October 20-23, 2022 I Westin Boston Seaport District

10/21/2022

Cyber: Writing Coverage Which is Claims Responsive

2:30PM -4:30PM

Richard G. Clarke

CEUs:2

Sponsored by:

Cyberwrite

Massachusetts Association of Insurance Agents

MAIA

Cyber: Writing Coverage Which is Claims-Responsive

Richard G. Clarke, CIC, CPCU, RPLU
Dick Clarke Insurance Answers
Woodstock, GA 30188
Phone: (678) 923-7034
Email: DickClarkeInsuranceAnswers@gmail.com

The Dramatic Rise of E-Business

- Estimated number of Internet "host sites" at 1/1/22:
- 8+ billion (approximately); (about 6 billion in the USA).
- Largest number of hosts "per capita": Greenland,
- The Netherlands, Norway, Antigua/Barbuda, Iceland.
- Estimated number of persons using the Internet at 1/1/22: 5.5 billion (298+ million users in USA; est. 1 Billion in China, at 01/1/22).

- (Source: www.internetworldstats.com and "USA Today")

The Dramatic Rise of E-Business

- Online sales (individual and business to business)
- are estimated to be in the $800 billion range in
- 2022

- (Comscore.com)

- Holiday 2021 Season online sales were estimated to be in the $300 billion range (125% increase from 2012). Busiest day is Cyber Monday – about $15 Billion

- (Comscore.com)

The Dramatic Rise of E-Business

- Average per transaction revenue per online customer:

Year	Amount
2004	$600
2008	$1,000
2012	$1,300
2016	$2,000
2022	$12,000 (projected)
2025	$20,000 (projected)

(Source: BankAmerica Corp./Robertson, Stephens & Co.)

The Dramatic Rise of E-Business

- Leading online purchases by selected retail category:

Retail	
Travel/Holiday	$19 billion
Household Goods	$17 billion
Computer Related	$20 billion
Automobiles/Parts	$15 billion
Apparel/Sporting	$16 billion
Books (e and hard copy)	$16 billion
Flowers/Gifts	$16 billion
Jewelry/Music	$20 billion

(Source: BankAmerica Corp./Robertson, Stephens & Co.)

Overview of Exposures and Insurance

- Privacy/Data Security Risks now significant; creating believers in IT personnel, management and Boards of Directors – high profile breaches becoming common;
- Data security breaches now easy to record, track and analyze (www.privacyrights.org and www.idtheftcenter.org);
- Federal, state and local laws make compliance both expensive and difficult (Feds may require banks to buy insurance in the future); NY – Required banks had to have "cyber security plan" in place by August, 2017. Strong state privacy laws now in CA, VA and CO (latter two have 2023 effective dates). Significant fines for non-compliance;
- Retaining public confidence and trust increasingly important ("Public Relations Expenses");

Overview of Exposures and Insurance

- 60% of participants in a recent survey say they purchase insurance for the exposures;
- Ransomware costs (including payments by insurers) is exploding;
- Notification costs to state residents now required by all states in the event of a "data breach" (insurance can handle actual notification, or reimburse costs);
- Insurance for regulatory fines/penalties is increasingly important ("PCI", for example – June 30, 2018 compliance date). Any business accepting electronic payments has the exposure;
- Commonality of telemedicine and telebanking;
- Hacking of computer-driven machinery is an increasing threat, with limited insurance available;

Overview of Exposures and Insurance

- Rise of social media: MySpace??, Facebook; Instagram; Pinterest; LinkedIn; TikTok, BizFluence; and use of these sites for marketing purposes (myspace??);
- Driverless vehicles; drone aircraft and watercraft;
- Decline/re-emergence of print media;
- Cellphone computing usual and . Google Glasses and AppleWatch; (total number of cellphones in USA: 410 Million; China 1.4 Billion; India 1.2 Billion);
- Online banking and bill payments – paperless invoicing and bill payments (how secure??);
- Use of credit cards; debit cards; electronic payments and tickets becoming the norm. What happens to cash purchases??

Overview of Exposures and Insurance

- Privacy more difficult to maintain – who is to have access, and how is it to be controlled? How effective is security? GDPR and CCPA, now joined by VA (2023) and CO (2023) (and non-compliance fines) to follow;
- Ransomware/Extortion insurance almost mandatory, with pricing increases; Understanding Social Engineering Fraud;
- More focus on intellectual property/reputation harm exposures;
- The "ricochet" to D+O insurance and aspects of Crime insurance (Computer Fraud and Social Engineering Fraud Coverages -
- "crossover" between Crime and Cyber insurance);
- Must understand the concept of "silent cyber".

Notification Laws – A Major Driver

- Data Security Breach Notification Costs (an unbudgeted expense) are a major driver of the purchase of "cyber" Insurance;
- As of 7/1/2018, all states have now passed these laws to protect state residents and requiring individual resident notification in the event of a data security breach (liberally defined). The laws vary greatly – at some point, we'll have overriding federal legislation;
- Excellent summaries of State Data Breach Laws: Foley & Lardner law firm (www.foley.com/state-data-breach-notification-laws); Interactive map of the states at www.eRiskHub.com;

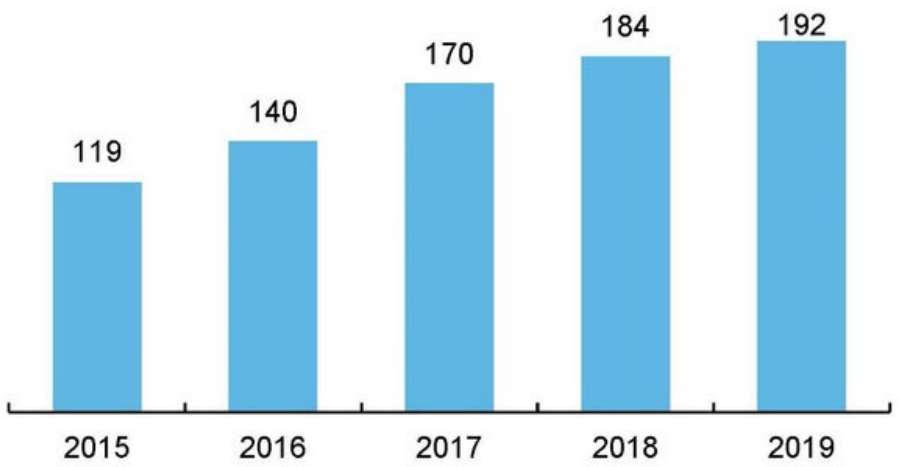
Notification Laws

- Federal law, effective 02/17/2010, and known as "HI-TECH", mandates notice to all persons whose medical information has been breached, or potentially so. If more than 500 persons affected, notice must also be given to state(s) attorneys general, HHS, and news media. This potentially affects every medical-related organization in the USA, as well as employers, and modifies the existing HIPAA legislation;
- Calculate about $10 - $20 cost per notice to be sent. Can empirically calculate the limit of insurance for Notification Costs;;
- Coverage provided as a sub-limit or number of notifications. Some insurers will handle notification, others will reimburse insured for costs;

Costs

A total of 192 US insurers reported direct cyber written premium to the NAIC in 2019, up from 184 in 2018. The new market participants averaged USD393,000 in premium each. Note that these numbers do not include MGAs, who do not file the NAIC supplement.

Number of US cyber insurers | 2015 – 2019

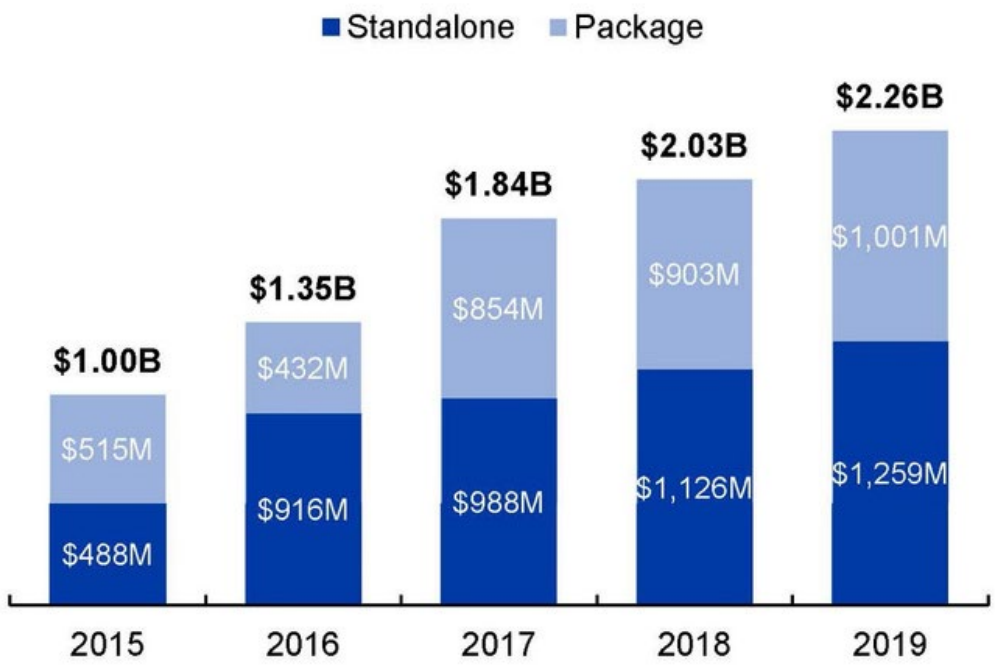


Source: Aon - US Cyber Market Update:2019

Costs

US cyber premiums grew to USD2.26 billion in 2019, an 11 percent increase from the prior year, with similar rates of growth observed for both package and standalone cyber products.

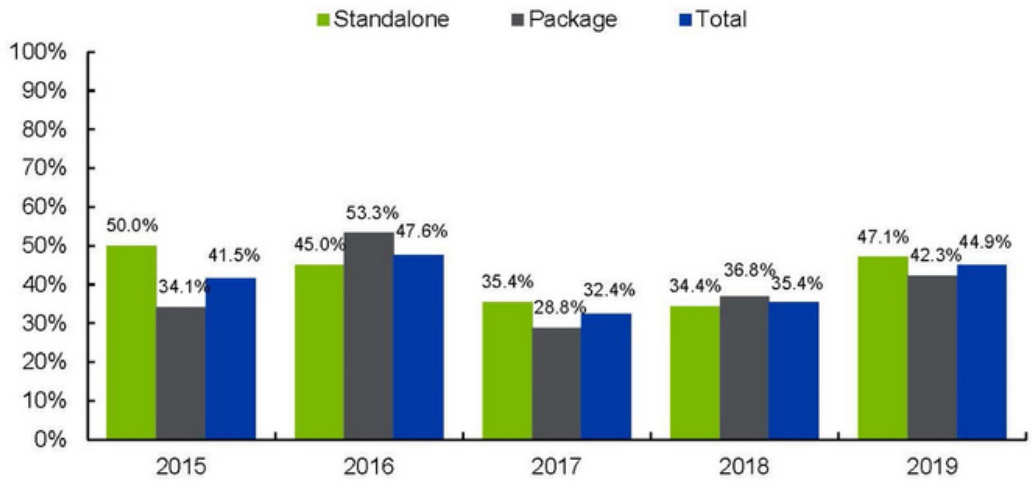
US cyber direct written premiums | 2015 – 2019



Source: Aon - US Cyber Market Update:2019

Crisis Service Costs

As one might expect, the 2019 loss ratio increase was primarily due to an increase in claim frequency. The average 2019 claim frequency across all companies was 5.6 claims per 1000 policies, up from 4.2 in 2018, and affected Standalone business to a greater degree than Package. This jump in frequency more than offset a reduction in the claim severity, where the average claim size fell slightly from USD50,401 in 2018 to USD48,709 in 2019. The premium per policy was essentially unchanged from 2018 – while this may seem unremarkable, it is a notable shift from the rate deterioration seen in 2017 (-18.3%) and 2018 (-1.7%). As we mentioned earlier, rates thus far in 2020 have been broadly increasing.



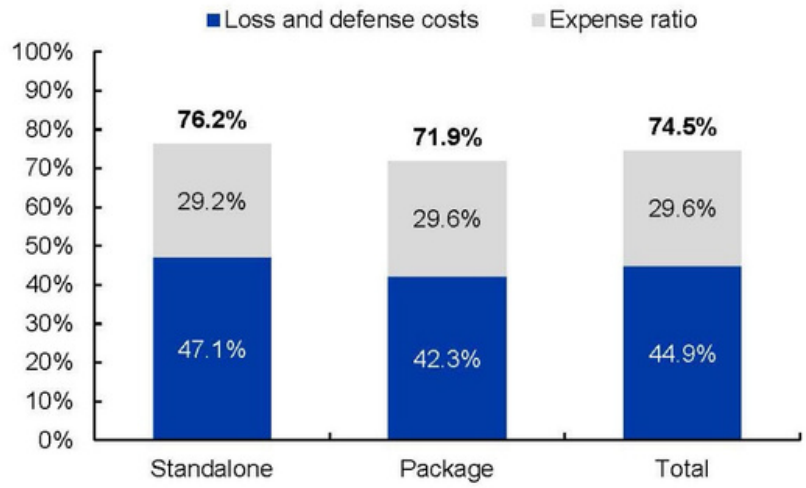
US cyber loss ratio | 2015 – 2019

Source: Aon - US Cyber Market Update:2019

Crisis Service Costs

These results suggest continued profitability for US cyber insurance in 2019, despite the loss ratio increases. However, we would make two caveats when interpreting the 2019 results:

- These expense ratios are estimated from "other liability-claims made" and "commercial multi peril" business, since Cyber is not a line in the IEE. Our experience with many insurers suggests that cyber expense ratios are higher than for other lines, perhaps by 5 points or more. This is not reflected in the NAIC data.
- Cyber insurance is a catastrophe-exposed line of business, and 2019 was a catastrophe-free year. While this does not change the 2019 results, we do recommend the inclusion of an appropriate catastrophe load for forward-looking projections. Aon has spent considerable time working with clients and models to define cat loads for the cyber business.



Estimated 2019 US cyber combined ratios

Source: Aon - US Cyber Market Update:2019

Cause of Loss

In 2019, claims against first party coverage outnumbered third party claims, accounting for 65 percent of all claims. For standalone policies, first party claims made up 57 percent of the total, while for package policies, first party was 75 percent of the total. The claims results are summarized below.
This is consistent with what we hear from conversations with our clients, with first party claims costs accounting for the majority of costs that insurers are paying.
Claims rates were significantly higher for standalone business. Cyber claims occur at a rate of 61.5 per 1000 standalone policies, versus a rate of 2.8 per 1000 package policies. Remember that 'package' business may vary in meaning for different insurers, ranging from cyber endorsements on small commercial or BOP policies to large cyber / technology E&O blended policies.

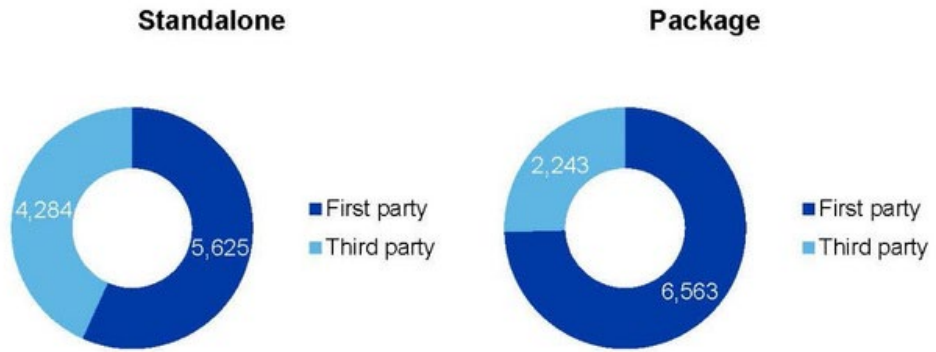


Exhibit 10: US 2019 cyber claims
Total Claims: 18,715
Total First Party Claims: 12,188 | Total Third Party Claims: 6,527
Source: Aon - US Cyber Market Update:2019

Losses, and why we can expect them to continue

- Ability of "techies" to hack vulnerable data, determine passwords and tie up systems;
- Ease of collecting ransom (to be paid in cryptocurrency, and often paid by insurers, on behalf of their insureds). Negotiation usually present;
- Sophistication of criminals, both technologically and intellectually, to access information (strong international element involved);
- Inadvertent media losses (copyright/trademark infringement);
- Federal Trade Commission – most common individual consumer complaint is individual ID Theft;
- OUTSOURCING of IT functions;

Losses, and why we can expect them to continue

- "Careless" losses/human error;
- Profitability of Identity Theft, especially to foreigners;
- Financing of terror activities, government sponsored hacking;
- OUTSOURCING, primarily of IT and related services (what are the critical issues when IT is outsourced?)
- Losses we haven't even thought of yet.

(see: www.attrition.org)

First Party Exposures ("Cyber Property")

- Virtual BI/EE: the BIG exposures are (generally) an interruption in the on-line earnings stream(s), and resultant loss of earnings and/or extra expenses;
- Denial of service – inflow artificially blocked, so that legitimate customers cannot have access to conduct business;
- Computer/System restoration costs sub-limit;
- Ransom demands, following encryption ("tie up") of networks/systems;
- Tricking of employees ("Social Engineering Fraud")

Third Party Exposures ("Cyber Liability")

- Breach of confidentiality/privacy (liability for ID theft
- fits here);
- Gaining unauthorized access to internal information;
- Failure/inability of IT security to prevent unauthorized access (a general allegation by plaintiff attorneys);
- Intellectual property infringement (most cyber liability policies will address media-related copyright and trademark, but not patent, and likely not trade secret infringement exposures);

Third Party Exposures ("Cyber Liability")

- Liability for virus-related damage;
- Defamation and other personal injury (e-mail and social media);
- Media/Advertising liability;
- "Credit injury" (as a result of defamation, improper reporting, etc.);
- Software development/performance ("Technology E+O"). Do not confuse with "cyber", although some insurers combine both coverages in a single policy;
- Sharing user information – big exposure!
- Where is commercial insurance coverage for "Breach of Privacy"??

Potential E-Business Exposures

First Party (interruption in online activities)	Third Party (That for which suits may be brought)	Notification, Crisis Mgmt and Misc. Exposures
Virus (which damages intangible property)	Virus (Traceable to insured)	
Interruption in online earnings stream ("virtual business interruption") Related extra expense Web site damage (requiring restoration) Digital asset restoration services Computer facilitated extortion Computer restoration expenses	Breach of privacy/confidentiality Personal injury (email) Unauthorized access Failure of IT security to prevent access E&O (varies greatly by insurer) E-theft (intangible property) Defamation/Advertising Liability	Payment Card Industry ("PCI" fines/penalties) Forensic-related expenses;; Notification Costs expenses; Social Engineering Fraud (many insurers handle under Crime); Ransomeware End't. (or, cyber extortion).

Cyber Exposure Effect on other Insurance Coverages

- Boomerang to D+O Insurance (cyber security and insurance is a governance function). Understand "silent cyber" exposure??;
- Overlap with basic CGL insurance (definition of "personal injury"), and maybe, EPLI. What about Fiduciary Liability??;
- Coordination with Errors + Omissions coverage:
  - Description of services covered vs. website info;
  - Are E+O and cyber combinable?
- Overlap with Employee Dishonesty/Crime Insurance??
- Any overlap with ID Theft Insurance (likely, no coverage for loss of money)?
- Is cyber endorsement on Management Liability or other package policy as effective as monoline cyber insurance?
- Website/app discrimination ("WCAG") – avoid "Internet" exclusion under EPLI (and other policies, as well);

Cyber Claims and Insurance Related Resources

- "The Betterley Report" (www.irmi.com). Annual analysis of individual cyber insurance policies, June of each year;
- NetDiligence Annual Cyber Claims Study;
- Access to www.eRiskHub.com;
- Summary of State Data Breach Notification Laws (various sources, including Foley & Lardner law firm (www.foley.com/State-Data-Breach-Notification-Laws);
- www.krebsonsecurity.com;;
- 2022 Ponemon Data Breach Study;
- Advisen/ZyWave Whitepapers and surveys helpful;
- GDPR Legislation in UK, effective May, 2017; CA (2020); VA (2023); CO (2023);
- Coalition Cyber Claims Study.

.

Essentials of Good Cyber Insurance

- Specific, broad coverage for Breach of Privacy/Confidentiality and Unauthorized Access;
- Specific coverage for Failure of IT Security;
- Specific coverage for Data Security Breach Notification costs (either sub-limit or "number
- of persons affected" approach). The "trigger" is the key here. Also, coverage for notification expenses not specifically required by law;
- Coverage provided on an "enterprise-wide" basis;
- No unencrypted device exclusion;

Representative Specialty Insurance Coverage Available

- AIG: "AIG CyberEdge" – Menu-driven coverage, with good flexibility:
  - Will consider coverage for almost any type of risk –
  - fast turnaround on indications (Coverage ALSO available for
  - E+O exposures.)
  - For Notification Costs Reimbursement ("Crisis Management"),
  - will offer sub-limit or pre-set number of notifications;
  - Excellent Risk Management ("CyberEdge Risk Tool")
  - Smaller risks (under $25 Million revenue) outsourced;

Representative Specialty Insurance Coverage Available

- CNA – NetProtect360, or ePack Extra (Basic Form)
  - Notification Costs Reimbursement ("Privacy Event Expenses")
  - generally provided on a sub-limited basis. Can do pre-set number of notifications;
  - Notification costs reimbursement differences between the two forms;
  - Good general appetite for variety of risks;
  - Often, wants to write Tech E+O AND Cyber cover together (ePack Extra);

Representative Specialty Insurance Coverage Available

- Beazley: "Breach Response" ["BBR"]
  - Good insurance for healthcare exposures, but not limited thereto;
  - Focus on Breach Response Services;
  - Capability to handle a pre-set number of notifications.

Representative Specialty Insurance Coverage Available

- AxisPro -"PrivaSure" and "PrivaSure Breach Response"
  - Also able to handle Notification costs Reimbursement or pre-set number of notifications;
  - Uses (optional) Breach Coach Services;
  - Underwriting options for Social Engineering Fraud and Ransomware endorsements on some accounts;
  - Generally, fast turnaround on indications and quotes;

Representative Specialty Insurance Coverage Available

- "CyberChoice 2" (Hartford Specialty Technology);
- Hiscox "CyberClear" (Insurance Times' Cyber Product of the year for 2019);
- BCS Insurance Company (reinsured by Lloyd's);
- Coalition and Cowbell products;
- Philadelphia Insurance Company;
- Business Risk Partners (www.businessriskpartners.com);
- IT Risk Managers (www.itriskmanagers.com).

Representative Specialty Insurance Coverage Available

- Chubb
  - Well-rounded coverage, but not cheapest premium.
  - Includes Data Breach Fund (Notification Costs with several good expansions of basic coverage - sub-limit or preset number of notifications);
- Travelers - "CyberFirst" or "CyberRisk"
  - Good coverage. Can provide notifications cost sub-limit or pre-set number of notifications;

Representative Specialty Insurance Coverage Available

- Coalition
  - A combination of First Party, Third Party with available. Also, includes "Pre-claim Assistance" sub-limit;
  - Need "Reputational Repair Endorsement"; and likely, negotiation in Hammer Clause percentage;
  - Heavily reinsured;
  - Great Annual Claims Study report.

Past, Current and Anticipated Losses

- 2021 NetDiligence Cyber Claims Study;
- Advisen Cyber Liability Insurance Market Trends (2021);
- Coalition Cyber Report (2021);
- International, government-backed hacking efforts directed at businesses and individuals;
- Employee-related (internal loss trigger still one of the largest sources of claims activity);
- Insurance carrier claims info and details.

Past, Current and Anticipated Losses

- Catastrophic losses, and difficulty to predict (underwriters more rigidly underwriting – supplemental applications the norm);
- Data Security Costs Notification expenses increasingly important to buyers of this insurance (all states with statutory law; Federal law effective in February, 2010 ("HI-TECH")), as these are unbudgeted expenses, which come as a surprise to the entity who must absorb them;
- Computer-controlled machinery hacking exposure emerging.

Anticipating The Future

- Increasing web sites/users, with much more "social media" activity ("Facebook", "Pinterest", "LinkedIn", etc.);
- Mobile computing and transaction payments. Cash??;
- Increasing forensic expenses (does insurance cover??);
- Proliferation of fraud and computer viruses, much from outside the USA;
- Constantly evolving insurance coverage provisions, new policies, new insurers, and court cases;
- Both catastrophic, as well as small losses (severity and frequency) are possible.

Exhibits