$32,469 per day – a 55-percent increase over 2012’s estimated average cost of $591,780 for a 24-day period.

- Information theft continues to represent the highest external costs, with business disruption a close second. On an annual basis, information loss accounts for 43 percent of total external costs, down two percent from 2012. Business disruption or lost productivity accounts for 36 percent of external costs, an increase of 18 percent from 2012.
- Organizations using security intelligence technologies were more efficient in detecting and containing cyberattacks, experiencing an average cost savings of nearly $4 million per year, and a 21-percent return on investment (ROI) over other technology categories.
- Deployment of enterprise security governance practices including investing in adequate resources, appointing a high-level security leader, and employing certified or expert staff can reduce cybercrime costs and enable organizations to save an estimated average of $1.5 million per year.

Survival of the Fittest

Given the level of risk to a business, cyber crime has been named the greatest global threat to an enterprise’s survival, says a study by Ernst & Young.

Under cyber-attack, EY’s 16th annual Global Information Security Survey 2013 that was released in October 2013, tracked...
the level of awareness and action by companies in response to cyber threats and canvases the opinion of more than 1,900 senior executives globally. The results show that as companies continue to invest heavily to protect themselves against cyber attacks, the number of security breaches is on the rise and it is no longer a question of if, but when, a company will be the target of an attack.

Thirty-one percent of respondents reported the number of security incidents within their organization has increased by at least five percent over 12 months. Many have realized the extent and depth of the threat posed to them; resulting in information security now being ‘owned’ at the highest level within 70 percent of the organizations surveyed.

Paul van Kessel, EY Global Risk Leader, said “The survey shows that organizations are moving in the right direction, but more still needs to be done – urgently. There are promising signs that the issue is now gaining traction at the highest levels. In 2012, none of the information security professionals surveyed reported to senior executives – in 2013 this jumped to 35 percent.”

Despite half of the respondents planning to increase their budget by five percent or more in the next 12 months, 65 percent cited an insufficient budget as their number one challenge to operating at the levels the business expects; and among organizations with revenues of $10 million or less this figure rises to 71 percent.

**Cyber Espionage and Insurance Coverage - continued**

**Is A Non-State-Sponsored Cyber-Terrorism Attack Excluded Under A Cyber Liability Insurance Policy?**

The question of whether a claim arising out of non-state-sponsored cyber terrorism is excluded from coverage under the “war exclusion” of a cyber liability policy is much more straightforward. Because terrorist activities – under most circumstances – do not constitute acts of war, they fall outside the ambit of the “war exclusion.” However, precisely because of this problem, many policies now explicitly exclude terrorism as well. In this instance, the issue confronting an insured is whether cyber-activity causing either first- or third-party damage constitutes terrorism?

The Terrorism Risk Insurance Program Act (as amended) may apply to cyber-terrorism. “The Act has two separate arms: the mandatory participation arm and the compensation arm.” The participation arm requires certain insurance providers to offer coverage including damage from terrorist activities. And, the compensation arm requires the federal government to pay claims against the insurer after certain deductible thresholds are met. Because the Terrorism Risk Insurance Program Act prohibits insurers from excluding claims arising out of terrorism, if the act applies to a cyber liability policy, then arguably the “terrorism exclusion” may be struck from the policies that contain them. In such a case, claims arising from cyber-terrorism may be struck from policies that contain a terrorism exclusion.

**Conclusion**

Ultimately, the “war” and “terrorism” exclusions in a cyber liability policy may preclude coverage for a cyber-espionage or cyber-activity attack. It appears that coverage turns on the intent of the attacker and the definition of war and terrorism. As one commentator has noted, “[t]he difficulty of attaining coverage for cyber losses stems not from exclusions to coverage . . . but from the absence of initial coverage in the basic agreement.” I leave you with one final thought, does a cyber liability policy afford coverage to a hacker that is part of a terrorist organization? The answer remains to be seen.

**About the Author:**

Alba Alessandro is a partner with the law firm Hodgson Russ LLP where she concentrates her practice on insurance coverage matters, with a focus on directors and officers liability. Prior to joining Hodgson Russ, Alessandro worked with several of the country’s leading insurance defense firms.