Cyber Insurance in the Hospitality Industry

June 25, 2020

State of the Cyber Insurance Market 2020 – Q1

Cost and Retentions	▪ As ransomware incidents across all industries increased dramatically in terms of frequency and magnitude in 2019, coupled with potential losses from high profile breaches, we are starting to see an uptick in premiums across the globe. ▪ As losses and potential losses rack up from several large breaches over the past year, carriers have been reevaluating their positions in large towers and looking more closely at rates in perceived "burn layers." ▪ Carrier focus for excess layers revolves around obtaining adequate premium for perceived risk. There is no longer competition to get on excess towers, especially if pricing is considered "too thin." ▪ Carriers continue to focus on better management of limits deployed on programs, with many offering no more than $10 million on a given placement. Some carriers will consider deploying additional limits but may require significant retentions or ventilation to do so.
Capacity	▪ Cyber capacity is starting to tighten, as insurance claims and losses continue to rise, especially with regard to ransomware as discussed above. ▪ According to the 2019 Cyber Risk Outlook, prepared by the University of Cambridge, incident response costs are driving the increase in the cost of data breaches. As the cyber threat landscape becomes more complex and demand for cyber security resources increases, the costs in remediating data breaches, particularly for large-scale events, has increased. ▪ Certain carriers are adjusting their ransomware coverage appetites and considering sub-limits and co-insurance alternatives.
Coverage	▪ Coverage continues to evolve and expand to cover regulatory risk, reputational damage, forensic accounting and gap exposures. ▪ The E.U. General Data Protection Regulation (GDPR) went into effect in May 2018, and the California Consumer Privacy Act will go into effect in 2020. We have seen cyber markets more affirmatively address coverage for claims stemming from the GDPR and for claims anticipated under the California Consumer Privacy Act. Markets are also offering expanded wrongful collection and "compliance" coverage largely in response to these regulations. ▪ Business interruption/system failure continues to be an area of concern for underwriters. Very exposed industry classes, such as aviation, manufacturing and transportation, have seen increased underwriting scrutiny. While the coverage remains available, certain industries will experience significant premium increases to obtain or retain the coverage. ▪ Cyber underwriters are working more closely than ever with their counterparts in other lines. Cyber and property underwriters in particular are combining forces as carriers continue to expand their coverage offerings in business interruption. Notwithstanding this cooperation, we are seeing carriers withdraw or limit cyber coverage in non-cyber insurance lines due to concern over aggregation.
Markets	▪ Carriers are exploring data analytics partnerships with InsurTech and FinTech firms in an effort to gather and optimize exposure data, allowing underwriters to assess how organizations and their employees handle sensitive data. Underwriters want to understand an organization's cyber culture; this can offer opportunities for buyers to differentiate themselves if they are developing holistic approaches to cyber risk across people, capital and technology. ▪ Carriers continue to accept manuscript applications and conference calls in lieu of standard applications. This has led to more market interest due to the increased amount of information provided.
Targeted Segments	▪ Industries: Retail, Healthcare, FI, Public Entities, Higher Education and Manufacturing. ▪ Layers: Primary and excess

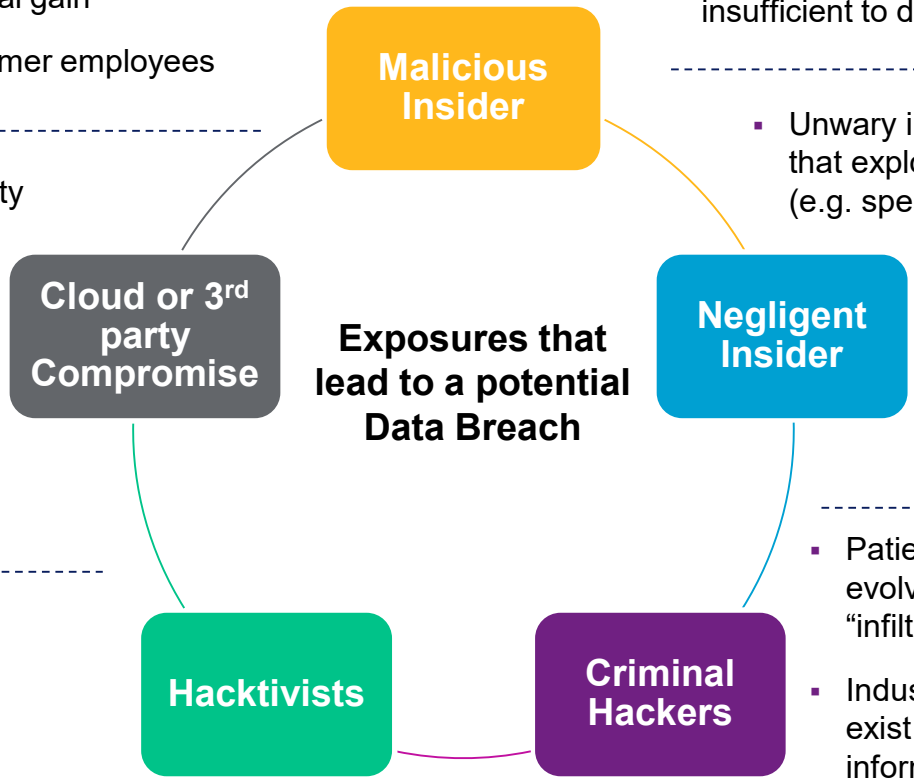
© 2020 Willis Towers Watson. All rights reserved. Proprietary and Confidential. For Willis Towers Watson and Willis Towers Watson client use only.

Cyber Environment Overview

- Growing incentive for insiders to abuse access to sensitive data for financial gain
- Disgruntled current and former employees exploit back-doors

- Theft of Intellectual Property
- Security compromise – loss of sensitive client data
- Infrastructure downtime may lead to Dependent Business Interruption claim

- Intent is to disrupt and/or embarrass a target
- Motivations are fickle and unpredictable
- Massive DDoS attack



- Access controls and behavior monitoring insufficient to detect insider threats

- Unwary insiders susceptible to attacks that exploit traditional security controls (e.g. spear phishing)

- Users who fail to embrace "culture of security" will find ways to circumvent 'inconvenient' security controls

- Patience is a virtue. Tactics have evolved from "hit and run" to "infiltrate and stay."
- Industrialization - Black markets exist for all types of personal information
- Proliferation of mobile platforms and BYOD policies creates new vectors

© 2020 Willis Towers Watson. All rights reserved. Proprietary and Confidential. For Willis Towers Watson and Willis Towers Watson client use only.

Old & New Threats

Existing

Privacy Violations

Data Compromise

Distributed Denial of Service (DDoS)

Evolving

Ransomware/Extortion

System Outage/Degradation

“Internet of Things” (IoT) vulnerabilities

Corporate Espionage

Property Damage

© 2020 Willis Towers Watson. All rights reserved. Proprietary and Confidential. For Willis Towers Watson and Willis Towers Watson client use only.

Common Problem Areas in Cyber Risk Management

Where are your areas of concern?

© 2020 Willis Towers Watson. All rights reserved. Proprietary and Confidential. For Willis Towers Watson and Willis Towers Watson client use only.

Technological & Digital Trends

What trends are shaping the future of Hospitality? What does this mean from a cyber perspective?

Construction and Franchising – building plans and designs integrated now with construction and business partners. Collaborative efforts can streamline business operations but can provide a roadmap for criminals to gain access to valuable personally identifiable information (PII/PCI) e.g. financial accounts and employee data. Terrorists or criminals seek access to data for reconnaissance purposes to plan terrorist attacks. Hackers try to steal IP or leak confidential information. Ransomware and malware attacks may disable hardware and cause network outages/business interruption

Intelligent Buildings - structure that uses automated processes to automatically control the building's operations e.g. heating, AC, ventilation, lighting and security. Sensors and microchips are used to collect data to manage business functions and services. However, Interconnected IP networks heightens cyber exposures, as critical networks become more open and vulnerable to malware and hackers. Trends in offering guests access to their own apps through smart TVs elevates the privacy concerns

New Regulations- GDPR and CCPA have heightened exposures concerning how PII is collected, utilized, stored and transferred. "Privacy by Design" programs now must address multiple layers of response and protections and individual consumers are now empowered to impose regulatory inquiries that could lead to significant fines and penalties. Privacy Officers and legal departments must be able to demonstrate a thoughtful and coordinate approach to privacy policies in coordination with information security practices.

Mobile Workforce – the global workforce has become decentralised and the numerous access points, creates opportunities for theft of information. BYOD to work policies means laptops, smartphones and tablets are expanding networks and creating more exposure points for hackers to access. Employee's own home networks may not be as secure as internal network and could be used to access such networks. Data breaches may also occur due to employee negligence.

© 2019 Willis Towers Watson. All rights reserved. Proprietary and Confidential. For Willis Towers Watson and Willis Towers Watson client use only.

Cyber Risks Gaps In Traditional Insurance

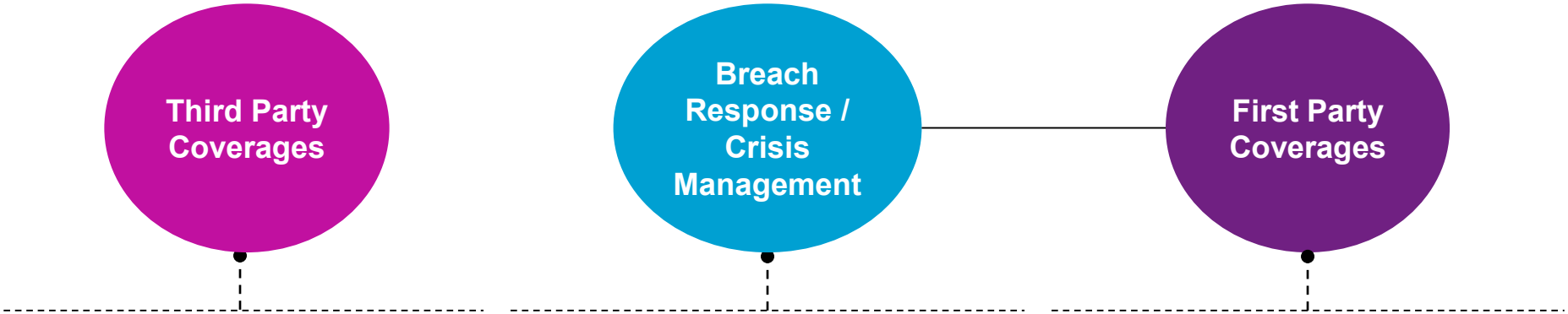
	Property	General Liability	Crime/Bond	K&R	E&O	Cyber/ Privacy
1st Party Privacy/Network Risks						
Physical damage to Data						
Virus/Hacker damage to Data						
Denial of Service attack						
B.I. Loss from security event						
Extortion or Threat						
Employee sabotage						
3rd Party Privacy/Network Risks						
Theft/disclosure of private info						
Confidential Corporate Info breach						
Technology E&O						
Media Liability (electronic content)						
Privacy breach expense/notification						
Damage to 3rd party's data						
Regulatory Privacy Defense/Fines						
Virus/malicious code transmission						

Coverage Provided	
Limited Coverage	
No Coverage	

© 2020 Willis Towers Watson. All rights reserved.

Network Security and Privacy Insurance

General coverage descriptions



- Network Security Liability
- Privacy Liability
- Internet/Media Liability
- Regulatory Fines & Penalties
- PCI/DSS Violations

- Legal Data Breach Coach
- Forensics Expense
- Notification
- Public Relations Cost
- Credit Monitoring/Fraud Remediation

- Network Extortion
- Business Interruption
- Dependent Business Interruption
- System Failure
- Digital Asset Loss
- Cyber Crime
- Reputational Harm

© 2020 Willis Towers Watson. All rights reserved.

Process

- Define risks to be quantified
- Identify client cross functional participants of relevant experts
- Long list of plausible risk drivers (likelihood)
- Data filtering survey to prioritise most relevant loss scenarios
- Identify cost drivers (impact)
- Articulate loss scenarios
- Undertake workshop to establish consensus in inputs for likelihood and impact
- Refine model
- Calculation of loss distribution curves

© 2019 Willis Towers Watson. All rights reserved. Proprietary and Confidential. For Willis Towers Watson and Willis Towers Watson client use only.

Top Five Considerations for Cyber Insurance

Reputational Harm

Adverse media coverage following a cyber event can cause customer dissatisfaction and future loss of profits, which could be costs prohibitive to remediate. Cyber policies can provide PR spin and revenue recovery

Regulatory Impact

Fines and penalties can be imposed when breach notification laws are not properly addressed and the amount varies depending on applicable state or foreign laws. Most notable to date are GDPR and CCPA, with other states following suit. Coverage can provide response costs and coverage fines, penalties or redress funds.

Revenue Impact

Responding to a cyber incident requires a high level of liquidity and can directly affect the bottom line of earnings capital. Network interruptions can immediately cost companies from the moment of disruption.

Vendor Expenses

Utilizing third party resources to respond to a breach can be costly and cause unnecessary delays. A cyber policy can streamline vendors and responses from forensics, PR, notification and monitoring, legal counsel and forensic accounting fees.

Ancillary Services

Carriers typically offer a number of resources in addition to insurance from training resources to free legal counsel and “best practices” checkpoints. They can also provide panel vendors or coordinate response with chosen, vetted vendors as preferred.

© 2018 Willis Towers Watson. All rights reserved. Proprietary and Confidential. For Willis Towers Watson and Willis Towers Watson client use only.