Intellectual Property Theft: Even your company is vulnerable

Intellectual property, whether owned by an individual or corporate, is at the heart of many company's value propositions: think of pharmaceutical patents, new satellite technologies, creative content like Harry Potter books, code that distinguishes new software products and formulas such as those that define Coca-Cola are inventions and creations that belong to their owners and which distinguish a very real economic advantage, one that was hard-won overs years of invention, innovation and research.

Starting with data theft by employees using the evil USB. For such a small device, a USB flash drive can allow an employee to copy large amounts of corporate IP such as client lists, databases, design drawings or legal and financial documents. Even if you have robust end-point security and establish rigid policies about employee use of these drives, employees still find a way to copy information onto these portable storage devices. While other security breaches are more traceable, a flash drive is more difficult to monitor, especially when it leaves the office.

Loss of intellectual property can have wide-reaching ramifications for a company: its loss affects first-to-market advantage, and can in some cases lead to the loss of an entire line of business to counterfeits and competitors. Understandably, intellectual properties such as these are high value targets for hackers and industrial spies. With the advancements in digital and information systems, as well as the flourishing of the internet into a globe-spanning network, intellectual property is now more vulnerable than ever.

The digital arsenal available to hackers and nefarious competitors is not only powerful, but grows in extent and sophistication daily: rootkits that can take control of individual systems; botnets that connect compromised machines to work in tandem to steal data or attacking servers; the interception of wireless systems or diversion of wireless networks; not to mention the host of social engineering methods such as phishing (fake emails) and vishing (fake voice calls) that can gain access to your employee's computers and by extension your company's critical and sensitive information.

The obvious line of defence against IP theft is a well-planned and extensive cybersecurity and data protection strategy. Such a strategy must be supported by careful contingency planning if and when a breach occurs.

Clear cut and well-planned cyber security is, however, often undermined by the very nature of innovation development. The cut and thrust of developing new commercial ideas and product innovations, combined with share-holder pressure for quick results, means internal project teams are governed by a need for action rather than caution. Flat structures, open access to project information by all members of the project team, free dialogue and debate (often over email) are the hallmarks of incubating great ideas. They are also unfortunately the hallmarks of high risk.

Add to that the natural resignations and movements of professionals and staff members between companies (often within the same market segment) and you have a veritable sieve of information. Whether conscientiously stealing information or innocently forwarding company emails to themselves as backups, the access key members of staff have to company information is as much an IP theft risk as online data breaches.

It is also critical to note that whilst most of us don't run big Pharma companies or Coca-Cola, we must frame our own company's risk of IP theft as highly. Whether you are a car dealership whose new contact list gets stolen, or a small business who has had details of their bank loans, lease agreements or other contracts stolen there is, relatively speaking, as much to lose.

The question remains: What can be done? Real-world management strategies and specialist online tools exist to protect companies from IP theft. A structured and clear-eyed audit of human resource processes, implementation of information controls and an approach to project management that is at once cautious and ambitious are just some of the tactics that need to be considered.

Our next post will be by Malcolm Burrows, Principal of Dundas Lawyers who will talk about what can be done from a legal perspective to limit loss suffered by organisations that have had their intellectual property or confidential information stolen.

ODS remains at the forefront of managing your informational risks, let's talk about solutions that protect your company, your proprietary and sensitive information and which enable better business.

By Johann Koelmeyer (CEH) - Cyber Security Engineer

ODS
Online Digital Security
Your trusted defence against Cybercrime