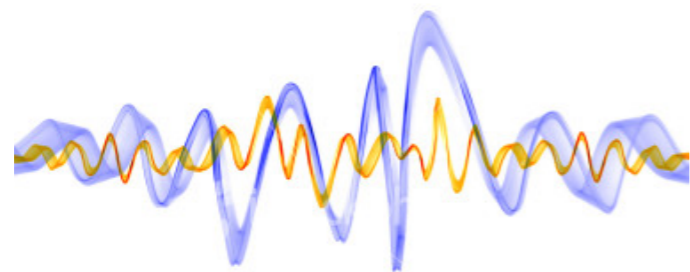


ASIS International 4th Asia-Pacific Conference - 2010

The Financial Crisis and Corporate Espionage



Julian Claxton

Jayde Consulting Pty Ltd
Servicing the Asia Pacific Region

Presentation Agenda

- Disclaimer
- Espionage - Who is at risk?
- Ways In Which Espionage Can Occur
- Case Studies and Lessons Learned
- Minimising The Risk
- Summary and Conclusion
- Questions

Disclaimer

- The information contained in this presentation provides an introductory overview to the everyday risks associated with corporate espionage, particularly during times of financial crisis. The aim of this presentation is to help raise awareness as to the threats associated with corporate espionage and the measures that can be taken to minimise such threats.
- The information relating to Starwood and Hilton Hotels; Air Canada and Westjet; and Coca-Cola and Pepsi-Cola, is entirely sourced from open-source media. Therefore, we will not accept liability for inconsistencies in the information provided and advise that further independent research be conducted for confirmation of the facts relating to each case.
- Other case studies and related advice, are based on Jayde Consulting's corporate experience in the counter-espionage sector. This presentation should not be taken to be a comprehensive assessment of the corporate espionage threat. Those attending are strongly advised to contact Jayde Consulting for further information concerning the topics raised.

Espionage - Who is at risk?

“Starwood sues Hilton, alleges corporate espionage”

“Deutsche Bank spy saga grows”

“Westjet apologises to Air Canada for snooping”

“Hewlett-Packard’s spy network more extensive than reported”

“Coke secrets case likened to spy novel”

Ways In Which Espionage Can Occur

- Technological Advances
 - Spy software, USB drives, email, recorders, mobile phones, transmitters (bugs)...
- Internal Sources
 - Staff - disgruntled, financially struggling, bribery, extortion
 - Opportunistic theft by employees, contractors or visitors
- Targeted Theft
 - Information specifically sourced and sold to competitors
 - Competitive intelligence (posing as potential employee or open-source info.)
- Workplace Negligence
 - Loose lips, failure to log-off computers, information left in the open, poor access control, complacency...

Case Study - Starwood / Hilton Hotels

- How did it occur?
 - Theft of confidential and commercially sensitive information by ex-employees
 - Personal email accounts allegedly used to steal information
 - Stolen information used to expedite new employer's entry to luxury hotel market
 - Plan backfired when theft was discovered
- Lessons Learned...
 - Restrict use of personal emails in the workplace
 - Monitor internet activity of all staff, and flag sensitive-file transfers
 - Carry out exit interviews upon resignation / termination

Case Study - Coca-Cola / Pepsi Cola

- How did it occur?
 - Trusted employee stole sensitive information purely for financial gain
 - Rival company blew whistle once approached
- Lessons Learned...
 - Utilise comprehensive security camera surveillance to help deter theft and provide evidence following an incident
 - Ensure that sensitive information is only accessible to those for whom it is absolutely necessary
 - Remember that even the most trusted employees carry out espionage, regardless of their tenure with the company, rank or status
 - Pay particular attention to employees with financial problems or those exhibiting an uncharacteristic dislike for colleagues and company

Case Study - Air Canada / Westjet

- How did it occur?
 - Former Air Canada employee retained access to company website (intranet) upon departure
 - New employer Westjet, used this access to influence expansion strategy and gain a significant competitive advantage. Access granted more than 240,000 times over a one year period!
- Lessons Learned...
 - Limit access to commercially sensitive information stored online to those who absolutely require it
 - Suitably plan and execute employee terminations and resignations, ensuring that access to corporate information is swiftly terminated or restricted
 - Closely monitor intranet access from unknown external sources

Jayde Consulting - Client Case Study (1)

- Significant international retail group
 - Individual socially engineered his way into client premises. He remained on premises overnight and without detection
 - Significant security vulnerabilities identified during counter-surveillance inspection
 - Eavesdropping equipment would not have been required to gather intelligence
- Primary actions taken... (albeit too late)
 - Security in depth - electronic access control quickly enhanced, including the installation of additional card readers, motion sensors and alarms
 - Closed circuit television cameras were installed at all entry / exit points and in critical working areas
 - Staff educated on threats to business as a result of social engineering

Jayde Consulting - Client Case Study (2)

- Logistics and transport firm
 - Precautionary counter-surveillance inspections requested and conducted
 - Wireless transmitter (bug) found operating in a power double adaptor
 - Perpetrator was identified as being a supervisor within the organisation
- Primary actions taken...
 - Examinations were conducted of perpetrator's computer, revealing numerous audio recordings of sensitive meetings
 - Perpetrator was interviewed and confessed, claiming it was for personal use!
 - Client reluctant to terminate the supervisor as he maintained control of a significant number of staff and the group's largest client portfolio
 - Still employed today, despite our findings and his confession

Minimising The Risk

- Install and monitor electronic security systems
 - Access control, alarms and closed circuit television systems all reduce likelihood of an incident occurring (deterrent factor) and provide an audit trail of events
- Monitor and review all contractor activity onsite
 - Provide internal escort of cleaners, plant and maintenance contractors, delivery staff and all other external vendors, when onsite
 - Issue visitor badges and log all onsite activity
 - Randomly review camera footage of works undertaken by contractors
- Conduct background checks of all employees and contractors
 - Verify employment and academic history
 - Criminal history checks locally and abroad

Minimising The Risk *(Continued...)*

- Instil strict computer and information technology security policies
 - Lockout USB and portable hard drives
 - Restrict use of personal email and web-surfing
 - Ensure laptops are secured at ALL times
 - Activate automatic logoff of all computer terminals after a set period of inactivity
 - Maintain a strict policy to ensure passwords are regularly updated
 - Password must NOT be written anywhere onsite!
 - Implement encryption programs that secure all information stored on laptops, computers, portable hard-drives (including USB's) and smart-phones
 - Conduct regular audits of staff to confirm compliance

Minimising The Risk *(Continued...)*

- Containment and security of sensitive information is essential
 - Limit access to sensitive information only to those who require it
 - Ensure that document controls and classifications are used to limit opportunistic theft
 - Maintain a clean desk policy across all areas as a matter of course
 - Cross-shred discarded paperwork
- Monitor employee attitudes
 - Be aware of sudden changes in personality and/or financial status
 - Investigate excessive sick leave or sudden unreliability
 - Implement a staff support programme, including confidential assistance

Summary & Conclusion

- Espionage typically increases during times of financial hardship and often goes undetected
- All organisations and most individuals are susceptible
- Electronic surveillance is becoming increasingly easy to undertake
- Preventative measures must be adopted to mitigate the risk
- Counter-espionage policy and practices should become standard within all organisations
- Don't be complacent, as the fallout could potentially be devastating for you and your organisation

Questions?



Jayde Consulting Pty Ltd | Level 4, 185 Elizabeth St. Sydney NSW 2000 | +61 2 8006 0635

Julian Claxton | +61 418 960 635 | julian@jaydeconsulting.com

www.jaydeconsulting.com

Australia | Hong Kong