~~ZL Nghondzweni - 45463~~

24 / Feb / 2026

- Executive Communication Team
→ CHANNEL SELECTION UNIT

- Phone Call channel, medium rich. According to the Daft & Lengel theory, phone calls are High Urgency and low Equivocality.

- CIO should've called CEO NOMSA to explain matter at hand in detail and emphasize on urgency. This will help Nomsa gain clarity, considering she has no background in IT. If a leaner channel had been chosen instead, same thing would've happened, ~~the~~ Delayed maintainance, public backlash, share price drops and etc.

03:47 - Breach detected
04:15 - Breach Confirmed
~~05:30 - CIO emails the CEO~~
~~06:15 - CEO reads the email~~
~~08:00 - PA tries to reach the CIO~~
~~10:30 - No response from leadership~~
05:30 - CIO calls CEO
05:35 - CEO call technical group
05:40 - Technical group

File Edit Format View Help

What happend

The attackers gained accesss to the central customer database by exploiting vulnarability in the online payment portal 11 days before the detection of the attack and 2.3 million customer records were compromised,which inlclude : Full names,ID numbers,email addresses,phone numbers and banking details.

What it means for the business(Impact)

Customers and investors lost trust in the company,thus this lead to the Share price dropping by 8% when the JSE opened,the Customer loyalty programme relaunch that was supposed to take place at March was also compromised.

What the board must decide (action).

First step is to allocate the budget to rectify the vulnerability in the online payment portal which was neglected 4 months back due to budget constraints,second step is to publish a public apology to the investors and customers to regain their trust.

Decision

Authorize the Immidiete execution of the Ter 1 Data Breach response plan, Including ~~mitigate~~ medatory Information regulator and direct-to-Customer disclose of Compromised banking details

Information needed to make decision
The Ceo requires the following information to make decision
1. The total impact of data Compromised which is 2,3 million Customer records, Banking details

2. ~~R~~ legal & Regulatory obligation (POPIA)
- Mandatory Reporting : Under the protection of personal Information Act (POPIA), RetailCo is legally required to notify the Information regulatory as soon as possible
- Customers Protection : Provide Credit monitoring Services or fraud alert for high risk Customers
- Duration : The ~~breach~~ went ~~undetected~~ detected for ~~11~~ days, 1

- Internal Reporting : Brief Store managers across all 340 Stores to handle Inevitable in-person Customer inquires.

1
At 02:47 IT security team leader Botha receives the alert on his phone.
At 06:13 The CEO was alerted by ~~on~~ via email that there was breach detected.
At 11:15 The post goes viral in social platforms like on Reddit facebook, and Whatsapp groups

Question Anticipation Unit

* > What kind of customer data was leaked?
- ID numbers, names and banking details
= Personal details like ID numbers, banking details and address of 2.3 Million customers.
> What is the scope of this breach?

✓ > How much money was lost because of this breach?
⇒ We lost about 8% in less than an hour

✓ > How much money will be needed to recover from this attacker?
—

✓ > What's plan to fix this breach?
- We will compensate all our customers with loyalty rewards, deploy IT response team to deal with ~~technical~~ technical matters ~~for~~ of the crisis

* > What ~~did~~ was done when we realised that there was a breach?
⇒ The CEO was informed CIO but did not clearify ~~the~~ the ~~mail~~ email

* > How long ~~is~~ it will take to fix this crisis
- We are not sure as we haven't received a report from the forensic about the severity of the breach

Confidence Framing Unit.

Panic:

On Monday 24th at 02:47, our systems detected a data breach and by 04:15 our IT Security team comprised the breach. It was found that attackers had exploited a vulnerability in our online payment portal to access our central customers database. Several data like names, emails, phone number etc, was found to be compromised

Control

~~We~~ there has been a data leak and 2.3 millions record were exposed. Our IT Security teams working on the matter and trying to patch the vulnerability exploited in our system. We will make sure to notify all customers who's data was breached along with tips on how they can go about protected protecting, making sure this breach does not negatively appects them. Sorry for the Incovience and thank you for yor patience.