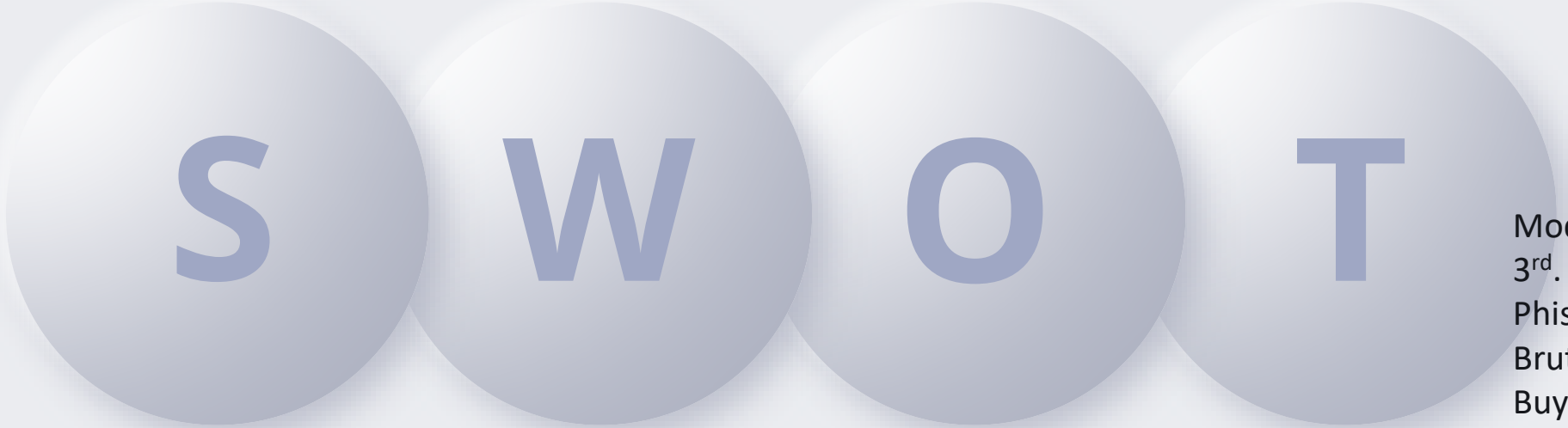
Targeted Attack- Big Game Hunting

Industrial Espionage

Retaliation/ Revenge

STRENGTH

OPPORTUNITY



WEAKNESS

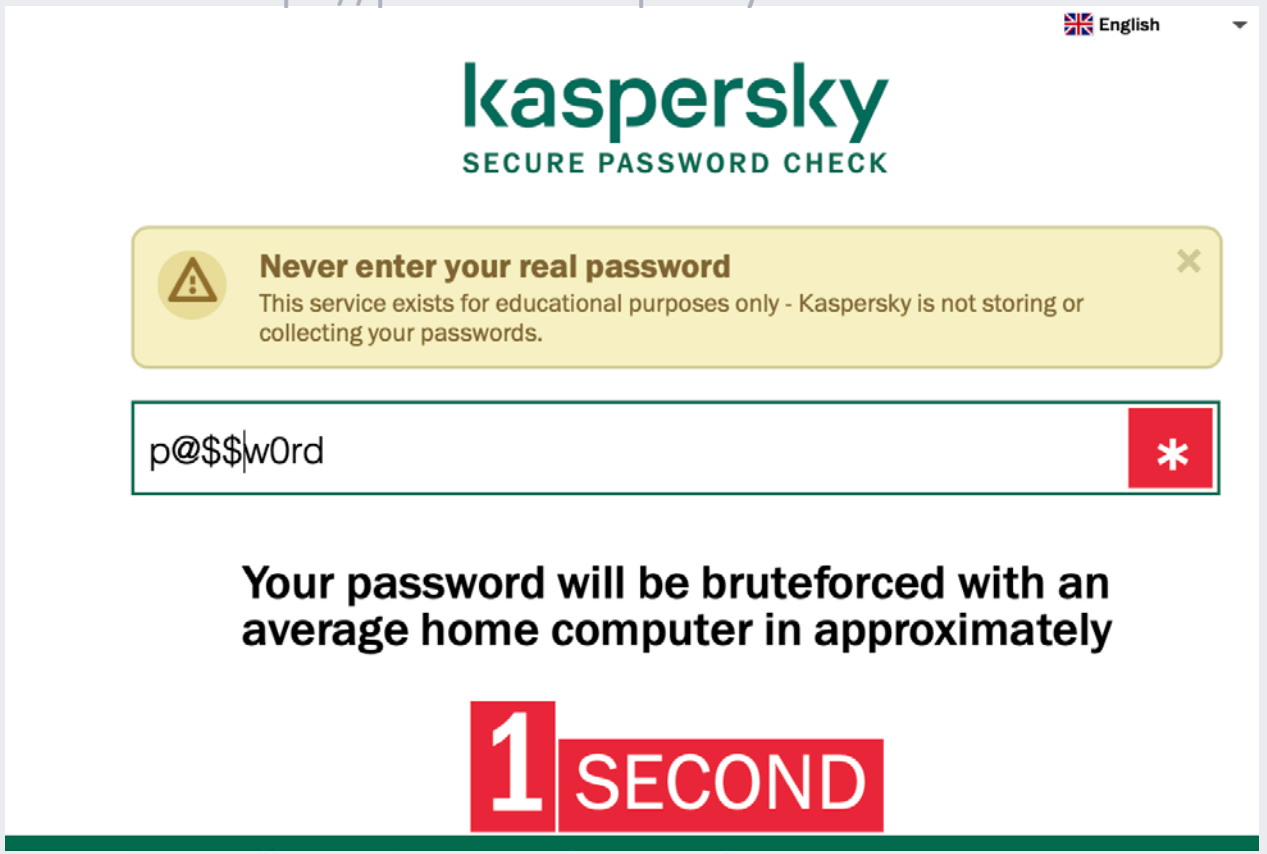
THREAT

Modus Operandi – POC
3rd. Party Breaches
Phishing
Brute force attacks
Buy Database - haveibeenpwaned
Unprotected mail/RDP
Known Vulnerability - outdated patch/ OS
Firewall Rules/open port
Passwords

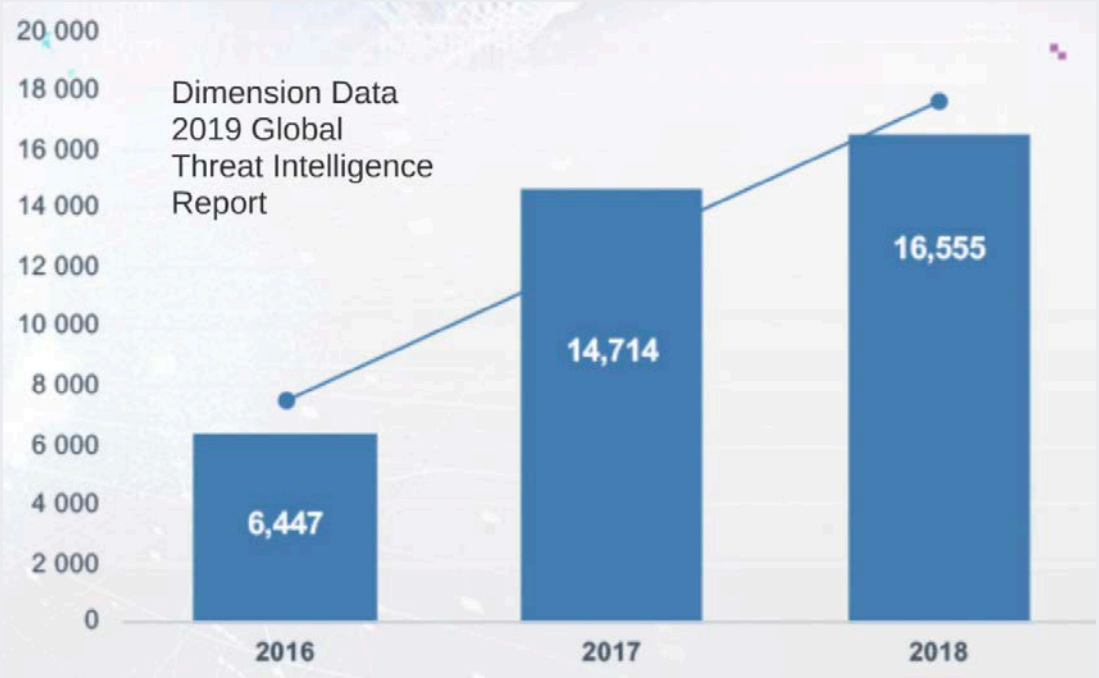
Password Problems

Rank	Password	Occurrences	% of Total	Rank	Password	Occurrences	% of Total
1	Password01	765	26.00%	26	Password15	7	0.24%
2	Client Name	120	4.08%	27	Password13	7	0.24%
3	Password02	54	1.84%	28	Password23	7	0.24%
4	Password03	39	1.33%	29	Password18	7	0.24%
5	Password06	26	0.88%	30	Password21	6	0.20%
6	Password04	24	0.82%	31	Password@01	6	0.20%
7	Password11	20	0.68%	32	Password44	6	0.20%
8	Password05	19	0.65%	33	Password16	6	0.20%
9	Password09	18	0.61%	34	Password30	6	0.20%
10	Password10	15	0.51%	35	Password27	6	0.20%
11	Password08	14	0.48%	36	Password012	5	0.17%
12	Password12	13	0.44%	37	Password55	5	0.17%
13	March2019	13	0.44%	38	Password2021	5	0.17%
14	Password14	13	0.44%	39	Password99	5	0.17%
15	Password22	12	0.41%	40	Gl0b@l	4	0.14%
16	Password1	11	0.37%	41	Password001	4	0.14%
17	April2019	11	0.37%	42	Password008	4	0.14%
18	Password07	11	0.37%	43	Password43	4	0.14%
19	Password20	10	0.34%	44	Password90	4	0.14%
20	Password19	9	0.31%	45	Password0000	4	0.14%
21	Password24	9	0.31%	46	Password33	4	0.14%

https://password.kaspersky.com



Security is not a priority



cident Response

Rapid Response

24/7 Level-4 Incident Response
Remote & Boots On–The–Ground Support
Initial Assessment
Cyber War Room

Containment

Stop the Spread
Limit Further Damage
Command & Control

Remediation

Restore or Rebuild Environment
Public Relations Services
Internet & Darkweb Monitoring
Data Subject Access Request
Notification Services

Eradication

Deploy Endpoint & Network Monitoring Tools
SOC Monitoring of Environment
Environment Foot-printing
Penetration Testing
Eradicate Hacker/Malware

Ransom Process

Negotiation with Threat Actors
OFAC Clearance Process
Ransom Payment

Deep-Dive Forensics

Triage Collection of Devices & Logs
Timeline Analysis
Expert Forensic Report

Stats on Ransom

35% of South African respondents paid the ransom, yet **43%** of those who paid failed to recover their data. *

Average ransomware attack costs a South African company over R6.4 million**
Average Data breach R46m***

More than 40% of victims of ransomware attacks in South Africa pay the cybercriminals***

Average time to discover a breach 279 days****

Average duration to contain a Breach – 56 days**** average downtime - 11days*
BI = 6.-47****
Days

*Mimecast – The state of email security 2022
**The State of Ransomware 2021
***Kaspersky
****IBM – Cost of a data breach report 2020/1
.SwissRe 2021)

How a Ransomware Negotiation plays out

Do not negotiate with Criminals
You are supporting and encouraging Crime

Situation to consider
Ransom payment

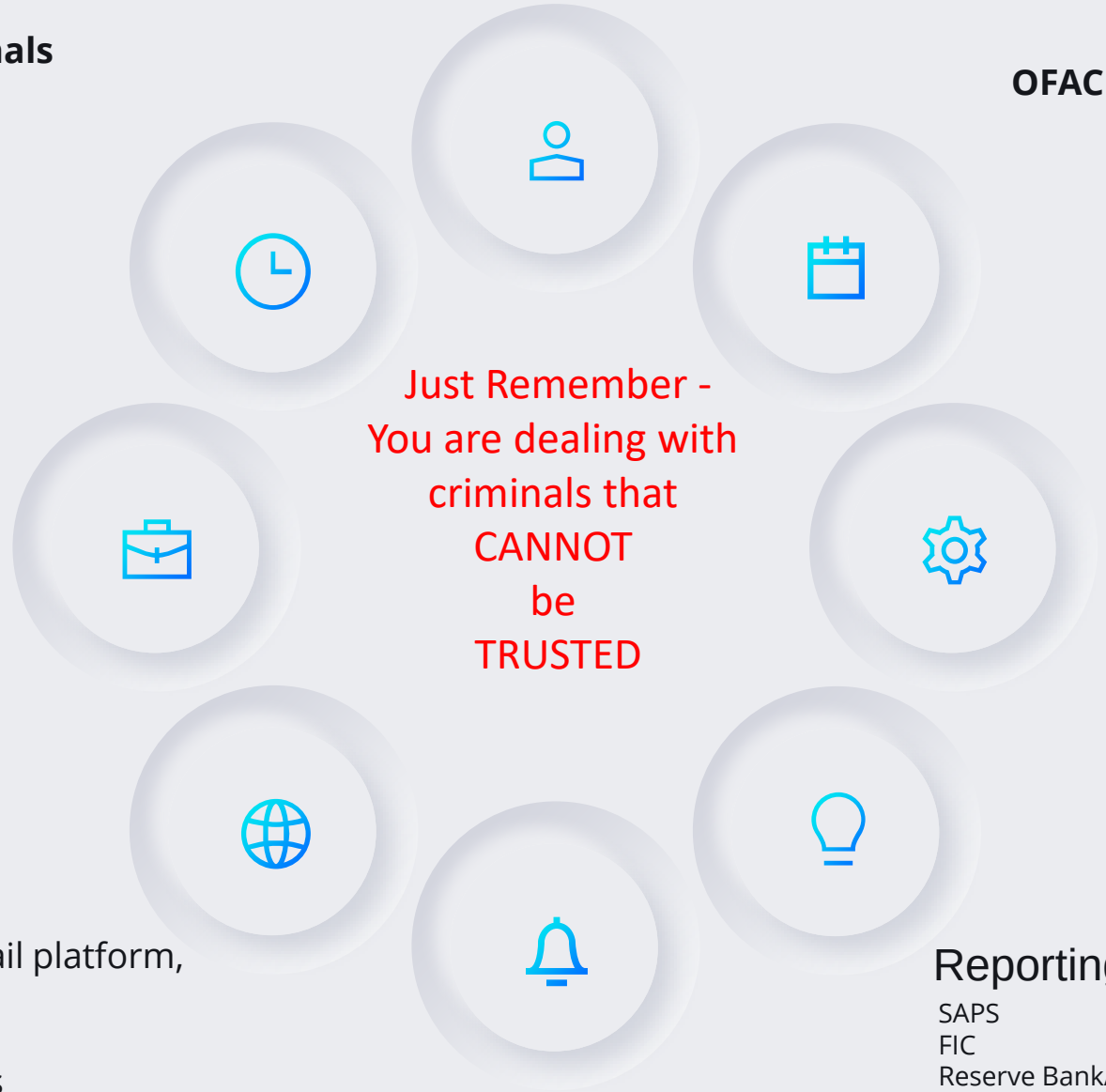
- Exfiltration of Data
- Encrypted Data –

what is your objective

Is it Legal ?

Intelligence Investigation

- Analise malware
- Research Darkweb
- Previous Victims
- Analise Ransom note, email platform, Darkweb publishing
- Crypto Wallet
- POC, Methodology, Scripts



Just Remember -
You are dealing with criminals that
CANNOT
be
TRUSTED

OFAC Clearance Process

Negotiation Process

3rd party mail account
Establish Trust
Two-edged sword
Act on behalf of management
What is objective – time or cost
Max Discount
Agree on Currency
Spell out payment process – Clarity
Spell out decryption process
Require Report
Require Support

Crypto Process

Act as Agent or self
Transfer of FIAT into Crypto Exchange - time
Procurement of Crypto – fluctuation
Test transfer – transfer fees
Segmented Payments vs Single Payment vs Multiple/single keys
Confirmation Process
Audit transaction

Reporting

SAPS
FIC
Reserve Bank/Treasury
Regulatory Bodies
Information Regulator
DSAR

Why is data the new oil?

- Data Enrichment
- Identity Theft
- Social Engineering
- Phishing Attacks
- Big Game Hunting
- BEC

Our data is out in the Wild – how do we live with it?

- Check for updates from the company
- Watch your accounts, check your credit reports
- Consider identity theft protection services
- Freeze your credit
- Find out what was Compromised
- Change your password for the compromised site.
- Change your security questions
- Find out what support the Responsible party will provide
- Consider your rights and legal recourse
- Dont use the same password everywhere
- Do not disclose personal information such as passwords and PINs when asked to do so by anyone
- Change your password and change it regularly and never share it with anyone else.
- Verify all requests for personal information and only provide it when there is a legitimate reason to do so.
- Do not use the information that may have been compromised. Rather use other personal information that you have not used previously to confirm your identity in future.
- 2FA

CLIFFE DEKKER HOFMEYR

ENEMY AT THE GATES

A discussion regarding the legalities surrounding ransom payments, as well as potential damages claims

Tim Smit – Director – Dispute Resolution

CDH
CLIFFE DEKKER HOFMEYR

INCORPORATING
KIETI LAW LLP, KENYA

A demonstrative scenario –

- Your company manages the investments of high net value individuals.
- Your service provider (providing data hosting and cloud services) suffers a system breach and your client's information is now the subject of a ransomware attack.
- The hackers demand payment of 100 bitcoin for the decryption of the data and its deletion from their systems.

Is it legal to pay a ransom in South Africa?

CLIFFE DEKKER HOFMEYR

- The crime committed by the hackers in demanding payment of the ransom is one of extortion.
- **Extortion** is defined as "*a person unlawfully and intentionally obtaining some advantage* (in this case the payment of money) *from another by subjecting them to pressure which induces them to submit to the demands*".
- In South Africa, there is no legal principle which makes the payment of a ransom illegal, but that does not mean that the party in respect of which a ransom demand is made can abdicate its responsibilities and not properly consider the facts surrounding the demand that has been made.

Reporting obligations:

CLIFFE DEKKER HOFMEYR

- Section 34(1)(b) of the Prevention and Combatting of Corrupt Activities Act.
- Section 7(1)(b) of the Prevention of Organised Crime Act.
- Section 29 of Financial Intelligence Centre Act.
- Section 34 of the Prevention and Combatting of Corrupt Activities Act.
- Section 54 of the Cybercrimes Act.

Damages claims:

CLIFFE DEKKER HOFMEYR

Section 99(1) of POPI provides that any data subject may or, at the request of the data subject, the Information Regulator may, institute a civil action for damages against a responsible party, which fails to adhere to the provisions of POPI as referred to in section 73, whether or not there is intent or negligence on the part of the responsible party.

As such POPIA imposes **strict liability** (negligence or intent are not requirements) on a responsible party, but only to the extent that there has been a breach of –

- the conditions for lawful processing of personal information;
- sections 22, 54, 69, 70, 71 or 72; or
- the code of conduct issued in terms of section 60.

Damages claims continued…

CLIFFE DEKKER HOFMEYR

- The quantification of any claim will be limited to what is "*just and equitable*" and each case will have to be determined by the courts on its own merits having regard to the facts and circumstances in each specific case.
- A data subject is not limited to a claim in terms of section 99 of POPI, but may have a claim against the company in terms of the contract that was concluded with the company or a claim in delict.

Other important considerations:

CLIFFE DEKKER HOFMEYR

- The company itself may have an indemnity claim against the operator in terms of –
  - its contract with the operator; or
  - in delict,

  in circumstances where the company (as the responsible party) has suffered damages as a result of acts or omissions of the operator.

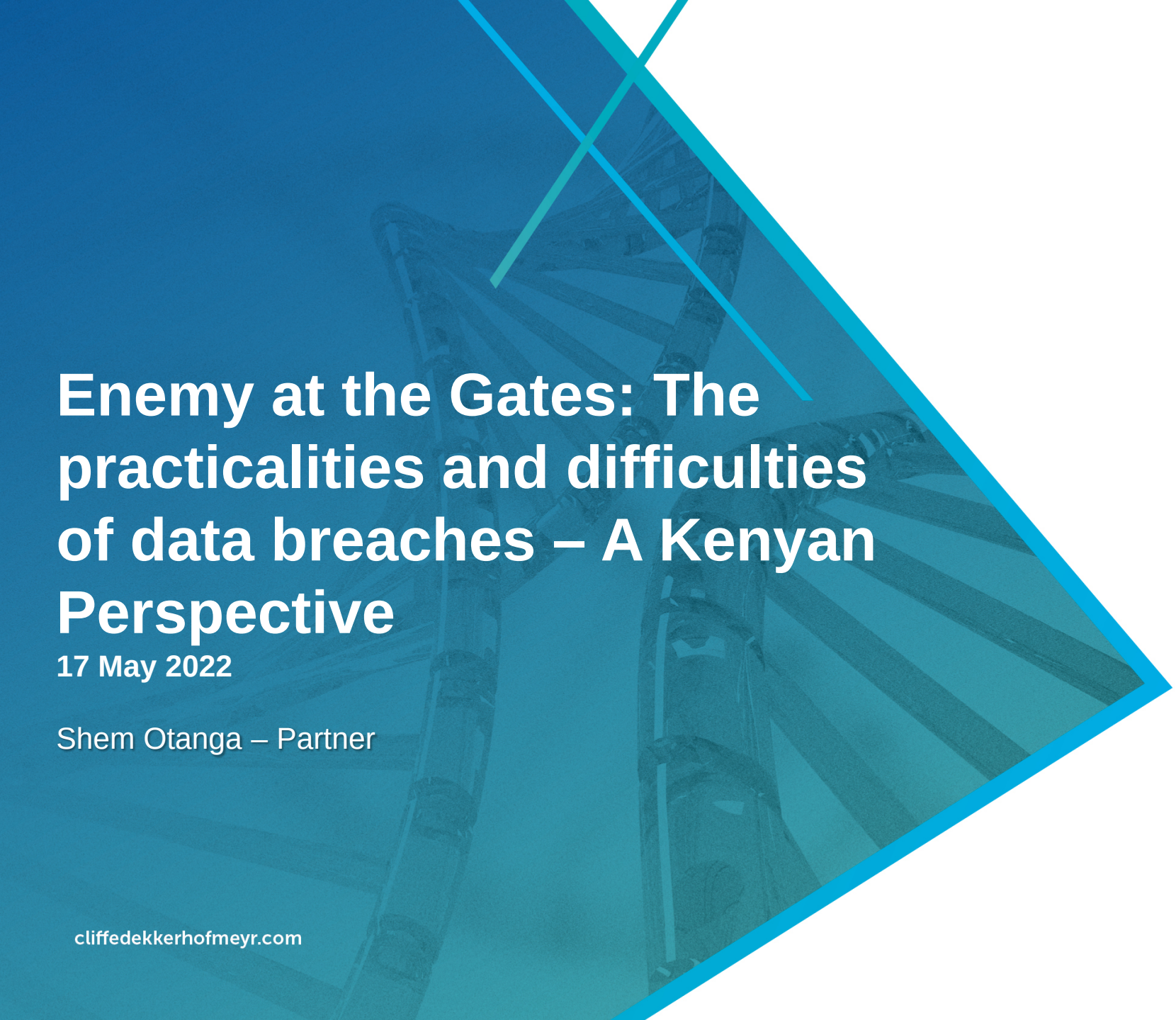
- Where a cyber risk policy is in place, the policy, its terms and its coverage must be understood and the company must ensure that it does not take any steps that might compromise any claim that the insurer might have (such as paying a ransom amount) if the policy responds to the claim, as such a compromise could result in a rejection of the claim by the insurer.

CLIFFE DEKKER HOFMEYR

Enemy at the Gates: The practicalities and difficulties of data breaches – A Kenyan Perspective

17 May 2022

Shem Otanga – Partner



cliffedekkerhofmeyr.com

CDH

CLIFFE DEKKER HOFMEYR

INCORPORATING
KIETI LAW LLP, KENYA

Summary of the Kenyan Legal Position

CLIFFE DEKKER HOFMEYR

Personal data breach

Section 2 - Data Protection Act, 2019 (the "**DPA**") defines "*personal data breach*" as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Breach Notification Criteria

- Unauthorised access or acquisition of personal data; **and**
- A consequential *real risk of harm* to the data subject.

Summary of the Kenyan Legal Position

CLIFFE DEKKER HOFMEYR

Real Risk of Harm (Regulation 37, Data Protection (General) Regulations)

A real risk of harm is deemed to arise where the breach relates to:

- the data subject's **full name or ID number** *and* any of a number of prescribed personal data types/classes including:
    - salary;
    - credit card information;
    - bank account number;
    - creditworthiness;
    - healthcare relating to STDs, mental health, substance abuse or addiction; *or*
- the following personal data relating to a data subject's account with a data controller or data processor—
    - the data subject's **account identifier**, such as an account name or number; and
    - any **password, security code, access code**, response to a security question, biometric data or other data that is used or required to allow access to or use of the individual's account.

Data Breach Obligations

CLIFFE DEKKER HOFMEYR

Data Controller

- Notify ***Data Commissioner without delay within 72 hours*** of becoming aware of the breach (and in default reasons for a delayed notification must be provided).

- Notify the ***data subject in writing within a reasonably practical period***:

    - save where:

        - the data subject's identity cannot be established; or
        - appropriate security safeguards have been implemented e.g., encryption of the affected data. or

    - subject to the need to delay or restrict such notice as necessary and proportionate for purposes of prevention detection or investigation of an offence.

- Record the facts relating to the breach, its effects and the remedial action taken.

Data Processor - Notify ***data controller without delay and where reasonably practicable within 48 hours*** of becoming aware of the breach.

CLIFFE DEKKER HOFMEYR

INCORPORATING
KIETI LAW LLP, KENYA

Practicalities and Difficulties of Data Breaches

- **High count of cyber attack incidents** - 79,175,429 overall cyber attacks attempted between the period of January to March 2022 (KE CIRT).
- **Limited capacity for enforcement** especially in view of the sheer number of cyber incidents and the common involvement of foreign actors/perpetrators.
- **Increasing levels of sophistication** and rapidly evolving cyber crime tactics. No-one is 100 immune. Kenya Revenue Authority Account Breach - USD 39M accessed and transferred.
- **Borderless Complexion of CyberCrime** - WannaCry Ransomware led to an estimated total of USD 4 billion in losses globally. At least 19 Kenyan institutions, including banks, were targeted in the large-scale attack against computers worldwide.

Practicalities and Difficulties of Data Breaches

CLIFFE DEKKER HOFMEYR

INCORPORATING
KIETI LAW LLP, KENYA

- Paying the ransom does not guarantee the return of breached data. In the WannaCry ransomware attack for example, it emerged that the hackers had no capacity to determine the computers that were linked with the payments they received so the return of data was a practical impossibility.
- The Computer Misuse and Cybercrimes Act (**CMCA**) creates several offences including unauthorized access to a computer system and computer fraud (including through use of ransomware). **Various penalties** are provided for the various offences under the CMCA in the form of from jail terms (the highest of which is life imprisonment) and/or fines of up to KES 25 million (USD approximately USD 200,000). It is silent on lawfulness of paying ransoms.
- Breaches can still occur in traditional ways - Radisson Blu Guest List.

COPYRIGHT

CLIFFE DEKKER HOFMEYR

INCORPORATING
KIETI LAW LLP, KENYA