For this system of control study, I am going to investigate the Information Technology computer security system in Canary Wharf, London. Canary Wharf is a development on the Isle of Dogs, a complex of Stone- and glass-sheathed office buildings begun in the 1980s and a central 50-story skyscraper, One Canada Square, dominates it. In 1987 a rapid transit system, the Docklands Light Railway, was built to link the Isle of Dogs and other areas. Some of the systems in the database that I will focus on include:

- What the Information Technology defense systems are
- If the system is penetrated, what happens?
- The techniques developed and used to protect single computers and the network
- The different types of harmful effects to hardware, software and physical loss of data
- The simple and then more complex methods of data protection and an in depth look at the Data Protection Act. (See appendix one)
- The different types of tracing a hacker and what they use to infiltrate
- The most widely used system of decoding in the US which is Data Encryption Standard (DES) (See appendix two)

Fig. 1.1

I will look at all of these points in depth to find out what and why hackers break into systems especially as Canary Wharf is already the third rated terrorist attackers point in the world even through computer security as well as through physical security.
The system itself has a very secure network and e-mailing system. There has been 1,000,000 sterling pounds spent on the network and the security alone. Canary Wharf uses some simple measures to ensure (along with complex as well) that there security system are kept their own and are never infiltrated.

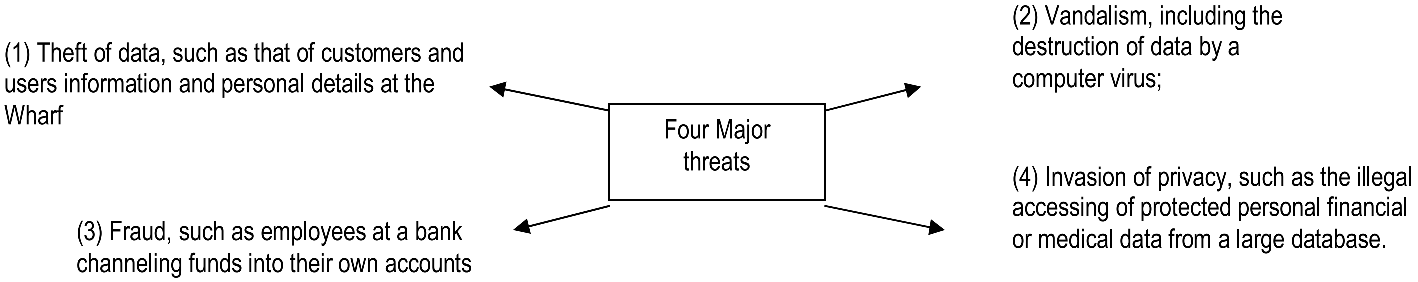
I am going to study this system because I am interested in computers and extremely intrigued as to how one man or women can infiltrate a system worth over 1,000,000 sterling pounds. These people are known as 'hackers'. (See appendix three) I would like to find out what the different systems measures are to protect the system are. I have thought of a few simple ones, none to complex:

- Passwords-either users passwords or some of a greater level
- Encryptions-why documents and such are in code so others can not read
- Authorisation-why only certain people are allowed on a whole network of files
- Firewalls-why some documents cannot even be viewed on a high security networks

By following and gaining information on this system, I hope to undertake an understanding of computer systems as a whole and why hackers are what they are and why even multi millionaires are feared of them just like the world.

I would like to find out about the different types of software such as Norton Anti virus, designed and made by Microsoft and see if Canary Wharf uses this system and type of virus program. I hope to have a greater understanding in this project, in the way of measures to stop hackers, the way hackers think, the views of some of the top people at Canary Wharf on hackers and why and how they can be stopped and found out. I will benefit from this, as I am extremely interested in computers and computer technology, this helps as I have some background knowledge. The Canary Wharf computer security system is obviously extremely well protected and well organized with the amount of expenditure and finance that was put into the system so I want to know where the majority of the money goes and what area is concentrated on and why.

The system at Canary Wharf has many measures to ensure a safe environment around the company with complex and simple measures. The protection of the computer systems at Canary Wharf and the information from harm, theft, and unauthorized use is a complex matter. Computer hardware is typically protected by the same means used to protect other valuable or sensitive equipment. At Canary Wharf this is namely- serial numbers, doors and locks, and alarms. The protection of information and system access at Canary Wharf, on the other hand, is achieved through other tactics, some of them quite complex.
The main aims of the system start with the security precautions related to computer information and access address four major threats:



Four Major threats

(1) Theft of data, such as that of customers and users information and personal details at the Wharf

(2) Vandalism, including the destruction of data by a computer virus;

(3) Fraud, such as employees at a bank channeling funds into their own accounts

(4) Invasion of privacy, such as the illegal accessing of protected personal financial or medical data from a large database.

The most basic means of protecting a computer system against theft, vandalism, invasion of privacy, and other irresponsible behaviors is to electronically track and record the access to, and activities of, the various users of a computer system. This is commonly done by assigning an individual password to each person whom has access to a system, which is one measure, used at Canary Wharf.

The computer system at the Wharf itself can then automatically track the use of these passwords, recording such data as which files were accessed under particular passwords and so on. Another security measure is to store a system's data on a separate device, or medium, such as magnetic tape or disks, that is normally inaccessible through the computer system also used. Computer security at Canary Wharf has become increasingly important since the late 1960s, when modems (devices that allow computers to communicate over telephone lines) were introduced. The proliferation of personal computers in the 1980s compounded the problem because they enabled hackers (See appendix three) to illegally access major computer systems from the privacy of their homes.

Security is particularly important for their computers that are connected to a communications network, because many users can freely access any computer. Entering an individual password authenticates authorized users, and then a computer usage fee is charged to the account of each user. Another measure used by the Wharf members is a user interface. The operating system provides a convenient interface between a computer and its users. In the case of batch processing with mainframes, for example, users may want to run their large programs only after midnight for several days until the execution of the programs is completed. In the case of personal computers and workstations, graphical user interfaces--such as windows and icons displayed on a monitor--are convenient for users. A window is a rectangular area on a monitor that displays a file or part of a file as the case on all computers including Canary Wharf's. On Canary Wharf's computers, many applications can be run concurrently, each in a different window. The main elements and what Canary Wharf uses to protect are as follows:

- Individual passwords
- Team passwords
- Firewalls
- Encryption
- No personal e-mails
- Anti virus software

How I will gather the information?

The information, which I have processed and explained on the page before, will be gathered and collected using a number of sources, both primary and secondary. My main source of information will be through an interview with the head of the I.T. department, a Mr. Paul Stubbs. I have processed a questionnaire, which he will answer along with a randomly chosen member of the department. This will help me complete the later section of the report. Other sources of information include, the Internet. The Internet however will be sensitive to questions that may exploit the Canary Wharf system in a way, which may danger the way in which they work. As information, which is sensitive, could be breeched using the Internet, it is not likely that explicit data will be shown. Another source could be Encarta, Britannica but again like the Internet, these may be hard to reach and question in certain areas. I may also use certain books such as the laws of computer security, data protection act etc.

Primary or secondary?

Below I have created a list of every source of which I am going to use and next to it is whether it is primary or secondary:

Internet - Secondary
Paul Stubbs- Primary
Random member of the IT department - Primary
Data Protection Act book- Secondary
Encarta-Secondary
Britannica- Secondary

As you can see from this, the main source of my information will be secondary; the main reason behind this will be that it is easier to get hold of. Secondary data however is not as reliable as primary data because it is second hand! This means as it passes hands, it can be changed and edited meaning it becomes not as reliable and biased. If I went to a website based, owned and created by a so called “hacker”, then he (based on research) will say that it is easy to break in etc. and that means that it is biased. Again if I asked a hacker (not saying I will!) he may either say that it was extremely hard, took hours, days etc. or he may say that it was easy. The outcome however will show the interviewer his facial expressions, telling them whether he is lying. I am obviously not going to be able to get an interview with a hacker but I have akready-accessed websites which I will explain about later.

The following two pages show a letter that I have written to Mr. Paul Stubbs following a phone conversation asking him to contribute in a way to this project that would be beneficial. The first page shows the questionnaire, which I have designed for my research. This has been answered by two of the staff, Mr. Paul Stubbs and Mr. Abal Mata. These filled questionnaires can be found at the back of this report in the appendices.

Paul please could you fill in this questionnaire and also get one other IT department member to fill in as well for my Product design coursework about the Canary Wharf Computer System:

Computer security

1: How many times has the system been infiltrated in the last three years?

2: What would you say is the strongest force that you have against hackers? For example, firewalls, passwords, encrypted data etc?

3: Being hypothetical, what part of the Canary Wharf system do you think a hacker would attack first if it happened?

4: Following on from question 3, what is the most vulnerable part of the system on the computers?

5: Would you say that the computers are “hacker proof” and secure on the network?

6: Do you have any virus software on your computers, e.g. Norton Anti-virus, bulldog etc?

7: On average how much have the company spent on securing the Canary Wharf system?

8: Would you say that your computer security system efficient; meaning is it fast, does it crash or freeze a lot, is it easy to use etc?

9: Would you say that your computer security system is effective meaning does it works properly in all areas and does it prove sufficient most of the time?

10: Not speaking on security terms now but are the computers easy to use, are they simple to follow and are they user friendly overall?

Is the system effective?

To ask whether the system is effective is a varied answered question. I have completed much research on the computer security at Canary Wharf and found that since 1991 they have had only two break-ins into the network however a further four into the e-mail system at the Wharf and on their network. So after this the next question to ask is how severe the damage was, what was the damage, how were it fixed and what action was taken.

The first break-in into the network was on the 11th November 1991. This was 11 years ago now so remember the technology was not at all as sophisticated as it now. In 1991 the network was based on a Macintosh D32 machine. Now most of us would have never heard of this, but according to Mr. Stubbs and I quote “this was the most sophisticated machine that we could purchase so we thought, hey, lets get this one”. Unfortunately I was not able to take any pictures of these machines, as they do not exist any more!

Back to the break in of 1991, the damage of this infiltration was not severe but only in the matter of three peoples record accounts being changed and one unfortunately. Now you can make your own judgment to whether this was severe. The company may not see it as a big deal as financial records were not lost changed or not even looked at. Or you may look at it from the point of view from the four employees, especially the users account that was deleted. Now this could be there livelihood, as well as all of their personal details, and could be compared to “someone looking at your phone, your emails or reading your diary” was the example Mr. Stubbs gave me. The hacker in this case was not found, caught or prosecuted and the infiltration lasted approximately 12 minutes, not long enough for him/her to access the details. The Macintosh machine was then “chucked” by the company after bad results and according to some staff “hard to use”. I asked Paul the question of was the system on the Macintosh efficient and his answer was “no, simple as that!”

The next machine to be used by the wharf was a Mesh Computers, not to hot in 1992 but have broaden and have come through now as one of the leading manufacturers in PC manufacturing.

“MESH Computers plc, winners of the 'Best PC Manufacturer' at the 2001 PCW Technology Awards have grown by doing what we do best: Offering award winning machines (over 200 since 1998), containing cutting edge components at the most competitive prices. With over 13 years experience, MESH is an established direct sales manufacturer with offices and showrooms throughout the UK supporting the consumer, business and educational sectors”. Quote from the website. (See appendix four)

This had two break-ins in the e-mailing system. These were not however classed as break-ins by Paul and he told me why.

“In 1997, an employee who was extremely computer literate and who was able to access many parts of the system others couldn’t thought maybe an e-mailing scam would be funny. What he did was to start up a program that when opened deletes every document in your hard drive finishing with .exe at the end. These are mostly word documents and text rather that pictures, photos, graphics and drawings. The file also, when opened sends itself to the outbox and then sends itself to every person in your buddies list. Now I was not happy when I found out that hundreds of word documents had been deleted and even more disgusted when I found that it was started by and employee, which I hired. I then analysed the damage and fired him, then the authorities were alerted and the matter was in their hands. It was amazing how easy it was to create though and to access other peoples drives. For me too easy so a new computer system had to be installed. And I no what your going to say, was the system effective, I believe so until the emailing thing occurred”

Paul and I then talked about the new system, which is still there at the present time. It is made by Dell computers, an extremely well known and globally trusted. It also runs on a windows system and Paul told me Windows XP Business Edition because of its excellent security system, something that is obviously important to a system like this one.

On the following pages are some pictures of the Dell computers that are used and the specifications. I also found out that certain members of the department use different machines to others but all run on the same network. This is all shown and explained below.

Dell Precision 350

Fig 1.2

This computer (according to Paul) is the main computer that all of the staff use. The specifications are below:

Fast Intel® Pentium® 4 Processor. 533 MHz front side bus, Dual Channel Rambus® PC1066 RDRAM® ECC or Non-ECC memory, Gigabit[1] Ethernet, USB 2.0 and ISV certified Open GL graphics for application-focused performance. This is now installed with XP and is extremely effective as installed is Norton Anti-virus and Bull Dog security. Both have the option to secure the PC as a unit.
You may also notice that a 3.5 floppy drive is I the unit. Canary Wharf have had the Dell machines customized allowing them o have no drive. This ensures that employees do not bring viruses into the system. Paul also thinks a flat tip monitor is better as it takes up less room, important at the Wharf.

Precision 450

This is the next machine I will show you
Fastest Intel® Xeon™ processor available but in a slim, size-optimized chassis.

Balanced 533 MHz front side bus and high-speed dual channel DDR 266MHz SDRAM memory for the most demanding power users working in space-constrained environments.

This machine is using by a Mr. Greg Fellows. Mr. Fellows's job description is web designer. This obviously means that he works with web pages meaning he will have many large pictures along with text and will need a fast machine with optimum specs. It also had cd-re writer and a floppy disk so he can take documents home and store them using the re-writer.

Fig 1.3

Fig 1.4

Precision 650

Fastest Intel® Xeon™ Processor Available

Balanced 533 MHz front side bus and high-speed Dual Channel DDR 266MHz SDRAM memory for blistering performance

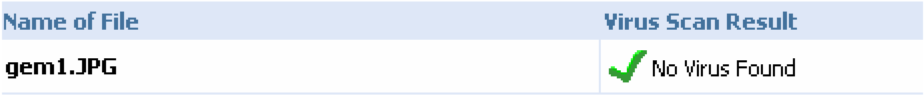
Right this is the top spec computer at the company and is available to managers of the departments. Paul has one and all the managers are all linked to the same network so work; financial information and such can all be exchanged and traded.

"These make an effective system when combined with XP, Norton anti-virus and Bulldog programs"- Mr. Paul Stubbs

Is the system efficient?

Efficiency comes down to how well the system works along with factors like usage, how easy and user friendly it is, and how fast the system e.g. virus programs, run. My interview with Paul helped me a lot in this section.

As Dell computers is an extremely well published, well known and well trusted brand, speed and efficiency in that sector is not really going to be a problem. So in this category, yes the system is efficient.
When you look into the fact is it user friendly then you either have to have a go yourself! Or ask a member of the staff as to what they think of the system. To get the best results and experience I decided to do both.
What happened was, Mr. Stubbs sent an e-mail to a neutral computer and it appeared with the message- " you have received an e-mail form an un-known sender, would you like to virus scan the document (recommended)". Then it showed a scan and a no button, I clicked scan and a message appeared allowing you to either scan it with Anti Virus or Bulldog, I selected Ant-virus. A bar with percentages appeared on screen and can not off been there for more than five seconds. Then a message (see below) appears.



Name of File	Virus Scan Result
gem1.JPG	✓ No Virus Found

Fig 1.5

Did you know that 1 in every 5 computers is infected with a virus? Don't become a statistic! Click here to find out how easy it is to help protect your PC

Fig 1.6

I was extremely impressed when this message appeared and admired how user friendly it was. The amazing point though was how fast it actually ran the virus scan, I was actually a bit worried that it had not checked it properly! As I said before, another way of seeing whether it is efficient was to ask an employee, someone who uses it every day. At the back of this report (see appendix), there is the filled in questionnaire explaining whether the user found the system easy to use.

All in all, I found the system both extremely efficient and there are no known break-ins since July 2002, I think that the system also proves effective.

What are the systems good points?
Where des the system fail?
For this section I have created a table (see below) showing the points of where the system excels on the left and where it is weak on the right hand side.

Systems good points	**Where the system is weak**
The system has many people working on it. This means that they can all see when their system ahs been infiltrated e.g. documents missing etc. This allows something to be done quickly.	The system has many people working on it. This point can also be turned against the user. Because so many users are using the system, then the damage can be huge if it is spread. This is why it is important that the system is never infiltrated.
The amount of money spent on the system is vast. This means that because so much money has been put into the system, the system has the latest hardware and the latest software. This technology allows Canary Wharf to keep up with what infiltrators knows and what knowledge they would have gained.	The fact that the information that's important is accessible to most workers. When I was looking around the system I found that one simple password was all you needed to access financial information and I thought this was a bit floppy in protection measures. An improvement has been shown later (see improvements to system)
The amount of techniques to stop infiltrators This means that the Wharf's system has many different measures; these include firewalls, password barriers and encrypted coding. These however are not least matched by the outstanding virus checking process, which the Wharf has in place. The virus check was so simple to use and the process was extremely simple. With Norton Anti-virus and Bulldog virus programs installed along with McAfee Virus protection in the development stage, Canary Wharf computers have extreme measures, which work throughout.	
The standard and speed of their computers Now although this does not have a direct effect of security, as the Wharf has the latest technology of the hardware that they use. By having Dell as their "sponsor" if you will, they particular have good after sales service meaning the computers will always being running efficiently and hardly ever down.	
The security of the e-mailing system This was probably one of the most impressive factors when I visited Canary Wharf was how easy the virus checking was when I received an e-mail. The Bulldog program was used for this. I also scanned the whole system by double clicking the Norton Ant-virus symbol, it was really that easy!	

How could your system be improved?

Right, I have made a list of recommendations shown below showing you what measures could be put in place and secured to make the system more effective ad efficient:

- Recommendation number 1:

The first recommendation and enhancement that I would make to the system a little bit more secure by using new technology. By making this statement, I mean adding a feature that would perosnallise each users workstation. There are many measures that could be put in place, and they are listed below:

Voice locking system: This means each station ahs a voice lock on it and can only be unlocked when wither a certain word is said and is said with that one voice. Now this would perosnallise every user and also not allows a physical break-in. There is still however the same chance of a break-in through hackers outside of the system, the same as the manual password protection.

Fingerprint access: This means each time a user logs onto the computer, instead of a password, the user has to place his or hers finger onto a plasma screen allowing the computer to identify the print and allow them to access or deny them. This would make the security extremely secure allowing the users to work with safety knowing that there is no way that any one would or could access there system.
Both of these ideas would work well (I recommend the fingerprint access) but would both cost a lot to install on the system and onto every single computer. It is something though which they may want to consider.

- Recommendation number 2:

Every single e-mail that is sent through the Canary Wharf system that is not text is sent straight into quarantine. Once the person has alerted you that they have sent e-mail, you have to ring up the IT Help desk (where I worked for work experience) and ask them to check it and forward it. This is because the helpdesk computers are neutral and have many virus programs. The problem with this is that it takes a long time to ring up, ask for it to be forwarded and then wait to receive it, must be extremely annoying if you receive a lot of e-mails.
What I propose for this problem is a have an individual quarantine for each computer or have a digital message appear on your screen when you have a message waiting there. This would make the system more efficient but keep it the same in effectiveness.

Has my study been effective?

From all of my research to all of the evaluation of this report, I think that my study has been extremely effective. I also got the chance to go up to Canary Wharf again and see every one from work experience! The day that I spent up there showed me what each user goes through with there e-mails every day and how they have to ring up when they receive an e-mail with an attachment on it. This was particularly funny when I was on Greg Fellows area (web designer) and as a web designer he obviously receives a lot of documents with images attached to them, he asked me to ring up for him and this was frustrating the amount of times he received one. (See above for recommendation)

Overall though I am glad that this system of control and protection was chosen because I got to learn how to protect a wide system used by many many users and make it as safe as possible. The report must have also had an effect on me because since visiting Canary Wharf I have downloaded Bulldog virus scan and installed it onto my computer allowing documents and the whole system to be virus checked. This means the study has been effective.

Mr. Stubbs has also asked to see my recommendations to this system so maybe in the near future you will see upon the market the Filmer Touch sensitive locking device compatible for all workstations, who knows if the study was that effective!