Industrial Espionage and Information Security

Professor Mark Button

Director of the Centre for Counter Fraud Studies
Outline

• The nature of industrial and economic espionage
• The value of trade secrets
• The scale of the problem of industrial and economic espionage
• Research on the issue
• Focus upon cyber, with particular reference to research from Government’s annual Cyber Security Breaches Survey
  • Nature of problem and what organisations doing in the UK
  • The opportunity for cyber to help
• Conclusions
Defining industrial and economic espionage

• ‘Economic espionage refers to targeting or acquiring trade secrets from domestic companies or government entities to knowingly benefit a foreign state’ and

• ‘Industrial espionage is the same as economic espionage, except that rather than benefiting a foreign government, it benefits another private entity’

• Wagner (2012, p. 1040)
The pursuit of industrial espionage

• Open source intelligence (trade shows, reports, publications, social media, photos etc)
• Dumpster diving
• Reverse engineering
• Hiring employees of competitors
• Cultivating insiders
  • Disgruntled insiders
  • Luring insiders
  • Blackmailing insiders
  • Placing insiders
• Electronic surveillance
  • Bugs, surveillance etc
• Cyber
  • Hacking systems
  • Employees’ devices etc
Human element is the most important element in security failures, with many factors facilitating it in the socio-technical system.
The value of intangible assets in many companies is significant

- Intangible assets include brand, intellectual property, trade secrets etc
- Total value increased $19.8 trillion in 2001 to $47.6 trillion in 2016 (Brand Finance Institute, 2017)
Companies with the highest spending on research and development 2017

Ranking of the 20 companies with the highest spending on research and development in 2017 (in billion U.S. dollars)

Note: Worldwide

Further information regarding this statistic can be found on page 8.
Source: Bloomberg; Capital IQ ID 265645
How big a problem?

• Criminologists well versed in challenges of measuring crime
• ‘Gold standard victim surveys, but non existent for this ‘crime’
• Many organisations don’t know they are victims
• Criminal statistics , have many flaws but useful as barometer?
• Many do not report
  • Implications for reporting (share price, reputation etc)
  • Perpetrators abroad/state actors therefore any success unlikely
  • Criminal justice system perceived to be unlikely to have much interest
• Many countries no specific offences and other offences used
• Making identifying IR/ER cases difficult
• Where civil cases used don’t always reach public domain and/or harder to identify clearly as industrial espionage
• In the UK there have been a handful of successful prosecutions in the last few decades.
Illegal traders of T-Mobile customers' personal data fined more than £73,000

Former T-Mobile employees that stole customer information and passed it on to other companies have been fined more than £73,000 for violating UK data protection laws, the Information Commissioner’s Office (ICO) has said. | 14 Jun 2011

Under the Data Protection Act it is a criminal offence to knowingly or recklessly obtain personal data without consent.

Chester Crown Court ordered David Turley to pay £45,000 and Darren Hames £28,700 in costs under the Proceeds of Crime Act, the ICO said. Hames was also ordered to pay £500 to cover the prosecution’s legal costs, the ICO, the UK’s data protection watchdog, said in a statement.

UK's Dyson accuses Germany Bosch of paying "mole" for tech info

Stephen Eisenhammer

LONDON, Oct 24 (Reuters) - British appliance maker Dyson said on Wednesday it had launched legal proceedings against Bosch in the UK, accusing the German manufacturer of illegally acquiring its technology.

Information about the high-speed digital motors used in its vacuum cleaners and hand dryers had been passed to Bosch by a “mole” working at Dyson’s Malmesbury factory in the southwest of England, the UK company said.

Bosch said it was trying to establish what had happened and it regretted that Dyson had begun legal proceedings.
USA: Prosecutions under 1995 Economic Espionage Act (Priebe, 2014)

<table>
<thead>
<tr>
<th>Year</th>
<th>Number of Cases</th>
<th>Cumulative</th>
<th>Cumulative %</th>
</tr>
</thead>
<tbody>
<tr>
<td>1996</td>
<td>1</td>
<td>1</td>
<td>.9</td>
</tr>
<tr>
<td>1997</td>
<td>4</td>
<td>5</td>
<td>3.8</td>
</tr>
<tr>
<td>1998</td>
<td>7</td>
<td>12</td>
<td>6.6</td>
</tr>
<tr>
<td>1999</td>
<td>7</td>
<td>19</td>
<td>6.6</td>
</tr>
<tr>
<td>2000</td>
<td>5</td>
<td>24</td>
<td>4.7</td>
</tr>
<tr>
<td>2001</td>
<td>9</td>
<td>33</td>
<td>8.5</td>
</tr>
<tr>
<td>2002</td>
<td>12</td>
<td>45</td>
<td>11.4</td>
</tr>
<tr>
<td>2003</td>
<td>5</td>
<td>50</td>
<td>4.7</td>
</tr>
<tr>
<td>2004</td>
<td>2</td>
<td>52</td>
<td>1.9</td>
</tr>
<tr>
<td>2005</td>
<td>7</td>
<td>59</td>
<td>6.6</td>
</tr>
<tr>
<td>2006</td>
<td>7</td>
<td>66</td>
<td>6.6</td>
</tr>
<tr>
<td>2007</td>
<td>10</td>
<td>76</td>
<td>9.5</td>
</tr>
<tr>
<td>2008</td>
<td>7</td>
<td>83</td>
<td>6.6</td>
</tr>
<tr>
<td>2009</td>
<td>6</td>
<td>89</td>
<td>5.7</td>
</tr>
<tr>
<td>2010</td>
<td>10</td>
<td>99</td>
<td>9.5</td>
</tr>
<tr>
<td>2011</td>
<td>6</td>
<td>105</td>
<td>5.7</td>
</tr>
</tbody>
</table>
### Key Findings

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>13</strong></td>
<td>Between late 2015 and mid-2016, 13 suspected China-based groups have compromised corporate networks in the U.S., Europe, and Japan, and targeted government, military, and commercial entities in the countries surrounding China.</td>
</tr>
<tr>
<td><strong>25</strong></td>
<td>Since mid-2014, we have seen a notable decline in China-based groups’ overall intrusion activity against entities in the U.S. and 25 other countries. We suspect that this shift in operations reflects the influence of ongoing military reforms, widespread exposure of Chinese cyber operations, and actions taken by the U.S. government.</td>
</tr>
<tr>
<td></td>
<td>Since taking power in late 2012, Chinese President Xi Jinping has implemented significant military reforms intended to centralize China’s cyber elements and support a greater use of network operations.</td>
</tr>
<tr>
<td></td>
<td>Public reports in recent years have exposed Chinese cyber operations and heightened public awareness of China’s engagement in economic espionage. This likely provided the U.S. government with political support to publicly confront China over the issue.</td>
</tr>
<tr>
<td></td>
<td>In 2014, the U.S. government began to take unprecedented measures in response to claims of Beijing’s cyber-enabled economic espionage. Although many in the U.S. initially doubted that these actions would have any effect, they may have prompted Beijing to reconsider the execution of its network operations.</td>
</tr>
<tr>
<td></td>
<td>We have not seen evidence of a coordinated shift in the behavior of recently active China-based groups—tactical changes appear to be specific to each group’s mission and resources, and in response to public exposure of its cyber operations.</td>
</tr>
</tbody>
</table>
(Since 2013) Three years later, **we see a threat that is less voluminous but more focused, calculated, and still successful in compromising corporate networks.** Rather than viewing the Xi-Obama agreement as a watershed moment, we conclude that the agreement was one point amongst dramatic changes that had been taking place for years. We attribute the changes we have observed among China-based groups to factors including President Xi’s military and political initiatives, the widespread exposure of Chinese cyber operations, and mounting pressure from the U.S. Government. **Yet China is not the only actor in transition: we’ve observed multiple state-backed and other well-resourced groups develop and hone their operations against corporate and government networks.** The landscape we confront today is far more complex and diverse, less dominated by Chinese activity, and increasingly populated by a range of other criminal and state actors (p 15).
Serious political attention and action in some countries

Donald J. Trump
@realDonaldTrump

As China is built on corporate espionage, currency manipulation & cheap labor, its economy is a ticking time bomb

bit.ly/13pFxIz

1:45 PM - 28 Feb 2013

134 Retweets 50 Likes

Donald J. Trump
@realDonaldTrump

China is stealing our jobs. We need to demand China stop manipulating its currency and end its rampant corporate espionage.

11:26 AM - 28 Sep 2011

298 Retweets 120 Likes
Costs

• Lots of global and national estimates of varying quality
• Cross-over with other means to secure intellectual property
• Cost of counterfeit goods, pirated software, and theft of trade secrets and could be as high as $600 billion (IP Commission, 2017)
• Espionage via hacking costs the US economy $400 billion per year (IP Commission, 2017)
• Trade secret theft costs 1% and 3% of GDP, meaning that the cost to the $18 trillion U.S. economy is between $180 billion and $540 billion (IP Commission, 2017)
• Espionage via cyber $10-$12 billion cost to USA and $50-$60 billion globally (CSIS, 2018)
• An earlier report by CSIS estimated global cost of $445 billion or 1% of global income (Wahsington Post, 2014)
Cost to the UK

- Specific assessment in the UK found total cost of cyber crime to be £27 billion of which
  - £7.6 billion attributed to industrial espionage
- Specific sectors
  - £2 billion financial services
  - £1.2 billion aerospace and defence
  - £1.6 billion mining
- Cabinet Office/Detica (2011)
As a comparison to put in perspective

- Home Office last estimated the total cost of crime in 2000
- Commercial/public organisations (actual losses, excluding additional costs)
  - £1.5 billion theft from shop
  - £1.3 billion criminal damage
  - £1.1 billion burglary
- Of total of £10.3 billion property stolen/damaged (Home Office, 2000)
Industrial espionage in the news in the UK

Business suffering 'industrial scale' cyber theft, warns GCHQ head

Robert Hannigan, Director of GCHQ, warns of scale of hacking on business as he launches Britain's first National Cyber Security Centre

70 cyber-espionage attacks a month stealing UK business secrets on “industrial scale”

By Will Dalton  July 01, 2013  News

Hackers stealing trade secrets on industrial scale, warns spy chief

Business secrets in the UK are being stolen on an “industrial scale” in the growing cyber war, the head of the GCHQ has warned.

Corporate espionage on 'an industrial scale' targeting the UK

One company suffered £800m loss due to espionage, says MI5 head
Announcements: speeches

You can use the filters to show only results that match your interests

Contains
- espionage

Announcement type
- Speeches

Policy area
- All policy areas

Department
- Prime Minister's Office, 10 Downing Street

Person
- The Rt Hon Theresa May MP

World locations
- All locations

Include local news from UK embassies and other world organisations

2 announcements by Prime Minister's Office, 10 Downing Street by The Rt Hon Theresa May MP containing espionage

Get updates to this list
- emial
- feed

PM statement in Denmark: 9 April 2018
- 9 April 2018
- Number 10
- Speech

PM speech to the Lord Mayor's Banquet 2017
- 13 November 2017
- Number 10
- Speech
Research on industrial and economic espionage

• Given the scale of the problem and the political interest in this issue (in some countries) there is surprisingly little research
Thin base of ‘dedicated’ research

- Robbery 1931
- Fraud 5608
- Bribery 869
- Denial of service attacks 127
But, there are silos of knowledge
The Cyber Security Breaches Survey 2018 is a quantitative and qualitative survey of UK businesses and, for the first time in 2013, of charities. The survey was carried out in winter 2017 and the qualitative survey in early 2018. It helps organisations to understand the nature and significance of the cyber security threats they face, and what others are doing to stay secure. It also supports the Government to shape future policy in this area.

**Main report**

Dr Rebecca Kair, Joyesh Navin Shah, Paul Smith, Tom Reesington and Gemma Postle

**Institute for Criminal Justice Studies, University of Portsmouth**

**May 2016**

**Cyber Security Breaches Survey 2016**

**Main report**

Dr Rebecca Kair, Jyothi Amali and Jayesh Navin Shah

**Institute for Criminal Justice Studies, University of Portsmouth**

**April 2017**

**Cyber security breaches survey 2017**

**Main report**

Dr Rebecca Kair, Joyesh Navin Shah, Paul Smith, Tom Reesington and Gemma Postle

**Institute for Criminal Justice Studies, University of Portsmouth**

**May 2016**

**Cyber Security Breaches Survey 2016**

**Main report**

Dr Rebecca Kair, Jyothi Amali and Jayesh Navin Shah

**Institute for Criminal Justice Studies, University of Portsmouth**

**April 2017**

**Cyber security breaches survey 2017**

**Main report**

Dr Rebecca Kair, Joyesh Navin Shah, Paul Smith, Tom Reesington and Gemma Postle

**Institute for Criminal Justice Studies, University of Portsmouth**
Organisations experiencing cyber breaches

- Businesses experiencing cyber security breach in past 12 months
- Large firms experiencing cyber security breach in past 12 months
Figure 3.2: Updates given to senior management on cyber security

Q. Approximately how often, if at all, are your organisation's directors or senior management given an update on any actions taken around cyber security?

- % never
- % less than once a year
- % annually
- % quarterly
- % monthly
- % weekly
- % daily
- % each time there is a breach
- % don't know

Businesses

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>% never</td>
<td>20</td>
</tr>
<tr>
<td>% less than once a year</td>
<td>7</td>
</tr>
<tr>
<td>% annually</td>
<td>12</td>
</tr>
<tr>
<td>% quarterly</td>
<td>14</td>
</tr>
<tr>
<td>% monthly</td>
<td>19</td>
</tr>
<tr>
<td>% weekly</td>
<td>9</td>
</tr>
<tr>
<td>% daily</td>
<td>8</td>
</tr>
<tr>
<td>% each time there is a breach</td>
<td>5</td>
</tr>
<tr>
<td>% don't know</td>
<td>4</td>
</tr>
</tbody>
</table>
Figure 4.10: Whether organisations have formal policies or document cyber security risks in any way

- % with formal policy or policies covering cyber security risks:
  - Businesses overall: 27
  - Within micro firms: 20
  - Within small firms: 39
  - Within medium firms: 59
  - Within large firms: 74
  - Charities overall: 21

- % with cyber security risks documented in business continuity plans, internal audits or risk registers:
  - Businesses overall: 28
  - Within micro firms: 21
  - Within small firms: 37
  - Within medium firms: 59
  - Within large firms: 77

Base: 1,519 UK businesses; 655 micro firms; 349 small firms; 263 medium firms; 252 large firms; 569 charities

Figure 4.12: Whether organisations have board members or trustees with responsibility for cyber security

- % of organisations where there are board members or trustees with responsibility for cyber security:
  - Businesses overall: 30
  - Within micro firms: 28
  - Within small firms: 32
  - Within medium firms: 48
  - Within large firms: 62
  - Within info/communications: 49
  - Within finance/insurance: 47
  - Charities overall: 24

Base: 1,519 UK businesses; 655 micro firms; 349 small firms; 263 medium firms; 252 large firms; 99 information or communications firms; 105 finance or insurance firms; 569 charities
Figure 4.8: Organisations where staff have had cyber security training in the last 12 months

% of organisations where staff have attended internal or external training, or seminars or conferences on cyber security in the last 12 months

- Businesses overall: 20%
- Within micro firms: 16%
- Within small firms: 26%
- Within medium firms: 43%
- Within large firms: 65%
- Within info/comms: 38%
- Within finance/insurance: 59%
- Charities overall: 15%

Bases: 1,519 UK businesses; 655 micro firms; 349 small firms; 267 medium firms; 252 large firms; 99 information or communications firms; 105 finance or insurance businesses; 36 charities
<table>
<thead>
<tr>
<th>Step Description</th>
<th>How Derived from the Survey</th>
<th>Businesses</th>
<th>Charities</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Information risk management regime – formal cyber security policies or other documentation and the board are kept updated on actions taken</td>
<td>35%</td>
<td>27%</td>
</tr>
<tr>
<td>2</td>
<td>Secure configuration – organisation applies software updates when they are available</td>
<td>92%</td>
<td>75%</td>
</tr>
<tr>
<td>3</td>
<td>Network security – firewalls with appropriate configurations</td>
<td>89%</td>
<td>69%</td>
</tr>
<tr>
<td>4</td>
<td>Managing user privileges – restricting IT admin and access rights to specific users</td>
<td>78%</td>
<td>65%</td>
</tr>
<tr>
<td>5</td>
<td>User education and awareness – staff training, or formal policy covers what staff are permitted to do on the organisation’s IT devices</td>
<td>30%</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Incident management – formal incident management plan</td>
<td>13%</td>
<td>8%</td>
</tr>
<tr>
<td>7</td>
<td>Malware protection – up-to-date malware protection</td>
<td>90%</td>
<td>73%</td>
</tr>
<tr>
<td>8</td>
<td>Monitoring – monitoring of user activity or regular health checks to identify cyber risks</td>
<td>55%</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Removable media controls – policy covers what can be stored on removable devices</td>
<td>18%</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Home and mobile working – policy covers remote or mobile working</td>
<td>18% (versus 23% in 2017)</td>
<td>12%</td>
</tr>
</tbody>
</table>
Figure 4.16: Progress in undertaking action on the 10 Steps by size of business

- **Businesses overall**
  - % that have undertaken action on five or more of the 10 Steps: 55
  - % that have undertaken action on all of the 10 Steps: 4

- **Within micro firms**
  - % that have undertaken action on five or more of the 10 Steps: 49
  - % that have undertaken action on all of the 10 Steps: 2

- **Within small firms**
  - % that have undertaken action on five or more of the 10 Steps: 65
  - % that have undertaken action on all of the 10 Steps: 7

- **Within medium firms**
  - % that have undertaken action on five or more of the 10 Steps: 83
  - % that have undertaken action on all of the 10 Steps: 17

- **Within large firms**
  - % that have undertaken action on five or more of the 10 Steps: 94
  - % that have undertaken action on all of the 10 Steps: 27

- **Charities overall**
  - % that have undertaken action on five or more of the 10 Steps: 40
  - % that have undertaken action on all of the 10 Steps: 3

Bases: 1,519 UK businesses; 655 micro firms; 349 small firms; 263 medium firms; 252 large firms; 19 charities
Cyber Skills Shortage

• Booz Allen Hamilton (2017) estimate the number of unfilled jobs worldwide will reach 1.8 million by 2022.

• The Centre for Strategic and International Studies (2016) based upon a survey of IT decision-makers in eight countries found 82% of respondents reported a shortage of cyber security skills and that this shortage was worse than for other IT skills.

• The same research identified that 15% of cyber security positions could be unfilled by 2020.

• Booz Allen Hamilton (2017) found two-thirds of organisations surveyed would not have enough cyber security operatives to meet the challenges they face.

• The ISCA (2017) found that a quarter or organisations surveyed took on average six months to fill a position and that competition for such jobs was weak.
Much evidence of human weakness in IT systems

• Start of vast majority of cyber-breaches are phishing attacks
• Steyn et al (2007) found of 400 randomly selected staff in an organisation when asked to send their password 53% complied.
• Phishme (2016) 40 million simulated emails quarter to fifth regularly fall
• Goel et al (2017) study of students sent 7225 mails of which 27.3% opened, 13.3% clicked on the link embedded in the mail
• Kumaraguru et al (2007) 93% of spam email identified and embedded training increased detection by participants further
Opportunities for big data and other traditional methods to predict insider risks

• Extensive research on insider threats
• Insiders associated with
  • Workplace activities: unusual copying, IT activity, unauthorised storage of sensitive materials, commits security violations
  • Workplace attitudes: poor work attitude, stressed, exploitable lifestyle, negative life events
  • Psychological profiles (CPNI, 2013)
• Gheyas and Abdallah (2016) have identified most effective algorithms
The human element

• Central to the problem of industrial espionage is the human element
• Central to most cases will be: malicious insider or mistake by insider
• Central to tackling industrial espionage in the future is information security which fuses cyber-technical and human elements to enhance security
“An enthusiastic tale of how the humble leaf became a global addiction.”
—Financial Times

For All the Tea in China
How England Stole the World’s Favorite Drink and Changed History

Sarah Rose
Conclusion and further thoughts

- Economic and industrial espionage are significant problems and major risks to intellectual property risk organisations and countries
- Commitment and resources vary in countering the problem
- Lack of research on this very important problem
  - How much of a problem ‘what gets measured gets done’
  - What are organisations doing to counter this problem and what more could be done?
  - What works in tackling this problem?
- The information security community has major role to play in tackling this problem
  - Developing systems that minimise risks in human element
  - Developing robust secure systems
  - Using data to identify good ‘red flags’ to minimise false positives
Thank you
References


