



---

**PROGRAM MATERIALS**

**Program #29104**

**June 12, 2019**

## **Silent Cyber and War - Gaining Coverage for Cyber Losses Under Non- Cyber Policies and Excluded Losses**

**Copyright ©2019 by Michael Menapace, Esq. and Kevin  
Carroll, Esq., Wiggin and Dana LLP. All Rights Reserved.  
Licensed to Celesq®, Inc.**

---

**Celesq® AttorneysEd Center**  
**[www.celesq.com](http://www.celesq.com)**

**5301 North Federal Highway, Suite 180, Boca Raton, FL 33487**  
**Phone 561-241-1919      Fax 561-241-1969**



# SILENT CYBER AND WAR

Losses From Malware Under Non-Cyber  
Policies and the Hostile Acts Exclusion

Presented by

**Michael Menapace  
and Kevin Carroll**

Wiggin and Dana, LLP

# Silent Cyber



**Cyber Insurance**  
has dominated conversation



This presentation is **not about**  
**cyber insurance policies**

## Today's Topic

Losses that remain in  
liability, property and  
specialty policies related  
to cyber events

# War



## War exclusion

Now, often called the **Hostile Acts Exclusion**

# Context



**NotPetya**



**Russian involvement**



**Directed at  
foreign enemies**



**Caused collateral  
damage to private  
corporations**

# Cyber Loss

There are policies specifically written to cover cyber losses



And, there are endorsements to non-cyber policies that **can add cyber coverage**



But, most non-cyber policies now try **exclude cyber losses**

# Cyber Loss

There are policies specifically written to cover cyber losses



And, there are endorsements to non-cyber policies that **can add cyber coverage**



But, most non-cyber policies now try **exclude cyber losses**

**But, coverage can remain**

# History of Property Insurance... In 3 Minutes!



**Lombards**

# History of Property Insurance... In 3 Minutes!



**Lombards**

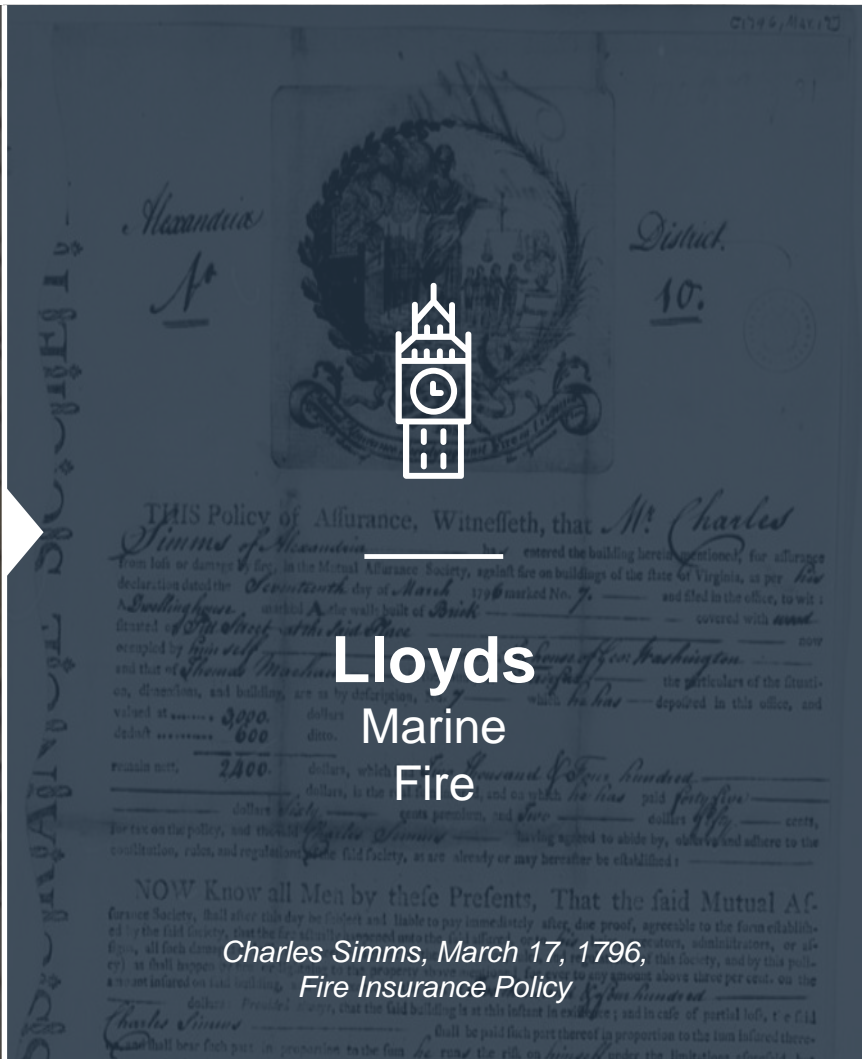


**Lloyds**  
Marine

# History of Property Insurance... In 3 Minutes!



Lombards



Lloyds  
Marine  
Fire

Charles Simms, March 17, 1796,  
Fire Insurance Policy

# History of Property Insurance... In 3 Minutes!



Lombards



Lloyds  
Marine  
Fire



Ben Franklin

# Modern Property Policies

## STANDARD PROPERTY COVERAGE FORM

**g. Business Income**

If coverage for Business Income applies to the policy, we will pay for the actual loss of Business Income you sustain due to the necessary suspension of your “operations” during the “period of restoration”. The suspension must be caused by direct physical loss of or physical damage to property at the “scheduled premises”, including personal property in the open (or in a vehicle) within 1,000 feet, caused by or resulting from a Covered Cause of Loss.



**Scope of risks  
has expanded**



**Language of terms  
has evolved**



**Purpose remains**  
1<sup>st</sup> party loss  
physical damage  
tangible property



**Added**  
Business interruption

# Writing Cyber Out of Non-Cyber Policies

## Property not covered

This policy does not insure the following property:

March 2, 2001

- **Money**
- precious metal in bullion form
- notes
- or **Securities**

March 2, 2003

- Spacecraft
- satellites
- associated launch vehicles and any property contained therein

March 2, 2005

- Bridges and tunnels when not part of a building or structure
- dams
- dikes
- piers
- wharfs
- docks
- or bulkheads

March 2, 2006

- Land **improvements**

March 2, 2007

- Land **improvements** at a golf course

March 2, 2002

- Watercraft or aircraft, except when unfueled and manufactured by the Insured

March 2, 2004

- Animals,
- standing timber
- and growing crops

March 2, 2006

- Land, water, or any other substance in or on land; except this exclusion does not apply to

March 2, 2006

- Water that is contained in any enclosed tank, piping system or any other processing equipment

March 2, 2015

**Electronic Data Programs and Software**; except when they are **Stock in Process, Finished Stock, Raw Materials**, supplies, or **Merchandise** or as otherwise provided by the Computer Systems Damage Coverage or **Valuable Papers**, and **Records** coverage of this policy.

# “Silent Cyber” Can Remain

Also called **Non-Affirmative Cyber**



Potential cyber-related losses covered by traditional property and liability policies that were not specifically designed to cover cyber risk.



They can be intentionally or inadvertently included.

# Examples of Silent Cyber

Property policies may cover hardware physically damaged by malware

Liability policies may cover bodily injury from:

a train **derailment** caused by computer **attack**;  
or an elevator **fall** from malware



Auto policies may cover damages due to a **malware-infected GPS-linked navigation system** incorrectly guiding a driver, perhaps on purpose, causing a traffic accident or trying to **kill** a passenger

# Other Examples



Fidelity Policy  
- crime loss



Directors &  
Officers Policy



Kidnap, Ransom  
& Extortion Policy



# Hostile Acts Exclusion



**Don't** rely  
on section titles



**Originally**, and  
often still, referred to as  
**war exclusion**



The **exclusion**  
wording has **evolved**



**Different** wordings  
between **non-cyber** and  
**cyber** policies

# Exclusions – Common and Necessary



**Approved by regulators,  
upheld by courts**

**Seeks to avoid/mitigate  
“correlated risks”**

Risks **emanating** from same source  
**destroys** risk spreading and **law of averages**  
e.g. homeowners on FL shoreline

# NotPetya



June 2017

There was an **attack** on the **Ukrainian government** just before Ukrainian **Constitution Day**

Attributed to the **Russian military**

**U.S.** and **U.K.** governments – in response, **sanctions** against the **Russian government** and certain related entities

# NotPetya



June 2017

Initially, experts thought **NotPetya** was a **ransomware attack**

Later realized that, instead, **infected files** were **not** recoverable

Type of **malware** sometimes referred to a “wiper” because it **destroys** data

**No ransom** – developers not financially **motivated**

# Viruses Spread



Spread from its original **target** to other computer systems **across the world** due to its **indiscriminant** design

**Among the high profile companies impacted by NotPetya were:**

shipping giant **Maersk**, pharmaceutical maker **Merck**, and food conglomerate **Mondelez International**

# What Has Been Reported?

NotPetya malware was based upon a leaked US National Security Agency penetration tool, [EternalBlue](#), and an older French digital skeleton key, [Mimikatz](#).

“Computer zero” was a Maersk finance executive in Ukraine asked IT administrators to install new accounting software on one computer. It was “the fastest-propagating piece of malware we’ve ever seen ... By the second you saw it, your data center was already gone.” “The malware’s goal was purely destructive” as it irreversibly encrypted computers’ master boot records.

At least \$10b in damages: \$129m to Durex, \$188m to Mondelez, \$250 to Maersk, \$400, to FedEx, and \$870m to Merck alone. “It took 45 seconds to bring down the network of a large Ukrainian bank” ... a major transit hub “was fully infected in 16 seconds.” “The government was dead” -- Ukrainian minister of infrastructure.

Over 300 companies hit worldwide, 10% of all computers in Ukraine wiped. Maersk recovered because one domain controller in Ghana had not been infected because it was disconnected due to a blackout.

“It was the equivalent of using a nuclear bomb to achieve a small tactical victory. That’s a degree of recklessness we can’t tolerate on the world stage” – former Homeland Security Advisor Tom Bossert.

Source: *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, A. Greenberg, WIRED (Aug. 22, 2018), available at <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>

# Claim Under Property Policies



## **Allegation**

Computers were rendered  
physically damages



## **Allegation**

Business  
interruption



## **Defense**

Hostile acts  
exclusion

# Scope of Exclusion



One standard exclusion

Losses due to “**war, including undeclared civil war**”

ISO CP 10 30 06 95 **(1994)**

# Modelez/Zurich Exclusion

“ This policy **excludes** loss or damage **directly** or **indirectly** caused by or resulting from any of the following regardless of any other cause or event, whether or not insured under **this policy**, contributing concurrently or in any other sequence to the **loss** ”

**Hostile or warlike action in time of peace or war by any:**

- (i) government or sovereign power (de jure or de facto),
- (ii) military, naval, or air force, or
- (iii) agent or authority of any party specified in i or ii above

# Modelez/Zurich Exclusion

“ This policy **excludes** loss or damage **directly or indirectly**

Hostile or warlike action in

**(iii) agent or authority of any party  
specified in i or ii above**

concurrently or in any other  
sequence to the **loss** ”

(ii) military, naval, or air force, or  
(iii) agent or authority of any party  
specified in i or ii above

# Text v. Context

## Text



**Insured** need not be the **target**,  
i.e. allows for collateral **damage**



War need not be “**declared**”



**Not restricted** to a physical war zone



**No requirement** for bullets and tanks

## Context



**Original** intent



**Reasonable** expectations

# Side Note – Exclusions in Cyber Policies Can Be Different

Y → **War or Civil Unrest:** based upon, arising out of, or attribute to

1

**War**, including undeclared or **civil war**

2

**Warlike** action by a **military force**, including action in **hindering** or **defending** against an actual or expected **attack**, by any **government**, **sovereign**, or other authority using military **personnel** or other agents or

3

**Insurrection, rebellion, revolution, riot, usurped, power, or action taken** by governmental authority in **hindering** or **defending** against any of these

**However**, this exclusion does not apply to **Cyberterrorism**

For the purpose of this **exclusion**, war shall also mean **kinetic war**

**Exception** for Cyberterrorism  
War = “**Kinetic War**”

# How to Prove Intent of Creators?

## Burden on Insurer to Prove Exclusion Applies



How to prove



Educating the judge or jury



Fact witnesses



Experts



Demonstrative exhibits

## Burden

On insured to prove  
a covered loss

# What Had the Russians Said Prior to Launch?

Nontraditional means of achieving political and strategic goals, including “military means of a concealed character” such as “actions of informational conflict” have “exceeded the power of force of weapons in their effectiveness”

“Long-distance, contactless actions against the enemy are becoming the main means of achieving combat and operational goals”

“Asymmetrical actions have come into widespread use, enabling the nullification of an enemy’s advantages in armed conflict” including “informational actions, devices, and means that are constantly being perfected.”

“The information space opens wide asymmetrical possibilities for reducing the fighting potential of the enemy ... It is necessary to perfect activities in the information space”

Source: *New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations*, V. Gerasimov, Chief of the General Staff of the Russian Armed Forces (Feb. 27, 2013)



# What U.S. Officials Have Privately Said – Evidence?

- It was not possible to either pay the ransom or decrypt the computers
- It was a deliberate Russian military intelligence (GRU) attack aimed at Ukraine
- The malware accidentally “escaped” to third countries and even boomeranged back to Russia
- The impact would have been worse if a country more computerized than Ukraine was the intended victim
- The impact would have been worse but for junior employees who violated corporate protocols and unplugged machines without authorization
- The impact of a similar attack in the future would be far worse in an “Internet of Things” environment and on automated vehicles



---

# Your Turn



**Questions**



**Comments**



**Concerns**



**Discussion**

# Thank You



Kevin Carroll  
[kcarroll@wiggin.com](mailto:kcarroll@wiggin.com)  
202.800.2475



Michael Menapace  
[mmenapace@wiggin.com](mailto:mmenapace@wiggin.com)  
860.297.3733