COMPANIES CHARGED WITH ESPIONAGE

PUBLISHED
18 December 2018

CATEGORY
Crime

CRIME · DECEMBER 2018

Companies Charged with Espionage

Thoughts of espionage often conjure up in one's mind images of shadowy government agencies stealing documents, tapping phones, compromising individuals, or using the Internet to gain information about other nations – both foe and ally alike, and, while it is true that such activities do occur, occur often, and will continue to occur in the future, there are other forms of espionage that are also significant threats to the public. Corporate espionage is one such threat. Corporate espionage involves either other companies – foreign or domestic – or other countries illegally acquiring competitive information – such as trade secrets, customer lists, pricing lists, etc. – and subsequently using such information to gain an advantage over the victim in a given market. It should be noted that this is different from competitive intelligence which is a legal practice that involves using legitimate methods to acquire an understanding about a competitor so that one's company is better equipped to succeed in a market; furthermore, although already mentioned, it is significant that corporate espionage is not simply an activity that companies engage in against one another. Rather, some nations – especially those with significant state-owned enterprises – have been credibly accused of engaging in corporate espionage against the foreign competitors of so-called national champions.

It may seem, to the average individual, that this is not necessarily an issue that ought to concern them; however, there are significant economic costs that impact businesses and, subsequently, impact employment. McAfee, in a research study, found that the total cost of cybercrime is $600 billion a year; notably, the largest category – comprising 25% of the total – is corporate espionage. In fact, in a recent report, the Director of National Intelligence noted that countries such as China have government associated hacking groups that use information technology to compromise foreign competitors to Chinese companies; this is in addition to complaints that non-Chinese companies have made that China's system of forced joint ventures involves using coercion to require the turnover of the intellectual property. The same report further noted that cybersecurity researchers found that there was a link between Chinese hackers and a backdoor in the extremely popular CCleaner utility that helped Chinese actors target American firms such as VMware and Google. Also, in 2017, the United States indicted three Chinese nationals for cybercrimes related to corporate espionage against a variety of American firms in finance, engineering, and technology.

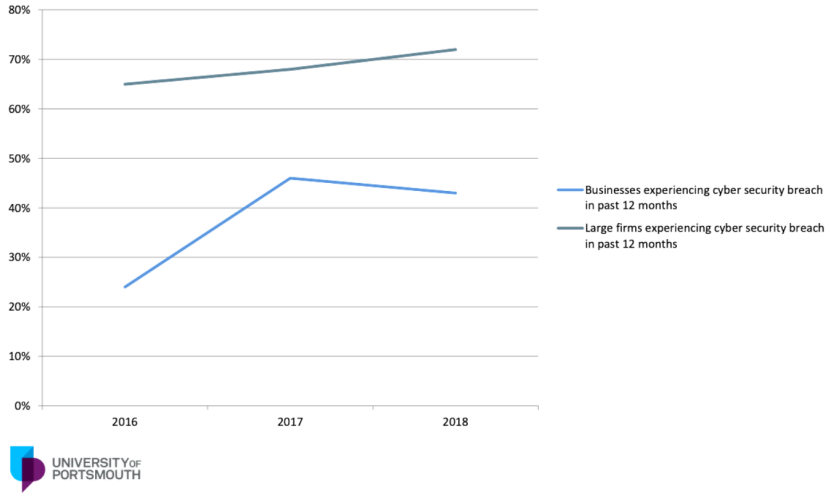
Outside of nation-states acting against foreign firms, prominent companies have engaged in such actions. Hilton Hotels, for example, hired away executives from Starwood – whose lifestyle resorts Hilton wanted to replicate – and acquired trade secrets of Starwood to attempt to disadvantage them. The final legal agreement required the payout of $75 million dollars to Starwood and Hilton undergoing numerous restrictions to remedy the damage. In another case, Hewlett-Packard spied on its own board members in an attempt to discern the source of specific leaks; the consequences, upon discovery, resulted in the departure of some executives.

With the growth of more targets – for example IoT and mobile devices – it is evident that the trend will be for some companies and countries to target competitors to attempt to attain an illegitimate advantage.

© 2018 ThreatRate Risk Management. All Rights Reserved

While organizations have been increasingly cognizant of their need to develop cybersecurity risk management plans, more work likely needs to be done to protect the integrity of trade secrets and other intellectual property from corporate espionage efforts.

ORGANIZATIONS EXPERIENCING CYBER BREACHES



Soundbite analytics

- In 2018, Iranian associated hackers stole IP from 144 American universities.
- The FBI, in 2015, noted an increase of over 50% in espionage cases.
- Espionage via hacking costs the US economy $400 billion per year (IP Commission, 2017)
- Trade secret theft costs the US economy 1% - 3% of GDP, or $180 billion - $540 billion (IP Commission, 2017)
- Espionage via cyber is estimated to cost $10-$12 billion to USA and $50-$60 billion globally (CSIS, 2018)
- The FBI noted that Chinese sources are alleged assailants in more than 90% of the cases.
- More than 25% of Pharma companies spend $2 million or more per year on Competitive Intelligence.

SOURCES

1 https://securingtomorrow.mcafee.com/business/economic-impact-cybercrime-cyber-espionage-isnt-just-militarys-problem/

2 https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf

3 https://www.csoonline.com/article/3285726/security/what-is-corporate-espionage-inside-the-murky-world-of-private-spying.html

4 https://www.csoonline.com/article/3285726/security/what-is-corporate-espionage-inside-the-murky-world-of-private-spying.html

© 2018 ThreatRate Risk Management. All Rights Reserved



Risk intelligence that keeps you safe

ABOUT THREATRATE

ThreatRate helps you benchmark your risk management strategy against rapidly evolving global and local trends, with real-time, actionable analytics and insights.

For more information contact us at

info@threatrate.com

MEMBERS HAVE ACCESS TO

100+
risk-focused reports published annually

API
customised access option

Dashboards
customised dashboards and infographics

Experts
ThreatRate analysts with cross-industry depth

© 2018 ThreatRate Risk Management. All Rights Reserved

ThreatRate RISK MANAGEMENT