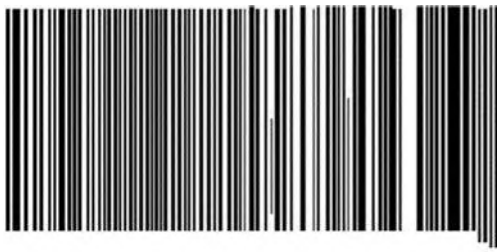

RMP-221-0001152-A

Extract - D4123

From: NORTHMOOR TEAM-T1-DSIO2 (Dempster, Mark WO2)
Sent: 16 August 2016 10:06
To: UKSF4 -COS (IIA7 OF3)
Cc: UKSF4 -8-OC N5966 NORTHMOOR TEAM-T1-SIO (Wright, Jason Capt); Spec Ops RMP-SPCB-3C-WOIC (Sivieri, Stuart SSgt)
Subject: FW: 20160812-Op_NORTHMOOR SFHQ (UK) Data_recovery_SIO-OS

Ma'am,

Good morning, I am the Deputy Senior Investigation Officer working with Capt Wright on Op NORTHMOOR. Capt Wright asked me to forward the below email in his absence.

Kind Regards

WO2 Dempster M P | Specialist Operations Regiment | Op NORTHMOOR | RAF St Mawgan| Cornwall | TR8 4HP
Contact Details

IIA7

I am the Senior Investigating Officer (SIO) for certain areas of Op NORTHMOOR and have a vested interest in the data recovery from your location.

SSgt Sivieri has briefed me on the very useful meeting held on 28 Jul 16 at UKSF4 I remain grateful for your support. I appreciate in terms of timing for you, this is not great as you are moving on. For me, this is a crucial phase of evidence recovery and I must be able to demonstrate that I have secured and preserved the relevant evidence. Not to do so will expose the investigation and MOD to potential criticism.

The cancellation of the proposed meeting scheduled for Tue 17 Aug 16 is unfortunate. I would ask that OR8 IIA8 provide the required information (set out below and the technical questions posed at the meeting on 28 Jul 16), at the earliest opportunity; this will enable our cyber team to prepare the necessary work in order not to impact on the operational effectiveness of your unit and those who you administer on an IT footing. Further delay will prevent the recovery of this evidence. As I understand (please correct me if I have got this wrong and excuse the technical ignorance), the following will take place as agreed:

1. The switch of data to a new server will take place imminently (grateful if you could confirm the exact date), with the redundant server being 'switched off'. RMP are to be present when this occurs.
2. Agreement has been reached that RMP will have unrestricted access to the powered down server, which contains all original data inclusive of deleted data.
3. The redundant server will then be able to be moved to another secure location for further forensic examination by RMP.

To date, we have sought the most pragmatic solution for data recovery which both satisfies the evidential process and one which enables those units concerned to maintain an operational capability; it is hoped this can continue. As the SIO, I have agreed that we can wait for the old server to become available so as not to negatively impact on your effectiveness; this has been prioritised over the need for securing and preserving evidence.

Separately, I would be keen to seek a solution regarding data recovery from the 'Old Faithful' server. In earlier discussions with your unit and others (meeting in Sep 15 at SFHQ(UK) we spoke about the intent to recover the above secret data. From the meeting I gleaned that due to the fragile nature of the old server, there may be issues with turning it back on again if we switch it off?

I would be most grateful if either you or N5966 could acknowledge this and would ask that we re-schedule the cancelled meeting at the earliest opportunity.

Happy to chat this through at your convenience.

Kind regards,

Jason

Captain J L Wright | Senior Investigating Officer | Operation NORTHMOOR Specialist Operations Regiment, Royal Military Police, RAF St Mawgan, Cornwall, TR8 4HP

Contact Details

SSgt S,

Apologies but OF3 N5859 is on leave at the moment. I have forwarded your request to OR8 IIA8 who is looking into it. We will get back to you.

Also, I'm afraid we need to postpone next week's meeting. I have handed this over to OF3 N5966 2IC-Des (cc'd) as I leave next week and he will be your POC in UKSF 4 from hereon-in.

Many thanks,

IIA7

-----Original Message-----
From: Spec Ops RMP-SPCB-3C-WOIC (Sivieri, Stuart SSgt)
Sent: 08 August 2016 17:22
To: UKSF4 COS OF3 IIA7
Cc:
Subject: FW: RMP

Ma'am,

I have attempted to make contact with OF3 N5859 on EXT but unfortunately I haven't been able to speak to him.

We are still waiting on the answers from the questions posed by WO2 Priddin on 29 Jul 16, which will enable us to expedite our ability to conduct R&D in the anticipation of working on ITS1.

Are you able to assist with either information on the progress or a POC for the interim?

Kind regards,

SSgt Sivieri

SSgt Sivieri SR AGC (RMP) | Manager Cyber Crime Centre (3C) | Specialist Operations Regiment | Service Police Crime Bureau, Cyber Crime Centre, Bassett Wilson Building, Southwick Park, Fareham, Hants, PO17 6EJ.

Contact Details

-----Original Message-----

From: NORTHMOOR TEAM-Cyber Lead-Priddin JR WO2 [Contact Details redacted]
Sent: 29 July 2016 10:21
To: UKSF4-COS IIA7 OF3
Cc: UKSF4-J7-CAP-IS (MULTIUSER); SFHQ (UK) INFOCOH-SO1 N2311 OF3; NORTHMOOR TEAM-HQ-OC (Stitson, Tina Maj); NORTHMOOR TEAM-T1-SIO (Wright, Jason Capt); Spec Ops RMP-SPCB-3C-WOIC (Sivieri, Stuart SSgt)
Subject: RMP

Ma'am

Just a quick follow up email regarding our meeting yesterday.

I can confirm the timeline for Afghanistan Operations we are interested in is YG to 2013. Please confirm where the data resides and what systems.

I have discussed the detail of the meeting with Capt Wright (NORTHMOOR Team 1 SIO), who agrees that working on your decommissioned data area in Sep 16, after you have transferred the data to your new system is the best course of action, as long as you can confirm that no data will be deleted from the decommissioned system during that process.

The benefits of taking this approach is that we will be able to achieve stages 1 and 2 for ITS1 in one hit and also remove the risk to your operational capability of ITS1.

You are going scope the viability of this option including locations that could be used.

Can I ask that OF3 N5859 or OR8 IIA8 confirm the following points to SSgt Sivieri (Cc'd above) ASAP.

1. Confirm the version of Microsoft Exchange used on ITS1 down to the specific service pack version.

2. Confirm the version of Microsoft Sharepoint used on ITS1 down to the specific service pack version.

We just need this basic information now so we can conduct some testing to allow us to be proportionate when recovering the relevant data sets.

Our next meeting is arranged for Tue 16 Aug 16 at UKSF4 Can you confirm a time for me.

I will be monitoring my email for the next two weeks when I am away.

Any more information or issues please contact me.

Kind regards

WO2 P