
ASIS INTERNATIONAL
Comprehensive Counterespionage Program for Businesses
Bruce Wimmer, CPP
Senior Director G4S Corporate Risk Services

# What is “Business Espionage”?

- **Corporate Espionage** – focused on companies spying on other companies and intra-national
- **Industrial Espionage** – also more intra-national and focused on processes
- **Commercial Espionage** – focused on companies spying on companies
- **Economic Espionage** – focused on business, not national security oriented but conducted by governments
- ***Business Espionage* – all types of spying, intra and internationally, by other companies and by governments with a business interest**

# Business Espionage Adverse Impact

- It is often a ***catastrophic*** adverse impact but does not get the attention it should be getting
- Compare:

Global ***Business Espionage*** - $***1.5 Trillion*** a year - or ***$7.5 Trillion*** over five years (U.S. House of Representative hearings)

All costs related to ***9/11*** over a five-year period - $3 Trillion (N.Y Times study)

Global ***Computer Hacking*** - $400 Billion a year (Lloyds of London)

Global ***Earthquakes*** in 2014 - $313 Billion (Insurance Information Institute)

Hurricane ***Katrina*** - $12.5 Billion (Aon Insurance)

Hurricane ***Sandy*** - $ 6.5 Billion (Aon Insurance)

***Severe Weather*** - $5 Billion a year average in U.S. (Aon Insurance)

***Theft of all types*** in U.S. - $200 Billion a year average (American Management Association)

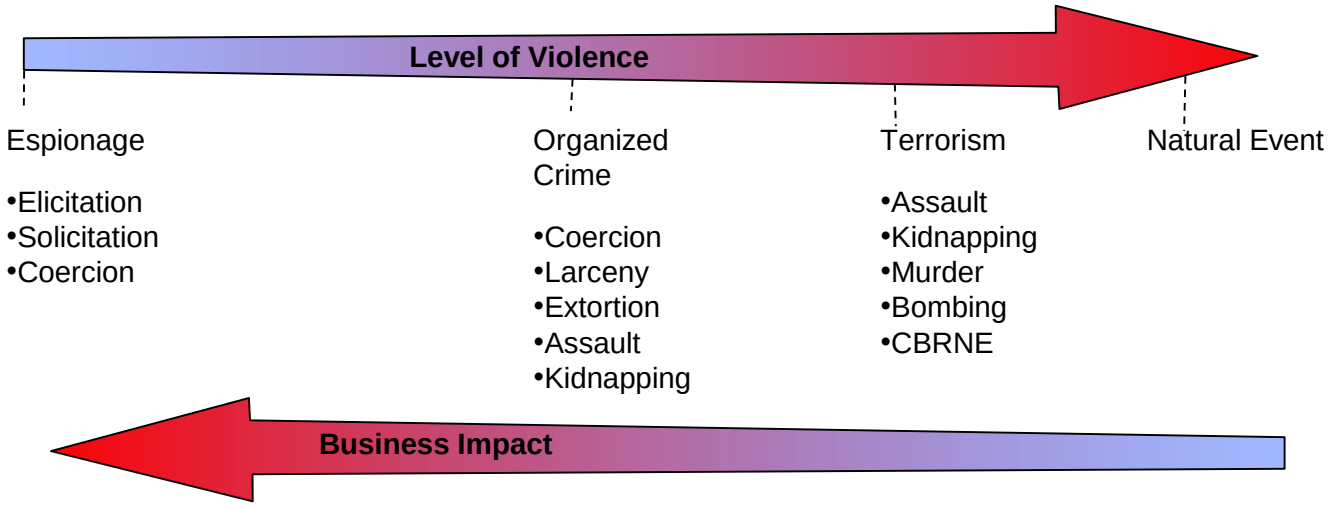
***Retail Theft*** in the U.S. - $44 Billion a year average (National Retail Federation)

***Fires*** in the U.S. - $20 Billion a year average (National Fire Protection Association)

# Business Espionage is an International Issue

The Business Espionage Threat in some countries is higher than others, just like the Physical Threats vary country-by-country.

Our ***travel intelligence*** inputs reflect the physical and political issues…how much emphasis is there on the Business Espionage Threats?



# PHYSICAL SECURITY

Much sensitive business information is stolen:

- Using all the latest eavesdropping equipment
- Printing off or grabbing up printed documents
- Trash covers
- Recruiting or ‘planting’ a spy within the organization
- **Social engineering**
  - In fact, social engineering is often used as a way to get into the IT systems


# CYBER SECURITY

- Theft of sensitive information often involves IT
- Much sensitive information is stored on IT systems (like banks store money)
- Cyber security has done a reasonably good job of articulating the Cyber only Threats


Willie Sutton – Bank Robber

# TOP COUNTERMEASURES

- Have a comprehensive program that looks at Cyber and Physical security holistically and not in silos
- Identify the most sensitive information and give it the highest levels of protection
- Education and awareness so you have an aware workforce that is reporting concerns and understands the consequences
- A good risk-based cyber security program
- A good risk-based physical security program where people understand the “why’s”
- Travel security that pro-actively looks at business espionage threats
- Top leadership support and example setting
- Risk-based Technical Surveillance Countermeasures

# G4S | Conclusion

- Business Espionage is occurring all over the globe
- Business Espionage can affect businesses of all types and sizes
- Business Espionage is not “James Bond” stuff
- Business Espionage deserves our attention
- Business Espionage involves **BOTH**
  - ***Cyber/IT Security***
  - ***Physical Security***
- We need a comprehensive, combined security approach for this significant and complicated security issue

- **For more details:**

  - Take a look at the poster
  - Contact me:

    Bruce Wimmer,
    Senior Director G4S Corporate Risk
    email: Bruce.Wimmer@usa.G4s.com
    phone:  352 238-0392

  - Or read my book:

**Business Espionage: Risks, Threats and Countermeasures**