Failure Analysis Unit

This is exactly what failed in the IT email.

1. Plain language

The email used complex technical language like 'SQL Injection vector exploit'. But the CEO is not a technologist so the message should have been simplified into clear, everyday business language

2. Function of communication

The email explained what happened but did not clearly state what the CEO needed to do. This message failed to give clear instructions, communication must guide action

3. Form of communication

Email is a digital form of communication, doesnt allow instant feedback. A richer form like phone call or face to face meeting would have been more effective in this situation

4. Mismatch between form and urgency

The chosen form (email) did not match the seriousness of the breach. Crisis situations require fast communication.

5. Internal communication

The email was not structured strategically, internal crisis communication should align leadership quickly & clearly. It did not help leadership understand severity or next steps.

Rewrite Unit

From: Pieter van der Merwe (CIO)
TO: Nomsa Dlamini (CEO)
CC: None
Subject: URGENT - System Breach Alert
Date: Monday 24 February, 05:30

Nomsa,

We have confirmed that hackers have accessed th our customer database through a weakness in our online payment system. About 2.3 million records were stolen including some banking details. The attackers used the access for roughly about 11 Days. We need to take action as soon as possible. We need to inform the Head of Corporate Communication, contain the system and prepare a public and customer statement.

Regards
Pieter.

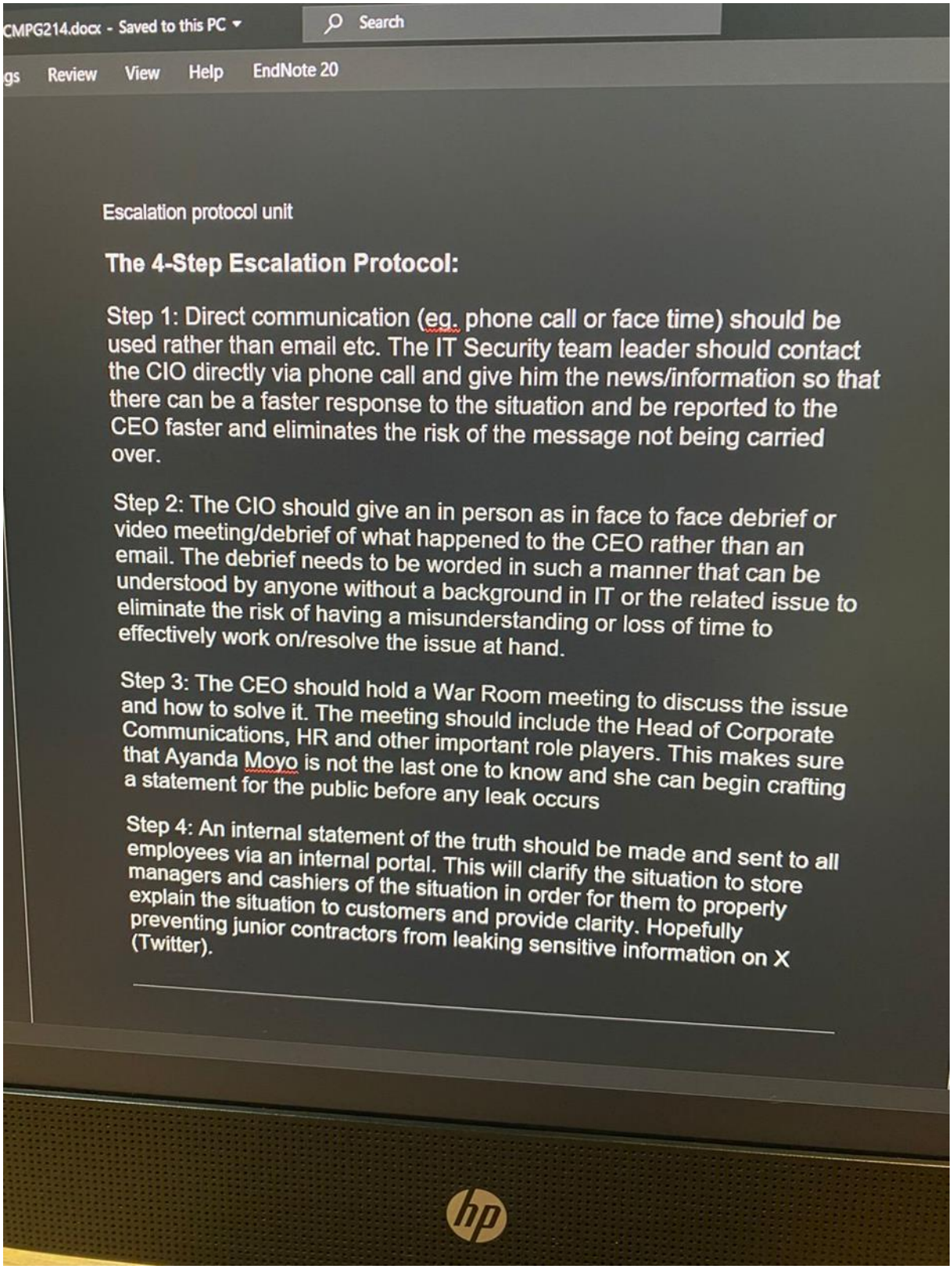
Tone Unit

From: Pieter van der Merwe (CIO)
To: Nomsa Dlamini (CEO)
cc: None
Subject: System Breach Alert
Date: Monday 24 February, 06:30

Nomsa,

We have confirmed that there has been a security breach in our customer database through a loophole in our online payment system. About a few million records were accessed including some important documentation. The attackers used the access for more than a week. We need to take action with immediate effect. We need to inform the Head of Corporate Communication, contain the system and prepare a public and customers statement.

Regards
Pieter


CMPG214.docx - Saved to this PC
Search
gs Review View Help EndNote 20
Escalation protocol unit
The 4-Step Escalation Protocol:
Step 1: Direct communication (eg. phone call or face time) should be used rather than email etc. The IT Security team leader should contact the CIO directly via phone call and give him the news/information so that there can be a faster response to the situation and be reported to the CEO faster and eliminates the risk of the message not being carried over.
Step 2: The CIO should give an in person as in face to face debrief or video meeting/debrief of what happened to the CEO rather than an email. The debrief needs to be worded in such a manner that can be understood by anyone without a background in IT or the related issue to eliminate the risk of having a misunderstanding or loss of time to effectively work on/resolve the issue at hand.
Step 3: The CEO should hold a War Room meeting to discuss the issue and how to solve it. The meeting should include the Head of Corporate Communications, HR and other important role players. This makes sure that Ayanda Moyo is not the last one to know and she can begin crafting a statement for the public before any leak occurs
Step 4: An internal statement of the truth should be made and sent to all employees via an internal portal. This will clarify the situation to store managers and cashiers of the situation in order for them to properly explain the situation to customers and provide clarity. Hopefully preventing junior contractors from leaking sensitive information on X (Twitter).

Risk Audit Unit

The risks of poor internal communication in this crisis

1. Employees learning about the breach from social media before management

- **What could go wrong:** Internal trust collapses, employees feel excluded and misled, rumours spread faster than official updates.
- **Who is affected:** All 12,000 employees, especially frontline staff who must answer customer questions without guidance.
- **SU2 concept:** *Internal vs External Communication Failure* — when external audiences (Twitter, Reddit) know before internal ones, credibility and morale are destroyed.

"Six hours after the CEO was notified. No internal communication to employees. No public statement." (CMPG.pdf)

2. Technical jargon blocking executive action

- **What could go wrong:** Leadership paralysis. The CEO did not understand the CIO's email, delaying urgent decisions and regulatory notification.
- **Who is affected:** CEO, executive team, regulators, and ultimately customers whose data was exposed.
- **SU2 concept:** *Shannon & Weaver's Semantic Noise* — jargon ("SQL injection vector exploit") created meaning failure. The message was technically accurate but ineffective.

"She did not know what happened, how bad it was, or what she needed to do." (CMPG.pdf)

3. Excluding Corporate Communications from the crisis meeting

- **What could go wrong:** No prepared public statement, media calls unanswered, share price drops further due to silence.
- **Who is affected:** Head of Communications, customers, investors, regulators, and the company's reputation.
- **SU2 concept:** *Channel Richness Spectrum* — a high-equity, high-urgency situation required rich, immediate communication (face-to-face with comms lead). Instead, leadership relied on silence, a lean "non-channel."

"Notably absent: Head of Corporate Communications (still not informed)." (CMPG.pdf)