

Five Biggest Mistakes Made in the Failure to Protect Intellectual Property

By Kevin Doyle, CISSP, ISSMP,
CISA, CISM

Introduction

United States Secretary of Commerce Gary Locke is quoted as saying, “Every year, American companies in fields as diverse as energy, technology, entertainment and pharmaceuticals lose between \$200-\$250 billion to counterfeiting and piracy.” U.S. intellectual property is worth \$5-5.5 trillion - more than the gross domestic product (GDP) of any other country. (Source: “The Economic Value of Intellectual Property,” USA for Innovation) Failure to protect these assets can have a devastating effect on an entity, depending on its size.

The most common mistakes entities make in protecting intellectual property are below, along with suggestions to mitigate the risk of these threats becoming a reality.

1. **Failure to define intellectual or trade secret assets by contract or by policy** If your employees and contractors do not know what intellectual assets belong to the business and are to be protected, shame on management. Similar to physical assets, identify your intellectual property. Protect those assets by policy, contract, or employment agreement. Reinforce the requirements to protect those assets at the time of hire, service acquisition, and through awareness training. Specialized users such as programmers, administrators, and contractors require different training.
2. **Not monitoring and filtering message content** Organizations should protect valuable information, including intellectual property, by monitoring their electronic communications. Filtering software can look for key words

and phrases. Restrict the use of hotmail and free mail sites that can bypass the filtering controls. Use search engine alerts to monitor for your organization's name and the posting of confidential information on personal blogging and social networking sites of employees, competitor sites, and contractor sites.

3. **Failure to control and monitor portable media and intellectual information storage** Portable media such as USB flash drives, music players and cameras are capable of transporting valuable intellectual property and trade secrets out your door if not controlled. This threat can be mitigated with data loss prevention solutions. Your policies should force users to save valued information only to the protected network. The most valuable information should be encrypted, both in storage and in transit.

4. **Not patching and updating at the device, operating system, and software levels** Unpatched vulnerabilities are the cause of the most widespread viruses, worms, and malicious code. Attackers can harvest millions of dollars worth of intellectual property and private information through these holes in the system. Management of businesses not diligent about patching and updating commit serious mistakes in judgment by protecting their intellectual property. Systems should be hardened and traffic into and out of the network should be controlled through firewalls and routers.

5. **Failure to manage mobile and telecommuting access for staff and vendors** Employees and business partners routinely need access to systems and servers within your network. It is a common business practice. However, they should only be connecting through secured tunnels such as VPN's and should only have access to what is need for their role or function. Smart phones and laptops have greater and greater storage capability. Limit to the extent possible the storage of valuable information on those devices, by policy and by access controls.



Kevin Doyle, CISSP, ISSMP, CISA,
CISM
Security Audit and Assessment
Manager, Reclamere