CLM 2016 Cyber Liability Summit
October 5, 2016 in New York City

The Impact of Cyber Terrorism on the Insurance Process: What Is It, How Do You Recognize It, and What Impact Does It Have on the Lifecycle of Insurance?

What is terrorism?

The concept of terrorism has been around for a very long time. However, it was not until the invention of computers, computer systems and networks in the 1900s that the concept of cyber terrorism developed. Even though it has been over 30 years since this time, we still do not have a consensus regarding this definition.

The traditional definition of terrorism includes certain key components. Generally, it includes the use of force or violence to achieve certain political or ideological goals. Cyber terrorism, while not as well-developed as traditional terrorism, includes similar commonalities among definitions. In 2003, the US National Infrastructure Protection Centre, a part of the Department of Homeland Security, defined cyber terrorism as "a criminal act perpetrated through computers resulting in violence, death and/or destruction, and creating terror for the purpose of coercing a government to change its policies." NATO, in 2008, defined cyber terrorism as "a cyber-attack using or exploiting computer or communication networks to cause sufficient destruction to generate fear or intimidate a society into an ideological goal." More recently, the FBI defined cyber terrorism as any "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents."

Thus, it appears safe to say that, at a minimum, cyber terrorism requires the use of computers and/or computer systems resulting in destruction for the purpose of accomplishing a political or ideological goal. From this point, however, the definitions differ. It is unclear whether using computers or

computer systems to cause fear, but not destruction, to accomplish a political or ideological goal would be considered cyber terrorism. Which leads us to the next question – what, exactly, is cyber terrorism?

What is cyber terrorism?

Cyber terrorism is not a new concept. The world has seen several examples of what could safely fit within the narrowest definition of cyber terrorism. For instance, in 2007, government workers in Estonia found their Internet interrupted and email accounts accessed by hackers. Government websites and services were overwhelmed by a large number of ping attempts. This was during a period when street riots were occurring in protest over the government's decision to move a war memorial for fallen Soviet soldiers from the capital to a military cemetery. The cyber-attacks, which occurred over a three-week period, significantly disrupted the Estonian government's ability to function. No group has claimed credit for the attacks. Interestingly, as a result of this event, NATO established a cyber defense center, which is located in Estonia.

More recently, on June 15, 2016, a 20-year-old Kosovar hacker pleaded guilty in U.S. Federal Court to providing material support to the Islamic State terrorist group. *United States v. Ardit Ferizi*, 1:15-MJ-515. Ardit Ferizi hacked into a company's database and obtained the names of over 100,000 customers. He then culled information from this database and obtained the PII of over 1,000 government employees and active military personnel. Mr. Ferizi then provided the information to the Islamic State of Iraq and the Levant (ISIL), a designated foreign terrorist organization, to be used against those individuals. This is one of the first cases of cyber terrorism leading to a conviction in the U.S.

A lot happened between 2007 and 2016, but some people are still questioning whether cyber terrorism is a real thing or if it's just hype aimed at getting people to come to seminars about cyber terrorism.

What is cyber terrorism in the insurance context?

As much as we struggle with the definition of cyber terrorism, insurers continue to struggle with how to address cyber terrorism in the insurance context. The U.S. government has recognized concerns in the insurance industry over a catastrophic terrorist event and attempted to address some of these concerns by enacting the Terrorism Risk Insurance Act of 2002 (TRIA) and the Terrorism Risk Insurance Reauthorization Act of 2015 (TRIRA), which extends the expiration date of TRIA to December 31, 2020.

TRIA was enacted following the attacks on September 11, 2001, to provide a federal backstop for catastrophic terrorist events above $100 million in losses. It was intended to apply to commercial property and casualty losses.

We have already seen cyber events in excess of $100 million, so it is conceivable that a cyber terrorist attack could similarly be in excess of $100 million. However, TRIA is intended to provide a federal backstop to acts that are dangerous to human life, property or infrastructure. It is important to note that commercial policies do not generally provide coverage for cyber terrorism. Thus, if a policyholder does not have cyber coverage, TRIA may not be implicated for a cyber terrorism event. Additionally, given the uncertainty behind what, specifically, constitutes cyber terrorism, it is clear this is an area full of ambiguities.

Which raises the question – do cyber policies cover cyber terrorism? If there are ambiguities in a policy and the parties cannot resolve the dispute informally, they resort to litigation. To date, there have not been any lawsuits addressing whether a cyber policy provided coverage for a cyber terrorism attack.

Most policies do not differentiate between a hacker, a hacktivist, a political hacker or a terrorist hacker. Arguably, insurers may not care who is behind a security incident or breach. Thus, regardless of whether an attack was conducted by a criminal attacker or a terrorist attacker, arguably the event would most likely be covered.

How does a security incident or data breach get recognized as a cyber terrorist attack?

The cyber insurance market is in its early stages of development. In the future, who conducted the attack may become a relative inquiry to determine whether coverage applies. Which raises an interesting question – how does a security incident or data breach get recognized as a cyber terrorist attack? Generally, a hallmark of cyber terrorism is politically motivated activity that includes resulting harm or violence.

While cyber policies may not have a specific exclusion for terrorist events, many do exclude an "act-of-war" or "warlike activity." The concept of "war" generally includes hostile activities of a sovereign or quasi-sovereign nation against another sovereign or quasi-sovereign nation. *Pan American World Airways, Inc. v. Aetna Casualty & Surety Co*., 505 F.2d 989 (2nd Cir. 1974). After the September 11

attacks, this notion was conceptually broadened to include irregular forces. While this holding was primarily limited to matters brought under the Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA), 42 U.S.C. §§9601-9675, the court noted that there was some weight to be given the comments made by the President and Congress that the September 11 attacks were an "act of war against the United States". *Id.* Thus, the government's response to an attack may impact whether such an event is deemed as cyber terrorism.

When does cybercrime cross over into cyber terrorism and vice versa?

For traditionalists, cybercrime does not include an element of violence. Recall that one of the key components of cyber terrorism includes an element of violence of harm, and the distinction between cybercrime and cyber terrorism becomes clearer. Both can be motivated by financial or monetary gain; both can be used to further certain agendas, but, without an element of violence, the attack does not constitute cyber terrorism.

The most recent high-profile discussion regarding a cyber terrorist attack involved the 2014 attack on Sony Pictures Entertainment prior to its release of a comedic film about a plot to assassinate North Korean leader Kim Jong-un. A hacker group called Guardians of Peace claimed responsibility for the event. This led, for the first time in history, to the President of the United States directly accusing another sovereign nation – North Korea – of ordering the attack. However, President Obama deemed the attack "cybervandalism" and not "cyber terrorism." One reason the Sony attack may have been called cybervandalism and not cyber terrorism was the lack of any violence or destruction. Without meeting that element, the attack was simply something less than cyber terrorism.

How do insurance companies underwrite risks related to cyber terrorism?

When it comes to cyber insurance, there is a lack of data, models, and other information that is generally available for other product lines. This makes the underwriting process for cyber insurance difficult. Additional complexities arise because of the lack of a consistent definition of cyber terrorism. Some insurance companies include coverage for cyber terrorism events, while other attempt to exclude such coverage. Even for those that attempt to exclude coverage for cyber terrorism, lack of a standard definition and ambiguity around what constitutes a cyber terrorist event could mean that insurers who think they have excluded such coverage may still be liable.

Can companies recognize forensically whether a cyber-attack is a result of cyber terrorism?

Individuals hacking into systems can be, and many times are, incredibly sophisticated. They know how to cover their electronic "tracks," mask their identity, delete records and logs that would provide information about their activities or their intent. Overall, sophisticated attackers understand how to stymie investigations if they are in the system for any significant period of time. This can make it difficult to determine who has perpetrated the attack.

On the other hand, if the organization catches the perpetrator quickly, the forensic investigator may be able to determine who the perpetrators are and what their intent was with respect to the security incident. But simply identifying the attacker, most likely, will not provide sufficient evidence to prove that an event is a result of cyber terrorism. The Sony attack is an excellent example of this conundrum. Undoubtedly, there were individuals that firmly believed the attack by North Korea was cyber terrorism, but the US government deemed it "cybervandalism." Thus, forensics may obtain information that assists with a final determination as to whether an event is a result of cyber terrorism, but forensics by itself cannot make that determination.

Conclusion:

The cyber insurance market is in its infancy, and the future is unclear. For cyber terrorism, without a static definition, it is hard for insurers, policyholders, and the average consumer to understand and anticipate what, specifically, would constitute a cyber terrorist attack.