Claim No: CFI-027-2014

THE DUBAI INTERNATIONAL FINANCIAL CENTRE COURTS

In the name of His Highness Sheikh Mohammad Bin Rashid Al Maktoum, Ruler of Dubai

IN THE COURT OF FIRST INSTANCE

BEFORE JUSTICE SIR RICHARD FIELD

BETWEEN

GRACIELA LIMITED

Claimant

and

GIACOBBE

Defendant

Hearing: **15, 16 & 17 September 2015**

Counsel: Duncan McCall QC (instructed by Al Tamimi & Company) for the Claimant

Dr Reyadh Kabban of Al Kabban & Associates for the Defendant

Judgment: **11 November 2015**

JUDGMENT OF JUSTICE SIR RICHARD FIELD

Summary of Judgment

The Claimant, Graciela Limited, brought a claim against the Defendant, Mr Giacobbe, for deliberately interfering with and interrupting the proper functioning of its IT system, a wrongful interference with property under Article 41 ofDIFC Law No. 5 of 2005. The Claimant sought compensatory damages under Articles 23, 24 and 25 of DIFC Law No. 7 of 2005.

The Defendant, a former employee of the Claimant, denied that he had sabotaged the Claimant's IT system. He denied that he had accessed the system after his employment had come to an end, until he was asked to return to help when the IT system crashed.

Justice Sir Richard Field adopted an approach whereby strong and convincing evidence would be required for serious allegations to be proved on the balance of probabilities. The case was based on circumstantial evidence.

Justice Sir Richard Field found the attack to be an internal, rather than an external, one. It was fanciful to suggest that a third party outsider would have had knowledge of accounts and password necessary to carry out the attack. Only the Defendant knew of the availability of IP numbers used to hide the Claimant's data. There was no tenable basis for suggesting that someone else within or outside the Claimant made changes, which constituted part of the attack.

The Defendant's secret creation of a server, secret copying of data onto that server (data that was later deleted in the attack) and his failure to disclose the existence of the server either during the handover prior to leaving employment with the Claimant, or when he returned to help after the attack, was very powerful evidence against him. There was no reasonable doubt but that the Defendant was the perpetrator of the attack.

Proof of motive was not necessary to establish the Defendant's role in the attack. Justice Sir Richard Field tended to the view that the attack was carried out to punish the Claimant for not appointing him to replace another member of staff, and to give himself the opportunity to appear to be the Claimant's saviour when called in to help after the attack, by `discovering' the secret server containing a copy of the deleted data.

The Defendant's denials that he was the perpetrator were found to be knowingly and dishonestly false.

The Claimant was awarded compensatory damages totalling USD 690,533. This comprised damages for the costs of an external company restoring the system and investigating the incident, the purchase of emergency servers, the cost of building emergency servers, and employee time incurred in dealing with the attack and its effects.

The Claimant had satisfied the requirements promulgated in *Aerospace Publishing Ltd & Anr ("Aerospace") v Thames Water Utilities Ltd* [2007] Bus L.R. 726, to support its claim for compensation linked to employee time incurred in dealing with the attack or its effects. It had produced such evidence as it could reasonably produce of the diversion of staff and had established that the diversion of staff caused significant disruption to its business. Had the staff not been diverted from their usual activities, they would have directly or indirectly generated revenue for the Claimant in an amount at least equal to the cost of employing them during that time.

The parties were invited to serve written submissions as to costs and interest.

This summary is not part of the Judgment and should not be cited as such

INTRODUCTION

1. On 21 June 2014, the IT system of the Claimant ("Graciela") was sabotaged.

2. This is the trial of a claim by Graciela that it was the Defendant ("Mr Giacobbe"), a former senior member of its IT team, who was responsible for this attack on the Graciela IT system by deliberately interfering with and interrupting its proper functioning.

3. The burden of proof is of course on Graciela and the standard of proof is the civil standard, namely the balance of probabilities. Lord Nicholls said in *In re H (Minors)(Sexual Abuse: Standard of Proof)*[1996] AC 563, 586D-H:

> "The balance of probability standard means that a court is satisfied an event occurred if the court considers that, on the evidence, the occurrence of the event was more likely than not. When assessing the probabilities the court will have in mind as a factor, to whatever extent is appropriate in the particular case, that the more serious the allegation the less likely it is that the event occurred and, hence, the stronger should be the evidence before the court concludes that the allegation is established on the balance of probability. Fraud is usually less likely than negligence. Deliberate physical injury is usually less likely than accidental physical injury.Built into the preponderance of probability standard is a generous degree of flexibility in respect of the seriousness of the allegation."
>
> "Although the result is much the same, this does not mean that where a serious allegation is in issue the standard of proof required is higher. It means only that the inherent probability or improbability of an event is itself a matter to be taken into account when weighing the probabilities and deciding whether, on balance, the event occurred. The more improbable the event, the stronger must be the evidence that it did occur before, on the balance of probability, its occurrence will be established."

4.The House of Lords has subsequently emphasised that Lord Nicholls was not saying that in civil cases involving serious allegations a "heightened" civil standard of proof is required, see *In re B (Children) (FC)* [2008] UKHL 35. This no doubt is true, but common sense tells one that in practice where serious allegations are made in civil proceedings, strong and convincing evidence will usually be required for such allegations to be proved on the balance of probabilities and this is the approach I propose to adopt in this case.

5.The case against Mr Giacobbe is based on circumstantial evidence. It is well known that whilst circumstantial evidence can be strong evidence, careful consideration must be given as to whether the evidence reveals any other circumstances which weaken or destroy the case against the accused and care should be taken to reach conclusions based only on reliable evidence and not on mere speculation.

THE FACTUAL WITNESSES

6.The witnesses of fact called by Graciela were: a Senior IT Analyst employed by Graciela, Graciela's CFO and Graciela's CEO. When I use the word "fact" I do not include any opinion that Mr Giacobbe was responsible for the sabotage or any conclusionary reasoning supporting an allegation that Mr Giacobbe was the culprit.

7.Dr Al Kabban, who appeared for Mr Giacobbe, made a number of criticisms of the evidence given by these witnesses. For instance, he observed that some amendments were made to some of the witness statements before the witnesses gave sworn evidence and in the case of Senior IT Analyst that he (Senior IT Analyst) had changed in his second witness statement what he had said in his first statement about how data was copied onto a virtual server. In my judgment, none of Dr Al Kabban's criticisms undermine the reliability of the sworn factual evidence given by Graciela's witnesses from the witness box. In my judgment, the factual evidence given by all of these witnesses was truthful and reliable.Graciela's CEO had a tendency to argue Graciela's case from the witness box but abstained from doing so after a comment from myself. Notwithstanding these lapses into advocacy, I have no hesitation in accepting Graciela's CEO's factual evidence.

8. Mr Giacobbe was the sole factual witness called by his side. He gave evidence by video link from Australia and had a tendency to speak very fast. Unfortunately, many of his answers in cross-examination were not picked up in the recording of his evidence. Both sides have provided such notes as they were able to produce of his answers which I found very helpful. In the circumstances, I propose to give my considered assessment of the reliability of Mr Giacobbe's evidence after I have considered Graciela's case based principally on undisputed facts and Mr Giacobbe's response thereto. Suffice it to say at this stage that I did not find Mr Giacobbe to be a reliable witness on a number of important matters and I am therefore prepared to accept only those parts of his evidence that are corroborated by the oral testimony given on behalf of Graciela or by other reliable evidence.

THE FACTUAL BACKGROUND: PART I - MR GIACOBBE'S KNOWLEDGE OF THE IT SYSTEM; THE IT TEAM; MR GIACOBBE'S'S RESIGNATION

9. Graciela was created by its Chairman, a wealthy investor. It is a private investment firm based in the DIFC, Dubai which invests proprietary capital in listed entities around the world. In carrying on its business it is highly dependent on its IT system. Data security is therefore extremely important to it.

10. Mr Giacobbe was employed as a member of Graciela's IT team from 16 September 2004 until 31 May 2014 when his resignation from the company became effective. His actual leaving date was 29 May 2014. On 16 March 2008 he signed a new contract of employment dated 12 February 2008 which described his role at that time as "Server Architect".

11.By early 2014, when Graciela's CEO asked each member of the IT team to describe his role in the company, Mr Giacobbe's role had expanded considerably over the previous 9 years 10 months. In a memorandum he produced in response to Graciela's CEO's request, Mr Giacobbe described himself as "IT Vice President" and stated that his role was

> ". to take complete responsibility of data centre systems, servers, applications and DR [Disaster Recovery] functionalities for Graciela and private offices across the globe. This includes research, planning, designing, implementing and maintaining all Graciela systems and server projects (such as Tradar, SUN and Data archive etc). The role also helps Head of IT with yearly budgeting, decision making, and IT strategy planning".

12.Amongst the specific responsibilities Mr Giacobbe went on to list in this memorandum were responsibilities for all server hardware and data storage systems, backup support, and all disaster recovery systems.

13.It is clear that over the 10 years he was with Graciela Mr Giacobbe acquired a detailed knowledge of all aspects of Graciela's IT system. During that period owing to his seniority he was involved in every single IT project, whether in a planning capacity or in implementing or running projects. Also, all members of the IT team covered for each other where necessary and thus Mr Giacobbe would have had a good understanding of that part of the system that was the direct individual responsibility of each of his colleagues.

14. Mr Giacobbe served notice of his resignation by an email to Graciela's CEO dated 17 April 2014. This followed the departure in early 2014

of the head of the Graciela IT team. A shared services survey conducted in December 2013 had shown that the IT team had been underperforming. Graciela IT team had been more a policy and strategy man than a hands-on man with a close knowledge of the system.

15. After Graciela IT team left the company, the IT team consisted of Mr Giacobbe, Senior IT Analyst and Technical Support Analyst. Later, on 11 June 2014, Ms Kerry joined the team as a Technical Support Analyst.

16. Senior IT Analyst was responsible for all network components and internet connectivity across all the Graciela sites and Technical Support Analyst was responsible for managing and maintaining all desk top and help desk level support including all of the IT user end facilities.

17. Mr O'Flynn testified that:

> (i) Mr Giacobbe felt insulted when asked by Graciela's CEO in March 2014 to put into writing his role and responsibilities; in Mr Giacobbe's view, senior management ought to have known what the role of each member of the IT team was.
>
> (ii) Mr Giacobbe also resented the fact that after Graciela's IT Team departure he had to seek authorisation from certain senior managers for purchases for the IT system, whereas Graciela's IT Team had been given prior authority to make purchases up to a certain value.
>
> (iii) Mr Giacobbe was upset when he learned that Graciela were intending to replace Graciela's IT Team by appointing someone from outside the company rather than himself.
>
> (iv) Mr Giacobbe felt that his services would be dispensed with in the near future.

18. Mr Giacobbe denied in cross-examination that he bore any resentment towards Graciela or that he thought that he would be let go if he did not resign. I reject Mr Giacobbe's denials and accept the evidence of Senior It Analyst.

19. Mr Giacobbe's last day in the office was 29 May 2014.

THE FACTUAL BACKGROUND: PART II - GRACIELA'S IT SYSTEM

20. Graciela's IT system consisted of: (i) the computers (work stations) located in Graciela's DIFC office for use by Graciela personnel; (ii) equipment located in a data centre in the DIFC office premises; (iii) further equipment sited at other small locations around the world.

21. The equipment in the DIFC data centre comprised a number of network components, primary and secondary domain controllers and all of the primary data servers and storage for the system. In total, there were approximately 55 servers. It was possible to gain access to the system from any of the work stations, as well as remotely over the internet via a secure and encrypted connection. Access to the system required the use of appropriate credentials and thus only people with the requisite knowledge thereof could do so.

22. Within the System, there were thousands of possible "IP addresses" (also known as "IP numbers") though only a small number were used at any one time. An IP address is a unique number assigned to a device (e.g. a computer) which is part of the network. Graciela's IP addresses/numbers were organised in ranges of 254 addresses per range. Servers were held on one range, PCs on another range, phones on another, and so on. Given the large number of IP addresses/numbers, there was no need to reassign an IP address to another device once the device to which that IP address has been assigned was no longer in use.

23. The IP addresses/numbers were dynamically assigned using a Dynamic Host Configuration Protocol (DHCP), which allowed IP addresses to change after a period of inactivity of 14 days. However, given the infrequent changes of machines and the fact that PCs were rarely shut down for longer than 14 days the DHCP, IP addresses/numbers at Graciela usually stayed assigned to individual PCs as the preferred IP addresses.

24. Access to the servers was administered and controlled by three Microsoft domain controllers in Dubai and three other domain controllers in different locations. The servers ran a variety of applications, including e-mail, file and print sharing, SQL databases and various business applications which accessed either databases or files. These applications included all of Graciela's financial applications (SUN Financials and 4Series), two document management systems (CODEX and eDocs), Graciela's intranet system, including Sharepoint, and Graciela's external websites. Most critical data was replicated to the disaster recovery site in Thailand and data was backed up to physical tapes incrementally each night as a safeguard. Usually, there would be one up-to-date copy of all of the company's data on tape each week. These backup tapes were kept in a small room adjacent to the data centre itself.

25. If the domain controllers were immobilized, access to the system would be rendered impossible.

26. The network storage SAN had connectivity with two physical servers, each of which ran six mounted "virtual" servers. A "virtual" server is not a physical piece of hardware but is instead comprised of a set of electronic specifications and configuration files which run on a "host" server or computer. If a virtual server is "mounted", it can be seen on the system. If it is "unmounted" it is invisible on the system.

27. The Graciela IT system used Active Directory (AD) which is a centralised and standardised system that: (i) automates network management of user data and security and distributes resources; and (ii) enables interoperation with other directories. Active Directory worked with the Primary Domain Controller (PDC) to authenticate and authorise all users and computers in the Windows domain network - assigning and enforcing security policies for all computers and installing or updating software. Thus, when a user logged into a computer that was part of the Windows domain, Active Directory checked the submitted password and determined whether the user was a system administrator using an administrator account or a normal user using a user account.

28. An administrator account is an account that can be used to change security settings, install software and hardware and access all files on the computer. It can also be used to make changes to other user accounts.

29. A user account is a collection of information that tells Windows which files and folders can be accessed, what changes can be made to the computer and the user's personal preferences.

30.	The Primary Domain Controller and Backup Domain Controller (BDC) are functions that can be assigned to a server in a network of computers that use the Windows NT operating system. Windows NT uses the idea of a domain to manage access to a set of network resources (applications, printers, and so forth) for a group of users. The user needs only to log into the domain to gain access to the resources, which may be located on a number of different servers in the network. The Primary Domain Controller manages the master user database for the domain. One or more other servers are designated as backup domain controllers.

31. Mr Giacobbe's workstation at the DIFC office had the designation (DBX-ANS-1) within the Graciela IT system.

32.	Before he left Graciela on 29 May 2014, Mr Giacobbe made available to Senior IT Analyst handover notes about Graciela's IT system. These notes took the form of over 1,000 pages of Excel spreadsheets, Word documents and screenshots. The handover was done, as Mr Giacobbe well knew, to enable the IT team to run the IT system in Mr Giacobbe's absence, Mr Giacobbe knowing far more about the IT system than the remaining members of the IT team. Included in the notes was a list of IP numbers for servers, workstations and printers and a list of passwords for numerous accounts.

33.	After Mr Giacobbe's departure, his passwords on his own personal account ("Giacobbe's") and the Active Directory system user accounts identified in the handover file were changed.

THE FACTUAL BACKGROUND: PART III - THE GRACIELA IT SYSTEM CRASHES

34.	The first signs that Graciela's IT system had been sabotaged emerged on Saturday 21 June 2014 when Gracile's CFO was unable to access his emails whilst in Scotland on business. This led to Senior IT Analyst going to Graciela's DIFC office to investigate the problem where he found that no access could be obtained to the Primary Domain Controller, the Active Directory or the servers.

35.	At about 11.00 am that morning Senior IT Analyst telephoned Mr Giacobbe's to ask for his help. Mr Giacobbe gave Senior IT Analyst some details of what to check in order to try and get the system back up and running, including old recovery passwords for the PDC and local administration accounts that were set on the machines. However, none of these worked. It was at this point that Senior IT Analyst first called Mr Giacobbe to verify the passwords on the handover sheet and to check if there were other passwords that could be tried to gain access to the domain controller.

36.	Mr O'Flynn asked for Mr Giacobbe's help several times that day and at one point asked whether he might be willing to come into the office, as he understood the system better than anyone else. Mr Giacobbe's enquired several times whether Senior IT Analyst had been asked by anyone in management to request his help. He wanted any involvement to be cleared with senior management first, in particular with Graciela's CEO. He also asked if Graciela's CEO had been in touch with Senior IT Analyst and whether he had mentioned anything about asking him (Mr Giacobbe) to come in. He raised the same enquiry in respect of the Chairman.

37. Mr Giacobbe eventually arrived at the Graciela office at approximately 6 pm on the Saturday evening. Having first asked if it was all right for him to do so, he sat at his old computer and logged into his old account to see if he could restore some of the servers from there. Since the domain controllers were down, along with the AD, his old account could not be re-activated and the password reset to allow him to log back in with his former Windows account. He therefore had to set up a profile on the PC, so that he could log in and get access to the network and systems. Senior IT Analyst believes that Mr Giacobbe created another "Giacobbe" account with which to log in and get access to the servers using remote desktop connections.

38. Mr Giacobbe said he wanted a contract to cover his work in assisting the recovery of the IT system and asked for an assurance from Graciela's CEO that he would not be held responsible for any actions that he may take to retrieve our IT system.Graciela's Senior Vice President (Legal), prepared a draft contract for Mr Giacobbe to sign. However, two days later, Mr Giacobbe refused to sign the contract and gave a number of vague reasons as to why he would not agree to the terms outlined in the draft contract, including that his brother, whose sponsorship he was then under, did not approve of him entering into a consultancy contract. Mr Giacobbe also said that he had plans to fly to Australia with his family on holiday that week. However, when Graciela's CFO asked him whether he had booked his tickets, he said he had not.

39.	On Sunday 22 June 2014, it was agreed that an individual called Chris from ITSec would try to restore the domain controllers using software that needed to be on either a USB key or a DVD and inserted into the server located in the data centre. Mr Giacobbe proceeded to make an issue over the fact that a DVD was being used in preference to a USB notwithstanding that if the machine could read the files on the media storage, it mattered not if the files were stored on a CD/DVD or on a USB key. Mr Giacobbe also became quite agitated in the data centre when the ITSec man, attempted to work on the domain controllers. At this point Mr O'Flynn received a call from representative from ITSec who said that Mr Giacobbe was interfering with ITSec man's work and making it difficult for him to do his job. Later, when Senior IT Analyst spoke to Mr Giacobbe about this, he said that representative from ITSec did not know what he was doing. However, one of the domain controllers was restored.

40. Graciela's CFO, Graciela's Senior Vice President, Senior IT Analyst and Giacobbe then had a meeting to come up with a plan of action. Mr Giacobbe said he was confident that he could restore the system if only he was left alone to do it. He said that he could not help if others were making changes or trying different things. Senior IT Analyst thought he clearly seemed unhappy that other professionals had been asked to assist with the response to the crash of the system.

41.	McAfee Foundstone Professional Services ("McAfee") was engaged by Graciela on the Sunday to help recover Graciela's lost data.Graciela's expert witness, was the first IT McAfee professional to arrive at the office at around 7pm on that evening. After explaining how McAfee worked and what they would be doing, Mr Wright started asking basic questions to gain an understanding of what had occurred and what the Graciela people knew. A number of his questions were directed to Mr Giacobbe but Mr Giacobbe did not answer all the questions and was quite vague in his responses to others. This was surprising to Senior IT Analyst because some of the questions were pretty basic and involved matters he would have expected Mr Giacobbe to know about.

42.	The following day (23 June 2014) the IT team met with Graciela's CFO and discussed a plan that envisaged Mr Giacobbe leading the

recovery effort. Mr Giacobbe told Graciela's CFO that he would like to run the entire recovery project, clean up whatever had happened, come up with a revised infrastructure and network, write new policies and procedures for the system globally and separate the Neritum domain that served Mr Chairman personally from the Graciela domain. Mr Giacobbe said that he could only do this if and when all external professionals had been removed. He said his concern was that too many people were making attempts to recover the system and it was difficult to track what was being done.

43. At one point, Mr Giacobbe suggested that he could try a few things to recover the virtual host machines and said he was confident of doing so. Senior IT Analyst was keen for him to get started but Mr Giacobbe then hesitated to get started and when he realised that Senior IT Analyst and several others were not leaving his desk, he said that he needed time to think about the situation to see what needed to be done and to read a few notes or emails. Whilst Senior IT Analyst and Graciela's Senior Vice President were standing at his desk, Mr Giacobbe appeared to be playing around with his computer mouse and not doing very much at all. However, Senior IT Analyst eventually left Mr Giacobbe's desk and a short time later Mr Giacobbe recovered some of the virtual host servers. In light of this behaviour of Mr Giacobbe, Senior IT Analyst reset the passwords again on those parts of the system that he knew were now up and running.

GRACIELA'S EXPERT WITNESS, MR PAUL WRIGHT

44. As stated above, the expert witness called by Graciela was Mr Paul Wright. Mr Wright has an MSc (with Distinction) in Professional Computing from Staffordshire University. From 1987 to 2009 he was a Detective Sergeant with the City of London Police working in the area of computer crime during which period from mid November 2001 he was a member of the National Hi-Tech Crime Unit. Since February 2009 he has held high-level civilian positions as a consultant investigator into computer incidents and as an advisor on computer security. He joined McAfee in June 2014 as EMEA Technical Director for Cybercrime Consulting.

45. In the course of investigating the crash of the Graciela IT system, Graciela's expert witness captured a number of forensic images from computers and servers located in the Graciela IT network and conducted a forensic analysis on the workstations of the past and current members of the Graciela IT team, save for that used by Ms Graciela's IT representative who had only joined the team very recently.

46. Graciela's expert witness also investigated Graciela's Windows Event logs for 2014 which are a repository of digital information about particular computers showing every activity on the System. However, he found that the VPN logs relating to the secure and encrypted connection - Remote Access Connection, Dynamic Host Configuration Protocol ("DHCP"), Domain Name Server, and Core Switches and Cisco network devices - had been immobilised and rendered unavailable.

47. In the course of his investigation, Graciela's expert witness identified login activity between March and June 2014 linked to the IP numbers 172.25.25.16, 172.20.0.240 and 172.25.26.29 and the accounts "clsadmin", "dxbbackup" and "spsadmin". The IP number 172.25.26.29 was the IP number assigned to Mr Giacobbe's workstation.

48. On 17 July 2014, Graciela staff discovered that a new virtual unmounted device existed on the Graciela IT system and learned later it had been named "Ptolemy 1". A screen shot of Ptolemy 1 shows the IP number for that device as 172.25.25.35 and also that the credential "Mr Giacobbes" made 9 attempts to logon to Ptolemy 1 on 31 March 2014. It was also discovered that the files for a user profile for the account "clsadmin" had been created on Ptolemy 1 at 15:57 hours on 6 May 2014.

49. Further investigation revealed that the data that had been deleted from the IT system during the sabotage carried out on 21 June 2014 had previously been copied from an existing server called "Ptolemy" onto the virtual, unmounted Ptolemy 1, where it remained.

50. Using the information found on the Windows Event logs and the forensic analysis of images taken from the computers he examined, Graciela's expert witness produced what he called the "Attack Timeline of Events", the final version of which was set out in his Second Report. The events identified in this list ("the Attack Timeline") and their dates and times were not disputed at the trial by Mr Giacobbe's expert witness. This, however, did not deter Dr Al Kabban from contending in his closing submission that since Graciela's IT system has been rebuilt, there is no alternative to relying on the information made available by the Claimant to the Court, "[h]owever the validity and the truthfulness of this information is doubted." Mr Giacobbe's expert witness having accepted the accuracy of the Attack Timeline and the trial having progressed on this basis, this judgment will also proceed on that basis.

51. It was Graciela's expert witness opinion that the sabotage inflicted on the Graciela IT system was not carried out by an external third party but by someone with intimate inside knowledge of the system. Mr Giacobbe trailed the possibility that an external consultant who had worked on the system was responsible by mistake or design for the incident on 21 June 2014, but the main thrust of his defence, as we shall see, was that a fellow member of the IT team had caused the incident by mistake.

52. In Graciela's expert witness judgment, the fact that data was copied onto a hidden virtual server, Ptolemy 1, before being deleted on the other servers indicates that the attack was carried out by an insider who wanted the option to recover the data from Ptolemy 1 at a later stage. Also, there was no evidence of any external reconnaissance before the attack, only internal reconnaissance both before and after the attack. Further: (i) there was no evidence of the use of Trojans (programs designed to breach the security of a computer system while ostensibly performing some innocuous function) or a rootkit (a set of software tools that enable an unauthorised user to gain control of a computer system without being detected); (ii) no ransom demand was received and no mention was made on the internet of the attack or that Graciela data was being disseminated; and (iii) there was no evidence that anyone outside had carried out a reconnaissance of the physical Graciela environment.

53. Graciela's expert witness's opinion that the damage done to the Graciela IT system was not carried out by an external third party but by someone with intimate inside knowledge of the system was not seriously challenged on behalf of Mr Giacobbe.

54. On 2 July 2015, Graciela made voluntary disclosure of a hard disc containing Event Logs and Forensic Images of various hard discs. Included in that disclosure was this screenshot taken from a text Notepad file:

55. The highlighted middle section of the screen shot appeared to show that Technical Support Analyst had logged on to the Graciela IT system

using the "clsadmin" account on 21 June 2014 at 4:35:17 hours. In a supplementary Third Report produced on the second day of the trial, Mr Giacobbe's expert witness, expressed the view on the basis of this screenshot that Technical Support Analyst had accessed the invisible virtual server Ptolemy 1 on 21 June 2014 after Mr Giacobbe had left Graciela. If this conclusion were soundly based it would have seriously undermined Graciela's case that the existence of Ptolemy 1 was not known to Graciela until it was discovered on 17 July 2014.

56. Graciela's expert witness answered Mr Giacobbe's expert witness third report in a further (third) report which he confirmed on oath in the witness box. His evidence was that the screenshot was taken from a text Notepad file and was not an event log as had been assumed by Mr Giacobbe's expert witness; rather, it was a draft working document in text format he had created in the course of his investigation. It had been included in Graciela's voluntary disclosure in error and had not found its way into his finished work product. He further testified that he had once again checked the original event logs and was able to confirm there was no log of any type showing that the user "GRACIELA\Srdnanr" had accessed Ptolemy 1 at any time on 21 June 2014. Graciela's expert witnesss evidence as to what the text Notepad file was, how it had been included in the voluntary disclosure made on 2 July 2014 by mistake, and his confirmation that having rechecked the original event logs there is no log of any type showing that the user "GRACIELA\Srdnanr" had accessed Ptolemy 1 at any time on 21 June 2014, was not challenged on behalf of Mr Giacobbe. Further, Mr Giacobbe's expert witness expressly accepted when cross-examined that he was not suggesting that Graciela's expert witness had deliberately doctored any material.

57.&#65533;In his written closing submissions, however, Dr Al Kabban, asserts that the screen shot shows that Technical Support Analyst accessed Ptolemy on 21 June 2014 and concludes, "As such, the Claimant's contention that they were not aware of the existence of Ptolemy 1 and they did not have knowledge about the password to the clsadmin account is false." And Dr Al Kabban does not stop there. He goes on:

> "The Claimant expert's justification and reasoning that the log is an amalgamation of entries is absurd as one cannot see any common factor or link between the three log entries in the screenshot. As confirmed by the Claimant's Counsel that logs cannot be altered, it is the Defendant's position that indeed logs cannot be altered but they can be copied onto a note pad document as seen in the screenshot thereby concluding that the entries are genuine log entries taken from the Claimant's data base which confirms the Defendant's position that selective information has been made available to the Defendant and the Honourable Court" [paragraph 47].
>
> "Even, if one were to believe that the inclusion of this log in the hard drive was a part of the rough work file belonging to the Claimant's expert, the authenticity of this log cannot be ignored or denied. A detailed review of that particular log indicates that the Claimant's expert obtained this piece of information from the Claimant's data base and accidently forgot to erase it before sending over the hard drives to the Defendant. This revelation clearly indicates that the Claimant's expert has been selective in the information he has made available to the Defendant and the Honourable Court. The Claimant's expert has deliberately provided the Honourable Court with information that supports the case filed by the Claimant's management against the Defendant while concealing information that clearly shows that the Defendant was not responsible for the alleged System Incident ." [paragraph 51].&#65533;
>
> "With regards to the Defendant's last expert report submitted on 16/09/2015, the Defendant's expert discovered a new log entry in one of the hard drives handed over by the Claimant to the Defendant. The hard drive contained a log entry which shows that one of the Claimant's employee accessed Ptolemy 1, a few hours before the System Incident was allegedly launched. The Claimant's expert has made a futile attempt of dismissing the Defendant's new finding as a part of his work file which does not hold any relevance in this case. The Defendant's expert refuses to believe the same as the Defendant's expert was given the hard disks in sealed plastic containers that declared the "Chain of Custody". However, the Claimant Expert's statement that the new piece of information in the form of a log entry is a part of his rough work states that the hard disks provided to the Defendant were contaminated with the Claimant expert's personal files. The hard disks made available to the Defendant were supposed to be images of Ptolemy 1 and other systems and this statement raises a doubt about the veracity of all the event logs and data that has been supposedly analysed and reported to the Honourable Court throughout the course of these legal proceedings" [paragraph 74].

58. None of these criticisms and serious allegations was put to Graciela's expert witness in cross-examination or asserted in evidence by Mr Giacobbe's expert witness and it is most regrettable that they are now advanced by Dr Al Kabban.

59.&#65533;In my judgment, Graciela's expert witness was a transparently honest witness and I accept his evidence about how the Notepad text came to be included in the material disclosed on 2 July 2015. Accordingly, I reject the contention that the screen shot shows that Technical Support Analyst accessed Ptolemy 1 on 21 June 2014.

60.&#65533;Indeed, I found Graciela's expert witness to be an impressive expert witness. The mistake over the Notepad text apart, the investigation he carried out was technically extremely proficient and he presented his findings clearly and objectively.

61.&#65533;In his first two reports he concludes that his factual findings coupled with information provided by Senior IT Analyst and Technical Support Analyst establish conclusively that it was Mr Giacobbe who sabotaged Graciela's IT system. Whether or not Graciela's expert witness was entitled to state this opinion on the ultimate question to be decided in this trial, I place no reliance on it since it is for the court, not the expert witnesses, to decide whether the case against Mr Giacobbe has been established to the necessary standard of proof.

THE KEY EVENTS IN THE ATTACK TIMELINE VIEWED IN THE LIGHT OF OTHER EVIDENCE

Change of Encryption Key and Backup System Passphrase.

62.&#65533;On 7 April 2014 the encryption key and passphrase for Graciela's backup system were changed using IP address 172.25.25.213. The back-up system was Mr Giacobbe's responsibility. It was Senior IT Analyst's evidence that neither he nor Mr Radivojeric (the only other members of the IT team on 7 April 2014) carried out this operation.

63.&#65533;No mention was made in Mr Giacobbe's handover notes that the backup tapes were encrypted or that the encryption key and passphase had been changed on 7 April 2014.

64. Mr Giacobbe denied that it was he who had changed the encryption key and passphrase. He testified that he was unaware that there was an encryption key and passphrase because when using the back-up tapes system, these were never required. It was also his case that during the attempts to recover lost data after 21 June 2014, an external consultant had mistakenly overwritten the database related to the tape backup software and it was only after this there was any prompting for the encryption key and passphrase.

Deletion of 300,000 files from Mr Giacobbe's hard drives

65. Graciela's expert witness examined the hard drive found in Mr Giacobbe's Graciela computer and another hard drive hidden within Mr Giacobbe's work station.

66. On three occasions on 27 and 28 May 2014 approximately 300,000 files were wiped from Mr Giacobbe's two hard drives using "CCleaner" software.

67. Prior to the trial, Mr Giacobbe claimed that he only deleted personal information, but artefacts discovered on his Graciela computer show that he kept company data on his computer including "audit information", "minutes and resolutions" of meetings and a large number of other Graciela documents. In cross-examination,Mr Giacobbe first denied deleting company data from his hard drives but when shown the evidence that he had deleted a large amount of company data, he maintained that this must have happened without him being aware of it.

Ptolemy 1

68. The operating system for Ptolemy 1 (the invisible virtual server discovered on 17 July 2014) was installed on Ptolemy 1 on 31 March 2014 and the "clsadmin" account was created on it on 6 May 2014. This was admitted by Mr Giacobbe. Ptolemy 1 itself was therefore created some time prior to 31 March 2014.

69. Between 4 and 13 June 2014 (after Mr Giacobbe's departure from Graciela on 29 May 2014) there were interactions between the "clasdmin" account, Ptolemy 1 and IP address 172.20.0.240. This latter address came from the Graciela's disaster recovery range of IP addresses and I accept the evidence of Senior IT Analyst that it was an inactive address.

70. At 10.30 pm on 17 June 2014, "clsadmin" was used to trigger a run on a "Robocopy" file on Ptolemy 1 using a program called "Task Scheduler". This task was completed the following day. Task Scheduler is used to arrange for a task to run at future point in time. The Robocopy software was used to copy Graciela's data to Ptolemy 1.

71. Further copying of data to Ptolemy 1 triggered by "clsadmin" occurred on 18, 19, 20 June 2014, on each occasion at 10.30 pm, the same time of day that the copying began on 17 June 2014.

72. The "clsadmin" account was also used to connect to Ptolemy 1 on 21 June 2014 at 04:31 am.

73. The data copied to Ptolemy 1 was not deleted during the sabotage carried out on 21 June 2014. It consisted of all of the Graciela data that was deleted from elsewhere on the Graciela IT system on 21 June 2014, save for a few emails. This data on Ptolemy was not discovered until after the existence of Ptolemy 1 emerged on 21 June 2014.

74. Forensic traces of "Robocopy" executable, namely the file or program that causes a computer to execute a task, were found on Mr Giacobbe's workstation during the McAfee investigation. The use of Robocopy to copy material onto Ptolemy 1 prior to his departure was admitted by Mr Giacobbe when interviewed by Mr Wright on 7 August 2014 ("the interview"). No such traces were found on the workstations of any of the other members of the IT team.

75. It is not disputed that Mr Giacobbe did not disclose the existence of Ptolemy 1 (which was invisible on the IT system) in the handover notes provided to Senior IT Analyst. He also did not disclose the existence of Ptolemy 1 when he was being asked to help in the recovery of Graciela's lost data over the phone and at Graciela's office, although he must have known that at least some of the lost data had been copied from Ptolemy to Ptolemy 1, since he carried out the copying operations that were undertaken before his departure from Graciela.

76. At the interview, Mr Giacobbe said that he did not disclose the existence of Ptolemy 1 in his handover notes because the migration of data from Ptolemy to Ptolemy 1 was not yet complete; he was still testing how this migration should be done. And when Graciela's expert witness put it to Mr Giacobbe that since the copying was incomplete, Ptolemy 1 should have been included in the handover notes, Mr Giacobbe said, "Yeah, it should have been."

77. In his first witness statement made almost a year after the interview, Mr Giacobbe stated that:

> "Ptolemy 1 was purely a test server which was built in April- May 2014 when the data migration project was underway in the Claimant's office. Ptolemy 1 server was created for a project under the instructions of the management whereby they instructed me to migrate data from one of the old servers (Ptolemy) to the newly built virtual environment servers called Host1 and Host2. The purpose of Ptolemy 1 server was to test the various methods that can be used to transfer data from the old server i.e. Ptolemy. Once the testing was done and the method(s) to be used for data transfer was selected through the testing done on to Ptolemy1, it was meant to be deleted and replaced with a fresh and newly built live server. The old Ptolemy was to be decommissioned after the selected data transfer method was used and data was transferred on the newly built live server. Emitec Consultants were also involved in this project. This project was not completed when I had resigned from my position and left the company." (paragraph 33).
>
> "All the members of the IT team and the external consultants were aware that the company data on Ptolemy1 server was being copied using test scripts to see and test how the data would be migrated from the existing old servers to the newly created servers . The test scripts were automated and schedule to run for a number of days to ensure that they are working properly before they could be used for real data migration". (paragraph 35).

"The Claimant has also accused me of failing to mention the details of Ptolemy1 in my handover notes, however in my opinion it was not necessary to mention this information as Ptolemy1 was an ongoing project, it was in the testing phase and everybody in the IT team including the external consultants were aware of its existence. Nevertheless, its exclusion from the handover notes was not deliberate and was a mere lapse. The fact that Ptolemy1 was not mentioned in the handover notes is irrelevant, particularly when everybody in the IT team including the management were aware of the existence and purpose of creation of Ptolemy1". (Paragraph 40).

78. The external consultants referred to by Mr Giacobbe were Emitec who between 18 and 24 March 2014 did work on the virtual environment of the Graciela IT system.

79. Graciela's CFO's evidence was that until Ptolemy 1 was discovered on 17 July 2014, no-one at Graciela knew of the existence of Ptolemy 1, let alone that data had been copied thereon from another server. The evidence of Senior IT Analyst (who had received Technical Support Analyst's confirmation that he had not known of Ptolemy 1) was to the same effect. Graciela's CFO also testified that the several consultants who in the past had done different work on the Graciela IT system had each completed a questionnaire sent to them by Graciela that asked for details of any work carried out, when, the servers accessed, the account names seen, who provided the access credentials, any use or receipt of the credentials for the "clsadmin" account and any connection to the IP numbers 172.25.25.16; 172.25.26.29; nd 172.20.0.240. In answering the questionnaire sent to it, Emitec reported that between 18 and 24 March 2014 they had installed 2 HP DL585 G7 Servers and installed and enabled Windows 2012 R2, Hyper-V services and SCVVMM 2012 R2 using a service account the credentials for which were provided by Mr Giacobbe. The "clsadmin" account had been used to configure Windows 2012 R2 Hyper-V cluster and SCVMM but the password was inserted by Mr Giacobbe whenever required.

80. All of the respondent consultants approached by Graciela reported that they had not connected to any of the specified three IP numbers.

81. Mr Wright's forensic examination of the workstations of the other members of the IT team showed that none of those devices had been used to access Ptolemy 1.

82. Included in Mr Giacobbe's handover notes was a section headed "Graciela device server roles" under which, inter alia, four test servers were identified and three "Interaction" servers. When asked in cross-examination why he identified these servers but not Ptolemy 1 he replied that these servers were old physical servers that had been turned into test servers whereas Ptolemy 1 was a new virtual server.

83. When asked during the interview why he did not tell the Graciela IT and McAfee recovery teams about Ptolemy 1 and the data that was on it, Mr Giacobbe said the project was on-going, he was testing it and he had not copied everything.

84. In cross-examination he said that he did not tell the recovery teams about Ptolemy 1 because only a small amount of data had been transferred and it may have been overwritten.

85. Whilst management may have approved the expenditure on the work done by Emitec in March 2014, I accept the evidence of Graciela's CFO and Senior IT Analyst that neither the Graciela IT team (other than Mr Giacobbe) nor Graciela's management knew anything of Ptolemy 1 until it was discovered on 17 July 2014; and that accordingly they knew nothing about any copying onto a new virtual server of Graciela data until this too was discovered after 17 July 2014. If they had had this knowledge, Ptolemy 1 and the data it contained would certainly have been revealed in the early days of the recovery attempts. Also, Mr Giacobbe's evidence involves the suggestion that many individuals within Graciela have conspired falsely to allege that Ptolemy 1 was unknown until 17 July 2014, which I regard as a fantastic and wholly unrealistic proposition.

86. I also find that Emitec did not know Graciela data was being copied on to one of the new virtual servers and did not know the password for "clsadmin".

87. I further find that Mr Giacobbe deliberately omitted to disclose the existence of Ptolemy 1 both in his handover notes and when he returned to Graciela's offices on 21 June 2014 and thereafter. On his own evidence the test copying of data from the old Ptolemy to Ptolemy 1 was on-going and therefore incomplete when he left the company. He therefore had as much reason to disclose the existence and purpose Ptolemy 1 in his handover notes as he did to disclose the four test servers and three Interaction servers he did disclose under the heading "Graciela device server roles".

88. As to his failure to tell the recovery teams about Ptolemy 1, I find his different explanations for this to be wholly unconvincing and contrived. Mr Giacobbe well knew that the recovery teams were working on the basis that the whole of Graciela's data had been deleted from the IT system. In these circumstances, even if only part of the data on old Ptolemy had been transferred to Ptolemy 1 by the time Mr Giacobbe had left on 29 May 2014, it is incredible that he did not disclose or mention to the teams the existence of Ptolemy 1 and his copying thereon of Graciela data, especially since it is clear from Mr Wright's Appendix K, which is a sample of many Ptolemy 1 artefacts found on Mr Giacobbe's work station, that a considerable quantity of corporate data had been copied over pre 29 May 2014, including information relating to Middle East benefit packages, Graciela salary review and settlements, asset register reconciliation, sovereign finance and Indian banks.

Use of the "clsadmin", "spsadmin" and "dxbbackup" accounts to access the Graciela IT system

"clsadmin"

89. Prior to his departure from Graciela on 29 May 2014, Mr Giacobbe frequently used the "clsadmin" account from his workstation to access the IT system. On 27 May 2014 "clsadmin" accessed the Graciela IT systems' domain controllers and the Disaster Recovery server, all from Mr Giacobbe's workstation. In particular at 4:45 pm the "clsadmin" account was used to make multiple connections within a few seconds of each other to six disaster recovery servers.

90. On 28 May 2014, the "clsadmin" account was used from Mr Giacobbe's work station to access the Zeus backup server at 08:38 am and 12:07 pm, the Zeta2 at 08:40 am and the Beta domain controller at 12:07 pm, 4:10 pm and 4:23 pm.

91. On 29 May 2014, the "clsadmin" account was used from Mr Giacobbe's workstation to access the Zeus backup server at 08:10 am and the

Beta domain controller at 2:53 pm and 3:03 pm.

92.&#65533;After 29 May 2014, the "clsadmin" account was used to access the IT system (Ptolemy 1 in particular, see paragraphs 68 - 72 above) from IP number 172.20.0.24 and from 20 June 2014 this account was also used on occasion from IP number 172.25.25.35 and on other occasions from IP number 172.25.25.16.

93.&#65533;On 21 June 2014 (the day of the sabotage) "clsadmin" logged on to Graciela's financial system's data base from IP number 172.25.25.16 and was used from the same IP number to delete that database at 05:27 am.

94.&#65533;At 06:07 am on 21 June 2014 Graciela's SOGNO domain controller was shut down by the "clsadmin" account.

95.&#65533;At 06:15 am on 21 June 2014 Graciela's Beta domain controller was shut down using the "clsadmin" account from IP number 172.25.25.16.

96. Graciela's expert witness's forensic examination of the workstations of Senior IT Analyst, Technical Support Analyst and Graciela IT Team revealed that none of these devices ever used the "clsadmin" account.

97.&#65533;I accept Senior IT Analyst's evidence that whilst Mr Giacobbe was employed by Graciela he (Mr Giacobbe) must have been the only member of the IT team to use the "clsadmin" account and that neither he (Mr O'Flynn) nor Technical Support Analyst knew the password to the "clsadmin" account.

98.&#65533;I find that Mr Giacobbe did not disclose the "clsadmin" account in his handover notes, as alleged by Graciela. In cross-examination he suggested for the first time that he may have disclosed the account in some part of the notes other than the materials that had been included in the trial bundle. Until this point, he had impliedly accepted that "clsadmin" had not been disclosed and his case was that he may have missed a few details as he prepared the notes from memory based on what his replacement might need to know to start work with the servers.

99.&#65533;The entire handover notes had been available to Mr Giacobbe throughout the proceedings. Graciela had found no mention in the notes of "clsadmin". In these circumstances it was for Mr Giacobbe to examine the notes to make good his late-in-the-day suggestion that he did indeed disclose the account. However, he failed to produce any evidence from the notes to make good his assertion and on the evidence before me I have no hesitation in finding that he did not reveal the existence of "clsadmin" in his handover notes.&#65533;

"spsadmin"

100.&#65533;On 3 May 2014 at 11:07 am the "spsadmin" account was used to access the Graciela IT system (Seti04) from Mr Giacobbe's workstation (IP number 172.25.26.29). I find on the basis of Senior IT Analyst's evidence in paragraph 18 of his first witness statement that this use by Mr Giacobbe of the "spsadmin" account before he left Graciela can have had nothing to do with his normal duties.

101.&#65533;On 4 June 2014 the "spsadmin" account accessed Zeus from IP number 172.20.0.24.

102.&#65533;On 9 June 2014 the `spsadmin" account was created on Ptolemy 1 (8:57 pm) and accessed Zeus from IP number 172.20.0.24 (9:40 pm).

103.&#65533;On 13 June 2014 the "spsadmin" account from IP number 172.20.0.24 accessed: (a) Zeus at 8:09 pm; and (b) Seti04 at 8:38 pm.

104.&#65533;On 21 June 2014 the "spsadmin" account from IP number 172.20.0.24: (a) accessed Zeus at 06:03 am; and (b) shut down the Alpha domain controller at 06:27 am.

105.&#65533;The forensic examination of the workstations of the other members of the IT team conducted by Mr Wright showed that those devices had not accessed the "spsadmin" account.

106.&#65533;I find that the existence of the "spsadmin" account was unknown by the Graciela IT team. It was not referred to in Mr Giacobbe's handover notes.

"dxbbacup"

107.&#65533;On 9 June 2014 at 9.37 pm; and on 10 June 2014 at 7:31 pm; and on 13 June 2014 at 02:03 am, the "dxbbackup" account accessed Zeus from IP number 172.20.0.24.

108.&#65533;On 21 June 2014 at 05:45 am "dxbbackup" from IP number 172.20.0.24 was used to shut down Zeus (Symantec Backup Exec system).

109.&#65533;The forensic examination of the workstations of the other members of the IT team conducted by Graciela's expert witness showed that those devices had not accessed the "dxbbackup" account.

110.&#65533;I find that the existence of the "dxbbackup" account was unknown by the Graciela IT team and was not referred to in Mr Giacobbe's handover notes.

The use of IP numbers 172.20.0.24 and 172.25.25.16

111.&#65533;On 27 May 2014, Mr Giacobbe's workstation (DBX-ANS-1) attempted to connect to IP 172.25.25.16 between 6:54 pm and 7:02 pm.

112.&#65533;On 29 May 2014, Mr Giacobbe's workstation (DBX-ANS-1) again attempted to contact to IP 172.25.25.16 between 08:24 am and 08:25 am.

113.&#65533;As recorded above, IP numbers 172.20.0.24 and 172.25.25.16 were used in conjunction with accounts "clsadmin", "spsadmin" and "dxbbackup" after 29 May 2014 to gain access to the Graciela IT system and on 21 June 2014 to sabotage it.

114.&#65533;I accept the undisputed evidence of Senior IT Analyst that: (i) the IP number 172.25.25.16 had last been assigned to a very old server (one of the company's first), which had been decommissioned and switched off in July 2013; and (ii) the device to which IP number 172.20.0.240 was allocated was part of the disaster recovery system in Thailand and was an inactive address.

115.&#65533;I find on the evidence that the existence of IP numbers 172.20.0.24 and 172.25.25.16 was unknown to the Graciela IT team. It is not disputed that they were not mentioned in Mr Giacobbe's handover notes.

Attempt to contact IP number 172.20.0.240 on 21 June 2014

116. Graciela's expert witness's forensic examination of Mr Giacobbe's workstation revealed that it had not been used after 29 May 2014 until it was employed in an attempt to access IP number 172.20.0.240 at 7:17 pm on 21 June 2014, at which time Mr Giacobbe was at Graciela's office apparently to assist in the recovery of the lost data.

117. Mr Giacobbe did not deny that he was at Graciela's office at 7:17 pm on 21 June 2014 and that his workstation was made available to him but he denied in cross-examination that it was he who used his workstation in an attempt to connect to IP number 172.20.0.240.

The usability of the "clsadmin", "spsadmin" and "dxbbackup" user accounts to achieve remote access to the Graciela IT system

118.&#65533;It was the evidence of Graciela's expert witness and Senior IT Analyst that the Graciela virtual private network ("VPN") uses "split tunnelling" which allows a remote VPN user to access the internet at the same time as the user is accessing resources on the VPN. In this way, a user can connect to file servers, database servers and other servers on Graciela's network through the VPN connection by allocating a Graciela internal IP number to the accessing device. At the same time, the user can access the system through an alternative IP number allocated to the user's machine.

119.&#65533;In cross-examination in answer to a question how Mr Giacobbe could have had remote access to the Graciela IT system after 29 May 2014, Graciela's expert witness explained that "the Active Directory gives permission to people with certain accounts to come in to Graciela from outside. We know from witnesses and from the interview of Mr Giacobbe that "spsdmin" could do so. Looking at the . the user of the Active Directory, we can see that "spsadmin" is in a container folder named "location global". Therefore other accounts in that will also have access from the outside. "Clsadmin" is in the same container".

120.&#65533;This evidence of Graciela's expert witness was not challenged or disputed.

121.&#65533;It was Mr Giacobbe's case until a fairly late stage in his cross-examination that the user accounts "clsadmin", "spsadmin" and "dxbbackup" could not be used to gain remote access to the Graciela system because they were Graciela internal IP addresses and accordingly could not be directly utilised or connected to from outside the company premises.

122.&#65533;To begin with Mr Giacobbe stoutly adhered to this contention but it was then put to him that if this were true, whoever carried out the attack on 21 June 2014 using "clsadmin" would have had to be present in Graciela's office pretty much all night on 21 June 2014. At this point Mr Giacobbe&#65533;stated that "clsadmin" could be used remotely if the user had first connected to system using a user account with VPN access enabled on it. He also confirmed that he was not suggesting that whoever perpetrated the incident must have been in the office all night on 21 June 2014.

123.&#65533;In light of: (i) the evidence of Graciela's expert witness and Senior IT Analyst referred to above in paragraphs 118-120 above; and (ii) Mr Giacobbe's admission that "clsadmin" could be used remotely if used in the right way, I have no hesitation in finding that the user accounts "clsadmin", "spsadmin" and "dxbbackup" could indeed be used remotely to access Graciela's IT system as Graciela has contended at all material times.&#65533;

THE INTERVIEW

124.&#65533;As mentioned above, Mr Giacobbe was interviewed by Graciela's expert witness on 7 August 2014. The interview was recorded and a transcript was in evidence at the trial. Mr Giacobbe attended the interview voluntarily.

125.&#65533;In the course of the interview, Graciela's expert witness reviewed the many factors which he maintained linked Mr Giacobbe to the attack on the Graciela IT system and accused Mr Giacobbe of having perpetrated the attack, to which Mr Giacobbe responded with neither a protest of his innocence, nor an admission that he was the culprit but instead insisted he was telling Graciela's expert witness what he knew and reiterated the help that he claimed to have given to recover the lost data.

MR GIACOBBE'S CASE

126. Mr Giacobbe's case is fully set out in his two witness statements. In these statements he denies that he was responsible for the sabotage of Graciela's IT system, maintaining that he did not access the system on any occasion in the period after his departure from Graciela on 29 May 2014 down to his return to the office in the evening of 21 June 2014.

127.&#65533;In summary form, in addition to the contentions and evidence of Mr Giacobbe already referred to above, his contentions are as follows:

(a)&#65533;He had a very limited knowledge of the networking aspect of Graciela's servers and other networking equipment.

(b) His account passwords had been re-set on his departure so that he was completely removed from and could not access the Graciela IT system after his departure on 29 May 2014.

(c)&#65533;The system could have been attacked by a Graciela insider or by an external consultant who had acquired knowledge of the "clsadmin", "spsadmin" and "dxbbackup" user accounts and the passwords thereof.

(d)&#65533;Since the VPN logs were deleted, Graciela cannot prove who had attacked the IT system.

(e)External consultants had been given full privileges and access to the IT system over time and therefore had access to the internal systems from their offices via VPN.

(f)As for Graciela's allegation that Mr Giacobbe used the IP number 172.25.25.16 before 29 May 2014, in preparation for the handover, he must have gone through all the servers and tried to connect to all (old and new) of them.

(g)In the period March - May 2014 Emitec was assisting Graciela in installing and upgrading the old backup system and were given access to the "dxbbackup" account.

(h)External consultants used the "clsadmin" account to log onto the system and Mr Giacobbe's use of the account was within his job profile.

(i) Members of the Corporate Communications team, knew of and used the "spsadmin" account.

(j) Mr Giacobbe was not the only one who knew the system's passwords; the IT team knew them and some were stored on the RDC manager. Accordingly, Mr Giacobbe was not required to remember all the passwords.

(k)The handover notes were sufficiently detailed and thorough. Mr Giacobbe believed that the notes would be scrutinised by Graciela who would raise any omissions from the notes.

(l)There was nothing strange or unusual about Mr Giacobbe's behaviour when he returned to the Graciela office to help recover the lost data.

(m)The Graciela IT system was not secure and was vulnerable to attack.

(n) Mr Giacobbe denied the alleged motive he had for the attack, namely that it was a response to his having been passed over as Graciela IT Team's replacement that would allow him to show himself as a saviour of the company.

THE EXPERT EVIDENCE OF MR DINESH BAREJA

128.The expert witness called by Mr Giacobbe was Representative who has worked for many years as an information security consultant and investigator into digital information security incidents. Amongst the positions he has filled are: (i) Chief Surveillance Advisor, Jharkhand Police - Cyber Defence Research Centre (Special Branch), Ranchi, Jharkhand (India); Principal Consultant, CSI Consulting Inc., Toronto (Canada); Principal Consultant, Secure Matrix Pvt Ltd, Mumbai (India).

129. security consultant is based in Dubai. He left it to his team in India to examine the event logs relied on by Graciela's expert witness that had been disclosed by Graciela in the proceedings. The examination was not carried out until after the service of his First Report.

130.I have dealt with security consultant's Third Report above. His first two reports effectively reiterated Mr Giacobbe's Defence and proceeded on the basis that what Mr Giacobbe said there was true. The First Report responded to a preliminary statement of findings produced by Graciela's expert witness on 28 August 2014 as part of his investigation. Graciela's expert witness's report as an expert witness was not served until after security consultant's First Report had been served. The principal conclusions security consultant reached at the end of his First Report were: (i) the breakdown of the Graciela IT system was a systemic risk waiting to happen; (ii) the absence of the VPN logs (the DHCP, DNS and Core Switches and Cisco networks logs) meant that Graciela had no proof to establish its claim against Mr Giacobbe; (iii) the failure of various of the Graciela team members to practise security hygiene and their common use of credentials had led to a situation where anyone could use any other person's machine or username-password; and (iv) the incident on 21 June 2014 appeared to be the result of a big error committed by some team member.

131. security consultant's Second Report responded to Graciela's expert witness's First Expert Report along the lines of his (security consultant's) First Report. In particular, he maintained that Mr Giacobbe could not have gained access to the Graciela IT system after he had left the company on 21 June 2014 and all users at Graciela's office had free access across the networks.

132.It was security consultant's opinion that: (i) during a handover there is mutual responsibility on both parties to enable a complete transition; (ii) in view of the overwriting by Mr SAM of the backup data during the recovery period, it is incorrect to attribute any sort of malicious intent to Mr Giacobbe in not sharing encryption keys which were never in his possession and basing this demand on a system error message that can be traced to a mistake by an external consultant.

133.In cross-examination, security consultant conceded that in reaching the conclusion expressed at the end of his First Report that Graciela's loss of data was the result of a big error he had not considered the evidence provided by the event logs studied by Graciela's expert witness that had previously been made available through disclosure. And this was despite that fact that in his preliminary statement of findings, Graciela's expert witness had stated that Windows Event Logs for 2014 had identified suspicious logging activity between March and June 2014 linked to IP numbers 172.25.25.16 and 172.20.0.240 and "clsadmin", "dxbbacup" "spsadmin" and the IP number for Mr Giacobbe's computer 172.25.26.29.

134.Indeed, Mr Giacobbe's expert witness conceded that not a single one of his conclusions was based on forensic evidence. Instead he had built an image in his mind of what had transpired at Graciela with the IT team and the system growing organically.

135. Mr Giacobbe's expert witness also frankly and very properly conceded that where he made factual statements about the Graciela IT system and its operation, for instance the statement that clsadmin account could not be used remotely, he was relying on what he had been told by Mr Giacobbe.

136. Mr Giacobbe's expert witness also agreed that Graciela's expert witness's attack timeline was accurate and went on to state that Mr Giacobbe had had "God rights" when employed by Graciela in that he had domain administrator rights by which he could change the privilege

settings - the things a user is allowed to do on the system - in any way he wanted on any account.

137.&#65533;In addition, Mr Giacobbe's expert witness accepted that once a user gained remote access to the Graciela network, he could use internal IP addresses to access the different parts of the system.

CONCLUSIONS

Factual culpability

138.&#65533;In my judgment, notwithstanding the absence of evidence as to which particular computer was used to carry out the attack, the evidence and findings set out above in paragraphs 45 - 137, constitute strong and convincing proof that satisfies the civil standard of the balance of probabilities that it was Mr Giacobbe who sabotaged Graciela's IT system.

139.&#65533;I accept Graciela's expert witness's opinion that the 21 June 2014 attack was not perpetrated by an outsider (or outsiders) but by an insider.

140.&#65533;The user account "clsadmin" was used on 21 June 2014 to: (i) delete Fin2 (Graciela's financial systems database) [05:27 am]; shut down the SOGNO domain controller [06:07 am]; (iii) shut down the Beta domain controller [06:15 am].

141.&#65533;On 27 May 2014, two days before he parted company with Graciela, Mr Giacobbe used "clsadmin" to access the Graciela IT systems' domain controllers and the Disaster Recovery server; in particular at 4:45 pm the "clsadmin" account was used to make multiple connections within a few seconds of each other to six disaster recovery servers. As Graciela's expert witness observed in his First Report these mirrored the sabotage method and were unnecessary for the fulfilment of Mr Giacobbe's daily duties.

142.&#65533;And, as recorded above in paragraphs 90 - 91: (A) on 28 May 2014 the "clsadmin" account was used from Mr Giacobbe's work station to access the Zeus backup server, the Zeta2 and the Beta domain controller; and (B) on 29 May 2014, the "clsadmin" account was used from Mr Giacobbe's workstation to access the Zeus backup server and the Beta domain controller. There can be no doubt in my view that it was Mr Giacobbe himself who used the "clsadmin" account on these occasions on 27, 28 and 29 May 2014. This is because only Mr Giacobbe knew the password for the "clsadmin" account and the occasions all took place during office hours, so that if another member of the IT team all of whom worked from the same table, had dared to use Mr Giacobbe's computer, he would have been quickly spotted doing so.

143. Mr Giacobbe also created the "clsadmin" account on Ptolemy 1 on 6 May 2014 and, as recorded in paragraphs 68 - 72 above, that account was used on a number of occasions to access Ptolemy 1 between 4 and 21 June 2014. In particular, "clsadmin" was used to run a Robocopy file on Ptolemy 1 using the Task Controller program, after which data was copied onto Ptolemy 1 on 18, 19 and 20 June 2014.

144.&#65533;No-one within Graciela knew of the "clsadmin" account. The workstations of Senior IT Analyst and Technical Support Analyst had never used this account. Emitec knew of the existence of the "clsadmin" account but they did not know the password. Mr Giacobbe did not disclose the account in his handover notes. This in my judgment was a deliberate act. He knew that following his departure from Graciela the passwords on his own company account (Graciela\Giacobbe's) and the main administrator account (Graciela\administrator) would be changed and so he suppressed the existence of the "clsadmin" account (whose password of course he knew) so that he could use the account after his departure to sabotage Graciela's IT system.

145.&#65533;On 21 June 2014: the "dxbbackup" account shut down Zeus (Graciela's Symantec Backup Exec system); and the "spsadmin" account was used to access Zeus at 06:03 am and to shut down the Alpha domain controller. Previously, on 3 May 2014, "spsadmin" was used by Mr Giacobbe to access the Graciela IT system (Seti04). This latter use had nothing to do with his normal duties.

146.&#65533;As recorded above in paragraphs 101 - 103 above, the "spsadmin" account was used: (i) on 4 June 2014 to access Zeus; (ii) on 9 June to access Ptolemy 1; and (iii) on 13 June 2014 to access Zeus and Seti04.

147.&#65533;No-one in Graciela knew of the "spsadmin" and "dxbbackup" accounts. They had never been used on the workstations of Senior IT Analyst and Technical Support Analyst. They were not disclosed in Mr Giacobbe's handover notes. It is fanciful to suggest that a third party outsider would have known of these accounts and their passwords and that the accounts continued to be available for undetected use after Mr Giacobbe's departure.

148.&#65533;As recorded in paragraphs 92 - 95; 100 - 104; 107 - 108 above, the IP numbers 172.20.0.24 and 172.25.25.16 were used in conjunction with the accounts "clsadmin", "spsadmin" and "dxbbackup" after 29 May 2014 to gain access to the Graciela IT system and on 21 June 2014 to sabotage it.

149.&#65533;As I have already found (see paragraphs 118 - 123 above) those accounts could be used to access remotely the Graciela IT system.

150. Mr Giacobbe attempted to connect to IP address 172.25.25.16 on 27 May 2014 and on 29 May 2014, his last day at Graciela. As Mr Giacobbe well knew from his extensive knowledge of the Graciela IT system: (i) the IP number 172.25.25.16 was inactive having last been assigned to a very old server switched off in July 2013; and (ii) the IP number 172.20.0.240 was also an inactive address having been originally allocated to part of the disaster recovery system in Thailand.

151.&#65533;No-one within or without Graciela other than Mr Giacobbe was in a position to know of the availability of the IP numbers 172.20.0.24 and 172.25.25.16 out of the thousands of IP numbers within the Graciela IT system. Nor was anyone other than Mr Giacobbe in a position to know that these IP numbers could be used without a conflict occurring with other IP numbers, which can happen when two computers on a local area network have been assigned the same IP number.

152.&#65533;On 21 June 2014 at 7:17 pm when Mr Giacobbe was back in the Graciela office ostensibly helping to reactivate the Graciela IT system and recover the deleted data, his Graciela workstation was used in an attempt to access IP number 20.0.240. I have no doubt that it was Mr

Giacobbe who made this attempt. I am also in no doubt that it was no coincidence that he tried to access IP number 172.20.0.240, this being the IP number from which: (A) the "spsadmin" account was used to access: (i) Zeus on 4 June 2014; (ii) Ptolemy 1 on 9 June 2014; (iii) Zeus and Seti04 on 13 June 2014; (iv) Zeus and Alpha domain controller on 21 June 2014: (B) the "clsadmin" account was used to access: (i) Ptolemy1 three times on 9 June 2014; (ii) Ptolemy 1 on 17 June 2014; (iii) Ptolemy 1 on 21 June 2014: (C) the "dxbbackup" account was used to access: (i) Zeus on 9 July 2014; (ii) Zeus on 10 June 2014; and (iii) Zeus on 13 June 2014; (iv) Zeus (Symantec Backup Exec System) on 21 June 2014.

153. As recorded in paragraph 62 above, on 7 April 2014 the encryption key and passphrase for Graciela's backup system was changed. I accept the evidence of Senior IT Analyst that neither he nor Technical Support Analyst, the other two members of the IT team, made these changes.

154. The backup system was Mr Giacobbe's responsibility. He alone had the necessary knowledge to make these changes. On the evidence before me I have no doubt that it was he who made the changes and that he deliberately failed to disclose them in his handover notes. His defence that he did not know the encryption key or the passphrase and his reliance on the overwriting on the system during the recovery operation do not hold water, for they ignore the facts that: (i) the encryption key and passphrase were indeed changed on 7 April 2014; (ii) the backup system was his responsibility; (iii) there is no tenable basis for believing that anyone else, whether within or outside Graciela, made the changes.

155. Almost all of the Graciela data that was deleted on 21 June 2014 had been copied onto Ptolemy 1, and remained on that invisible server after the attack. Mr Giacobbe admits that it was he who created Ptolemy 1 and that before his departure from Graciela he had migrated data from the old servers (Ptolemy) to this new virtual server and that this process was on going at the time of his departure. In accessing Ptolemy 1 prior to his departure, Mr Giacobbe used the "clsadmin" account. As recorded in paragraphs 69 - 73; 102 above, Ptolemy 1 was accessed after 29 May 2014 numerous times using the "clsadmin" and "spsadmin" accounts, neither of which was disclosed by Mr Giacobbe in his handover notes. During this period, Robocopy was used to copy further data onto Plotemy 1. Forensic traces of the use of Robcopy prior to 29 May 2014 were found on Mr Giacobbe's workstation. No such traces were found on the workstations of Senior IT Analyst and Technical Support Analyst. Although what had been copied onto Ptolemy 1 by the time Mr Giacobbe left Graciela was not the whole of Graciela's data, a significant amount of the data had been migrated to Ptolemy 1, including Middle East benefit packages, Graciela salary review and settlements, asset register reconciliation, sovereign finance and Indian banks.

156. Ptolemy 1 was unknown to anyone within or without Graciela. Mr Giacobbe listed in his handover notes four other test servers and three "Interaction" servers but he deliberately, as I have found, failed to disclose in those notes Ptolemy 1's existence. Mr Giacobbe also deliberately made no mention of Ptolemy 1 to the recovery teams after he returned to Graciela's office ostensibly to help in recovering the deleted data.

157. Mr Giacobbe's secret creation of Ptolemy 1, his secret copying onto Ptolemy 1 of almost all of the data deleted in the attack and his failure to disclose Ptolemy's existence in his handover notes and when he returned to Graciela's office after the attack, is very powerful evidence against him.

158. The attack on the Graciela IT system targeted Graciela's most vital data both at the Dubai office and at the recovery site in Thailand. This plainly shows, as Graciela's expert witness opined, that the perpetrator had an intimate knowledge of the system. Mr Giacobbe had such knowledge. On the evidence before the court there is no reasonable doubt but that he was the perpetrator.

159. Reliance was placed by Mr Giacobbe's expert witness on what he said were serious shortcomings in the Graciela IT system's security in support of his view that the 21 June 2014 incident was a big accident. Although the security of the system could have been improved, it is clear from the evidence of Senior IT Analyst that it was not nearly as bad as asserted by Mr Giacobbe's expert witness. But in any event, even if there were a serious lack of security, Mr Giacobbe's expert witness's point goes nowhere because the evidence I have rehearsed at length in this judgment is consistent only with the attack having been carried out by an insider.

160. The establishment of Mr Giacobbe's role in the attack on Graciela's IT system does not depend on the proof of a motive for the attack and I make my finding that it was Mr Giacobbe who sabotaged Graciela's system independently of any consideration of motive. That said, it is inconceivable that he did not have a motive for the attack and as to that I tend to the view that he carried out the attack in order to punish Graciela for not appointing him to replace Graciela IT Team, whilst at the same time giving himself the opportunity of appearing to be Graciela's saviour when, having been called in to help as he correctly predicted he would be, he "discovered" Ptolemy 1.

Mr Giacobbe's evidence

161. It follows from the above conclusions that Mr Giacobbe's denials in his evidence that he was the perpetrator were knowingly and dishonestly false. He also knowingly gave false evidence when he at first denied that he had copied corporate data from his second hard drive (see paragraph 67 above). Hence my conclusion expressed in paragraph 8 above that Mr Giacobbe was an unreliable witness whose evidence I was not going to accept unless it was corroborated by the oral testimony of the Graciela witnesses or by other reliable evidence.

Legal culpability

162. Article 41 of DIFC Law No. 5 of 2005 (the "Law of Obligations") states:

> "(a) A defendant is liable to another person if he wrongfully interferes with property in which the other person has an interest such that the other person suffers loss.
>
> (a) A defendant interferes with property if:
>
> ...
>
> (b) he deals with or (in respect of property as to which he owes a duty of care) neglects the property so that it is destroyed or damaged.
>
> ...

(c)	A defendant's interference is wrongful if it occurs without the permission, express or implied, of the person with an interest in it.

163.	By sabotaging Graciela's IT system in the manner I have described, Mr Giacobbe wrongfully interfered with Graciela's property under Article 41. Dr Al Kabban submitted that, assuming Mr Giacobbe had carried out the 21 June 2014 attack, his actions were not covered by Article 41 because he had not used or acquired Graciela's information to cause damage. I reject this submission. In my view the sabotage inflicted on Graciela's IT system by Mr Giacobbe could not be a plainer instance of someone interfering with the property of another so as to cause that other person to suffer loss.

164.	Pursuant to Articles 23, 24, and 25 of the Law of Damages and Remedies (DIFC Law No 7 of 2005), Graciela has a right to damages to compensate it for its losses resulting from Mr Giacobbe's breach of Article 41 of the Law of Obligations. The measure of those damages is that sum of money which would put it in the same position as it would have been in if it had not sustained the wrong committed by Mr Giacobbe.

Loss and damage

165. Graciela claims loss and damage in the sum of USD 690,533, calculated as follows:

Description	**Invoice (USD)**
McAfee's costs for restoring the IT System and investigating the incident	189,750
Network Rebuild	20,926
Network Rebuild Contractors' Fees	62,605
Indirect costs	417,252
Total	690,533

166. Details of the first four heads of loss were given in evidence by Graciela's CFO. "Network Rebuild" is a reference to the emergency servers that Graciela purchased following the 21 June 2014 incident. In my judgment, there is no basis for requiring Graciela to give credit for the value of these emergency servers: the cost involved does no more than to put Graciela back in the position as near as may be to that obtained before the attack.

167.	"Network Rebuild Contractors' Fees" refers to consultancy costs incurred to engage the appropriate contractors with relevant expertise to build the emergency servers in an expedient manner.

168.	"Indirect costs" refer to the value of estimated Graciela employee time incurred in dealing with the attack or its effects, which could have been spent elsewhere. The value of this time was calculated by reference to the relevant employee's salary and the proportion of the relevant employee's contractual time engaged.

169.	Mr Sheriff believed that the personnel identified in the table below had spent the corresponding proportion of their contractual time in dealing with the attack or its effects. He testified that these costs cover the period immediately after the attack and do not cover the indirect costs Graciela has suffered due to the extensive management time involved in preparing its legal case.

Personnel engaged in response to Attack	Period engaged	Proportion of time engaged for relevant period
IT Team:		
Senior IT Analyst	25 weeks	100%
Technical Support Analyst	25 weeks	100%
Ryan Smiley (from 16th July)	21 weeks	100%
Ms Representative	25 weeks	100%
Mister	12 weeks	50%
Graciela's CFO	12 weeks	50%
Graciela's CEO	6 weeks	20%
Lost productivity as a result of not having access to data/e-mails for remaining employees over a period of 6 weeks	6 weeks	25%

170. Mr Sheriff accepted that the indirect costs claimed are based on an estimate of the cost of wasted Graciela employee time in dealing with the incidents and its effects. He told the court that a conservative estimate had been used. In almost all cases where a claim is made for staff time spent in the aftermath of a wrongful act, the amount of time so spent will be based on an estimate rather than on specific time-keeping records. So long as the court is satisfied that the estimate is reasonable, as I am in this case, the estimate can found a recovery for staff time if the first two of the following three propositions propounded in the English Court of Appeal's decision in *Aerospace Publishing Ltd & Anr ("Aerospace") v Thames Water Utilities Ltd* [2007] Bus L.R. 726, the Court of Appeal are satisfied:

(a)	The claimant must adduce such evidence that it could reasonably adduce to show the extent of the diversion of staff;

(b)	The claimant must also establish that the diversion of staff caused significant disruption to its business;

(c)	If the first two elements can be established, the court may infer that, had the staff not been diverted from their usual activities, they would have directly or indirectly generated revenue for the claimant in an amount at least equal to the cost of employing them during that time.

171.	In my judgment, Graciela have satisfied the first two requirements promulgated in *Aerospace Publishing Ltd & Anr ("Aerospace") v Thames Water Utilities Ltd.* It has produced such evidence as it could reasonably produce of the diversion of staff and has established that the diversion of staff caused significant disruption to its business. Accordingly, it is open to me to find, and I do find, that had the staff not been diverted from their usual activities, they would have directly or indirectly generated revenue for Graciela in an amount at least equal to the cost of employing them during that time.

172.	The damages I award Graciela are therefore the total it claims, namely USD 690,533.

173.	Following delivery of this judgment, the parties are invited to serve written submissions as to costs and interest in accordance with the following timetable: (1) Claimant's first round of submissions to be served within 7 days of the hand down date; (2) Defendant's reply submissions 7 days thereafter; (3) Claimant's responsive submissions 7 days thereafter.

	

Issued by:

Natasha Bakirci

Assistant Registrar

Date: 11 November 2015

At: 10am