



# Emerging Risks in Digital Transformation

## Second XM Forum

Cartagena, Colombia

September 6<sup>th</sup>, 2019

# Old & New Threats

## Existing

Privacy Violations

Data Compromise

Distributed Denial of Service  
(DDoS)

## Evolving

Ransomware/Extortion

System Outage/Degradation

“Internet of Things” (IoT)  
vulnerabilities

Nation-State Attack

Corporate Espionage

Property Damage



# Notable Cyber Incidents – Based On Impacted Firms’ Reporting

## System Outages

Industry	Event	Financial Impact	Description
Company A	NotPetya - 2017	4Q18: <b>\$740 million loss</b> , of which approximately \$410 million was lost revenue and \$330 million was expense. There is both property and cyber insurance available. The cyber has paid \$45 million and is not in dispute.	Company experienced a network cyber-attack that led to a disruption of its worldwide operations, including manufacturing, research and sales operations. August 2018: Coverage dispute initiated by firm in NJ Superior court over Property program use of the war and terrorism exclusion in denying coverage.
Company B	NotPetya – 2017	<b>\$387 million lost sales</b> by year end	The attack led to downtime of IT systems and supply chain disruptions.
Company C	NotPetya – 2017	<b>\$300 million</b> impact on results	Worldwide operations of a subsidiary were significantly affected - operations and communications were significantly affected - we are now focused on finalizing the restoration of key customer-specific specialized solutions and systems in time for the peak shipping season
Company D	NotPetya - 2017	<b>\$250 to \$300 million</b> impact on profitability	System shutdowns resulted in significant interruption, affecting our customers as well as our employees - lost volumes during the incident as well as extraordinary costs in IT and operations
Company E	NotPetya – 2017	Estimated <b>\$294 million</b> loss	A protracted period required to restore some of the support systems led to a backlog in a finely balanced supply system, with which we have still not fully caught up - A change in distribution arrangements during the period of the cyber-attack led to a period of misalignment within our S&OP process
Company F	System Failure – 2018	Estimated £176 million (~ <b>\$205 million</b> ) in additional post-migration costs including £115.8 million in customer redress and fraud costs, £30.7 million in system remediation, and £29.9 million in waived fees (2H18 report).	A planned system migration went poorly, leaving approximately 1.9 million out of 5.2 million customers without access to their accounts following the weekend upgrade. This interruption lasted weeks for some customers, with reports that a full one month later some customers were still unable to make payments or access accounts.
Company G	NotPetya – 2017	<b>4Q17: \$188 million loss</b> through 4Q17, split between \$84 million in expense and \$104 million in lost net revenue.	The malware affected a significant portion of global sales, distribution and financial networks - restoring our North America systems has taken longer, resulting in additional lost revenue for the year. August 2018: Firm sought coverage under their property program for this loss, Zurich denying citing the war exclusion.

# NotPetya

27 June 2017

- Data wiper disguised as a ransom-worm
- Originated in Ukraine; spread globally
- Exploited the Eternal Blue vulnerability (NSA) and other methods to spread
- 2M computers within 2 hours of release
- Many prominent firms were impacted; over \$10 billion in damages
- US and British governments have publicly blamed Russia



## TRITON/TRISIS ICS Attack

2017: Attack on critical infrastructure Safety Instrumented System (SIS)

- **SIS are uniquely configured per facility and provide the last line of defense to preserve safety in any off-normal event.**
- **Attacker achieved access to and control of both industrial control system and SIS.**
- **While attacker had control of SIS, a bug in their code caused the SIS to crash, shut down facility, and then the discovery of the intrusion.**
- **Attacker also went after SIS, clearly indicating that they wanted to cause harm to people and damage to equipment.**

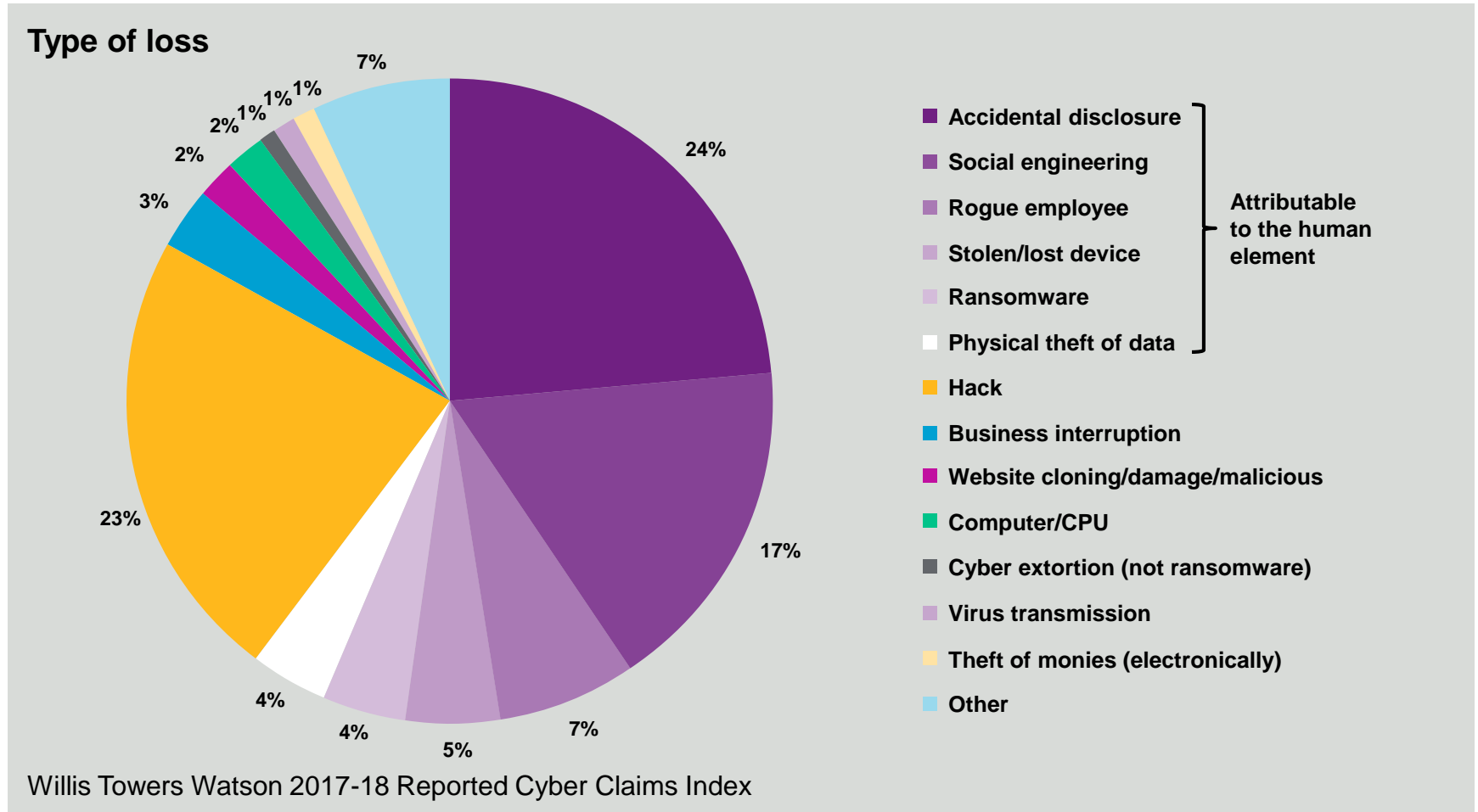
### 2019 ATTACK

- **An unnamed “Critical Infrastructure Facility” in April reported TRITON attackers have been present inside their system for a year.**



# CLG Proprietary Cyber Claims Data




## 2017-2018 Reported Claims Index – Type of Loss



# Some Key Cyber Coverage Considerations

- Expanded business interruption and extra expense coverage arising from damage to reputation following adverse publicity following a cyber incident
- Bodily Injury/Property Damage arising from a cyber peril
- Prior acts coverage
- Social engineering coverage
- Expanded cover for regulatory inquiries and investigations
- Cyberterrorism cover
- Voluntary shutdown coverage
- Affirmative coverage for non-compliance with GDPR, CCPA and similar laws
- “Bricking” coverage

# State of the Cyber Insurance Market – Q2 2019

 <p><b>Capacity</b> Plentiful</p>	 <p><b>Coverage</b> Careful Expansion</p>	 <p><b>Claims &amp; losses</b> Rising</p>	 <p><b>Premiums &amp; retentions</b> Normalizing</p>	 <p><b>Markets</b> Maturing</p>
<ul style="list-style-type: none"> <li>With over 100 markets offering some form of cyber coverage, there is over \$700M of capacity available in the marketplace</li> <li>Primary and Excess capacity are available both in the US and in London. Excess capacity over \$25M is available in Bermuda</li> <li>However, some carriers reviewing their aggregate capacity on large programs following recent breaches and cutting back where they offered limits in both the US and London/ Bermuda markets</li> <li>Growing capacity and interest in LatAm</li> </ul>	<ul style="list-style-type: none"> <li>Cyber product offerings vary widely, there are no uniform set of coverage terms, exclusions, definitions, or conditions</li> <li>Competition drives coverage expansion as carriers seek differentiation</li> <li>Coverages previously subject to sublimit are increasingly available at “full limits”</li> <li>Various approaches by insurers to covering “Dependent Businesses”</li> <li>“System Failure” coverage now available from many insurers</li> <li>Cyber-related Reputational Income Loss Coverage now available from some insurers (at sublimits)</li> <li>Bodily injury &amp; property damage cover available</li> </ul>	<ul style="list-style-type: none"> <li>Cyber claims continue to increase each year</li> <li>New threat vectors are added to consistent activity in existing threats</li> <li>Ransomware/Extortion claims dominated 2018, FBI reported a 300% increase in such attacks since 2015</li> <li>Insurers’ are seeing more business interruption claims with losses exceeding the waiting period</li> <li>The costs associated with managing cyber and privacy claims including forensic investigations and defending regulatory actions and associated fines are on the rise</li> <li>Over 66% of claims are from employee behavior</li> </ul>	<ul style="list-style-type: none"> <li>First time-buyers are enjoying competitive market conditions</li> <li>“Hard market” conditions seen earlier in Retail and Healthcare have improved over the last several years</li> <li>Retentions at all levels are available but can vary greatly based on industry class, size of organization and loss history</li> <li>Pricing less competitive for companies that have not addressed vulnerabilities or make continuous improvements in IT security and training</li> <li>After several years of price decreases, renewal pricing beginning to increase in Q2 2019 for firms with no material change in risk profile</li> </ul>	<ul style="list-style-type: none"> <li>Markets continue to insert InfoSec professionals into the underwriting process and are getting more granular with submission questions</li> <li>Insurers who have been in the space longer, especially in primary positions are becoming more comfortable with the risks they are taking</li> <li>However, there is considerable uncertainty surrounding expanding global regulation such as GDPR and how those will be enforced and impact insureds</li> <li><i>Note: material price changes based on macro risk issues in specific sectors or across the Cyber market place could occur at any time.</i></li> </ul>



# Emerging/Evolving Technologies

Artificial Intelligence

Big Data / Analytics

Blockchain / DLT

Encryption

Internet of Things (IoT)

