To: CEO
From: Chair of the risk committee
Date: 18 November 20X3

Data breach at NCTech data centre

System breach

On 21 October, sensitive details belonging to several large clients were accessed by an unknown external party following a secret attack on our core systems. The data breach was identified by an internal security tool which alerted the data centre staff that there had been an attempt to access the core client database and client servers.

My investigations found that the firewall had not been operating fully since 10 July. The unauthorised party [hacker] accessed and copied client data, and then attempted to delete it from the database. However, no data was actually deleted so the clients affected were unaware of the breach and continued to use NCTech's servers and data storage facilities.

The data hacked is very likely to have included some commercially confidential information. If this is misused, or shared by the hacker, it could expose those affected clients to significant financial losses and other commercial damage.

It is vital that we are always honest with our clients. Should the security breach become public knowledge, it is likely to generate concern and anger, and harm NCTech's reputation. Therefore, we need to undertake further detailed investigations to determine exactly which clients were affected by the breach, and to what extent they were exposed.

Breach of trust

A related concern is that although NCTech data centre staff had actually identified the data breach, it had not been brought to the attention of senior management or even internally reported. It appears that the breach was rapidly and effectively closed, without being properly investigated. It was only reported to the board following an internal audit of the data centre. By failing to report this incident, there has been a serious breach of trust. Trust has always been a key feature of the NCTech business model and culture and is part of our core values. It is possible that similar data breaches have occurred in the past but have not been reported.

Those members of staff involved in the incident may need to be referred for disciplinary action. However, it is equally important to remind all staff of the importance of complying with NCTech's internal procedures and practices to maintain the integrity of the systems and services which we provide to our clients.