



Insurance Coverage for Cybersecurity Issues

28th Annual David W. Robertson Admiralty and Maritime Law Conference

November 22, 2019

Leslie C. Thorne
haynesboone

1

Cyber Risks & Liabilities



"I divide the entire set of Fortune Global 200 firms into two categories: those that know they have been compromised and those that don't know yet."

Dmitri Alpervitch
Former VP Threat Research, McAfee

2


Threat Environment

Trends – The Ransomware Crisis

Trending 

WannaCry was likely enabled through phishing emails

i.e., employees had to click on an infected link, likely a malicious Microsoft Word file, to enable the ransomware



This is another reminder that employees are the weakest link in any organization's cybersecurity strategy

and are also the strongest defense.

Source: Willis Towers Watson

Ransomware is a virus that is typically delivered via phishing email campaigns. All the target victim has to do is click on a link to immediately become infected. Once infected all their data is encrypted until a ransom is paid to the attacker, typically in Bitcoins, to get the encryption key to restore their data. Locky Ransomware is a fast moving virus, infecting as many as 90,000 victims per day.

To effectively manage the people risk, organizations should consider the following:



Increase the level and regularity of employee awareness training in your organization

Assess whether your organization's IT department has the right or sufficient talent and skills needed in today's environment to effectively be prepared to handle these emerging threats





Evaluate whether your organization's culture is supportive of cyber awareness and action-oriented behaviors

Not Petya Global Attack: Financial and Operational Impacts

7 firms in 5 industries

Pharmaceutical



\$620 million or more through year end 2017

Disruption of worldwide operations, including manufacturing, research and sales operations.

Logistics/Shipping



\$300 Million

impact on results

Significant impact to worldwide operations and communications.

\$250 – \$300 Million

impact on profitability

Lost volumes as well as extraordinary costs in IT and operations-

Consumer Goods



Estimated 3Q17

\$294 Million

Protracted period required to restore some systems resulted in a backlog in supply system processes.

\$154 Million through 3Q17

The malware affected a significant portion of company's global sales, distribution and financial networks.

Construction



\$387 Million

lost sales by year end

Downtime of IT systems and supply chain disruptions.

Technology

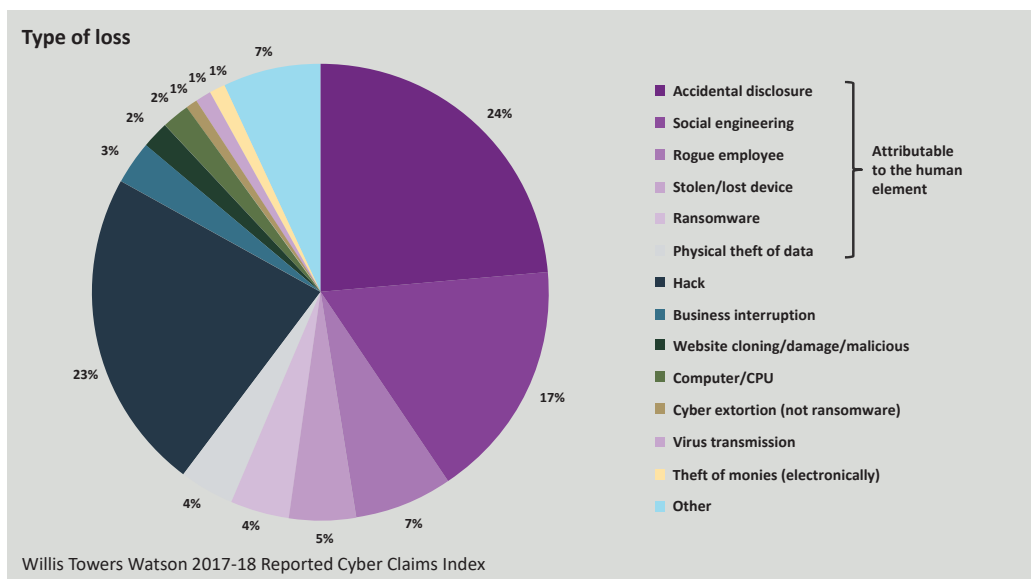


\$90 – \$110 million

Malware affected company systems to receive and process orders.

CLG Proprietary Cyber Claims Data

- 2017-2018 Reported claims index



Cyber Risks & Liabilities

- Third-Party Liability
 - Consumer/employee PII
 - Notification
 - Credit monitoring
 - PCI Compliance fines under merchant agreements
- Loss and Damage to Property
 - Physical injury to property
 - Business interruption
 - Intellectual property loss
- Regulatory Investigations
 - Compliance with subpoenas/orders
 - Fines and penalties
- Brand restoration
- Computer forensics to identify the cause of the breach and fix it



Find the full text of this and thousands of other resources from leading experts in dozens of legal practice areas in the [UT Law CLE eLibrary \(utcle.org/elibrary\)](https://utcle.org/elibrary)

Title search: Insurance Coverage for Cybersecurity Issues

Also available as part of the eCourse

[2019 David W. Robertson Admiralty and Maritime Law eConference](#)

First appeared as part of the conference materials for the
28th Annual David W. Robertson Admiralty and Maritime Law Conference session
"Cybersecurity Insurance"