1. Contents Page
   1. Firstly, I’m going to mention some news stories involving data being lost or exposed
   2. I’m going to show some of the techniques we can use to secure & back up data
   3. I’m going to demonstrate how those techniques could have helped and show some of them in action
   4. And I’m going to end with 5 questions on data security that every tester should ask.
2. The first story is that of Marie Lupe Cooley
   1. She was employed as an assistant at the offices of Steven E Hutchins Architects in Jacksonville, Florida
   2. One day, while reading through the classified adverts she read a job advertisement that closely matched her own job. The duties were the same, and the contact details were those of her boss.
   3. Cooley thought that the job offer was for her job and that she was about to be fired.
   4. That Sunday, at 11pm she went to her employer’s offices, logged on to the network and deleted 7 years of architectural plans
   5. The damage was estimated at $2.5 million.
3. Part 2
   1. The irony was that the job being advertised was for her boss’s wife’s firm and she was not about to be fired after all.
   2. There was a problem. The files she deleted had not been backed up at all.
   3. Hutchins had to hire a specialist firm to reconstruct the files. When a file is deleted its name is removed from the lookup table but the segments in memory that held the files will still hold them until they are overwritten.
   4. But what if Cooley had known this and uploaded junk data to overwrite the segments?
4. The next person is Edison Chen
   1. Chen was a Canadian-born singer and actor working in the Hong Kong film and entertainment industry
   2. He sent his laptop in to be serviced and gained notoriety
   3. The technicians working on the laptop found literally hundreds of pornographic photographs of Chen with various female stars
   4. They immediately published these photos on the internet
   5. As a result of the scandal, Chen, aged just 27, had to announce his retirement in February.
5. Who knows who Francis Ford Coppola is?
   1. It was reported that he was trying to recover a computer stolen during a burglary
   2. The computer wasn’t valuable, but the data on it was. It contained a script Coppola had been working on for years.
   3. Coppola was aware of some of the risks and had backed the script up on an external Hard Drive.
   4. The thieves also stole the hard drive.
6. This story occurred in November 2007
   1. 2 CDs containing the banking details of 25 million Britons were posted to London from Newcastle
   2. The data was collected and posted by HM Customs and Excise, which is a branch of the UK’s Revenue Service.
   3. Somewhere along the route, the disks went missing and haven’t been recovered. 32 police officers were on the case at one point.
7. Who knows who Jeremy Clarkson is (host of Top Gear and a journalist)?
   1. Jeremy Clarkson did not believe the data could be used to hack the bank accounts.
   2. To prove it, he printed his own banking details in a British newspaper.
   3. Bad move. An ethical hacker was able to use the data and set up a direct deposit of £500 from his account to the Diabetes Foundation (a charity).
8. The last story is of Jerome Kerviel. Not data, but techniques could have helped
   1. Kerviel worked as a trader at Societe Generale in Paris
   2. His first job was working in the Back Office. He gave people network IDs, reset passwords etc.
   3. Then he became a Hedge Trader. A Hedge Trader bets against what the Main Traders think. Their job is to ensure that, if the Main Traders get it wrong, there is enough diversity in the bank’s portfolio to limit the damage.
   4. When Kerviel became a Hedge Trader, the bank failed to cancel his back office rights.
   5. Kerviel wanted to work on the main trades. To this end, he set up a number of trader personas and traded under them
9. Kerviel part 2
   1. At first, all went well. In fact one trade made 1.4 billion Euros for the bank
   2. Then the market turned. The subprime crisis in the States occurred.
   3. Kerviel’s deals went down, losing 5.8 billion Euros in all. You could buy 2 nuclear super carriers, over 27,000 Porsche 911 GT2’s (R2.6 million), more than 500,000 Yarises or Golfs or 4,200 R15-million houses.
   4. Kerviel is now on trial for fraud.
10. Now for the techniques
    1. The simplest technique is to use a backup server. A big co. can have a server at each of its offices. Hutchins could have used a home office. Data must be backed up at a separate location. Don’t use a main server as a backup server
    2. If a backup server is impractical, there are co’s that will back up data for a monthly fee.
    3. Break away at this point and show the user groups. Mention that this could have stopped Cooley.
    4. Encryption involves scrambling the bits (binary digits) making up a file. Demonstrate it in XP. Mention Edison Chen. There are also commercially available programs to encrypt data. Mention the banking data.
    5. Erasing data off old hardware before selling it. The US Department of Defense has old hard drives degaussed or destroyed. Xperien makes a digital shredder that deletes data beyond forensic recovery.
11. Control in action
    1. Folder named Budget and a document that needed a password to modify.
12. Questions to ask
    1. Are users prevented from editing or deleting data they shouldn’t?
    2. Are users prevented from accessing data unrelated to their job?
    3. If a user’s role changes, are any current access rights inappropriate to the new role revoked?
    4. Is all vital data backed up in a geographically separate location from the primary data source?
    5. When sensitive data is transmitted or stored what steps are taken to guard against exposure and corruption?