To: **Goldman Sachs**
From: **Ibrahim Abdinur**
Date**: Fri 28th Oct**
Email Subject: **Cracked leaked Password Database**

e10adc3949ba59abbe56e057f20f883e:**123456**
25f9e794323b453885f5181f1b624d0b:**123456789**
d8578edf8458ce06fbc5bb76a58c5ca4:**qwerty**
5f4dcc3b5aa765d61d8327deb882cf99:**password**
96e79218965eb72c92a549dd5a330112:**111111**
25d55ad283aa400af464c76d713c07ad:**12345678**
e99a18c428cb38d5f260853678922e03:**abc123**
fcea920f7412b5da7be0cf42b8c93759:**1234567**
7c6a180b36896a0a8c02787eeafb0e4c:**password1**
6c569aabbf7775ef8fc570e228c16b98:**password!**
3f230640b78d7e71ac5514e57935eb69:**qazxsw**
f6a0cb102c62879d397b12b62c092c06:**bluered**
8d763385e0476ae208f21bc63956f748:**moodie00**

What type of hashing algorithm was used to protect passwords?

- Hash modes: MD5

What level of protection does the mechanism offer for passwords?

- MD5 Hash algorithm is weak and therefore breakable because it works too fast and conserves RAM memory when cracking. Hence the level of protection is lower than other Hash algorithms.

What controls could be implemented to make cracking much harder for the hacker in the event of a password database leaking again?

To ensure cracking is made harder in the event of database breach I would suggest the following changes.

- Users must create sophisticated passwords that's configured of alphabets, caps, numbers as well as symbols
- Use better algorithm to encrypt in place of MD5 like SHA-2
- Configure longer salts on each hash password in storage
- Use multi-factor authentication such as passwords & temporary security code

What can you tell about the organization's password policy (e.g., password length, key space, etc.)?

- Policy is relatively weak and prone to attacks as users have easy/common passwords that have weak hash functions with little to no salting

What would you change in the password policy to make breaking the passwords harder?

- User must avoid password with common names, phrases and year of birth
- Users must create unique and sophisticated passwords using mix of characters.
- Minimum password length requirement: 12
- Minimum password characters requirement: Alphabet, Capitals, Numbers & Symbols