PLUS – Cyber Liability

Alex Hamer
Cyber risks
Cyber risks
Security breach notification

- Data security – Data Protection Act, 7th principle
- Information Commissioner – no duty to notify security breach
- Citizens’ Rights Directive 2009
  - A compulsory notification regime
  - Limited to ‘serious’ breaches?
  - Proposals by end of 2010
Cyber risks

- The perception of a professional services firm
  - The perceived risk
  - Experience of the insurance market
Cyber risks – features

- A hybrid risk: PI, products and first party
- Predominantly a contract risk
- Liability principles still being developed
- Incidence of claims
- Jargon
- No standardisation – a developing market
Cyber risks – features
Cyber risks – features

- A hybrid risk: PI, products and first party
- Predominantly a contract risk
- Liability principles still being developed
- Incidence of claims
- Jargon
- No standardisation – a developing market
PLUS EUROPEAN CHAPTER: CYBER LIABILITY – A BROKER’S VIEW
Key Verticals

- Financial services companies
- Healthcare
- Merchants/retailers
- Hospitality and travel
- Professional services firms that have access to personal non-public financial or medical information
- Technology companies who provide services and solutions to the above
- Business Process Outsourcing/IT Outsourcing companies
- Telecommunications companies
- Staffing, charities and social service organizations, etc.
- Governmental entities
Direct Loss of Data Breaches—U.K. Voluntary Notification

- Costs reflect voluntary notification; regulatory exposure; reputation
- Average organizational costs - £1.68M.

### DATA BREACHES CONTINUE TO BE A VERY COSTLY EVENT FOR ORGANIZATIONS
*(Ponemon 2009 Annual Study of a Data Breach)*

<table>
<thead>
<tr>
<th>Cost</th>
<th>2007</th>
<th>2008</th>
<th>2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detection &amp; Escalation</td>
<td>£15</td>
<td>£11</td>
<td>£12</td>
</tr>
<tr>
<td>Notification</td>
<td>£1</td>
<td>£3</td>
<td>£7</td>
</tr>
<tr>
<td>Response</td>
<td>£15</td>
<td>£14</td>
<td>£17</td>
</tr>
<tr>
<td>Lost Business</td>
<td>£17</td>
<td>£32</td>
<td>£29</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>£48</strong></td>
<td><strong>£60</strong></td>
<td><strong>£65</strong></td>
</tr>
</tbody>
</table>
Data breach front-end, direct costs are a major component of loss.

Average direct costs average $6.65M. Variance by industry and if fraud/identity theft involved.

### Data Breaches Continue to be a Very Costly Event for Organizations

*(Ponemon 2009 Annual Study of a Data Breach)*

<table>
<thead>
<tr>
<th>Cost</th>
<th>2007</th>
<th>2008</th>
<th>2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detection &amp; Escalation</td>
<td>$9</td>
<td>$8</td>
<td>$8</td>
</tr>
<tr>
<td>Notification</td>
<td>$15</td>
<td>$15</td>
<td>$15</td>
</tr>
<tr>
<td>Response</td>
<td>$46</td>
<td>$39</td>
<td>$46</td>
</tr>
<tr>
<td>Lost Business</td>
<td>$128</td>
<td>$139</td>
<td>$135</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>$199</strong></td>
<td><strong>$202</strong></td>
<td><strong>$204</strong></td>
</tr>
</tbody>
</table>
Security and Privacy in An Outsourced World

- Business Associates/Partners
- BPO
- ITO such as IT programming/code maintenance
- Hosting, IT security management and support
- Accounting
- Customer relations
- Call center
- Customer support
- Fulfillment
- Telemarketing
- HR and Payroll
- Employee Benefits
- Data storage/repository
Important Contractual Developments – Service Providers, Processors, and Vendors

- **Beyond negligence to strict liability**

- **Expanded Contractual Indemnity Provisions** – all aspects of data breaches (civil claims, regulatory investigations and notification costs) – from clients and sponsoring banks

- **Due diligence and security requirements** – more detailed in contracts including triage/reporting of potential breaches

- **Insurance requirements** – specific requirements for professional/cyber insurance
Why should you transfer data protection risks through your own insurance program?

- Many functions are conducted by outside vendors and contractors who may lack insurance and assets to respond. What if the vendor makes a systemic mistake? What if they fail to purchase insurance or keep it? What if they are located in a country where this insurance cannot be obtained? What if the policy they purchased denies coverage or has inadequate limits?
- PCI (which is the credit card industry security standards) compliant companies have had their security compromised from processes lapse, human error, or criminal insider.
- No system can be designed to eliminate the potential for loss, as people and processes failures cannot be eliminated. Insiders may be perpetrators.
- Responsibility rests with the data collector/owner from a legal, regulatory perspective, and credit card association operating regulations.
- Investor fallout from uncovered losses with large claim and class action potential and major impact on brand and reputation.
- Traditional insurance does not cover security liability or adequately cover privacy risks – we provide gap analysis assistance to support this conclusion.
What the Hack?

Ken Munro
Penetration testers

‘Good’ hackers: ‘ethical’ hackers
   Paid by organisations to see how good (or bad!) their security is

Developers and network engineers with a deep interest in breaking things

Have never been to the ‘dark side’, despite it probably being a whole lot more profitable!
What are we up against?
Comedy defacements

The Fluffy Bunny strikes again!
The Fluffy Bunny wants a McBoobie
The Fluffy Bunny wears flip-flops
The Fluffy Bunny thinks Canada is good
The Fluffy Bunny thinks Canada is NOT to blame
The Fluffy Bunny smells real good!
The Fluffy Bunny likes egg fried rice!
The Fluffy Bunny is big n scary!
The Fluffy Bunny is small n cuddly
The Fluffy Bunny has a pancake ass!
The Fluffy Bunny shops at baby gap
The Fluffy Bunny says no to yayo!
The Fluffy Bunny eats fluffy sheep!
The Fluffy Bunny would like to take this moment to thank jeeves
The Fluffy Bunny wasn't born yesterda
The Fluffy Bunny likes to make little bunnies
The Fluffy Bunny does not eat at McDicks
The Fluffy Bunny is a liar
The Fluffy Bunny does not like pizza's
The Fluffy Bunny says hi mo
The Fluffy Bunny wonders who the REAL fluffy bunny was
The Fluffy Bunny is just a manufactured product
The Fluffy Bunny is the star attraction of the London fashion show
The Fluffy Bunny is not wearing any panties
The Fluffy Bunny does not like Dittrich
The Fluffy Bunny hacked the bunny planet!
The Fluffy Bunny is inspired by the Boobies at Spearmint Rhino
The Fluffy Bunny would like to thank Crispy Duck for best Hot & Sour Soup
The Fluffy Bunny thanks Selfridges for free gloves.
The Fluffy Bunny does not condone scrabbles *ahem* mojo

Special Greetings go out to the members of etCl and xing
(c) Brought to you in Bunny Vision, Fluffy Style since 1996
The Fluffy Bunny greetz APACHE, torrer, Danny-Boy, Annihilat, or, Beast, dEX, random.
Saddam is gone(?)

☠️☠️☠️☠️ who's next? ☠️☠️☠️☠️

cracked by a anti-war coalition as a protest against war

In a war, there are no winners!

Start with saying "NO!" to war, and mobilize local forces to oppose violence and hate. Remember the innocent victims. The fallen soldiers on both side. Everyone is responsible.

Greetings to all the people who support peace, and who are putting effort to making the world a better place. Theli, DkD[], USG, Kafka, Furax ....

www.indymedia.org| www.aljazeera.net| www.iraqwar.ru|

Robert Oppenheimer, who had directed the project(building the atomic bomb), said: (.....)We knew the world would not be the same. A few people laughed, a few people cried. Most people were silent.

I remembered the line from the Hindu scripture, the Bhagavad-Gita: Vishnu is trying to persuade the Prince that he should do his duty and to impress him he takes on his multi-armed form and says, 'Now I am become Death, the destroyer of worlds.' I suppose we all thought that, one way or another.
Protestors

THE UNITED STATES WILL DESTROY YOU!

PROJECT AFGANISTAND!!! KNOCK THEM OUT!

Hacked by MaxMouse

YOU WILL PAY FOR THIS YOU STUPID FOOLS!!!!!!!!!!!!

GOD BLESS THE UNITED STATES OF AMERICA!
The Inquisitive?

Gary McKinnon

USD 700,000 of damage, DoS of 2000 US Army computers, "intentional and calculated to influence and affect the US government by intimidation and coercion". (Mark Summers, representative of US Government).

“Bumbling computer nerd”, looking for information on “suppressed technology”, logging into systems with no password present.

If so, begs the question; ‘why is he appearing as a security commentator and paid for speaker’
Muppets

The courts start taking hacking seriously

Sussex computer hacker jailed for online fraud scam

A 21-year-old computer hacker has been jailed for 20 months for carrying out a complex online fraud which netted him tens of thousands of pounds.

Alistair Peckover, 21, of London Road, Hailsham, East Sussex, bought luxury items and more than £30,000 worth of gold bullion with the proceeds.

He was sentenced at Southend Crown Court after pleading guilty to two fraud charges at an earlier hearing.

Peckover asked for 50 other offences to be taken into consideration.

Sussex Police said Peckover used sophisticated computer programmes, some he had written himself, to remotely view files of other computers.

He then used the information, including credit card details, to buy gifts for himself and family.
Isn’t hacking getting worse?

It’s a **bit** worse
It’s just that you get to hear about it now
Commercial hacking

Court filing suggested ~65 million Visa and ~29 million MasterCard PANs stolen

Hence, PCI DSS & emergence of disclosure

Attention to Zeus, Stuxnet etc is primarily a result of security industry realising there’s an interest in mainstream media
Commercial hacking

Hugh Rodley
David Nash

Convicted along with

Kevin O’Donoghue
Jan Van Osselaer
Gilles Poelvoorde

Conspiracy to steal nearly £229M from
**Sumitomo Mitsui Banking Corp**

Coerced building security manager

Installed software keyloggers, captured passwords

Silly errors...
Commercial hacking

Vulnerability found in WorldPay, detail not disclosed

Card databases found

Card numbers taken with PINs, sent on to network of ‘cashiers’

One transaction per ATM, $9M stolen in ONE DAY

Hackers used RBS systems to MONITOR their cashiers’ withdrawals
“But we’re not a bank”

So you don’t need the same level of security as a bank?
Cross Site Scripting

Why you increasingly need **user data** to hack

AKA advanced ‘phishing’
No dodgy URLs
Looks totally legitimate
Phishing filters won’t help
SSL certificates are still green!

This attack needs to be delivered to the user as a link
Hence we need email addresses, Messenger, Facebook or Twitter profiles
Just by your mouse moving over my Tweet, I can steal information about you, or send you to a malicious web site that will infect your PC.
My Favourite Hacking Tool

Google
The hacker moves on
The hacker moves on
Card numbers?

MySQL dump 9.08 -- Host: localhost Database: travelagent ...
VALUES (2070, 2005-10-01, 6333041539238576L, Dale Martyn, "Switch"), ...
www.csd.abdn.ac.uk/.../C5502/practicals/travelagent-model-2/travelagent-model-
2/travelagent_data.txt - 28k - Cached - Similar pages

From: "William S. Morton" <borscht9@earthlink.net> Subject ...
... and Fractint failed to switch video mode back to text 320x200. ...
param="300.633320108458937=5.44066755882442/2.91459728995638/1.3999=450\ ...
www.xmission.com/pub/lists/fractint/archive/fractint.199903-393k - Cached - Similar pages

Switch
Compare all energy and home telephone providers and save £170
www.upmystreet.com
Cut business & home bills
Energy, gas, electricity & phone price comparisons. Switch online
www.thepowerswitch.com
Switch
PriceGrabber.co.uk
Switch
Independent electricity and gas supplier bill comparisons online!
www.efficienciesolutions.co.uk
Cut UK bills by up to 90%
Check how much you can save quickly and completely free
www.checkmybill.com
Missed an Episode?
Download Switch episodes to watch at any time!
www.TVShows.org
Woxa To Music & Song
1 Billion songs, movies & videos!
Unlimited Downloads. VIP Support.
www.mp3cucumber.com
switch
Buy It Cheap On eBay
Low Prices, New and Used
ebay.co.uk
Other sources
So easy

There are tools to do this for you
e.g. Maltego

There are exploit frameworks that will help the low-skill hacker automate the process
e.g. Metasploit

Undetectable vulnerability exploits can be bought for around USD 1,000

  Don’t go browsing for these using Internet Explorer!

Yet there are relatively simple defences against all of this

  It’s just that things get overlooked or ignored in the melee of business
Be Sure To consider

See if the prospect has a security policy

Ask if they comply with any recognised security frameworks
   ISO27001, PCI DSS etc

Ask if they have been hacked, or had a security incident

Ask how they would know if they had been hacked

Find out if they’ve had any independent reviews of their security, and whether it’s been tested
Hacking iPhones

PIN bypass #1

Press emergency call
Enter three hashes
Hit dial
Then power button, immediately
Launches phone app
Further compromise by adding contacts pictures
Hacking iPhones

PIN bypass #2

Press button for 3 seconds

Say ‘voicemail’

Do anything that the regular user could do with voicemail
Hacking iPhones

‘libimobiledevice’ library aka ‘iFuse’

Simply connect laptop to phone with Apple cable

Run the tool

Access to all user data
Worse if the iPhone is ‘jailbroken’
Why test anything?

Questions?

Slides available
ken.munro@pentestpartners.com
Cyber insurance – an underwriter’s view

Tom Allen
Aspen Insurance UK Ltd.
22 November 2010
Cyber Insurance Products

- Not standardised, but a consensus is developing in the market as to what a “cyber” policy contains
- Country–by–country needs driven by distinct regulatory approaches
- Commercial sector influences: PCI, contracting practices
- Distinction from technology PI
- Popularity of modular/menu–driven approaches
  - Sublimits for more volatile covers
Key concepts

Privacy liability
- Breach of common law rights
- Breach of relevant regulations concerning personal data
- Needn’t be tied to a computer

Security Liability
- Arising from deficiencies in an organization’s computer security. Some typical perils:
  - Compromise of Confidential information
  - Cybercrime, fraud, theft of data
  - Unauthorised access
  - Denial of service attacks
  - Malware transmission
Heads of cover

- First Party cover:
  - Business interruption
    - Impact on profits and extra expense
    - Substantial time retentions
  - Digital asset protection
    - Restoration/replacement costs
    - Some offerings cover operational errors
  - Notification costs/reputation protection
    - Statutory duties
    - Mitigation (discretionary)
    - PR expense
    - Forensics
    - Legal costs
    - Credit monitoring
    - Customer support
Heads of Cover (continued)

- Privacy/Security Liability
  - Liability for employees’ data
- Regulatory defence and penalties
  - Insurable if occasioned by a fortuitous breach (?)
  - Consumer redress funds etc
- Media liability
- Cyber extortion
- Professional liability
Characteristics

- Breach events – short tail, not much scope for adjustment, investigation costs can vary widely
- Cybercrime scams can inflict a great deal of loss before detection
- BI exposures can be difficult to assess
- Diverse approaches on pricing – a ‘market price’ is sometimes hard to establish
- Long sales cycle
- Specialist distribution
Looking ahead

- More segmentation by industry and geography
- Emergence as a mainstream cover
  - Already in some industry contracts
- More clarity around cyber crime and offshoring/outsourcing/cloud computing issues
- Losses – expect the unexpected!