Technical and legal aspects of security

Assignment

Case Description:
National Bank Plc.
Case Number: 000001
Investigators Names:
Emmanuel Baudvin
Lucien Cassagnes
Lucas Laville
Antoine Puissant
Investigator ID: 007

Teachers : Carla and Arnim

2014 - 2015

Abstract

Ceci est le résumé

Contents

1 Management summary

2 Case outline

2.1 Assignment description

2.1.1 Initial assignment

At the beginning, the assignment was about civil law: Mrs. Marian Maid was complaining about the behavior of M. John Little. Indeed, it appears that M. John Little has been shared some private data about Mrs. Marian Maid to his colleagues during work time.
Our assignment has to conclude if M. John Little behavior is violating the company policy or not.
To do so, we first had access to two emails between Mrs. Marian Maid and M. John Little and Mrs Marian Maid and M. John Little HR files.

2.1.2 Second assignment

While doing the investigation on the first assignment, we discovered some strange emails exchange between M. John Little and M. Fred Tuck about some projects which could be concerning some money embezzlement.
After talking with M. Norman Sherriff (Legal Director), he conclude that this was a more important matter to investigate: it was going under criminal law.
The first assignment was then put on hold to focus only on this one.

2.2 Time-line and case information

Summer 2013 Mrs. Marian Maid and M. John Little went on vacation together. During those vacations, Mrs. Marian Maid allowed M. John Little to take some pictures of her in some embarrassing positions.

December 2013 (Christmas party) During a Christmas party, Mrs. Marian Maid heard M. John Little was going to show some of the pictures taken during previous summer to some colleagues of him (salesmen).

2014-02-03 – Between 02:14 and 12:56 Mrs. Marian Maid and M. John Little exchanged some emails concerning the fact that M. John Little had been showing some pictures to M. Fred Tuck. In those emails, the conversation became heated and threat were made from both sides.
Those emails also teach us that M. John Little may have a drive containing more pictures of Mrs. Marian Maid in some embarrassing positions.

2014-02-27 – 14:26 Mrs Marian Maid informed M. John Little that she was moving in with her sister. Their personal relationship was over.

2014-12-16 – 09:30 Mrs. Marian Maid contacts her friend Mrs. Olivia Oyle in HR and is extremely upset about a personal matter. They both arrange to meet in the canteen to have a coffee and discuss the issue.

2014-12-16 – 10:15 Mrs. Marian Maid and Mrs Olivia Oyle meet in the canteen. It is obvious to Mrs Olivia Oyle that Mrs Marian Maid has been crying and is visibly upset. Mrs Olivia Oyle, stating that she is concerned for Mrs Marian Maid's well being, talks to her about what has upset Mrs Marian Maid.

2015-01-06 We, the investigation team, are called into the office of Mrs. Jenny King (HR) to discuss a matter of concern. She explain to us the matter and ask us to perform an investigation over M. John Little behavior.
She hands out to us two emails between Mrs. Marian Maid and M. John Little and Mrs Marian Maid and M. John Little HR files.

2015-03-07 – 10:53 to 13:29 After getting the legal authorization, a search and seizure was done at M. John Little and M. Fred Tuck's offices.

3 Investigation results

3.1 Disciplinary matter involving John Little and Marian Maid

3.1.1 First emails

At the beginning of the investigation, we had been handed two emails conversation between Mrs. Marian Maid and M. John Little. In those conversations, we can denote some important information:

- Mrs. Marian Maid wants to talk to M. John Little about a picture he has potentially showed to M. Fred Tuck.
  M. John Little doesn't deny on this and add there "there's way more exciting stuff on the drive".
- We then learn that M. John Little may have a drive with some compromising pictures of Mrs. Marian Maid. Since the company's HR policy allow to bring some personal devices at work, he might have took it to his workplace.
- Mrs. Marian Maid tells M. John Little that this kind of personal matters don't belong in such a working place.
- Mrs. Marian Maid then threatens M. John Little when saying "I know about Project "Snow King" and "Nomad". You ought to have remembered that I live with you and know more that you may think before embarrassing me to the entire office".
  With this threat, we learn something valuable about those projects. Why would she use them as leverage against M. John Little if they didn't had something suspicious?
- Finally, M. John Little threatens back Mrs. Marian Maid. He also insults her in the email.

With all those information, we were able to ask M. Norman Sherriff the authorization to perform a search and seizure at M. John Little and M. Fred Tuck.
We also had the permission to access the email database for Mrs. Marian Maid, M. John Little and M. Fred Tuck.

3.1.2 Search and seizure

M. John Little's desk

During the search and seizure of M. John Little's desk, we found the following evidences:

AEI 001 (loc B) CD named "NOMAD" found under the desk of M. John Little (with a post-it "FP-05 14:45")

AEI 002 (loc E) USB key taped behind M. John Little's screen

AEI 003 (loc G) Desktop computer (Dell Optiplex GX620)

MCO/001 (loc J) USB key hidden in a desktop vacuum cleaner (Henry Hoover)

AEI 004 (loc K) Hard disk drive inside a Pelican case inside a drawer (with a post-it "SB02 7/3/15 13.54")

MCO/002 (loc L) CD named "MM PIX" inside a drawer

MCO/003 (loc L) Camera Canon inside a drawer. We don't know if it contains a memory card and if it is empty or not.

With a first look, we can already be concerned about the contains of evidences *AEI 001* and *MCO/003*. Those two evidences may be linked to the strange project (*NOMAD*) and to the pictures of Mrs. Marian Maid ("*MM PIX*").

M. Fred Tuck's desk During the search and seizure of M. Fred Tuck's desk, we found the following evidences:

MC0/004 Laptop Vostro 1540, USB key (MC0/005) plugged in, CD (MC0/006) inside. Shutdown, battery unplugged

MC0/005 USB key plugged to the laptop

MC0/006 CD named "MM PIX" inside the laptop

MC0/007 CD named "NOMAD" taped under M. Fred Tuck desk

MC0/008 Hard disk drive case (SATA to USB) empty

AEI 005 USB key taped under M. Fred Tuck

With all those evidences, we can correlate with the ones from M. John Little. They both have two CD's named "NOMAD" and "MM PIX". Depending on the content of those CD's, it could prove that M. John Little has been sharing some pictures to M. Fred Tuck.
Also, the fact that all those devices were hidden (under a desk, inside a vacuum cleaner, etc...) is suspicious about their contents.

3.2 Embezzling matter involving M. John Little, M. Fred Tuck and Mrs. Marian Maid

3.2.1 All emails

3.3 Discoveries

3.4 Recommendations

From the evidences and the discovery we made on previous sections, we can provide the following recommendations:

- Conduct some interviews of the three protagonists (M. John Little, M. Fred Tuck and Mrs. Marian Maid) about the projects NOMAD and SNOW KING
- Conduct an throughout investigation on all the company's accounts to verify if there is some embezzlement or money laundering

- Contact the authorities to let them realize a full investigation with the power vested in them. We can already give them all the evidences proving all the suspicions this investigation found

3.5 Suspicious activities regarding "Project Nomad" and "Project Snow King"

We changed the investigation orientation when we digged deeper about what Mrs. Marian Maid said in the email provided to us. She has clearly threaten M. John Little with two project's names: "Project Snow King" and "Project Nomad". As explained before, it was this threat which caused Mrs. Jenny King to call us in order to investigate the subject told in the previous section.
While processing and analyzing emails from M. John Little, M. Fred Tuck and Mrs. Marian Maid, it has been discovered that the two projects were linked. As it can be found in a mail from M. Fred Tuck and M. John Little:

```
From: Fred Tuck <fredtuck-natbank@inbox.com>
Received: from fredtuck-natbank@inbox.com by (127.0.0.1:25) via inbox.com
  (127.0.0.1:25) with [InBox.Com SMTP Server] id 1402031231095.WM55 for
  johnlittle-natbank@inbox.com; Mon, 3 Feb 2014 12:31:08 -0800
To: John Little <johnlittle-natbank@inbox.com>
MessageID: <EF2F31F9CFC.00000662fredtuck-natbank@inbox.com>
Date: 2014-02-03 21:31:08
Subject: Project Snow King

We have a go on this. Contract will be signed by tomorrow.

Contacts and supporting contracts are now ready to implement Nomad.

Desert Walker and Bedouin are up to support.

I'll PM you the password for those books

Fred.

-------------------------------------------------------------
FREE 3D EARTH SCREENSAVER - Watch the Earth right on your desktop!
Check it out at http://www.inbox.com/earth
```

The subject "Project Snow King" and the mention of "Nomad" in the same mail prove that these two projects are working together. Nomad is most likely a subsection of Project Snow King. Moreover, it has been found suspicious that two nicknames "Desert Walker" and "Bedouin" were mentioned. At this time, we can not explicitly found the identities of these two supports because of the lack of informations regarding them. Adding this, M. Fred Tuck wrote that he has communicate the password of some books, number of them can not be told, but he did not use the standard mail of his company to do so. Instead he "PMed" them to M. John Little by any over communication system.
This email was the starting point of the orientation's change of our investigation. With these informations, the team went to M. Norman Sherriff and presented the proof to him on the 10th of October 2015. As the subject of these mails is most likely speaking about embezzlement, our affectation changed. We stopped the work on M. John Little behavior and started a new one under the criminal law on what can be found about these two projects, who were the actors and what were their subjects.

3.5.1 Project Nomad

Project Nomad was the first to be analyzed. This decision was made according to the mails dates found concerned on the name of the project. To do so, we filtered all mails which contained the word "Nomad" in their subject or content. Two mails poped up from the other, both including M. John Little and M. Fred Tuck; email 1 4.1.1 email 2 4.1.1.

4 Evidence log

4.1 Key evidence items

4.1.1 Emails

Email 1

```
From: Fred Tuck <fredtuck-natbank@inbox.com>
Received: from fredtuck-natbank@inbox.com by (127.0.0.1:25) via inbox.com
  (127.0.0.1:25) with [InBox.Com SMTP Server] id 1402030751100.WM55 for
  johnlittle-natbank@inbox.com; Mon, 3 Feb 2014 07:51:40 -0800
To: John Little <johnlittle-natbank@inbox.com>
MessageID: <ECBE881F87D.000002E9fredtuck-natbank@inbox.com>
Date: 2014-02-03 16:51:40
Subject: RE: Just heard the good news!

Sounds good to me.

Let's get into our petty cash account, just the two of us so we can discuss Nomad going fo

> -----Original Message-----
> From: johnlittle-natbank@inbox.com
> Sent: Mon, 3 Feb 2014 04:39:13 -0800
> To: fredtuck-natbank@inbox.com
> Subject: Just heard the good news!
>
> Calls for a celebration!
>
> What do you say we do a proper lunch tomorrow?
>
> ---------------------------------------------------------------
> FREE ONLINE PHOTOSHARING - Share your photos online with your friends and
> family!
> Visit http://www.inbox.com/photosharing to find out more!


---------------------------------------------------------------
FREE 3D EARTH SCREENSAVER - Watch the Earth right on your desktop!
Check it out at http://www.inbox.com/earth
```

Email 2

```
From: Fred Tuck <fredtuck-natbank@inbox.com>
Received: from fredtuck-natbank@inbox.com by (127.0.0.1:25) via inbox.com
  (127.0.0.1:25) with [InBox.Com SMTP Server] id 1402030752042.WM55 for
  johnlittle-natbank@inbox.com; Mon, 3 Feb 2014 07:52:37 -0800
To: John Little <johnlittle-natbank@inbox.com>
MessageID: <ECC0A8E7878.000002EDfredtuck-natbank@inbox.com>
Date: 2014-02-03 16:52:37
```

Subject: RE: Nomad

Sure.

Let’s go for a pint close to end of day, then we can pop back to do what we need to prepar

> -----Original Message-----
> From: johnlittle-natbank@inbox.com
> Sent: Mon, 3 Feb 2014 04:56:51 -0800
> To: fredtuck-natbank@inbox.com
> Subject: Nomad
>
> Fred,
>
> Let’s dust this off sharpish.
>
> We’re on a deadline
>
> _____
> GET FREE SMILEYS FOR YOUR IM & EMAIL - Learn more at
> http://www.inbox.com/smileys
> Works with AIM®, MSN® Messenger, Yahoo!® Messenger, ICQ®, Google Talk™
> and most webmails

_____
FREE 3D MARINE AQUARIUM SCREENSAVER - Watch dolphins, sharks & orcas on your desktop!
Check it out at http://www.inbox.com/marineaquarium

4.2 List of actors / personalities involved

Code	Name	Job title	Email	Phone	Address	Remarks
MM	Marian Maid	Associates traders	marianmaid-natbank@inbox.com	–	National Bank Plc., Dublin center, Ireland	Complainant
JL	John Little	General Trader	johnlittle-natbank@inbox.com	–	National Bank Plc., Dublin center, Ireland	Subject of complaint
FT	Fred Tuck	General Trader	fredtuck-natbank@inbox.com	–	National Bank Plc., Dublin center, Ireland	Accomplice of fraud
NF	Norman Sherriff	Legal Director	normansherriff-natbank@inbox.com		National Bank Plc., (Dublin center, Ireland) ?	?

Table 1: List of actors / personalities involved