The Cyber-Wave Continues – Insurance Coverage for Cyber Attacks, Breaches and Lawsuits
By: Adam M. Smith, Daniel L. Pascoe
October 11, 2012

Over the past year the use of the internet to communicate and transact business has continued to grow, which has left individuals and businesses more and more vulnerable to attacks on the systems and infrastructure that support these interactions.

Despite the rise in awareness of cyber-attacks and the increase of resources being devoted to combat the problem, there has been a surge in the incidences of cybercrime affecting individuals and businesses using the internet. As a result, the number of cyber liability claims has also risen in 2012.

In a recent report, nearly all major industries are affected by cybercrime, with companies in the "accommodation and food services," "retail trade" and "finance and insurance" industries being hit particularly hard in 2012.[i] In fact, just this year, some of the most successful businesses in the world, such as Google, Apple, Visa® and Amazon, have been victims of data breaches. Further, as major social networking sites have gained popularity those sites have increasingly been targets of cyber-attacks in 2012, with Twitter and LinkedIn being the latest victims. These attacks expose a variety of individuals' personal information to criminals and result in businesses scrambling to gauge the scope of the breach so they can inform their customers while attempting to limit the damage to their reputations. It is not uncommon for lawsuits, whether filed individually or as class actions, to be filed against the businesses who suffered the cyber-attacks within weeks or even days of such breaches.

The costs of cybercrime and the amount of money expended in an effort to prevent it are astronomical. In one recent report, cybercrime is estimated to cost consumers $21 billion in the United States and $16 billion in Europe annually.[ii] Another recent report concludes that businesses globally expend approximately $10 billion annually in efforts to curtail cybercrime, which includes firewalls, intrusion detection systems, software maintenance and deployment, and user training.[iii]

Given the proliferation of cyber-attacks over the last decade and the rising costs associated with cybercrime, insurance coverage for cyber liability claims is itself in flux and evolving as cybercrime grows and becomes more sophisticated. In previous papers we have discussed general trends in cyber liability claims and the rise of specialty cyber-risk insurance products. This paper focuses on the cost of cybercrime, the latest major data breach claims in 2012, and recent cases analyzing whether cyber liability claims are covered under traditional insurance policies, including commercial crime policies and commercial general liability policies.

Read More

---

[i]Verizon RISK Team with cooperation from the Australian Federal Police, Dutch National High Tech Crime Unit, Irish Reporting and Information Security Service, Police Central e-Crime Unit and United States Secret Service, "2012 Data Breach Investigations Report" (hereafter "Verizon 2012 Report").

[ii] "2012 Norton Cybercrime Report."

[iii] Ross Anderson, et al., "Measuring the Cost of Cybercrime," 11th Annual Workshop on the Economics

of Information Security 2012 (hereafter “WEIS 2012 Report”).