Attorneys:

- **Timothy G. Ronan**
  tronan@pullcom.com
  203.674.7933

CYBER LAW TRACKER: March 2010

The Latest in Cybersecurity and Infrastructure Protection Legal Developments

CYBER WARFARE TARGETING THE PUBLIC AND PRIVATE SECTORS IS ESCALATING

Posted on March 24, 2010, by T. Scott Cowperthwait.

The United Kingdom's Intelligence and Security Committee (ISC) has released its 2009-2010 annual report which details widespread cyber attacks launched by foreign intelligence services – most frequently, China and Russia – targeting the security of many of Britain's largest companies. Jonathan Evans, the Director General of the Security Service, told the Committee that "there's no doubt that the Internet is a strong vector of threat as far as espionage is concerned." According to the report, the objective of the vast majority of computer-related operations has been to disrupt and steal government, defense and technology information.

Similarly, the United States and many of its largest companies are under attack by computer and technology operations being conducted by not only foreign intelligence services, but organized crime and terrorist operations. The United States Department of Defense recently reported that it detects more than three million scans per day of its official networks conducted by foreign sources. Many of these scans are likely probes for vulnerabilities in the Department of Defense's critical infrastructure. As cybersecurity risks continue to escalate, the public and private sectors need to increase information sharing and form stronger partnerships to combat cyber warfare.

PULLMAN & COMLEY

CYBER LAW TRACKER: March 2010

Below is a link to where you may download a copy of the ISC's 2009-2010 Annual Report:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61295/isc-annualreport0910.pdf

AUSTRALIAN ISP WINS PIRACY BATTLE AGAINST HOLLYWOOD STUDIOS

Posted on March 5, 2010, by T. Scott Cowperthwait.

At the conclusion of an eight week trial in a closely followed case filed in the Federal Court in Australia by a consortium of the biggest Hollywood studios, Internet service provider iiNET was found not to have encouraged illegal downloading by its users.

Although Judge Dennis Cowdroy found that the evidence established the copyright infringements of the plaintiffs' films was occurring in Australia on a large scale and that iiNet had knowledge of the infringements occurring and did not act to stop them, he found it impossible to hold iiNET responsible for any copyright violations that may have been committed by its subscribers. Judge Cowdroy said that while iiNet was aware of the infringements and did act to halt them did not necessarily justify a finding that iiNET had "authorised" the users' actions. Rather, Judge Cowdroy observed that the law imposes "no positive obligation" on any person to act to protect the copyright of another. Thus, he found that it was "impossible" to conclude that iiNET should be held responsible for any copyright violations its users had committed.

STUDY CONFIRMS THE SUBSTANTIAL COST OF DATA SECURITY BREACHES

Posted on March 2, 2010 by Timothy G. Ronan.

A recent study done by PGP Corporation, an enterprise data protection company, and the Poneman Institute, a privacy and information management research firm, confirms that the average total per incident costs of data security breaches are in the millions of dollars and are rising.

According to the ***2009 Annual Study: Cost of a Data Breach*** -- *Understanding Financial Impact, Customer Turnover, and Preventive Solutions*, although negligent insider breaches have decreased in frequency and cost -- most likely due to increased employee awareness about the need to protect personal information and other data security measures, including the increased use of encryption protection -- data breaches caused by malicious attacks and botnets have doubled from 2008 to 2009. The study shows that data breach costs to U.S. companies continue to rise with average organizational costs increasing to $6.75 million and average cost per compromised record increasing to $204.

CYBER LAW TRACKER: March 2010

The study also notes that companies that notify victims “too quickly” may experience certain “inefficiencies,” which result in higher per record cost than their slower responding peers.

Here is a link to where you may download a copy of the 2009 *U.S. Cost of Data Breach Study:*

https://citadel-information.com/wp-content/uploads/2010/12/2009-ponemon-report-us-cost-of-data-breach.pdf