From: Alisdair Cameron GRO
Sent: Fri 01/03/2019 4:09:40 PM (UTC)
To: Tim Parker GRO
Subject: Alex Chisholm briefing and general update
Attachment: TPAC - final- 2802.docx

Tim, I attach an updated briefing for your meeting with Alex Chisholm. As discussed it starts with our core concern and sets down some measures of success. We have included detailed answers for each of the issues raised. I am sure you will only need a fraction of the material but it's intended to be helpful if he probes a little in any given area. If you have any questions while I am in Belfast, Patrick Bourke put together the material and will help.

In terms of general updates, given I am not there on Tuesday, and in the spirit of never wanting to be surprised, my list is:

1. We are just closing the books on P11 and trading is slightly ahead of forecast (£0.6m) on an underlying basis. Other movements are positive and we still expect trading profit nearer to £60m than the planned £50m for the full year.
2. We have been told that the GLO verdict will be given to us on an embargoed basis next week and is likely to be published on 11th, the first day of the Horizon trial.
3. On Interim CFO, you have a straight choice, having exchanged with Jane and Tom, between having an " Interim Group Finance Director" who does not sit on the Board, could nonetheless attend the bulk of Board meetings and would not need SoS approval OR an Interim CFO who sits on the Board and does need SoS approval. In the former case, I would be both CFO and Interim CEO. If we go down the SoS approval route, Tom would be keen to present it as "we are doing this unless you say no" but whether that will work, I don't know. You are meeting a candidate on Tuesday who is full of potential but is not a grizzled veteran and we have some other CVs for comparison. Let me know how you want to proceed.
4. On Back Office, we make progress but slowly. We still have a substantial balance of transactions that haven't got through to CFS. The good news is that we now have transaction listings that support almost all of the historical differences, so we can prove they exist and can start clearing them. However, we are still getting new differences through. Transtrack are under tremendous pressure from us but they have limited resources and are one paced, with fortnightly drops of code change. On the cash counts, we don't believe we have a problem but I have a great need to absolutely prove we haven't and the focus is on clearing some initial exceptions in Birmingham in particular. We have increased resource including Internal Audit to make sure.
5. On a minor matter, the letter exchange between Alex Chisholm and Paula where they reminded us that we mustn't use Government money for the GLO and we said we had (£2m) but we would give it back will be made public as part of a FOIA request.
6. Finally, Rob's note below details another cyber issue. My sense is it doesn't need to go to the Board yet but if you disagree, we can do so straight away.

Problem Outline

- On Tuesday 26th February 19 Verizon Cyber Risk Program advised Post Office that a collection of 29 billion of stolen users' credentials (usernames and passwords) had been published in the Dark web in January.
- From these stolen users' credentials there were 100 that appeared to be from the Post Office.
- The Post Office user accounts had weak passwords associated with them.
- Multiple threat actors claimed to be the source of the data, and were distributing these databases

throughout the dark web.

Current Status

- On receipt of the list of 100 Post Office usernames, Post Office IT Security requested Computacenter to:
  - Disable the user accounts with immediate effect as a precaution
  - Reset the user accounts with strong complex passwords
  - Inform the IT Helpdesk to provide the users with additional advise around strong passwords when they called to have their accounts re-enabled
- Computacenter identified that of the 100 users on the list only 40 were actual Post Office accounts and the remaining were fictitious.
- Verizon Cyber Risk Program advised Post Office IT Security that the list of user accounts had a very high probability that they were not obtained from Post Office systems rather from users registering for external non-work related services (e.g. utilities, myfitnesspal etc) and those systems had been compromised.
- Post Office IT Security worked with Internal Comms to send an update to all Post Office employees to remind them that:
  - They need to use strong complex passwords to protect the business
  - They should not be using their Post Office email account to register for non-work related services or applications
- Post Office Data Protection team contacted the ICO on 27/02/19 to discuss the Verizon incident to determine whether this was a notifiable breach. Having advised the ICO that Post Office considered that the breach was as a result of employees using Post Office email accounts on external, non-work related sites, it was agreed that the providers of those sites were the Data Controllers and should be reporting the incidents themselves.
- However, the ICO did state that Post Office should consider whether the company had weak policies in place which allowed for individuals to use their post office email address in these circumstances, and to determine if that in itself was sufficient to meet the criteria of a notifiable breach. The ICO did state during these discussions that they were satisfied with the measures that Post Office had immediately put in place to reduce the risk of access to those accounts.
- The Data Protection team do not consider that the criteria for reporting the incident has been met and it is not necessary to formally notify the ICO.

Additional Controls

- Since November 18 IT Security have implemented the following controls that would further protect Post Office from a compromised account:
  - Implemented mutli-factor authentication to ensure an additional security check before

someone can access the Post Office Network

  - Improved detection of any suspicious activity on the network by implementing the Security Operations Centre

  - Improved password strength by running password audits to detect any weak passwords that users are using

- The Acceptable Use Policy is being amended to ensure employees do not use their Post Office accounts for non-business related services.

Sorry for a long note Al

Alisdair Cameron
Chief Finance & Operating Officer

20 Finsbury Street
London
EC2Y 9AQ

GRO