Landscape – Ransomware on the rise

85% ↑

INCREASE IN VICTIMS COMPARED TO 2020

144% ↑

AVERAGE DEMAND IN 2021

78% ↑

AVERAGE PAYMENT IN 2021

On average, we calculated that actual payments ended up being **42.87%** OF THE INITIAL RANSOM AMOUNT

85% ↑

IN PUBLICLY POSTING VICTIMS ON LEAK SITES COMPARED TO 2020

Victim shaming is on the rise

Ransomware-as-a-Service is quickly lowering the technical bar

Attackers are making increasing use of zero-days

2021

R35,415,195.84

R8,656,152.96

█ Average Ransom Demand   █ Average Ransom Paid

* Based on 1 USD = 16 ZAR

Unit 42 Ransomware Threat Report 2022

2014: Dragonfly attack on pharma suppliers

In September 2014, it emerged that a cyber-espionage campaign had turned its focus to the pharma industry.

2017: NotPetya attack on Merck

One of the most devastating cyberattacks in history, the NotPetya attack was first and foremost a Russian attack against Ukraine. However, it affected hundreds of companies as a form of 'collateral damage'.

2020: Attacks on Pfizer/BioNTech and AstraZeneca

Dr Reddy's data breach wasn't the only attack on a vaccine maker. In December 2020, the European Medicines Agency (EMA) announced that it had been subject to a cyber attack. During the breach, some documents relating to the Pfizer/BioNTech vaccine had been unlawfully accessed.
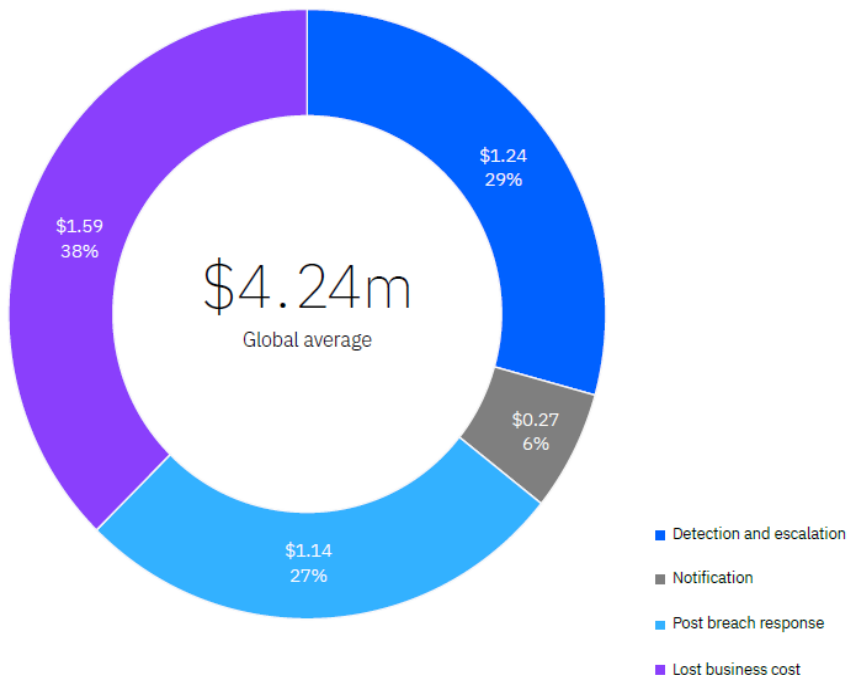
Over 3.6m records exposed in Dis-Chem cyber attack

TransUnion cyber attack – hackers demand R225 million ransom

Staff Writer   18 March 2022

Average total cost of a data breach divided into four categories

Measured in US$ millions

- $1.24 — 29% (Detection and escalation)
- $0.27 — 6% (Notification)
- $1.14 — 27% (Post breach response)
- $1.59 — 38% (Lost business cost)

$4.24m — Global average

Legend:
- Detection and escalation
- Notification
- Post breach response
- Lost business cost

Healthcare remains the **#1 attacked industry** and one of the least prepared to deal with a breach

Average cost of a breach in SA – **US$ 3,21m** up from **US$ 2.14m***

Most common type of record compromised – **Customer PII 44%***
Average duration to detect and contain – **287 days***
Average loss of business accounts for – **38% of total cost***

75% of companies were hurt by a ransomware attack, up from 61%**

When faced with a ransomware attack, **64%** of companies **paid the ransom**, yet nearly **4 out of 10** of them failed to recover their data.**

89% of healthcare organizations have experienced a data breach involving loss of or theft of patient data.

*IBM – Cost of a data breach report 2021

** Mimecast – State of email security 2022

BYOD

Passwords

Wi-Fi hotspots

Think before you click

Antivirus

Default passwords

Remote wipe

Cloud storage

USB charging

Updates and patches

Geo tagging

Cyber insurance

WHAT DOES IT COVER

Incident Response

- Incident triage
- Data and system recovery
- Forensic investigations
- Legal guidance
- Crisis management
- Notification costs
- Remediation services
- Cyber extortion

Financial Impact

- Business interruption
- Increased cost of working
- Fines and penalties

Liability

- Defence and settlement
  - Compromised data
  - Environment used to cause damage to others
- Digital media liability

Cyber insurance – Broader than you'd think

- Network security breach
- Privacy breach

- Includes:
- Corporate espionage
- Cyber extortion
- Denial of service
- Downstream attack (your environment damaging others)
- Hacking
- Insider and privilege misuse (internal and service provider)
- Malware
- Physical theft and loss (devices and hard copy data)
- Threats posed by a 3rd party access or usage of 3rd party systems

Closing Thoughts

Cyber crime is on the RISE and SA is not immune

POPIA and GDPR

Hacking is INDISCRIMINATE

No security is INFALLIBLE

Disgruntled STAFF and accidents can trigger an incident

Can't pass the buck, you remain the DATA CUSTODIAN

DAMAGES can be significant, directors are exposed

Effective INCIDENT RESPONSE is key

THANKS!

Any questions?

musawenkosik@itoo.co.za

011 351 5378