Willis Towers Watson

1

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

What Information/Data is at Risk?

- **PII – Personally Identifiable Information**
  - SSN
  - Date and place of birth
- **PHI – Protected Health Information**
  - Medical history
  - Health insurance information
- **PCI – Payment Card Information**
  - Credit Card #
  - CVV/Service Code
  - Expiration date
- **Corporate**
  - Trade secrets (3rd party)
  - Merger and acquisition plans/information
  - New product plans

3

Cyber Coverage Overview

LIABILITY COVERAGE ('THIRD PARTY' COVERAGE)	
Privacy Liability	Liability costs associated with an inability to protect personally identifiable information, personal health information or a third party's corporate confidential information.
Network Security Liability	Liability costs associated with an inability to prevent a computer attack against your computer network or a third party's network.
Regulatory Fines	Fines assessed by a federal, state, local or international regulatory body due to a data breach.
PCI Fines	Costs associated with any written demand from a Payment Card Association (Mastercard, VISA, AMEX) or bank processing payment card transactions for a monetary assessment in connection with non-compliance with PCI Data Security Standard as a result of a security breach.
Media Liability	Liability associated with disseminated content, including social media content.

4

Cyber Coverage Overview

LIABILITY MITIGATION COVERAGE	
Breach Response Costs	Direct costs expended to respond to a privacy incident. Costs typically include legal, public relations, notification, identity theft restoration, credit monitoring and forensic investigation expenses.

FIRST PARTY COVERAGE	
Income Loss / Extra Expense	Income Loss / Extra Expense associated with a computer attack or system failure which disables your network.
Data Reconstruction	Costs to recreate, recollect data lost, stolen or corrupted due to an inability to prevent a computer attack against your network.
Extortion Costs	Costs expended to comply with a cyber extortion demand.

5

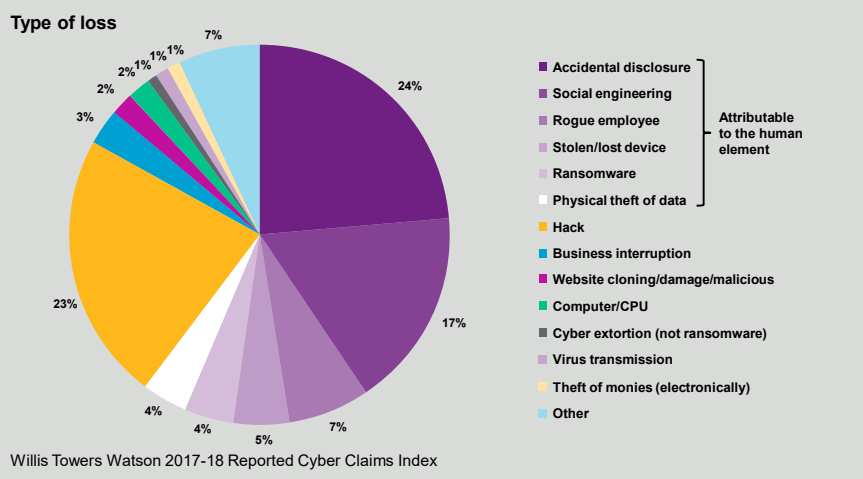
Cyber Coverage Overview

Additional Enhancements around the market place	
Cyber Crime Coverages	Fraudulent Instruction, Funds Transfer Fraud, Telephone Fraud, Invoice Manipulation, etc.
Reputational Damage Loss	Coverage for reputation loss due to a cyber event
Computer Hardware Replacement (Bricking)	Replacement costs for hardware that is compromised and deemed useless after a cyber event

6

CLG Proprietary Cyber Claims Data

2017-2018 Reported claims index

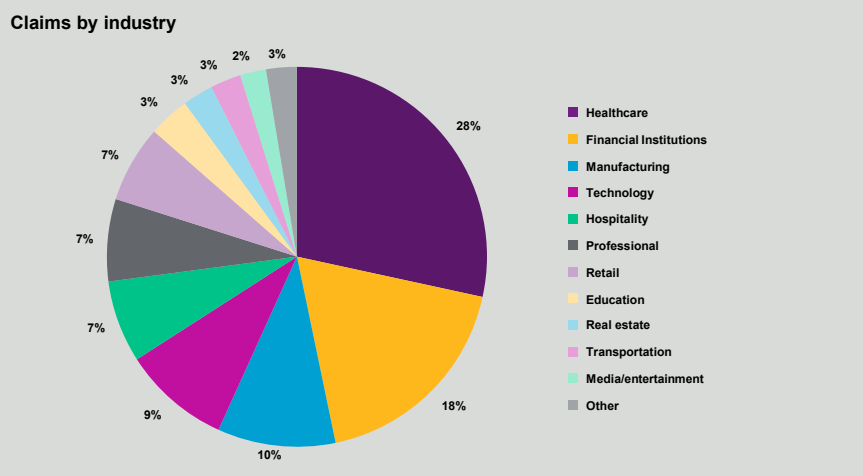


Willis Towers Watson

7

CLG Proprietary Cyber Claims Data

2017-2018 Reported Claims Index



Willis Towers Watson

8

Cyber Insurance Trends to watch for in 2020

- Midsize companies will drive market growth
- Premiums on the rise due to ransomware claims
- Evolving coverage due to increased regulatory risks
- Increased attention on the war exclusion and cyber-terrorism
- Capacity continues to tighten

9

Cyber Liability

Noteworthy Decisions/Lawsuits

- **Veronica George v. Bricton 191 Associates and Marriott International Inc.**

A proposed class action lawsuit filed against Marriott and a hotel management company in Illinois state court on March 27 alleged that the fingerprint scans employees were forced to provide for timekeeping purposes were shared with third parties. Former employee Veronica George alleges some of Marriott's affiliated properties collected her and other workers' fingerprint data without ever providing the necessary disclosures to receive informed consent, as the Illinois Biometric Information Privacy Act requires. Plaintiff seeks a court order declaring the Marriott defendants' conduct violates BIPA and requiring that they award statutory damages of $5,000 for each intentional or reckless violation, or $1,000 for each negligent violation.

- **Attias et al v. CareFirst Inc. et al**

CareFirst policyholders, who filed a class action over a 2014 data breach, again saw most of their claims dismissed on January 30, when a federal judge ruled that the alleged injuries that prompted the D.C. Circuit to resurrect the suit weren't enough to establish the actual damages necessary for the plaintiffs to move forward with the bulk of their allegations. While plaintiffs claimed to have suffered "economic and non-economic loss" in the form of mental and emotional pain, suffering and anguish as a result of CareFirst's alleged failure to secure their confidential information and the "years of constant surveillance of their financial and personal records" that they would have to endure, only two of the named plaintiffs, claimed actual misuse of their personal information in the form of tax-refund fraud that they allegedly experienced as a result of the breach.

10

Cyber Liability

Noteworthy Decisions/Lawsuits

- **Patel v. Facebook**
  A three-judge panel of the U.S. Court of Appeals for the Ninth Circuit held in August that Illinois Facebook users may bring claims for privacy violations under state law for the use and storage of biometric information on the company's platforms and servers. Three Illinois residents alleged that face templates of them were created and used by Facebook Inc. without sufficient notice, agreement and protection under the Illinois Biometric Information Privacy Act. Insurers may be expected to assert that BIPA is a "state or local statute that addresses, prohibits, or limits the printing, dissemination, disposal, collecting, recording, use of, sending, transmitting, communicating or distribution of material or information," and that, as a result, BIPA claims are already being excluded from many cyber policies. The results under cases involving the TCPA strongly suggest that policies with such exclusions may well have no duty as to BIPA class actions.

- **Saul Hymes et al. v. Earl Enterprises Holdings Inc.**
  A proposed class of restaurantgoers urged a Florida federal judge in October to keep intact their lawsuit over a data breach at Buca di Beppo and other popular chains. Earl Enterprises, the owner of Buca di Beppo, argued that the case should be thrown out because the customers haven't shown they've suffered concrete injuries from the breach, which compromised more than 2 million credit cards. The customers argued in their brief that they've sufficiently alleged fraudulent conduct that is "fairly traceable" to the breach. The fight over the dismissal bid is the latest in a lawsuit that was filed after the company announced in March a data security incident that compromised customer credit card information at approximately 100 eateries. The company said the breach involved transactions between May 23, 2018, and March 18, 2019.

- **Landry's Inc. et al v. The Insurance Co. of the State of Pennsylvania**
  Paymentech is seeking to recover $20 million in assessments it paid to Visa and Mastercard after cardholders' personal information was stolen when they made purchases on allegedly unsecured, unencrypted payment card networks at Landry's properties, which operates a host of hotels, casinos and popular restaurant chains. In December 2015, Paymentech discovered a credit card data compromise at multiple Landry's properties. The breach compromised millions of credit card accounts from May 2014 through December 2015. Landry's is now urging the Fifth Circuit to reverse a lower court's decision by ruling that its liability insurer must fund its defense of JPMorgan Chase's $20 million lawsuit claiming the Houston-based hospitality company refused to compensate the bank for costs related to a data breach at Landry's properties