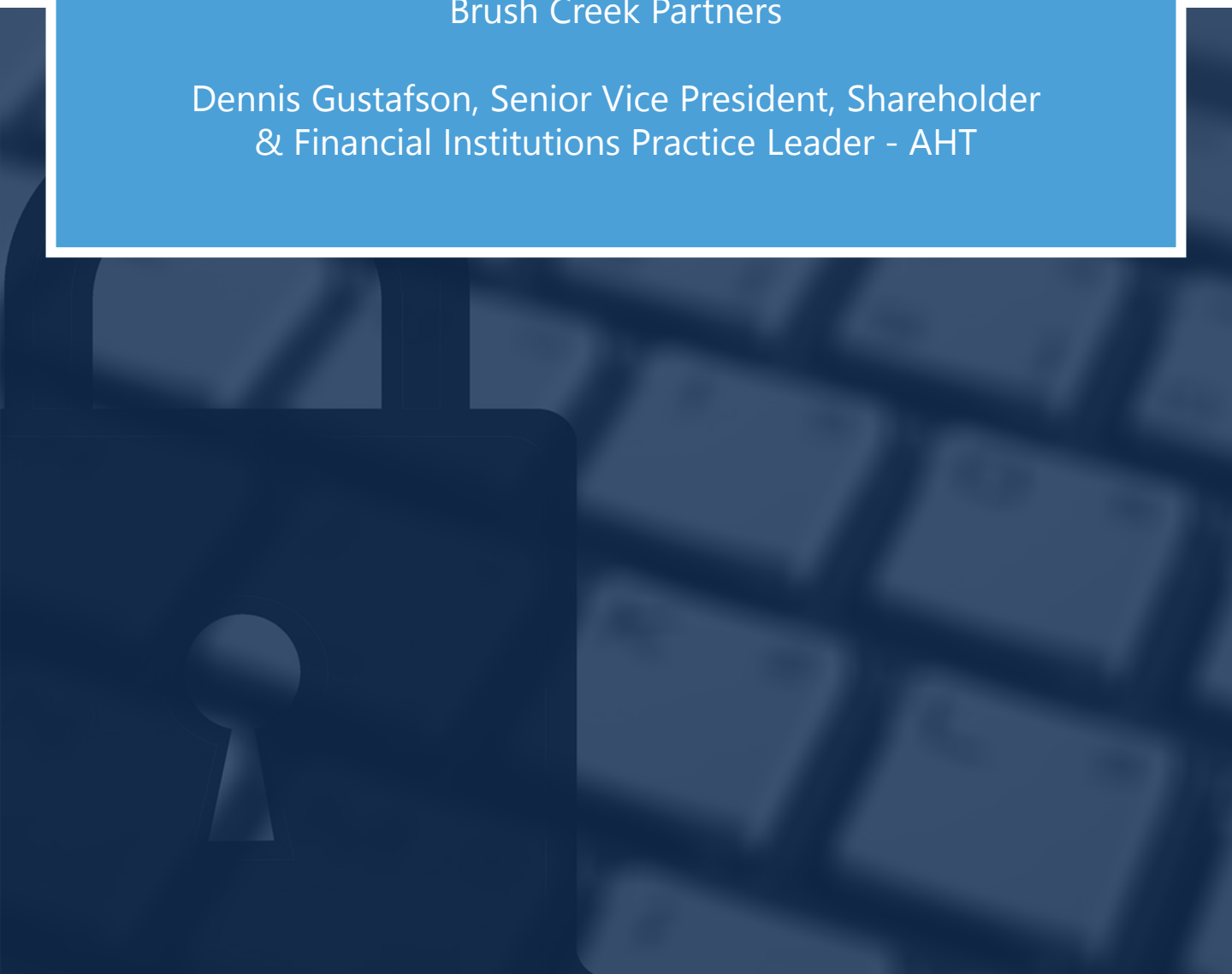
AHT INSURANCE

bcp tech
powered by | BRUSH CREEK PARTNERS

# WAR EXCLUSIONS – HOW DOES YOUR CYBER POLICY COMPARE?

By: Travis Holt, Partner & Co-Founder bcp tech – a division of Brush Creek Partners

Dennis Gustafson, Senior Vice President, Shareholder & Financial Institutions Practice Leader - AHT



**"The Internet is a prime example of how terrorists can behave in a truly transnational way; in response, States need to think and function in an equally transnational manner."** *- Ban Ki-moon, Secretary General of the United Nations*

For over 20 years, companies of all sizes have been impacted by the ever-growing list of various cyberattacks. Over the years, these cyberattacks have grown in frequency and severity and, now, rank at the top of many executives' concerns related to business stability. These concerns are not surprising considering it's almost impossible to predict how and when a company might fall victim to a cyberattack as the threat vectors continue to evolve.

In the past, companies were mainly focused on the loss of personally identifiable information, and the idea of a state-sponsored cyberattack was not even on the radar. Unfortunately, some of these state-sponsored cyberattacks have led to the largest losses and can no longer be ignored. They have impacted millions of companies and have caused billions in financial harm.

According to the Verizon 2020 Data Breach Investigations Report, Nation-State or State-affiliated players were the second largest group of cyber criminals behind Organized Crime. One can look at the recent history and find multiple significant state-sponsored cyberattacks.

- **2017 –** WannaCry ransomware launched by North Korea
- **2018 –** NotPetya ransomware launched by the Russian Military
- **2019 –** Several major German industrial firms, including BASF, Siemens and Henkel announced that they had been the victim of a state-sponsored hacking campaign reported to be linked to the Chinese government
- **2019 –** Nation state hackers breached the networks of two U.S. municipalities, exfiltrating user information and establishing backdoor access for future compromise
- **2020 –** U.S. officials accused hackers linked to the Chinese government of attempting to steal U.S. research into a coronavirus vaccine
- **2020 –** North Korean state hackers sent COVID-19-themed phishing emails to more than 5 million businesses and individuals in Singapore, Japan, the United States, South Korea, India and the UK in an attempt to steal personal and financial data
- **2020 –** FBI chief slams Chinese cyberattacks on U.S. amounting to what he calls "one of the largest transfer of wealth in human history"

| HISTORICAL LOOK AT MAJOR CYBER ATTACKS | | |
|---|---|---|
| Cyber Attack | Year | Impacted parties |
| Melissa | 1999 | 1,000,000 accounts |
| ILOVEYOU | 2000 | 45,000,000 computers (in two days) |
| Anna Kournikova | 2001 | >100,000 computers |
| SQL Slammer | 2003 | 75,000 computers (in ten minutes) |
| My Doom | 2004 | > 1,500,000 e-mails |
| Heartland Payment Systems | 2007 | 130,000,000 payment cards |
| Conficker | 2008 | 6,500,000 |
| Stuxnet | 2009-10 | Iran's uranium facility |
| Epsilon | 2011 | 60,000,000 users' data |
| LinkedIn | 2012, 2016 | 6,500,000 passwords |
| Adobe | 2013 | 153,000,000 user records |
| ebay | 2014 | 145,000,000 users |
| Adult Friend Finder | 2016 | 412,000,000 accounts |
| Petya (also NotPetya) | 2017 | 300,000 computers |
| WannaCry | 2017 | 230000 computers |
| Equifax | 2017 | 163,119,000 |
| Dubsmash | 2018 | 162,000,000 user accounts |
| Marriott | 2018 | 500,000,000 customers |
| Canva | 2019 | 137,000,000 user accounts |
| Zynga | 2019 | 200,000,000 users |
| Robinn Hood | 2019 | Baltimore city government |
| Sina Weibo | 2020 | 538,000,000 accounts |

Cyber insurance carriers all address these nation state attacks differently and understanding the 'War Exclusion' is the key; many non-cyber policies contain language allowing carriers to deny these claims. Specifically, we have seen declinations related to the NotPetya attack in 2017. The delivery mechanism of this attack was encrypted malware. The initial target was allegedly a nuclear power plant in Ukraine, but the malware quickly spread and within days had paralyzed a number of large national companies, including Merck, Maersk, FedEx and Mondelez, by encrypting their hard drives. These companies spent hundreds of millions of dollars each in cleanup costs and lost business according to reports. The White House estimated the damage from NotPetya at $10B.

Victims of the attack were looking to insurance to cover the expenses and losses associated with the attack. However, in several cases, Insurance carriers referenced the 'War exclusion' incorporated in many of the policies to deny these claims. Subsequent lawsuits against the carriers are still playing out in the courts. The ultimate decisions of these cases can set the initial precedent about who pays when a cyberattack is attributed to a state-sponsored actor.

As we explore the War Exclusion in multiple policies, the cyber liability policies vary widely about how they address the topic. We reviewed 16 of the most popular cyber liability policies and none are the same**.**

**For the purposes of this whitepaper, we broke them down to the following 5 categories from most restrictive to broadest:**

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| Most Restrictive | Restrictive | Neutral | Broad | Broadest |

| LABEL | COUNT | SAMPLE LANGUAGE |
|---|---|---|
| **Most Restrictive**<br>Total Exclusion | 4 | This policy does not apply to and we will have no obligation to pay any loss, damages, claim expenses, or any other amounts for any claim or event directly or indirectly occasioned by, happening through, or in consequence of:<br><br>1. WAR: Confiscation, nationalization, requisition, strikes, labor strikes or similar labor actions; war, invasion, or warlike operations, civil war, mutiny, rebellion, insurrection, civil commotion assuming the proportions of or amounting to an uprising, military coup or usurped power<br>2. TERRORISM: Any act of terrorism, except for a terrorist event perpetrated by electronic or internet-based applications or means |
| **Restrictive**<br>Silent or partially address cyber terrorism | 2 | Similar war exclusion, but with carve back for:<br><br>▪ Threatened attack against a computer system with the intent to cause harm, or further social, ideological, religious, political or similar objectives…<br>▪ Cyberterrorism, however which does not include activities which are part of or in support of any military action/war |
| **Neutral**<br>Full Cyber-terrorism carve back | 8 | Similar exclusion, but with full carve back for Cyberterrorism with no restrictions how Cyberterrorism can be interpreted |
| **Broad**<br>Full carve back | 1 | Similar war exclusion, but with carve back for any cyber-related events that could impact your computer system |
| **Broadest**<br>No War exclusion at all | 1 | N/A |
| **Total:** | **16** | |

The 6 most restrictive examples are of most concern, as those policies not only exclude War but also offer some form of exclusion for Cyberterrorism activities. In those cases, although it may not be the carrier's intent to deny a claim related to a cyberattack from a foreign nation state, if that breach can fall under the broad definition of cyber terrorism, they will have the ability to either deny the claim or negotiate a settlement where the Insured has to agree to some type of participation in the claim resolution. Also, note that it is not uncommon for insurance carriers to change the war exclusion language that is built into the base form via endorsement. These endorsements can be used to either broaden coverage or make it more restrictive. If you would like a third-party independent review of the cyber liability policy to see how your policy stacks up against the 16 policies we have reviewed, please do not hesitate to reach out to Travis or Dennis.

AHT INSURANCE

ahtins.com

bcp tech
powered by | BRUSH CREEK PARTNERS

bcptech.co

## AUTHORS:

**Travis Holt**, Partner & Co-Founder bcp tech – a division of Brush Creek Partners

Travis is recognized as a national expert on the contractual transfer of technology risk and matching insurance requirements to the risk transfer and runs the technology, venture capital, and cyber liability practice groups for bcp tech. His areas of expertise include professional liability, management liability, technology risk management and due diligence, and cyber liability.

Travis.Holt@brushkc.com

bcp tech
powered by | BRUSH CREEK PARTNERS

**Dennis Gustafson**, Principal & Financial Services Practice Leader AHT Insurance

Dennis has extensive expertise in placing management liability, directors and officer's liability, professional liability, lenders liability and fidelity bond/commercial crime. In addition, he assists clients using his widespread knowledge of the risk exposures and coverage available for cyber liability/privacy for all industries. Dennis maintains AHT's relationships with Bank Director and Corporate Board Member publications and previously with the Americas Community Bankers Association. He is a frequent speaker about management liability topics at industry events and frequently authors D&O specific articles for Bank Director/Corporate Board Members. On March 12, 2013, he was quoted in the Wall Street Journal in an article titled "Small U.S. Banks Hit by Rising Insurance Cost". Most recently, Dennis was recognized by Risk & Insurance as a 2016 Power Broker of the Year for the financial services industry.

dgustafson@ahtins.com

AHT
INSURANCE