$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

Cyber Espionage and Insurance Coverage

In the United States alone, it is estimated that the cost of "[c]yber-espionage and other malicious cyber crimes . . . [is] between $24 billion and $120 billion annually." In 2008,


Alba Alessandro

the U.S. Department of Defense's classified security networks were significantly compromised by foreign cyber-espionage. Indeed, in June 2008, "150 computers in the $1.75 billion computer network at the Department of Homeland Security were quietly penetrated with programs that sent an unknown quantity of information to a Chinese-language Web site." In 2010, "[t]he reported hacking of Google . . . targeted not only access to dozens of Gmail user accounts of Chinese human rights activists, but also Google's Intellectual Property." In 2012, an average company experienced 1.8 cyber-attacks per year resulting in an average of $8.9 million in damages. So the question arises: "Are the cyber-activities of foreign countries against the United States "cyber-warfare?" If the answer is yes, do the "war" and "terrorism" exclusions of a cyber liability policy apply to bar coverage?

What Does a Cyber Liability Insurance Policy Cover?

A cyber liability policy covers e-business; the Internet; computer networks; the use of a computer; privacy issues; computer virus transmission; and other means by which compromised data is passed to a third party. Broadly speaking, a cyber liability policy affords first-party coverage (property and theft) and third-party coverage (privacy and data security).

First-party liability is for disclosure notification costs, crisis management expenses, business interruption expenses, damage resulting from theft, and damage resulting from threats (including the cost of professional negotiators and ransom). Third-party liability is for lawsuits that seek damages resulting from unauthorized access to or dissemination of an individual's private information, intellectual property infringement, and reputation injury (including suits alleging libel or slander). Damages incurred as a result of war are excluded from coverage under a cyber liability policy. Typically, a "war" exclusion precludes coverage for damage arising from "insurrections," "riots," "civil commotion," "hostilities" and "acts of war." These terms, however, are undefined in a cyber liability insurance policy.

What Is Cyber-Espionage, Cyber-Activity and Cyberwar?

Cyber-espionage is defined as a"[n]etwork penetration to learn how to steal information, prepare the network for theft, or commit theft." A cyber-attack and cyber-warfare, however, are defined more broadly. A cyber-attack is "any action taken to undermine the function of a computer network for a political or national security purpose." The U.S. Army's DCSINT Handbook No. 1.02 defines "cyber-attack" as "[t]he premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or to further social, ideological, religious, political or similar objectives. Or to intimidate any person in furtherance of such objectives." "Cyberwar is defined as the use of computers to disrupt the activities of an enemy country, especially the deliberate attacking of communication systems."

Is a State-Sponsored Cyber-Espionage Attack Excluded Under a Cyber Liability Insurance Policy?

In Pan American World Airways v. Aetna Casualty & Surety Co., the Second Circuit defines the scope of a "war" exclusion in an insurance policy. The Court held that hijacking did not constitute a warlike act for purposes of the war exclusion clause at issue. In coming to this holding, the Court first noted that the terms in the insurance policy's exclusionary provision all related to violent acts, and therefore for any action, state sponsored or otherwise, to fit within the exclusion, it too must be violent in nature. While the action of hijacking in Pan American was found to be violent, because the action was not state-sponsored, it could not fit within the relevant exclusionary provision at issue.

The "war" and "terrorism" exclusions in a typical cyber liability policy are similar to the one found in Pan American. The war exclusion at issue in Pan American excluded from coverage all damage resulting from:

1. Capture, seizure, arrest, restraint or detention or the consequences thereof or of any attempt thereat, or any taking of the property insured or damage to or destruction thereof by any Government or governmental authority or agent (whether secret or otherwise) or by any military, naval or usurped power, whether any of the foregoing be done by way of requisition or otherwise and whether in time of peace or war and whether lawful or unlawful (this subdivision 1. shall not apply, however, to any such action by a foreign government or foreign governmental authority follow-the forceful diversion to a foreign country by any person not in lawful possession or custody of such insured aircraft and who is not an agent or representative, secret or oth-

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 of 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*

erwise, of any foreign government or governmental authority);
2. War, invasion, civil war, revolution, rebellion, insurrection or warlike operations, whether there be a declaration of war or not [hereinafter "clause 2"];
3. Strikes, riots, civil commotion [hereinafter "clause 3"].

To the extent violence is a necessary component of establishing a warlike action, it is unlikely cyber-espionage will fit within the war exclusion provision of a typical cyber liability policy. By definition, cyber-espionage amounts to, at most, theft and spying. And moreover, in the field of international diplomacy, espionage in all forms has been long recognized as an acceptable and legal form of information gathering.

Others, however, opine that some cyber-activities can constitute acts of war. In 2009, President Obama declared that "our digital infrastructure – the networks and computers we depend on every day – will be treated as they should be: as a national strategic asset…" President Obama goes on to state, "In one of the most serious cyber incidents to date against our military networks, several thousand computers were infected last year by malicious software – malware. And while no sensitive information was compromised, our troops and defense personnel had to give up those external memory devices – thumb drives – changing the way they used their computers every day. And last year we had a glimpse of the future face of war. As Russian tanks rolled into Georgia, [cyber-attacks] crippled Georgian government websites. The terrorists that sowed so much death and destruction in Mumbai relied not only on guns and grenades but also on GPS and phone using voice-over-the-Internet. For all these reasons, it's now clear this cyber threat is one of the most serious economic and national security challenges we face as a nation."

Since President Obama's 2009 declaration, references to cyber-espionage and cyber-attacks as "cyber-warfare" have become popular rhetoric. One commentator has noted that, in light of the damage that can be inflicted via cyber-attacks, "[t]he question today is not whether a cyber-attack can constitute an armed attack – it can – but 'whether a cyber-attack with a specified effect constitutes a use of force.'" Another popular opinion is that even cyber-exploitation, though not cyber-espionage, in certain circumstances, can constitute an act of war. Based on the media commentary over "cyber-warfare," more severe cyber-attacks could arguable rise to the level of an act of war, and may be excluded from coverage.

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.