

# Errata

For years I worked at my English, to prove a point - the point was "Osborne can right a good report". It was hard work because, like anything that a person isn't naturally gifted at, it takes a while to gain the ability and keep it. And I felt I had something to prove, too many times skill-less bureaucrats point to a badly typed report from a technician and conclude that technical skills and business skills are mutually exclusive. One of the things I owe KPMG, was the testimonial that a report written by myself is worth thousands. Or more.

Unfortunately, these skills may have been taking a holiday or perhaps the editorial processes wasn't up to scratch, but my book has some shockers.

Please accept my most sincere apologies



**It starts on Page VII**

**I wrote in Line 20  
1995**

Played a part in two landmark legal cases:-

- Was KPMG 's security experts on the windup of a famous bank
- Expert witness on computer security in the cash-for-rides action (an extension of the Dirty Tricks campaign) between two major airlines. Misuse of the computer-held passenger lists was proved and an out-of-court settlement was reached in the UK

**Page 20**

**Last para**

Mark isn't a complete nerd – He is married to a wife that tolerates his behaviour and two fantastic kids that see him as an irresponsible older brother

**Should read**

Mark isn't a complete nerd – He is married to a wife that tolerates his behaviour and he has two fantastic kids that see him as an irresponsible older brother.

**Chapter 1 Page 4**



**Line 14**

Disadvantages of positioning the security team below the IT Director report include:

**Should read**

Disadvantages of positioning the security team below the IT Director include:

**Chapter 1 Page 8**

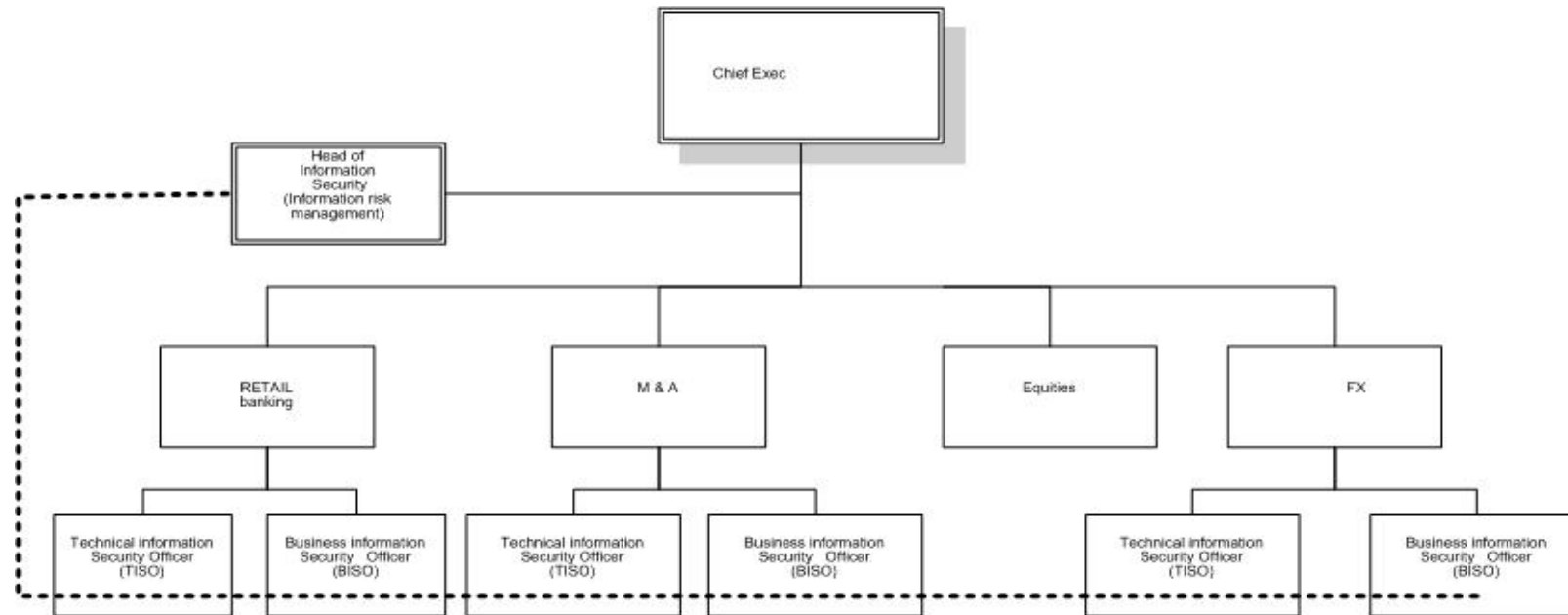
Because of the legal implication, evidence gathering, preservation and representation are paramount. Because of the specialist skills required to do this, often the team relies on external agencies to perform the bulk of these investigations.

**Should read**

The legal implications of evidence gathering, preservation and representation are paramount - and because of the specialist skills required to do this, often teams will rely on external agencies to perform the bulk of these investigations.



Figure 1.4 should be replaced by



**1<sup>st</sup> bullet**

getting it is your job whilst setting an example.

**Should read**

getting it is your job, whilst all the time setting a good example.

**Chapter 2 page 24**

**Line 27**

Live that experience a couple of times and you will soon understand the purposed of standards.)

**should read**

Live that experience a couple of times and you will soon understand the purpose of standards

**Chapter 2 page 37**

**Line 13** – desperately needed to be made *politically correct*, even if the meaning is lost as a result. Actually, I think many problems were introduced because it is traditional that the written word should not offend or provoke thought – or am I making a joke.



Flatly, it is his or her job

**should read**

Flatly, it is **NOT** his or her job

**Chapter 2 page 39**

**Line 18**

show that is just domain of tech support

**should read**

show that is **NOT** just the domain of tech support

**Line 27**

tell everyone it was great success.

**should read**

tell everyone it was a great success.

**Chapter 3 Page 53**



**Line 5**

or that of notary on a paper.

**should read**

or that of a notary on a paper.

**Chapter 4 Page 74**

**Line 5**

(12 jolly good people)

**should read unless your book has been censored by the political correct police.**

(12 good men and true)

I don't know about you, happy reader, but the flow of the text is so much improved by changing every single reference to "*he*" to the phrase "*he or she*" – ***NOT!!!***

**Chapter 4 page 86**



**Line 4**

we might need in

**should read**

into what is required in

**Chapter 5 Page 90**

**Line 8**

there was great feeling

**should read**

there was a great feeling

**Page 95 Line 10**

a list of controls that have been deemed not applicable

**should read**





a list of controls that have been deemed applicable and a list of those controls not applicable.

**Line 14**

Table 5.3 Example of Statements of Applicability

**should read**

Table 5.3 Example Scopes of Certification

**Page 96**

**Line 1**

Table 5.3 Example of Statements of Applicability

**should read**

Table 5.3 Example Scopes of Certification

**Page 98**

**Second bullet**



**should read**

a clearly defined risk analysis approach

a clearly defined risk analysis approach must be used

**Page 105**

**Line 2**

company system

**should read**

company's systems

**Line 24**

remove it.

**should read**

remove it from the MLPs.

**Chapter 6**



**Page 112 Line 10**

very large check

**should read**

very large cheque

**page 117 Line 13**

I know not

**should read**

I know nowt

**Chapter 8**

**page 146**

**bullet 6**

any address Web port

**should read**



any address any port

**Page 158**

**The title**

Commercial Firewalls

**should read to make it consistent with the other chapters**

For the Technically Minded

**page 160**

**last Line**

I am a deranged

**should read**



I am deranged

**page 161**  
**Line 3**

no sockets are

**should read**

sockets are

**Page 163**

**Line 10**

a wealth of experience managing routers.

**should read**

a wealth of experience in managing routers.

**Chapter 9**  
**page 179**  
**Line 26**

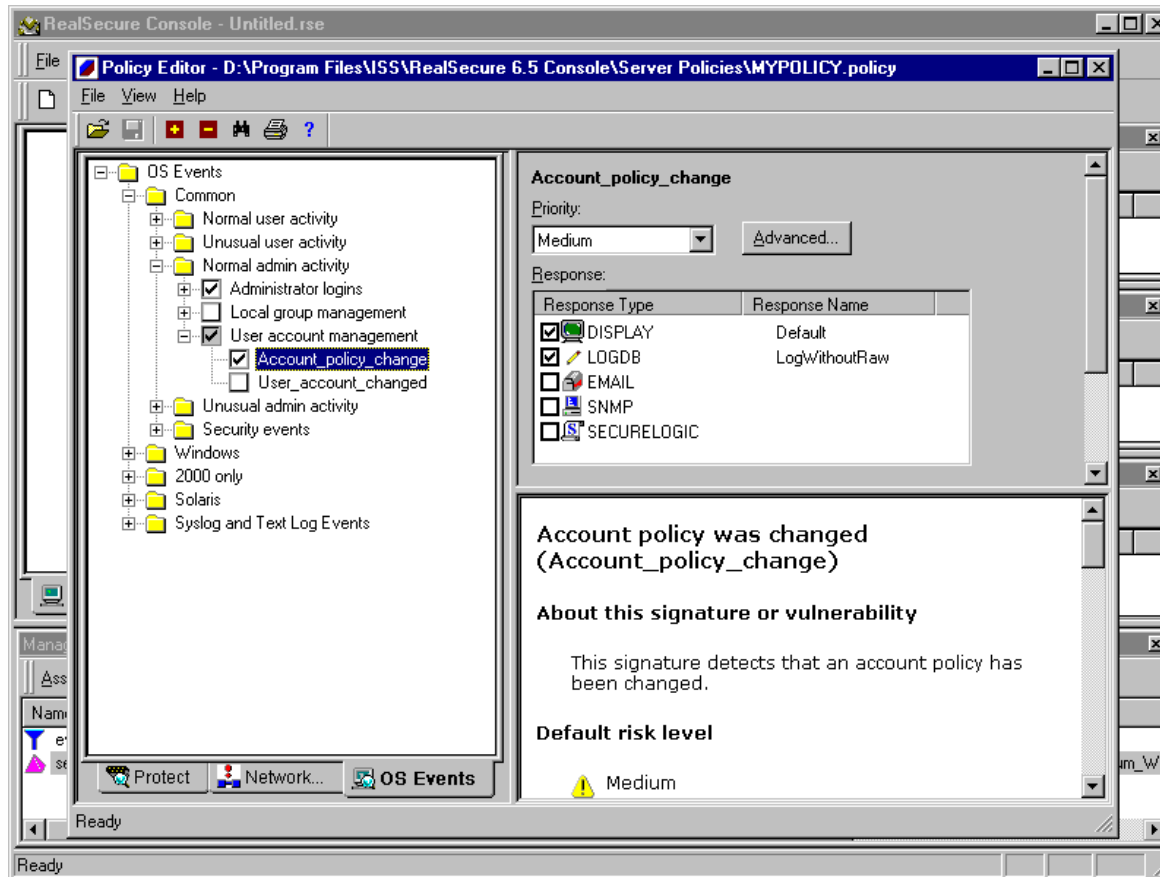
on intrusions

**should read**

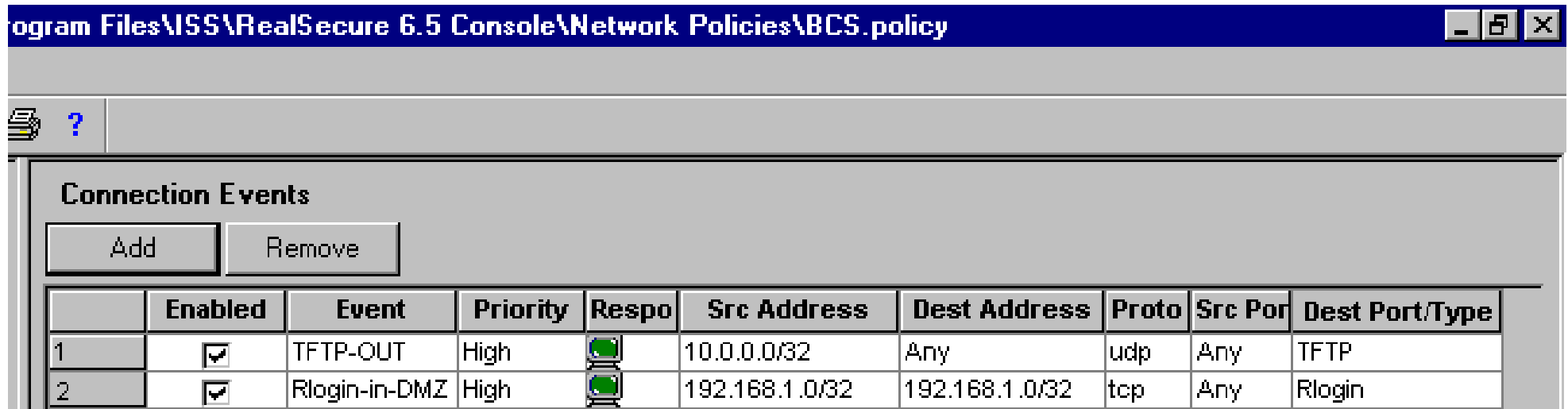
on attempted intrusions





Page 181 figure 9.1 – I cant read it, it should looks like



Page 198 figure 9.9 – I cant read it, it should looks like



The screenshot shows a window titled "ogram Files\ISS\RealSecure 6.5 Console\Network Policies\BCS.policy". Below the title bar is a toolbar with a question mark icon. The main content area is titled "Connection Events" and contains two buttons: "Add" and "Remove". Below these buttons is a table with the following columns: "Enabled", "Event", "Priority", "Respo", "Src Address", "Dest Address", "Proto", "Src Por", and "Dest Port/Type".

	Enabled	Event	Priority	Respo	Src Address	Dest Address	Proto	Src Por	Dest Port/Type
1	<input checked="" type="checkbox"/>	TFTP-OUT	High		10.0.0.0/32	Any	udp	Any	TFTP
2	<input checked="" type="checkbox"/>	Rlogin-in-DMZ	High		192.168.1.0/32	192.168.1.0/32	tcp	Any	Rlogin

The original text had some clever insets and call-outs so you could see the format of the screen – but also read the text. But these remain no more.



**Chapter 10**

**Page 213 Title**

IDS Deployment Methodology

**should read to make it consistent with the other chapters**

For the Technically Minded

**Page 218**

**Line 1**

methodology

**should read**

methodology in their product





**Chapter 11**

**page 236**

**Line 5**

in North

**Should read**

in the North

**Page 238**

**Line 22 table 11.1**

The classic situation

**should read**

The classic problem

**Line 29 table 11.1**



Arrangements are available

**should read**

Often commercial IPS support options

**Last 3 lines table 11.1**

All lines starting with “The reset” should have a bullet

**Page 247**

Example deployments

**should read to make it consistent with the other chapters**

For the Technically Minded

**Page 252**



**5 lines from bottom**

extensively:

**should read**

extensively. Example signatures are shown below:

**Chapter 12**  
**Page 257**

**first bullet**

in many companies

**should read**

in many countries

**Page 263**

Did I get ribbed for writing this, or what? – I don't know what happened.

**bullet six**



RST (or Xmas-tree) scan – Rarely used, not accurate but difficult to detect. This is similar to the SYN scan but uses a TCP reset.

### should read

Xmas-tree scan – Rarely used, not accurate but difficult to detect. This is similar to the SYN scan but has all the TCP FLAGS set (i.e. FIN, PSH, and URG). If the port is closed, a TCP reset will be sent. It is called Xmas tree because it has all the flags-set, all lights are burning, lighting the packet up like a Xmas Tree. See its poetic.

### Page 267

Here again, there are changes to the meaning of the book.

### First bullet

Resource overload These attacks intend to overload the resources (eg memory) of a target so that it no longer responds.

Was originally written to be a new paragraph followed by a series of bullets like

Resource overload – these types of attack are intended to overload the resources (eg memory) of a target so that it no longer responds: They include:

### bullet six



\* Other resource consumption attacks can include

Was originally written to be a new paragraph, to introduce a miscellaneous bunch of attacks, followed by a series of bullets.

Other resource consumption attacks can include:

### **bullet 11**

\* Out-of-band attacks These attempt to crash targets by breaking IP header standards

Was originally written to be a new paragraph followed by a series of bullets. I really don't get the point of running them all together like this.

Out-of-band attacks – These attempt to crash targets by breaking IP header standards:



**Page 268**

**bullet 1** - delete the line below as it is repetition

IP source address spoofing (land attack) – causes a computer to create a TCP connection to itself

**Page 276**

**Last Line**

I do not share this view.

**Was originally written to be**

So I have to categorically say I believe, in my opinion, this to be nothing short of ARSE.

**But probably should read.**

I do not share Denning's view.



Page 277

Line 7

Denning's book

**Should read (because it was only a short paper)**

Denning's paper

Chapter 13

Line 21 reads as

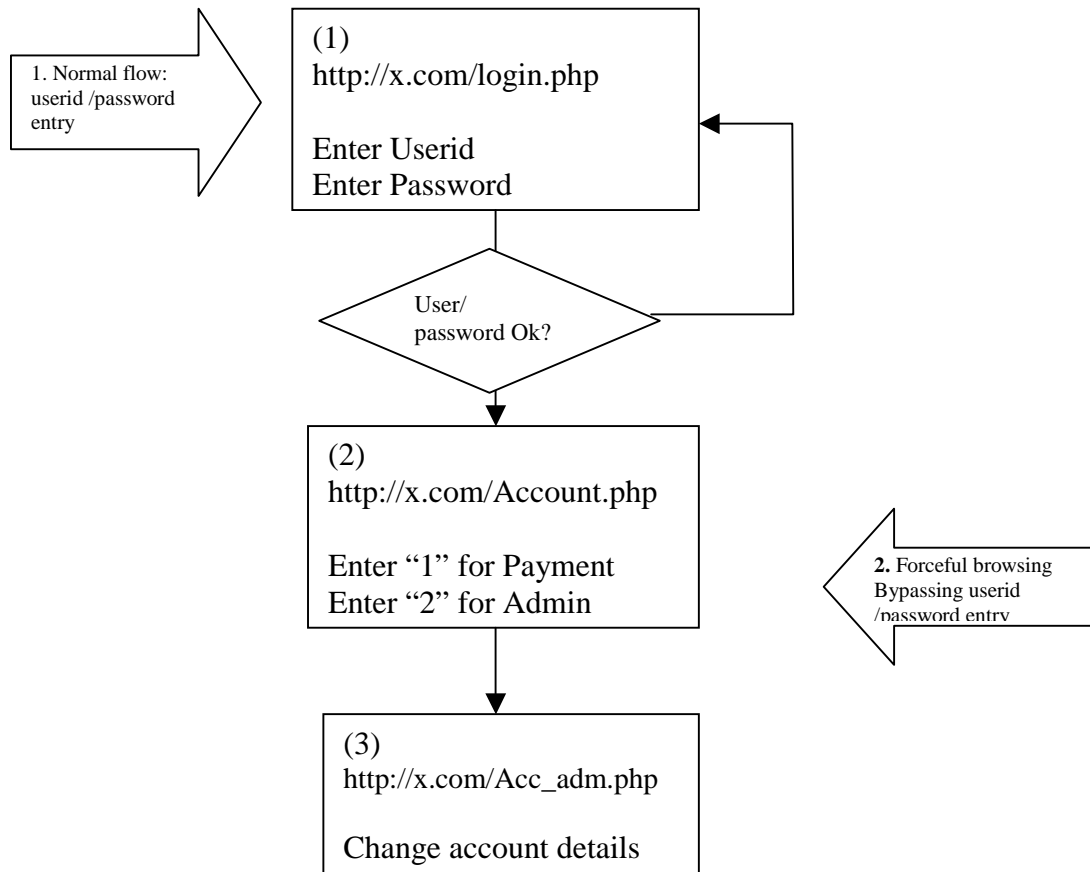
vulnerable:

**because the screen grab was meant to immediately follow it. Now that the picture has been moved and re-ordered, the sentence should be changed to :**

vulnerable.



Figure 13.10 should look like this





**Page 301**

**Line 2** reads

```
# line above looks for a stream containing the script directive – if spots #  
performs the defined action – block and alert in our case
```

should read

```
# line above looks for a stream containing the script directive – if spots it  
# performs the defined action – block and alert in our case
```

Config files and word wrap often don't make good bed fellows

-----

