Panel 2: Cybersecurity Insurance and the Nebulous Risk of Cyberwar and Cyberterrorism

JLCW
JOURNAL OF LAW & CYBER WARFARE

Moderator:

Aarti Soni, SVP/Cyber Claims Advocacy Leader, Marsh

Panelists:

Emy Donavan, Global Head, CUO of Cyber and Tech PI, Allianz Global Corporate & Specialty SE (AGCS)

Tom Ricketts, Senior Vice President & Executive Director, Aon Risk Solutions

Brad Gow, Senior Vice President & Head of Cyber, Endurance Insurance

James McQuaid, U.S. Head of Cyber Media & Technology, AIG Claims, Inc.

Matthew Prevost, Senior Vice President, Cyber and Product Line Manager, Chubb

Aarti Soni,
Senior Vice President / Cyber Claims Advocacy Leader, Marsh

Emy Donavan,
Global Head, CUO of Cyber and Tech PI, Allianz Global Corporate & Specialty SE (AGCS)

James McQuaid
U.S. Head Cyber Media & Technology, AIG Claims, Inc.

Matthew Prevost,
Senior Vice President, Cyber and Product Line Manager, Chubb

Tom Ricketts,
Senior Vice President & Executive Director, Aon Risk Solutions

Brad Gow,
Senior Vice President & Head of Cyber, Endurance Insurance

Disclaimer

This is not legal advice nor should it be considered legal advice

This presentation and the comments contained therein represent only the personal views of the participants, and does not reflect those of their employers or clients

This presentation is offered for educational and informational uses only

Cyber Insurance Landscape

- Cyber market is broadening-Significant capacity available
  - Growth coming from small to medium firms newly aware of the possible liability
- Organizations with a stand-alone cyber insurance policy 83 percent.*
  - Of the organizations without a stand-alone cyber policy, 84% indicated that other insurance policies include cyber liability coverage.
- Annual gross written premium estimate $3.25 billion.
- Global market is forecasted to garner $14 billion by 2022
- Improved Risk Management services
- Sublimits reduce insurer exposure
  - Sublimit - a limitation in an insurance policy on the amount of coverage available to cover a specific type of loss. It's apart of the limit that would otherwise apply to the loss.
  - Self-Insured Retention (SIR) -A dollar amount specified in a liability insurance policy that must be paid by the insured *before* the insurance policy will respond to a loss.
  - Eroding limits Policy - a policy where defense costs are considered part of the loss, and therefore reduce or exhaust, the available limits of the policy to pay damages or settlement cost

The Coverage Gap Created by Cyber Terrorism

- State Actor v. Non-State Actor
- Crime v. War v. Terrorism
  - Cybercrime includes unauthorized network breaches and theft of intellectual property and other data; it can be financially motivated, and response is typically the jurisdiction of law enforcement agencies.*
  - Cyberwar is typically conceptualized as state-on-state action equivalent to an armed attack or use of force in cyberspace that may trigger a military response with a proportional kinetic use of force. *
  - Cyberterrorism can be considered “the premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives.” *
- Analyzing Impact
- Who is the Target?

Primary Harms

Loss of revenue and extra expense

Brand and reputation

Direct business loss and costs (e.g., Ransomware and Cryptonapping attacks)

Physical damage to property or persons (e.g., Oil rig explosion through hijacking of control systems.)

JLCW
JOURNAL OF LAW & CYBER WARFARE

Secondary Harms

- Public relations/crisis management
- Remediation of system flaw that allowed breach including forensic consultants, both hardware and software
- Legal costs
- Forensic audit
- Notification costs
- Credit monitoring for third parties
- Defense of government investigation

Is cyber insurance covering cyber war and cyber terrorism…

War Exclusion: No Terrorism Exclusion or Provision

Alleging, based upon, arising out of or attributable to war, invasion, acts of foreign enemies, hostilities or warlike operations (whether war is declared or not), strike, lock-out, riot, civil war, rebellion, revolution, insurrection, civil commotion assuming the proportions of or amounting to an uprising, military or usurped power.

War Exclusion: Terrorism Carveback

An act of war, invasion, acts of foreign enemies, hostilities, civil war, rebellion, revolution, insurrection, military or usurped power or the seizure and nationalization of the Insured's Critical System or information assets by order of any governmental authority. Provided, however, this exclusion shall not apply to Cyber Terrorism.

For purpose of this exclusion, “Cyber Terrorism” means any actual, alleged or threatened attack against the Insured's Critical System, with the intention to cause harm or further social, ideological, religious or political objectives or to intimidate any person or entity in furtherance of such objectives.

War Exclusion: Terrorism Carveback (no definition of terrorism)

strikes or similar labor action, war, whether declared or not, invasion, act of foreign enemy, civil war, mutiny, coup d'état, civil commotion assuming the proportions of or amounting to a popular rising, military rising, insurrection, rebellion, revolution, military or usurped power, or any action taken to hinder or defend against these actions; provided, however, this exclusion shall not apply to any actual, alleged or threatened attack against the network, with the intention to cause harm or further social, ideological, religious or political objectives or to intimidate any person or entity in furtherance of such objectives.

War Exclusion: With Separate Terrorism Exclusion

Strikes or similar labor actions, war, invasion, act of foreign enemy, hostilities or warlike operations (whether declared or not), civil war, mutiny, civil commotion assuming the proportions of or amounting to a popular uprising, military uprising, insurrection, rebellion, revolution, military or usurped power, or any action taken to hinder or defend against these actions.

All losses or expenses arising from a terrorist act. For the purposes of this agreement, a terrorist act means an act or series of acts including the use of force or violence of any person or group(s) of persons, whether acting alone or on behalf of or in connection with any organization(s), committed for political, religious, or ideological purposes, including the intention to influence any government and/or to put the public in fear for such purposes;

War and Terrorism Exclusion: Extremely Onerous Burden of Proof Requirement

Directly or indirectly caused by, resulting from or in connection with any of the following regardless of any other cause or event contributing concurrently or in any other sequence to the loss;

war; invasion; acts of foreign enemies; hostilities or warlike operations (whether war be declared or not); civil war; rebellion; revolution; insurrection; civil commotion assuming the proportions of or amounting to an uprising; military or usurped power.

For the purpose of this Exclusion, an act of terrorism means an act, including but not limited to the use of force or violence and/or the threat thereof, of any person or group(s) of persons, whether acting alone or on behalf of or in connection with any organization(s) or government(s), committed for political, religious, ideological or similar purposes including the intention to influence any government and/or to put the public, or any section of the public, in fear.

This also excludes LOSS of whatsoever nature directly or indirectly caused by, resulting from or in connection with any action taken in controlling, preventing, suppressing or in any way relating to any of the above situations.

If the COMPANY alleges that by reason of this Exclusion, any CLAIM is not covered by this Policy, the burden of proving the contrary shall be upon the INSURED.

War Exclusion: Terrorism Carve Back, Onerous Burden of Proof Requirement

Any Act of terrorism; strike or similar labor action, war, invasion, act of foreign enemy, hostilities or warlike operations (whether declared or not), civil war, mutiny, civil commotion assuming the proportions of or amounting to a popular rising, military rising, insurrection, rebellion, revolution, military or usurped power, or any action taken to hinder or defend against these actions; including all amounts, Damages, or Claim Expenses of whatsoever nature directly or indirectly caused by, resulting from or in connection with any action taken in controlling, preventing, suppressing, or in any way relating to the above; however if We allege that by reason of this exclusion any Damages or Claim Expenses are not covered by this Policy, the burden of proving the contrary shall be upon You.

However, this exclusion shall not apply to Cyber Terrorism.

- Cyber Terrorism means the premeditated use of disruptive activities against Your Computer System by an individual or group of individuals, or the explicit threat by an individual or group of individuals to use activities, with the intention to cause harm, further social, ideological, religious, political or similar objectives, or to directly intimidate any person(s) specifically in furtherance of such objectives. Cyber Terrorism does not include any such activities which are part of or in support of any military action, war or warlike operations.

JLCW
JOURNAL OF LAW & CYBER WARFARE

Questions?

Appendix

Emy Donavan
Global Head, CUO of Cyber and Tech PI,
Allianz Global Corporate & Specialty SE Allianz Global Corporate & Specialty (AGCS)

Contact:
E: emy.donavan@agcs.allianz.com
URL: www.linkedin.com/in/emydonavan/

JLCW
JOURNAL OF LAW & CYBER WARFARE

Emy Donavan recently accepted a position with Allianz Global Corporate & Specialty as managing National Practice Leader for Cyber, Tech PI, Media and MPL lines. She is currently authoring AGCS's first-ever U.S. Cyber and Specialty PI policy wordings with anticipated launch in Q1 2016. She is also leading the effort to build Allianz's U.S. Cyber and Specialty PI team, and developing underwriting guidelines, rates, appetite, distribution strategy, reinsurance treaty, and vendor panel for these lines of coverage on a national basis. Ms. Donavan's previous experience spans more than a decade of Cyber, Technology, and Specialty E&O-dedicated experience at several of the largest PI and Cyber carriers in the U.S. market.

Emy also enjoys opportunities to educate; she trains brokers, underwriters and clients on emerging risks in the Cyber marketplace through her formal job functions, speaking engagements, and monthly LinkedIn Pulse Blog (Cyber Underwriting 101).

Ms. Donavan graduated from UC Berkeley with a BA in Rhetoric, focusing on legal writing and argument construction, and is a licensed CA surplus lines broker. Currently, she is serving as a member of the Advisory Board for Advisen's Cyber Insights Conference, which is scheduled for March of 2016. She is an active member of the Professional Liability Underwriting Society (PLUS) as a part of the Northern California Chapter Steering Committee, for which she most recently served as co-chair of the Communications subcommittee. Ms. Donavan is also a frequent speaker for PLUS, the American Bar Association, and other affiliation groups on Cyber & Professional Liability insurance topics.

Matthew Prevost
Senior Vice President, Cyber and Product Line Manager,
Chubb

Contact:
E: matt.prevost@chubb.com
URL: www.linkedin.com/in/matt-prevost-8b89581/

JLCW
JOURNAL OF LAW & CYBER WARFARE

Matt Prevost, RPLU, is Chubb's National Product Line Manager for Cyber and Technology E&O Product Lines. In this role, he is responsible for cyber product management in the United States, and plays a significant role in Chubb's Global Cyber Practice, which addresses growing risks as legislation and exposures for privacy and network security evolve around the world, and customer demands for cyber insurance and risk management solutions grow. Mr. Prevost is also responsible for underwriting and negotiating complex accounts, developing and maintaining a broad network of brokerage and vendor relationships, and developing and driving distribution and marketing strategies.

Mr. Prevost previously served as Assistant Vice President at Philadelphia Insurance/Tokio Marine Group, where he was responsible for the management and professional liability division for the Western U.S. Prior to accepting that role, he oversaw the carrier's cyber and miscellaneous professional liability portfolio in the U.S.

Mr. Prevost is a certified Continuing Education (CE) instructor in more than 36 states and regularly speaks on the topics of Directors & Officers (D&O), Errors & Omissions (E&O), cyber and privacy liability. He is a graduate of Lafayette College with a degree in International Economics and Commerce and also studied at Ecole Superieure de Commerce de Dijion in France.

Tom Ricketts
Senior VP and Executive Director,
Aon Risk Solutions

Contact:
E: tom.ricketts@aon.com
URL: www.linkedin.com/in/tomricketts/

JLCW
JOURNAL OF LAW & CYBER WARFARE

Tom Ricketts is a Senior Vice President and Executive Director of the Aon Risk Services Professional Services Group in New York. Tom heads up the New York client service team, providing risk management advice and insurance services to large, US-based law firms, accounting firms and consulting firms and is the Cyber-Insurance specialist for this group.

Tom has 30 years of international experience in the insurance broking industry and has worked in both the London and New York markets and for much of his career he specialized in advising communications media and technology firms on how to insure their risks. In the course of this work he created and placed the first open-market Technology E&O insurance policy. In his role as head of the Sedgwick Global Telecommunications practice, Tom carried out numerous engagements with banks and funding consortia on risk due diligence in relation to communications sector investments (including EBRD and the World Bank). Tom worked on numerous high-profile communications sector start-ups such as Global Crossing, FLAG and Iridium.

Tom has been recognized by Risk & Insurance Magazine as a "Power Broker" in Telecommunications (1996) and Construction (2011) and has published articles in Lloyd's List and the John Liner Review.

Brad Gow
Senior Vice President, Endurance

Contact:
E: bgow@enhinsurance.com
URL: www.linkedin.com/in/brad-gow-22b5658/

Brad Gow is a Senior Vice President at Endurance, where he provides global oversight of the company's cyber risk underwriting operations including underwriting management, product development and services coordination.
Prior to his current role, he was a Senior Vice President in Zurich's Specialties division where he led the Errors & Omissions liability unit.

From 2002 through 2008 he was with ACE USA's Professional Risk division, responsible for all professional liability product management operations. Mr. Gow also led ACE's technology E&O and network risk underwriting operations, including the development of the ACE DigiTechsm line of products.

Mr. Gow co-founded NetDiligence in 2000, a venture backed organization providing network security, incident response and forensic computer investigation programs specifically suited to the needs of insurance carriers and brokers.

Mr. Gow also spent eight years working in the Asian insurance markets for CIGNA International and American International Group.

Aarti Soni
Senior Vice Present/Cyber Claims Advocacy Leader,
Marsh

Contact:
E: aarti.soni@marsh.com
URL: www.linkedin.com/in/aarti-soni-67b5477/

JLCW
JOURNAL OF LAW & CYBER WARFARE

Aarti Soni is the Cyber Claims Advocacy Leader for our Professional Liability / Network Security and Privacy Practice (part of our FINPRO Practice) in New York, New York. She focuses her work on large, complex accounts in the cyber, technology, media and professional coverage arenas. Aarti's current responsibilities include supporting clients by reviewing and negotiating policy wordings and serving as a resource on cybersecurity offerings and services, both pre- and post-event. Aarti also assists clients throughout the claim life cycle. Aarti joined Marsh in July 2016. Prior to that time, she was a Claims Analyst at American International Group (AIG). She also worked an associate at two national law firms, where she handled complex insurance coverage litigation. Aarti most recently served as Assistant General Counsel, Professional Liability & Cyber Counsel at Chubb, where she was a member of the Cyber Product Board. There, she provided client support to Errors and Omissions (E&O) and cyber risk underwriters.

Aarti has a BA in International Studies, American University, Washington, DC and a JD from Washington College of Law, American University, Washington, DC.

James McQuaid
U.S. Head of Cyber Media & Technology
AIG Claims, Inc.

Contact:
E: Jim.McQuaid@AIG.com
URL: www.linkedin.com/in/james-mcquaid-28a32693/

Jim McQuaid is the U.S. Head of Cyber Media and Technology with AIG, Financial Lines Claims. In this role Jim is responsible for all U.S. claim activity in Cyber, Media and Technology products. He has developed Financial Lines expertise during his 19 years with AIG through a variety of technical and managerial roles in Claims and Litigation Management. Jim began his career as a litigator for another insurance carrier and joined AIG in 1998. He earned a B.A. in Economics from the State University of New York at Stony Brook and a Juris Doctor from Hofstra Law School.

Case Law

Universal Cable Productions LLC et al. v. Atlantic Specialty Insurance Co. case number 2:16-cv-04435

- **Facts:** Universal sought coverage under its policy with Atlantic Specialty Insurance Co., for the cost to move production of a TV series away from Jerusalem amid a 2014 armed conflict between Israel and the Hamas militant. Atlantic declined, citing exclusions for losses related to war and warlike actions. The TV production company countered that the exclusions are inapplicable because Hamas is not a sovereign state and has often been classified as a terrorist organization by governments around the world. Universal sued, asserting claims for breach of contract and bad faith and seeking damages of at least $6.9 million
- **Holding:** The Court found the 2014 conflict constituted a “war” under the exclusion in Universial’s insurance policy thereby, defeating the company's bid to get coverage.
  - The Court sided with Atlantic, saying California law requires him to adopt the common meaning of "war" in analyzing the policy, rather than the more specific technical definition suggested by Universal.
  - "In the common meaning, 'war' can include conflicts both between sovereign entities and between other groups; the word does not require a detailed assessment of the structure of one or more of the parties to the conflict or their precise international standing.”
  - The Court notes that even if the explicit war exclusion didn't bar coverage for Universal, the policy’s exclusion for warlike actions is even broader and would certainly encompass the 2014 clash.

P.F. Chang's China Bistro, Inc. v. Fed. Ins. Co.

Facts : P.F. Chang's was insured by a cybersecurity insurance policy through Federal by Chubb Policy ("Policy"). P.F. Chang's suffered a credit card data breach. P.F. Chang's acquiring/servicing bank pursued indemnification from P.F. Chang's under its service contract to recover fees for credit card assessments as a result of the breach.

Issue: Did the Policy's "Privacy Injury" coverage apply?

Holding: *No*, the coverage did not apply because the Policy's definition of "Privacy Injury" required that the compromised confidential records at issue be the claimant's.

- The payment card information stolen by the hackers belonged to Chang's customers and the card-issuing banks, not the acquiring bank that made the actual claim for reimbursement by Chang's.
- P.F. Chang's was on the hook for more than $1.9 million.

Aqua Star (USA) Corp. v. Travelers Casualty and Surety Co. of America

Facts: Aqua Star maintained a Wrap+ Crime Policy with Travelers. The Policy covered Aqua Star for its "direct loss of, or direct loss from damage to, Money, Securities, and Other Property directly caused by Computer Fraud."Aqua Star's vendor, Longwei, was hacked. Through social engineering and spoof emails, the hacker directed an Aqua Star employee to change banking credentials and wire $ into the hacker's account.

Issue: Does this exclusion apply? -- "Will not apply to loss resulting directly or indirectly from the input of Electronic Data by a natural person having the authority to enter the Insured's Computer System."

Reasoning/Holding: Yes, the "revised" banking details were information, which fell within the meaning of "Electronic Data." The employee in question was a natural person and had the authority to enter banking details into Aqua Star's computer system.