UID: U01155118

Analyzing the Consequences of Electronic Espionage on Modern Businesses

In this modern digital century, cyber security has been more concerning due to electronic espionage and unauthorized access to modern businesses, organizations and even governments and their organizations. It may pose to the target entity, a far greater and irreparable damage whether it be as small as financial statements getting leaked, to the entity shutting down once and for all. The below analysis explores four major harms businesses may face.

1. **Theft or exposure of trade secrets**
   Trade secrets such as formulas for a recipe, product designs, operational and/or structural blueprints, business logics and connections, etc are the most valuable assets for a business; and the very backbone of a company when revealed, the company most likely faces its downfall pretty soon.
   For example: In 2006, a Coca-Cola secretary attempted to sell new product samples to Pepsi for 1.5 million US dollars. However, Pepsi informed Coca-Cola and the FBI, preventing the theft. If the espionage had been successful, it could have jeopardized Coca-Cola's global market position, decades of investment and research, its customer base and a lot more.
   Trade secret compromisation leads decades if not years of research, investment and outcome to go in vain, in turn leaving a company shattered at its core while trying to compete from scratch with something new.
2. **Financial Loss or Market Devaluation**
   A business most likely faces direct or indirect financial loss and/or market devaluation due to cyber espionage. Such loss may cost a business a huge sum of money to recover from, and get back to a stable position in the market financially.
   For example: Imagine the top GPU manufacturing company - NVIDIA's business secrets such as research, GPU/CUDA blueprints and future projects got leaked to one of its top competitors, let's say Intel; then the stock price would rapidly drop leading NVIDIA to possibly lose tens of billions of dollars in market capitalization and contracts from various customers.
   Such incidents lead to shareholder conflicts, introduces duopoly to the market and undermines trust in trade secret and innovation safety, hollowing the company from inside out.
3. **Legal and Regulatory Consequences**
   Electronic espionage often includes legal authorities and investigations, lawsuits and penalties, especially when an entity being targeted is not fully in compliance with the laws and regulations.
   For Example: Snowden's disclosure of revelation of the NSA's *global surveillance programs* such as *PRISM*, *XKeyscore*, that collect the e-mail, voice, text and video chats of foreigners and a large number of Americans from Microsoft, Google,

Facebook, Yahoo, Apple and other tech giants along with other government agencies from Australia, the UK, the Netherlands, Germany, Sweden, and few more. These revelations raised global concerns about data privacy and compliance with international privacy laws, companies like Microsoft and Google faced lawsuits and heavy regulatory scrutiny in Europe,

Such a threat poses significant risk causing a business to face lawsuits and penalties while blurring the national and international mass customer relationship.

References:

- The real sting: how plot to betray Coke fell flat after Pepsi called in FBI | Marketing & PR | The Guardian
- Edward Snowden: the whistleblower behind the NSA surveillance revelations | The NSA files | The Guardian
- 2010s global surveillance disclosures - Wikipedia