

## Cyber Crime: The Impact on the UK Economy

### North West Institute of Risk Management Event

Ben Rendle, October 2011



## Contents

---

1. Setting the scene - what is meant by “cybercrime”?
2. Getting a handle on measuring cybercrime in the UK
3. Results: The economic impact of cybercrime on the UK
4. Conclusions: Where do we go from here?

# Setting the scene – what is cybercrime?

## It's all in the press.....but how much of it is hype?

***61% of organisations detected a significant attempt to break into their network during 2009, double the scale of the problem in 2008***

Information Security Breaches Survey (ISBS) 2010

***“The UK is under daily cyber attack...there have been 300 significant attacks on the government’s core computer networks in the last year”***

Lord West, speaking in The Observer, March 2010

***“We regularly face attempts to gain unauthorized access to our systems...which are sometimes successful...and could adversely affect our competitive position...causing significant disruption and monetary losses”***

Intel, in a filing to the Securities and Exchange Commission, 23<sup>rd</sup> Feb 2010

***Criminals were responsible for creating 240 million distinct new malicious programs in 2009 - a 100% increase on 2008***

Internet Security Threat Report (ISTR) 2010

## Where do we begin?

---

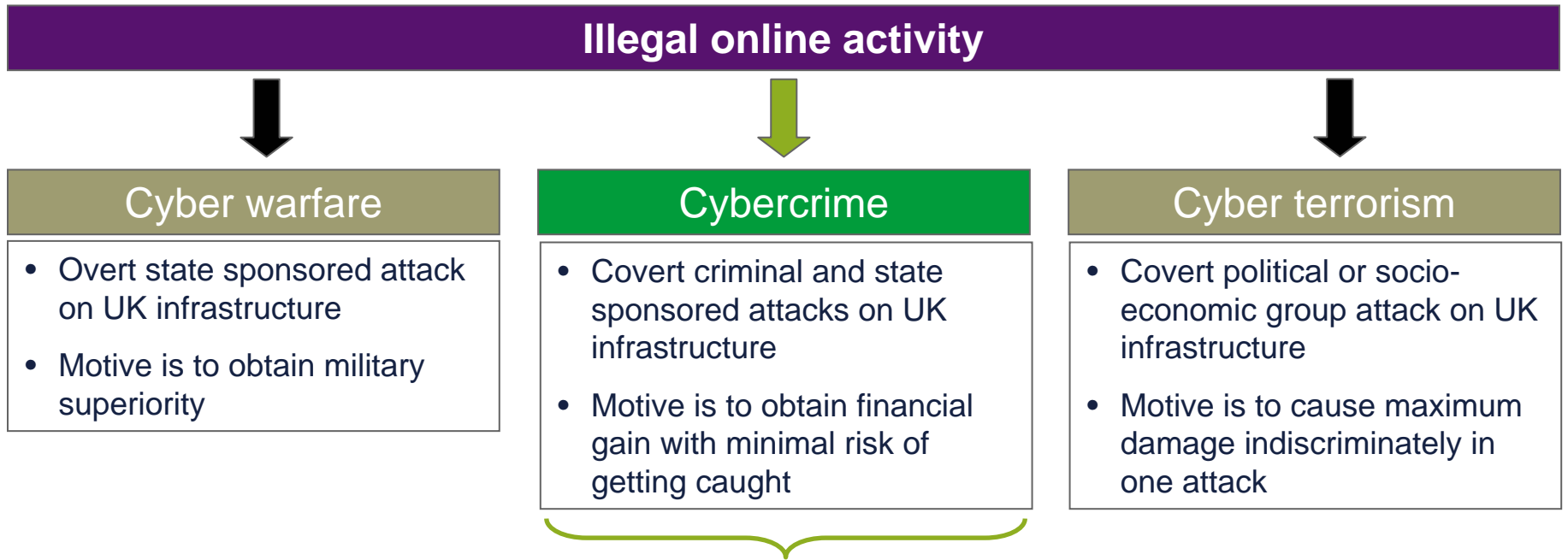


# CabinetOffice

- Detica was tasked by the Office of Cybersecurity and Information Assurance to estimate how much the economic impact of cybercrime was on the UK economy.
- No “top down” holistic estimate of this had ever been done before and the OCSIA recognised that it was highly challenging, if not impossible.
- We could only use open source material. We were allowed to interview some government bodies and industry contacts.
- The results were to be presented to the Baroness Neville Jones at the House of Lords (pictured).



## Cybercrime in context



## Cybercrime with economic impacts

- |                                                                                                                                                                                                             |                                                                                                                                                                                           |                                                                                                                                                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>✗ Methods used to undertake cybercrime or examination of specific case studies</li> <li>✗ Conventional criminal activity which happens to use cyber means</li> </ul> | <ul style="list-style-type: none"> <li>✓ <b>Overall economic impact</b> of cybercrime on the UK</li> <li>✓ <b>Exclusively online</b> criminal activity with an economic impact</li> </ul> | <ul style="list-style-type: none"> <li>✗ Cybercrime with no direct economic impact (e.g. uploading of indecent images)</li> <li>✗ Online media piracy (e.g. illegal music or film file sharing)</li> </ul> |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Cybercrime defined

This study defines cybercrime as *“Illegal activities undertaken by criminals for financial gain that exploit vulnerabilities in the use of the internet and other electronic systems to illicitly access or attack information and services used by citizens, business and government.”*

### Objective

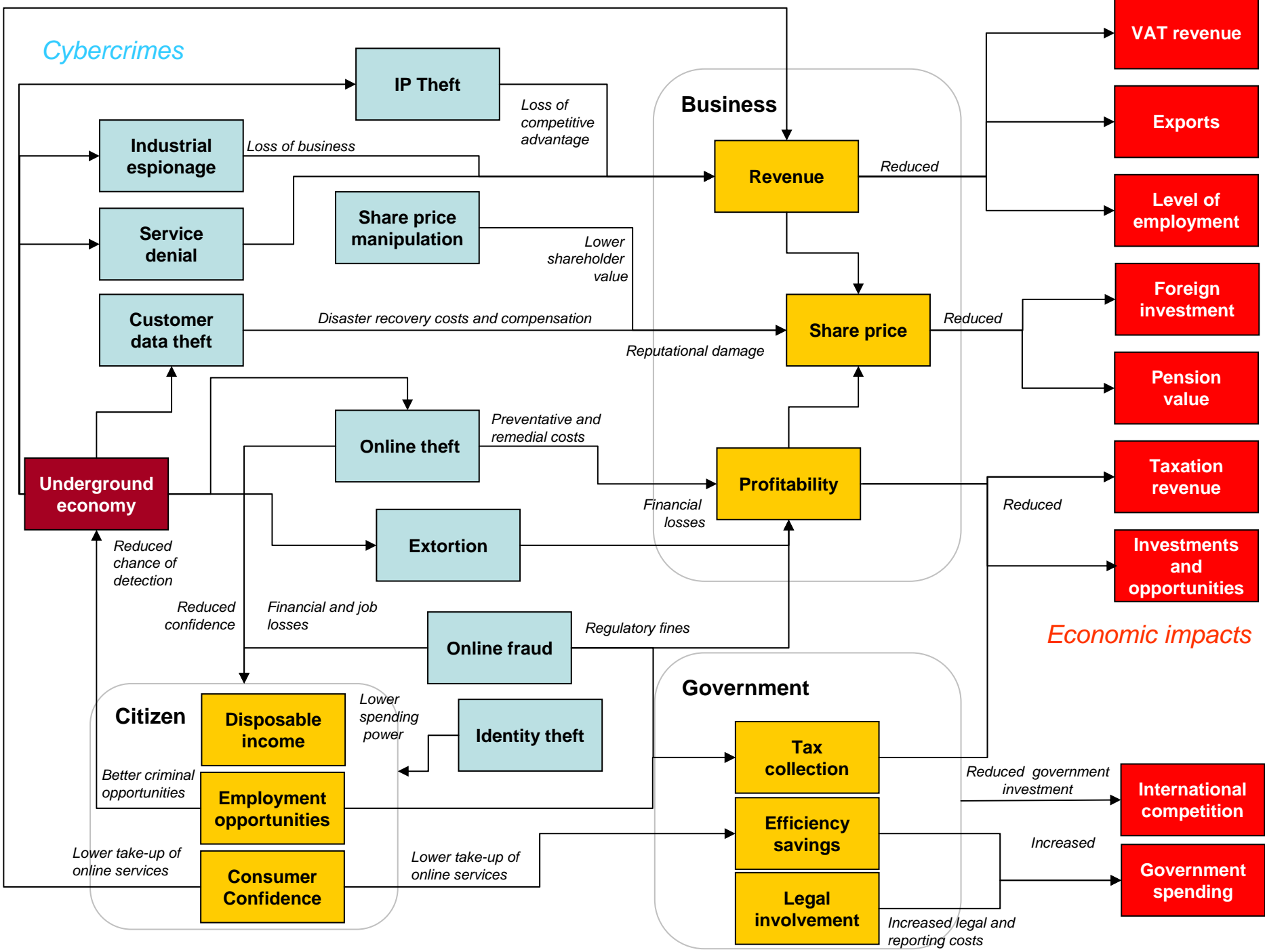
The aim of this study is:

- To determine the **overall impact** that cybercrime has on the **UK economy**
- This includes a specific focus on the impact on UK businesses of the **theft of Intellectual Property (IP)**

- **This was a bounded study** lasting two months, and no primary research was carried out into the economic impacts
- **Interviews were held** with various government and industry stakeholders throughout the study to verify emerging themes and obtain further information
- **The study used existing and up to date data from credible sources** where it was available. Where possible, under-reporting was accounted for
- **Estimates were produced conservatively** based on industry sector knowledge. Where there were high levels of uncertainty, three point estimates were used

# Getting a handle on measuring cybercrime in the UK

# Cybercrimes



## Business

## Government

## Economic impacts

IP Theft

Industrial espionage

Service denial

Customer data theft

Share price manipulation

Online theft

Extortion

Online fraud

Identity theft

Revenue

Share price

Profitability

Disposable income

Employment opportunities

Consumer Confidence

Tax collection

Efficiency savings

Legal involvement

VAT revenue

Exports

Level of employment

Foreign investment

Pension value

Taxation revenue

Investments and opportunities

International competition

Government spending

Loss of business

Loss of competitive advantage

Lower shareholder value

Disaster recovery costs and compensation

Reputational damage

Preventative and remedial costs

Financial losses

Regulatory fines

Lower spending power

Lower take-up of online services

Reduced

Reduced

Reduced

Reduced government investment

Increased

Increased legal and reporting costs

Reduced chance of detection

Reduced confidence

Financial and job losses

Lower spending power

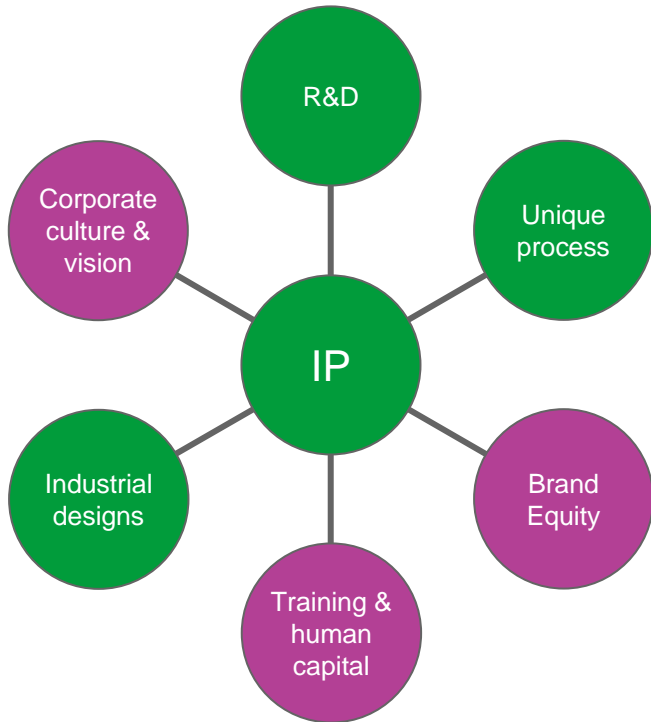
Lower take-up of online services

Better criminal opportunities

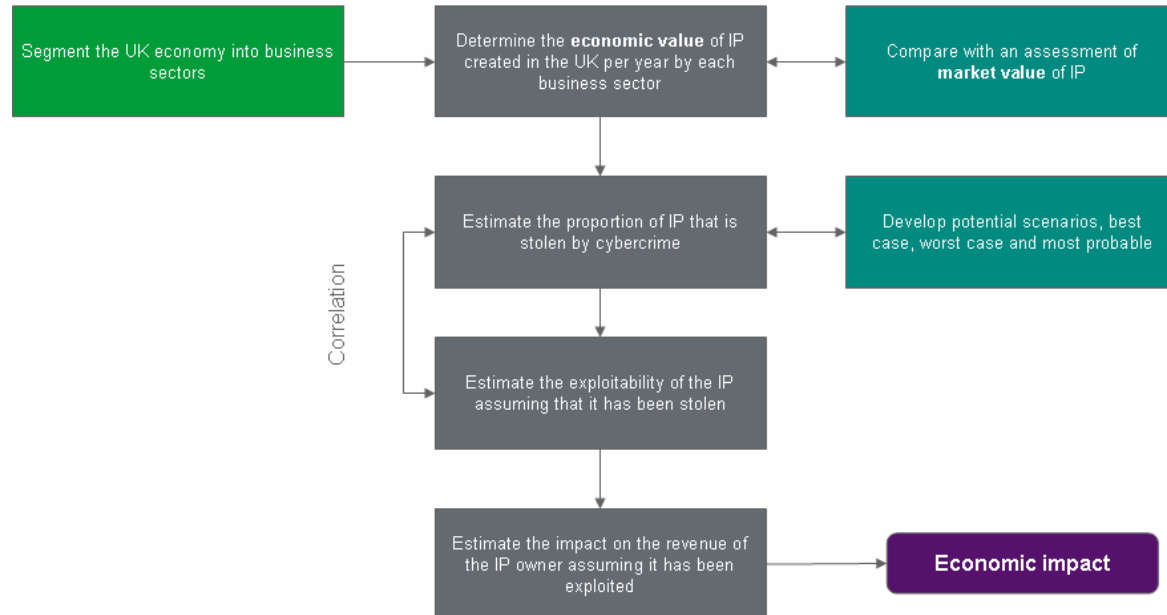
Lower take-up of online services

## Economic impacts

## How can you measure Intellectual Property (IP) theft?



- Not all IP is immediately exploitable or is exploited now
- Not all IP can be stolen by cybercrime
- Not all IP is easily exploitable by cybercriminals
- Different types of IP add different value to their industry sectors
- Patents, trademarks and other conventional IP protection offer limited defence against cybercrime. They do not prevent cybercrime and can have weak enforcement globally
- Theft of other commercially sensitive information covered under espionage



# **Results: The economic impact of cybercrime on the UK**

## Cybercrime cost to UK Citizens

Citizen

Disposable  
income

Consumer  
Confidence

Identity theft

Online fraud

Scareware

### Identity theft

- Defined as fraudulently exploiting stolen identity information (e.g. create a false bank account under someone else's name)
- In line with other estimations (e.g. CIFAS) [1]
- Estimated to cost **£1.7BN** to the UK economy

### Online fraud

- Defined as using the internet to obtain money from victims by deception (e.g. card not present, services not provided, phishing activities)
- It is difficult to estimate if the fraud is completely online or facilitated through online means [2]
- Estimated to cost **£1.4BN** to the UK economy

### Scareware and fake AV

- Defined as malicious software that internet users are persuaded to download
- By far the lowest cybercrime impact to the UK economy [3]
- Estimated to cost **£30M** to the UK economy, but, expected to increase especially in “software as a service” areas

## Cybercrime cost to UK Government

### Fiscal fraud

#### Government

Tax collection

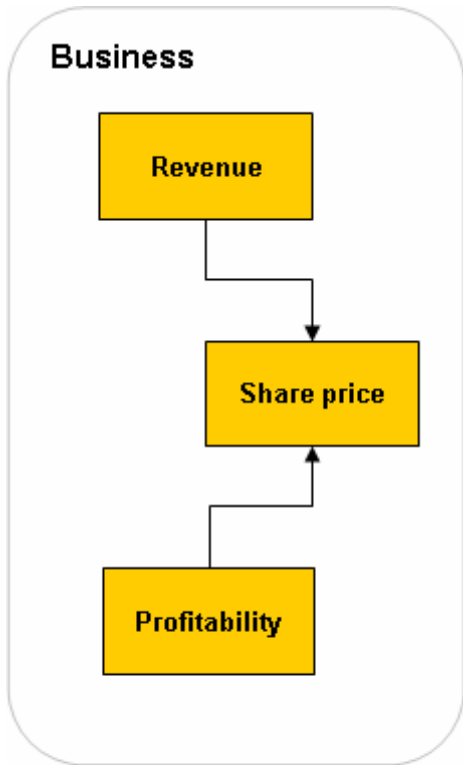
Efficiency savings

Law enforcement costs

Fiscal fraud

- Defined as money lost online by government either through uncollected revenue or fraudulent payment of benefits.
- It is difficult to estimate if the fraud is completely online or facilitated through online means [4]
- At this stage, it is hard to estimate how much of this is:
  - tax fraud
  - benefits fraud
  - local government fraud
  - central government fraud
  - NHS fraud
  - pension fraud
- Official figures produced are likely to be underestimated, and this may be worthy of further study. Estimated to cost **£2.2BN** to the UK economy

## Cybercrime cost of customer data loss

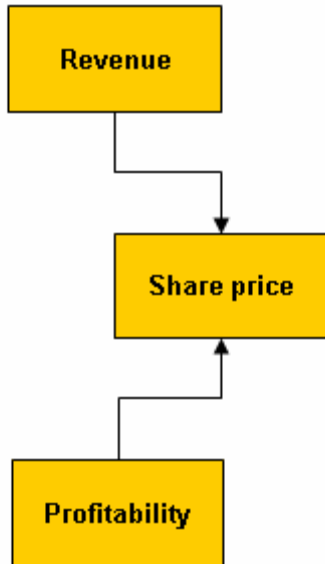


### Customer data loss

- Defined as illegally obtaining customer data online ***not*** through lost data sticks or laptops
- Estimated by:
  - Reported number of incidents and records compromised
  - Legal and regulatory fines
  - Handling costs per record to restore data
  - Business disruption costs (on average)
  - Direct financial losses as a result of the customer data loss [5]
- Challenges include estimating:
  - Damage to reputation through share price (ruled out of scope)
  - Subsequent losses from the use of customer data (ruled out of scope)
  - Average number of records compromised in each incident and what *value* each record had (e.g. financial or personal information)
  - Underreporting due to unawareness of loss or partial reporting
- Reported estimate cost is **£960M** to the UK economy Factoring in underreporting, this figure is more likely to be **£1BN**

## Cybercrime and extortion

### Business



Extortion

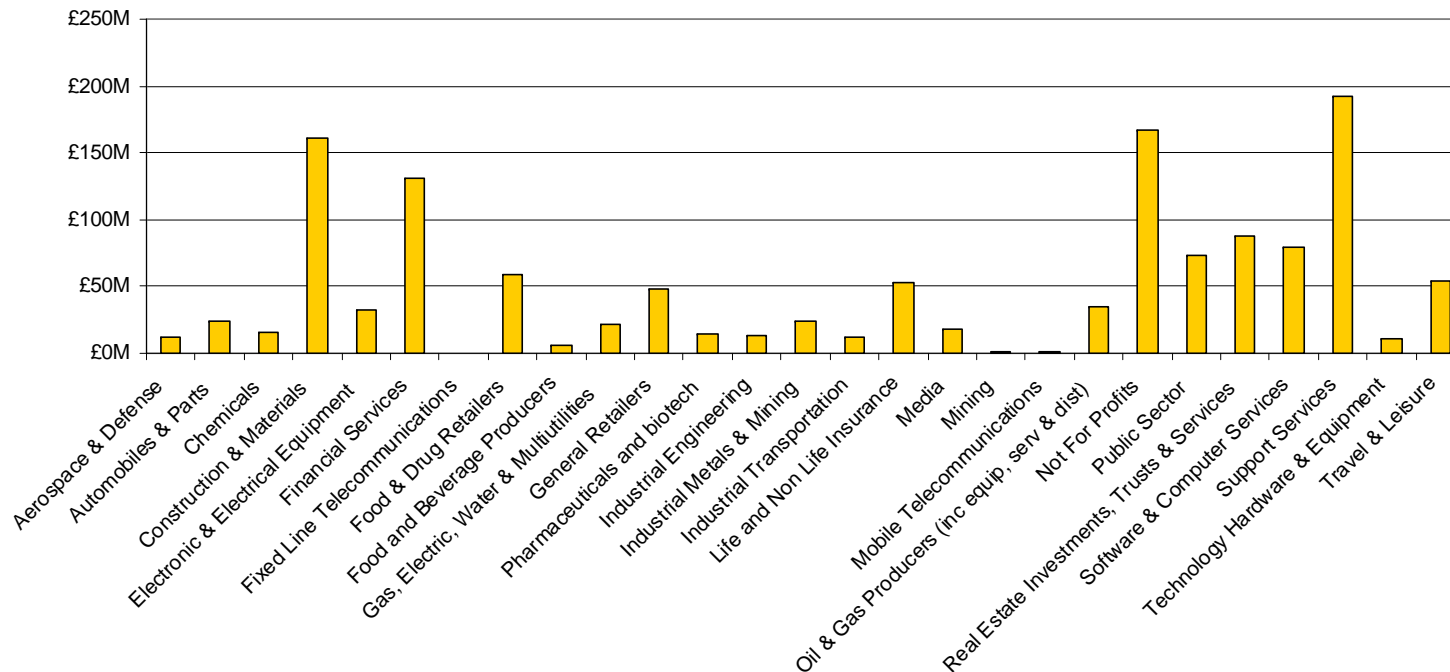
### Extortion

- Defined as holding an organisation to ransom through online means unless monetary payments are made (socio-political motives e.g. “hacktivists” are out of scope)
- This can be brand damage as well as denial of service (e.g. infecting legitimate site links with links to indecent imagery)
- The most difficult impact to estimate as there is no published data on:
  - The annual amount of extortion attempts suffered by industry
  - The amount of extortion attempts that succeed
  - The ransom payments made by industry [6]
- This cybercriminal activity is severely under-reported, due to reputation damage and no legal enforcement to disclose extortion attempts
- Estimated cost is **£2.2BN** to the UK economy based on the extent of under-reporting and limited information available

## Cybercrime and online theft

- Defined as online stealing of organisational money (e.g. by account takeover)
- Estimates were also made for how much theft revenue would be “tolerated” by the industry sector [7]
- The most vulnerable sectors were the support services, financial services, construction and not for profit sector. Estimated to cost **£1.3BN** to the UK economy

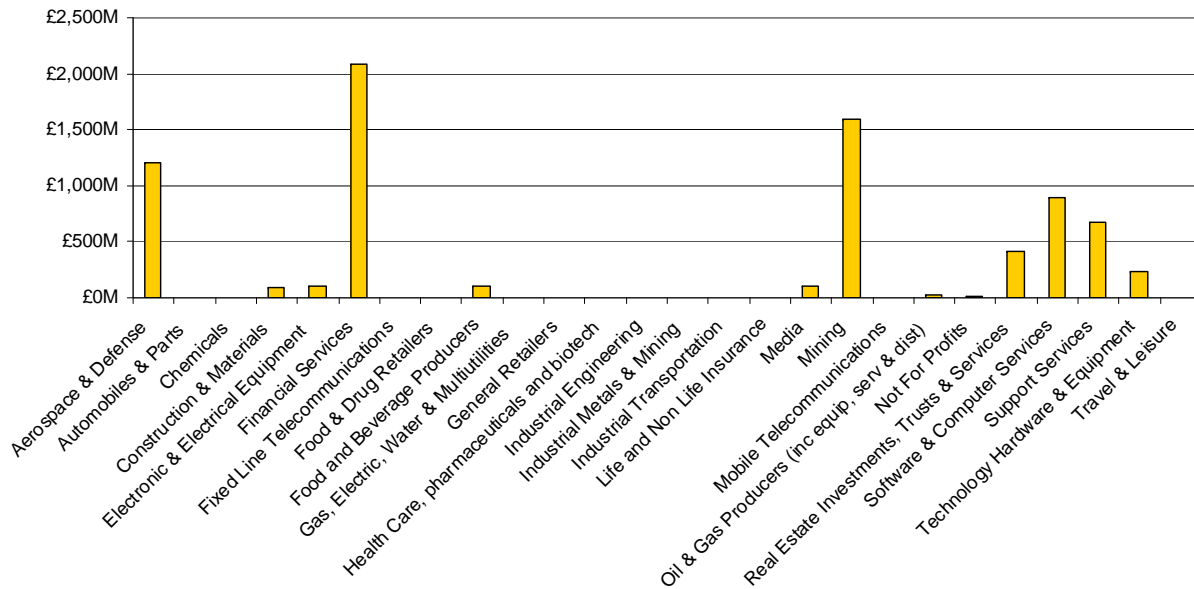
Online theft by business sector



## Cybercrime and industrial espionage

- Defined as acquiring and exploiting commercially sensitive information (e.g. competition sensitive, market sensitive, strategically sensitive)
- The impacts from industrial espionage are highly dependent on current market conditions, especially around M&A activity [8]
- The most vulnerable sectors are the financial services, the mining sector and aerospace & defence – but this is highly dependent on current market conditions. Estimated to cost **£7.6BN** to the UK economy

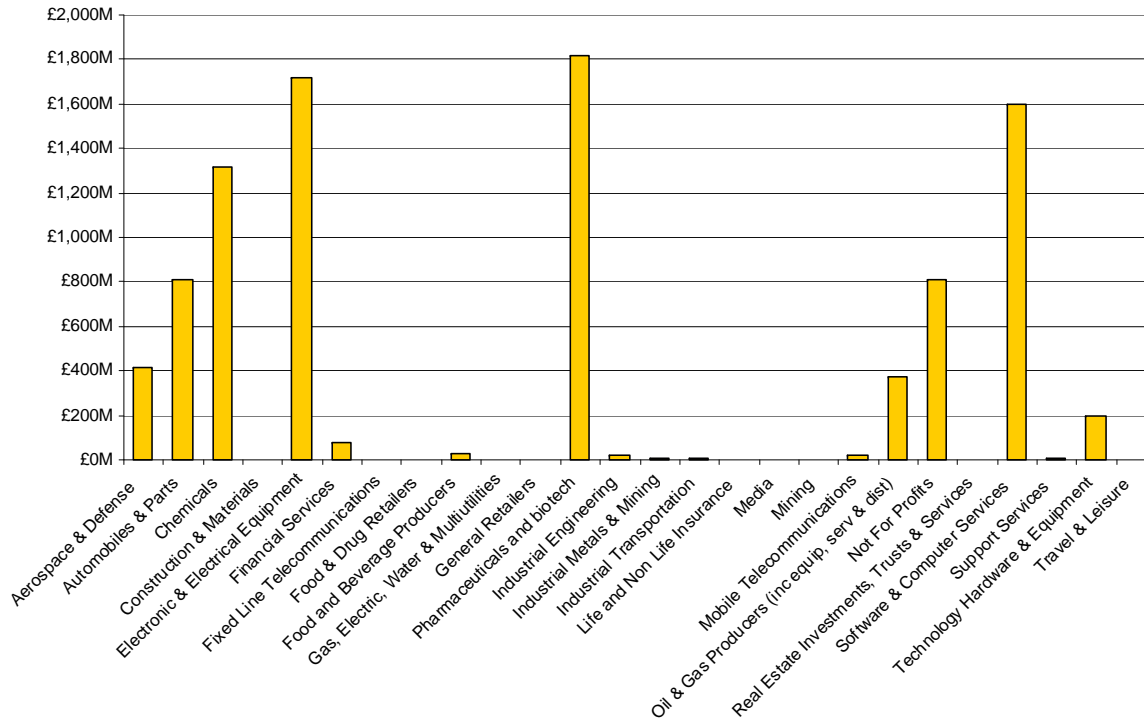
Espionage impact by business sector



## Cybercrime and Intellectual Property (IP) theft

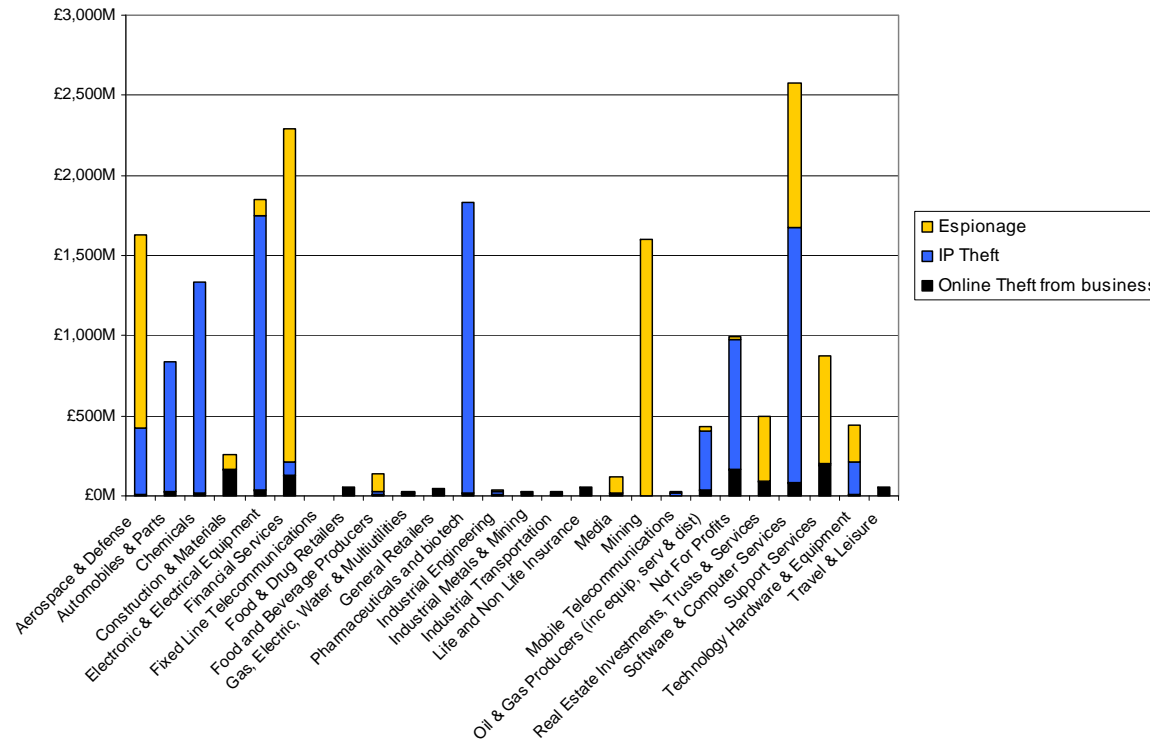
- Calculated by industry sector R&D spend, estimated ROI expected, and subsequent IP market value. Estimates were made for probability of IP theft for each industry sector [9]
- This was identified as the biggest cybercriminal impact on the UK economy. The most vulnerable sectors are pharmaceuticals and biotech, electronics and engineering, software and computer services, chemicals, automobiles and parts and not for profits. Estimated to cost **£9.2BN** to the UK economy

IP theft - Most likely economic impact by business sector

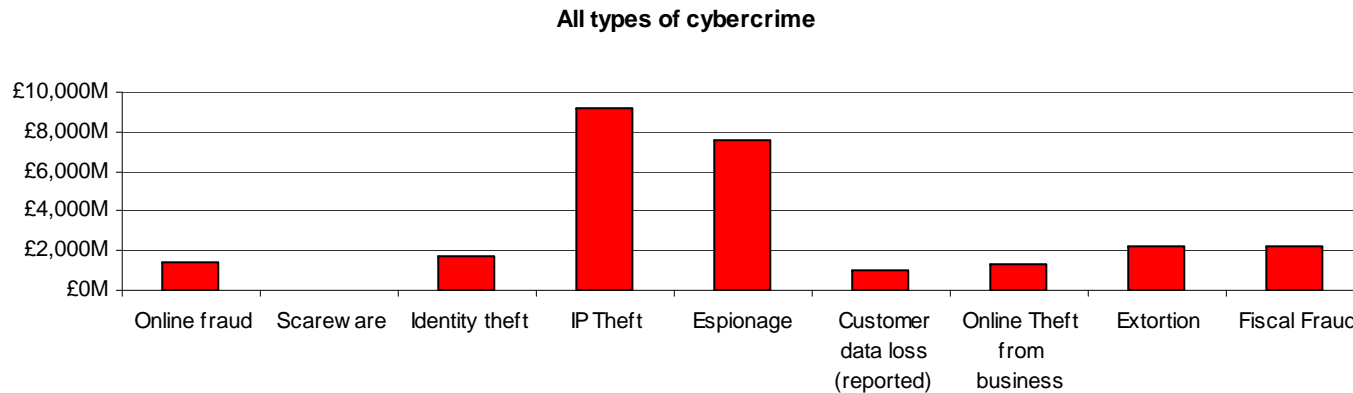


## Total breakdown of UK sector impact by cybercrime

- This includes online theft from business, industrial espionage and IP theft. It does **not** include customer data theft or extortion, as no information is available to make these cybercrimes industry specific
- The overall most vulnerable industry areas are the software and financial sectors



## Total UK economic impact of cybercrime



- These results are indicative and aim to factor in under-reporting where appropriate
- Based on each different type of cybercrime with an economic impact as outlined earlier
- Based on the “most likely” estimates, but can range from a “best case” more optimistic estimate to a “worst case” more pessimistic estimate
- At this stage, the most likely estimate for the economic impact of cybercrime to the UK is in the range **£13Bn to £42Bn**. The reported single estimate is **£27Bn**.
- Figures do not include preventative costs of security or classified information.

**Conclusions: Where do we go from here?**

## Is this number credible?

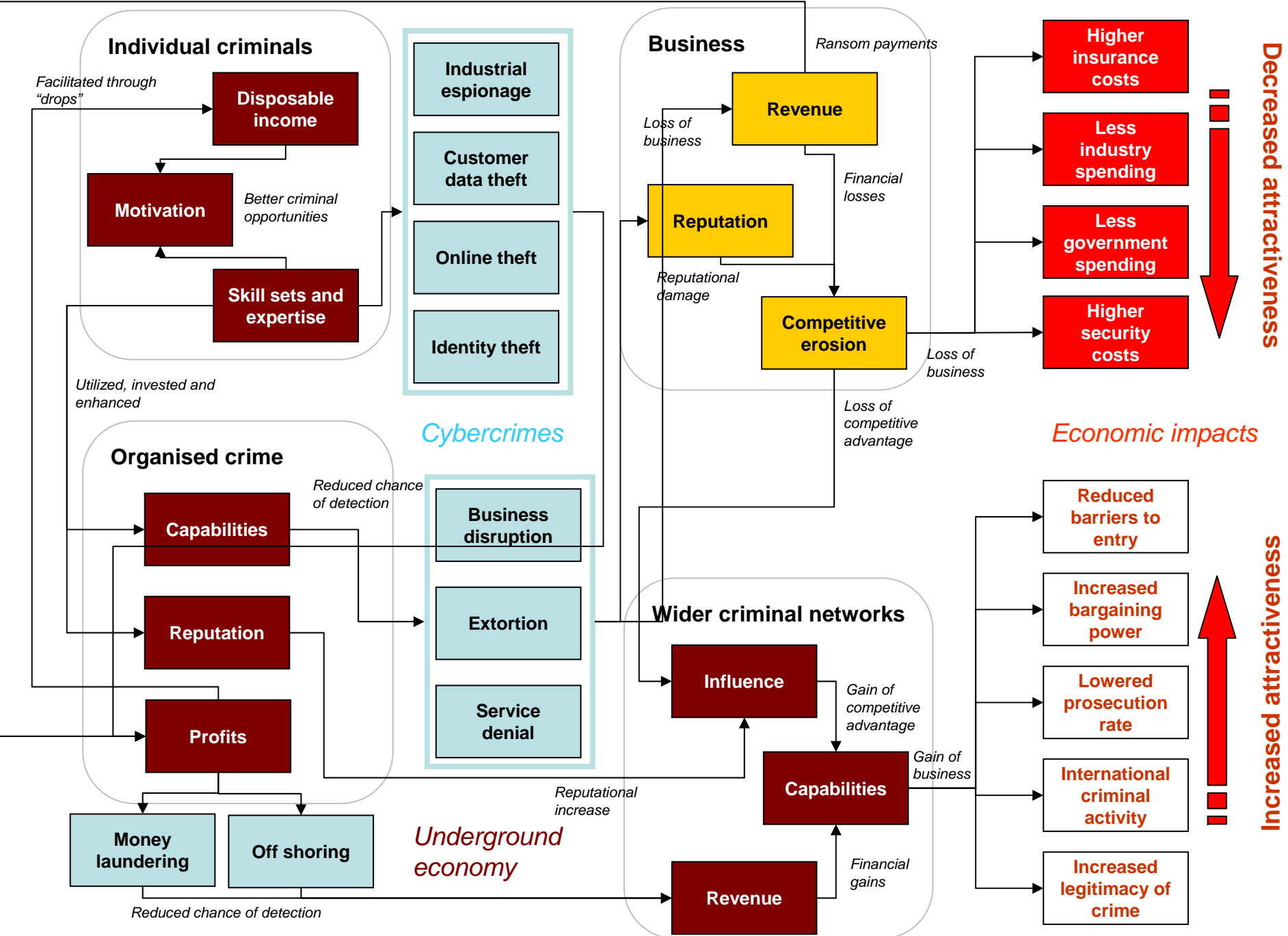
---

- The figure of £27Bn equates to
  - ~1.75% of UK GDP, or
  - ~£700 per person
- Global estimates put cybercrime at 1.6% of world GDP
- Major component is IP theft
  - Traditionally, the UK has a proportionately higher levels of investment in IP than the world average and is an obvious target. Will this be true in the future?
  - Iain Lobban, Director GCHQ: “intellectual property theft is taking place on a massive scale”
- Cybercriminals have a low risk of being caught, face relatively short prison sentences, high rewards and “infinite” potential victims
  - serious organised UK criminal gangs are known to be turning to cybercrime
  - cybercrime has a mature ‘business model’

## High level conclusions from the report

---

- **Cybercrime has a material impact on the UK economy.**
  - **The main impact of cybercrime is on business.**
  - **The impact of cybercrime differs widely across business sectors.**
  - **The level and scale of cybercrime are severely under-reported.**
  - **The profits from cyber crime are likely to be used to support other criminal activities.**
  - **Cybercrime is attractive to criminals.**
  - **The UK does not have a clear overall intelligence picture of cybercrime.**
-



*Cybercrimes*

*Underground economy*

*Economic impacts*

Decreased attractiveness

Increased attractiveness

## “That’s the UK government’s problem to solve”

**“Security firm RSA offers to replace SecurID tokens...It follows a hack against the company in March where information related to the tokens was stolen ”**

BBC Online June 2011

**“We've been hacked: Sony finally blames 'external intrusion' for PlayStation Network outage**

**The outage, which began on Wednesday, is affecting more than 70 million gamers worldwide, who use the network to play video games against friends online, stream movies and shop.”**

Daily Mail April 2011

**“The data theft from International Monetary Fund computers by hackers said to be linked to a foreign government follows incidents against companies and governments that illustrate the growth of cyber-attacks as an espionage tool.”**

Bloomberg Business Week July 2011



## “That’s the IT department’s problem not mine”

.....why is it the IT department’s problem?

“We don’t know when or how cybercriminals may attack our organisation”



Uncertainty.....

“We don’t know what methods they will use or what they are after”



Which may affect.....

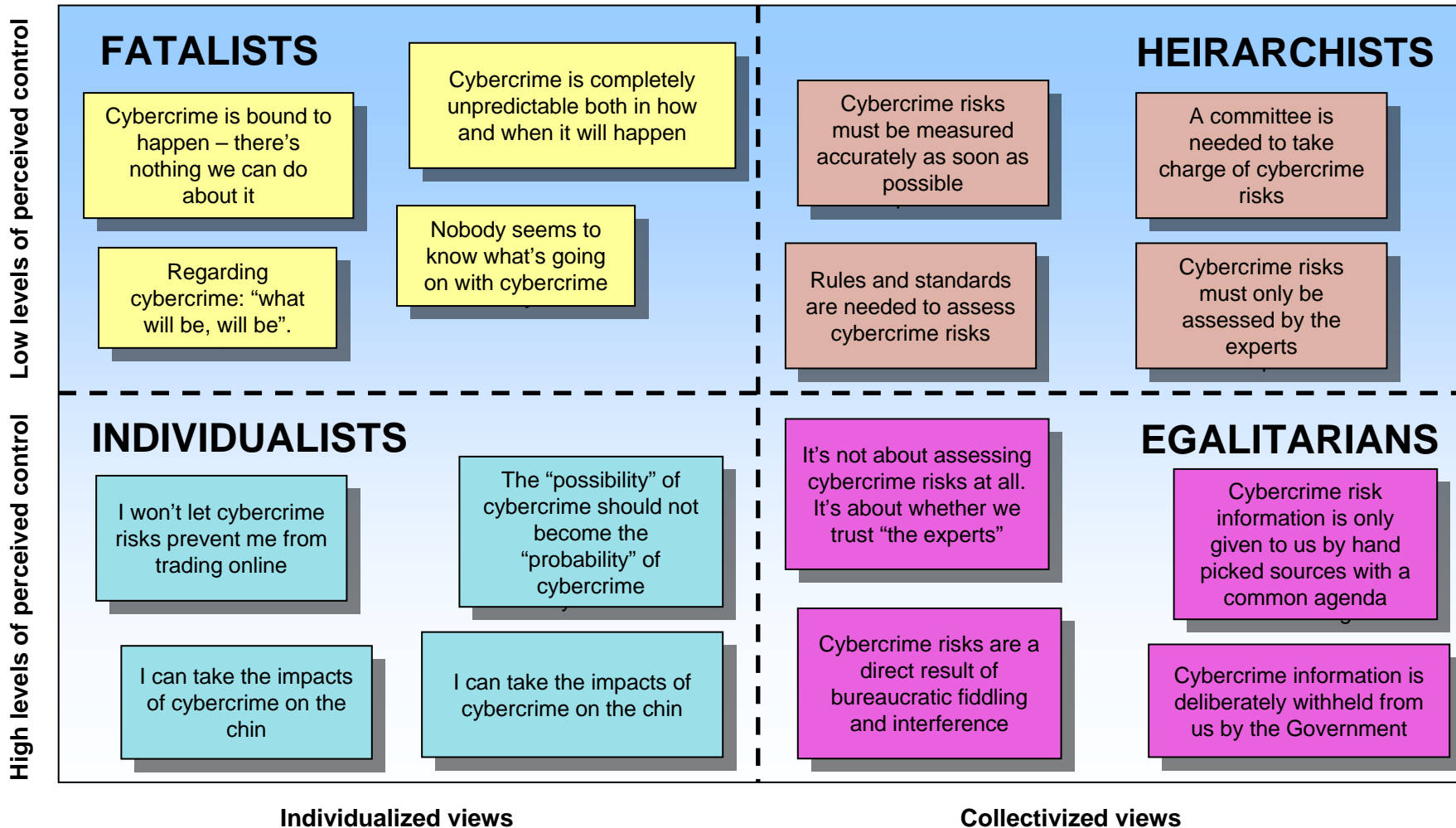
“We don’t know how it will affect our corporate goals if they succeed”



One or more objectives.

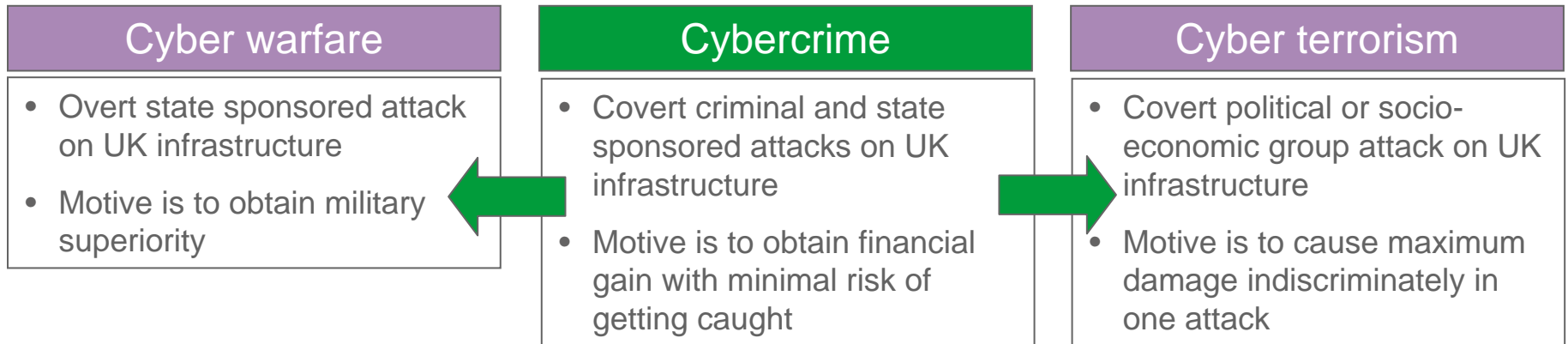
I think this should be a **risk management issue** and not just an IT issue.

## Perceptions of cyber risk matter if estimates are so objective



## One final point

With cybercriminal techniques and expertise growing, future threats to the UK economy may also look like this.....



**Cybercriminal skills and expertise can very easily be transferred to cyber warfare and cyber terrorism. The only difference is the motive.**

## Thank you

### Ben Rendle

t +44 (0)1483 816993 | m +44 (0) 7967 483887 f +44 (0)1483 816262  
a Detica | Surrey Research Park | Guildford | GU2 7YP | UK  
e [ben.rendle@detica.com](mailto:ben.rendle@detica.com)  
w [www.detica.com](http://www.detica.com)

## Assumption sources

- [1] **Calculated** by number of reported incidents x average reported cost and number of online UK citizens x reported probability of identity theft. **Source:** CIFAS estimates identity theft to be £1.7BN a year – <http://www.intellectuk.org/content/view/4348/377/>
- [2] **Calculated** by reported turnover of online transactions x reported probability of cybercrime x reported average cost. **Source:** Calculated using Get Safe Online Report of 2009
- [3] **Calculated** by reported probability of citizens being attacked x number of online UK citizens x reported average cost **Source:** Based on information provided by Symantec Report on Rogue Security Software July 08 – June 09
- [4] **Calculated** using the median difference between estimates of reported percentage of fraud due to criminal attacks from both the NFA Annual Fraud indicator and HMRC Measuring Tax Gaps Report 2010.
- [5] **Calculated** by number of reported incidents for small, medium and large companies x average number of records compromised x average estimated legal penalties. Then verified by reported and unreported handling cost per record x business disruption cost x direct financial losses x lost business due to damaged reputation. **Source:** Calculated using Ponemon Institute information and the DTI Survey Report
- [6] **Estimated** by average revenues of large, medium and small companies in the UK, how vulnerable they are to extortion attempts and how likely the extortion attempts are to succeed. **Source:** Based on estimations used in the Get Safe Online Report 2009
- [7] **Calculated** by assessing how attractive the industry sector is for cybercriminals through industry sector total cash flow compared against level of online presence, the dominant size of companies in the industry, the level of liquidity, and the perceived level of security. Once assessed, the probability and likelihood of online theft for each industry sector was estimated, factoring in the estimated value of stolen revenue that would be “tolerated” by each sector. **Source:** Overall industry turnover is calculated from sources such as the 2010 HMG Blue Book, UKTI publications and reputable industry websites.
- [8] **Calculated** by industry sector total revenues and estimated levels and values of competition sensitive information and commercially sensitive information (profits from merger activities, short selling and currency fluctuations). Estimates were made for probability of espionage for each industry sector and average return on investment made by cybercriminals. **Source:** M&A deals and values based on PKF Deal Driver reports, PwC M&A reports and EY Newsroom releases
- [9] **Calculated** by industry sector R&D spend, estimated ROI expected, and subsequent IP market value. **Source:** Estimates were made for probability of IP theft for each industry sector. R&D figures taken from BIS innovation.gov.uk