

Corporates run for cover to stave off espionage

Sruti Nayani HYDERABAD



CORPORATE espionage has hit the ground running and companies are hurriedly running for cover. While almost all organisations are at risk, it's companies that are engaged in big-ticket M&As and R&D and high attrition industries like IT/ITES that are particularly vulnerable.

Corporate espionage involves obtaining confidential information about an organisation without the holder's permission. This could be company property, software or intellectual property or customer information. While corporates admit, off the record, that it is quite rampant, they would not part with specifics for the same reasons of security.

"There is no product that can be plugged in to prevent corporate espionage. However, organisations are utilising new age counterespionage firms that work with clients

to establish frameworks, which minimise the chances of espionage and increase detection speeds," says Mahindra Special Services group CEO Captain Raghu Raman.

Some of the strategies used by companies involve tracking down patterns that show aberrations or using the barium feed, where sensitive data is fed deliberately to determine where and through whom it surfaces. Most of these strategies require a high degree of co-ordination to execute and track down the source. However, a handful of sophisticated companies



have also used the espionage channel to feed disinformation to their competition by giving them misleading information, says Raman.

These risks can also be prevented at the organisational level with good governance, good ethics and values practiced by senior management, experts say. Audits, benchmarking, best practices and active communication within the organisation are methods to check such situations. **“Further, the established processes need to be periodically reviewed and improved based on changes in technology and fresh evidence,” says Breakthrough Management MD Naresh S Shahani.**

Corporate espionage involves obtaining information by accessing the place where the information is stored or accessing people, who have access to information and will divulge it through some kind of subterfuge, explains Enforcers of Intellectual Property Rights chairman and managing director Zaheer Khan. Some information that is at risk could range from source code for new softwares, to intellectual property, marketing plans, and research documents, among others.

“At the implementation level, some use of appropriate technology will help,” says Mr Shahani. However, it is difficult to quantify the losses involved in corporate espionage.

“This is not a field where data is available,” says Capt Raman. Detection rate in corporate espionage is fairly low. There are also cases where even if instances are detected, people tend to shy from reporting it. “Establishing guilt is expensive and again requires specialist intervention. Finally, prosecution in such cases is rare,” adds Raman.

- Corporate espionage is obtaining crucial info of a co without holders’ permission

- Cos use counter espionage firms to increase detection
- Companies track down patterns which show aberrations
- Audits, benchmarking ways to curtail these practices