CYBERINSURANCE: COVERAGE, CLAIMS AND PRACTICAL GUIDANCE

THE FEDERATION OF DEFENSE & CORPORATE COUNSEL ANNUAL MEETING
7:00 AM TUESDAY JULY 31, 2018
Wailea Resort & Spa
Maui, Hawaii

MODERATOR:
David W. Zizik, Esq.
Sulloway & Hollis, P.L.L.C.
40 Westminster Street, Suite 201
Providence, RI 02903
Telephone: (401) 421-1238
Facsimile: (781) 658-2532
E-mail: dzizik@sulloway.com

SPEAKERS/AUTHORS:
Wesley H.H. Ching, Esq.
Fukunaga Matayoshi Ching & Kon-Herrera, LL
Davies Pacific Center
841 Bishop Street, Suite 1200
Honolulu, HI 96813
Telephone: (808) 533-4300
Facsimile: (808) 531-7585
E-mail: whc@fmhc-law.com

Peter W. Olson, Esq.
Cades Schutte LLP
Cades Schutte Building
1000 Bishop Street, Suite 1200
Honolulu, HI 96813
Telephone: (808) 521-9385
Facsimile: (808) 540-5059
Email: polson@cades.com

Craig Uradomo
AVP, Actuarial Services,
Product Development & Management
Island Insurance Companies
1022 Bethel Street
Honolulu, HI 96813
Telephone: (808) 564-8465
Facsimile: (808) 275-8465
E-mail: curadomo@islandinsurance.com

CYBERINSURANCE: COVERAGE, CLAIMS AND PRACTICAL GUIDANCE

***Wesley Ching, Peter Olson, and Craig Uradomo*[1]**

I. Introduction

Data breaches and other cyber attack crimes are an unfortunate side effect of our modern society's increasing use and reliance on technology to store and reproduce data. Insurance defense firms, which handle large volumes of oftentimes privileged and sensitive information, are especially vulnerable to cyber attacks and data breaches. As a result, cyber insurance is a rapidly developing area in insurance law.

Although cyber insurance coverage first started to be introduced about fifteen years ago, there are still many unknowns in this constantly evolving area of insurance coverage. While organizations may understand and see a need for cyber insurance, many organizations considering cyber insurance may question what cyber insurance typically covers, what types of events are typically excluded from coverage and how cyber insurance policies will evolve with time as cyber security needs change with further technological advances.

This paper addresses the growing need for cyber insurance, cyber coverage gaps in traditional insurance policies, the scope of cyber insurance coverage currently available, the types of cyber coverage forms and exclusions being developed by ISO and leading cyber carriers and evolving marketplace and coverage issues.

II. The Need for Cyber Insurance

Law firms have not been immune to the growing cyber risk crisis that is plaguing businesses and individuals alike. One needs only to read the news to hear of data breaches that have affected millions of people and businesses and causing millions if not billions of dollars of damages. Indeed, law firms have been the targets of notable cyber attacks over the past decade. The 2015 ABA Technology Survey Report notes that a quarter of all law firms with over 500 lawyers have suffered a data breach. Although Hawaii does not have law firms of that size, it would not be surprising to learn that some Hawaii law firms have suffered some type of data breach. Also, law firms (and other professionals such as medical practitioners) must be very careful with regard to cyber risks because attorneys have statutory professional and ethical duties to safeguard their clients' and possibly other third-party confidential information including client financial and billing information, confidential case information and client monies in trust accounts in addition to any personally identifiable information (PII), personal health information (PHI) or in cases where law firms accept credit cards, personal credit information (PCI). These types of client information are eagerly sought by criminals to sell or to disparage clients or their products and services. It has also been reported that adversarial law firms have been behind hacks into their legal opponent's computer systems to obtain confidential case information and the advantage that brings.

---

[1] Wesley H.H. Ching is a partner at Fukunaga, Matayoshi, Ching & Kon-Herrera; Peter W. Olson is a partner at Cades Schutte LLP; Craig Uradomo is an Assistant Vice President at Island Insurance Company, Ltd.

These hacks can occur not just through "direct" hacking activities by an individual who seeks to infiltrate a specific firm's computer system for nefarious reasons, but hacks can also occur through inadvertent security mistakes by a law firm's employees, service providers or vendors. For example, an employee can click on a link in a phishing email or download infected software or files which can provide inadvertent access to hackers.[2] According to a Report by Verizon on its Data Breach Investigations in 2013,[3] 75% of the hacks reported by businesses were not targeted infiltrations of specific businesses but were hacks accomplished by various schemes, such as phishing.[4]

The legal, professional and ethical implications of a privacy or security breach of a law firm's computer systems and trust accounts go well beyond third-party liability for damages. The possibility of severe reputational damage to a law firm is one reason that it appears that many law firms do not report or underreport privacy and security breaches that have occurred. However, in some cases, the negative publicity that is generated cannot be avoided, such as in a 2013 case where reports circulated that an amount in the high six figures was stolen from a prominent Canadian law firm's trust accounts.[5]

Today's reality is that a law firm that doesn't properly safeguard their clients' information and monies could be found in breach of their professional obligations. While a law firm can take many practical steps to protect its computer systems that will significantly reduce the risk of a privacy or security data breach, in the event of a breach, adequate cyber insurance will be of increasing importance and may serve as the last line of defense for a firm's balance sheet.

The following is a non-exhaustive list of some of the cyber threats facing law firms today:

- Hactivists
- Ransomware
- Nation-State Espionage
- Rogue Employees
- Accidental Exposure
- Technological Obsolescence
- Security Issues With Third Party Providers/Cloud Systems
- Password Management Being Weak/Non-Existent
- Lack of a Security Mindset
- Reduced Security Standards For Remote Workers

---

[2] How Attorneys Get Hacked (and What You Can Do About It), Sherri E. Davidoff, 39 Mont. Law. 25 (2014).
[3] "2013" Data Breach Investigations Report", www.verizonenterprise.com/DBIR/2013/
[4] How Attorneys Get Hacked (and What You Can Do About It), Sherri E. Davidoff, 39 Mont. Law. 25 (2014).
[5] "Law firm's trust account hacked, large six figure taken," Yamri Taddeed, Law Tiimes, www.lawtimesnews.com/201301072127/headline-news/law-firms-trust-account-hacked-large-six-figure-taken, Jan. 7. 2013.

The cyber security threats facing law firms were dramatically revealed in two highly publicized recent cases. In 2015, the Panama based law firm, Mossack Fonseca, at that time the fourth largest offshore law firm was hacked leaking more than 11.5 million documents to the public. The breach ultimately leaked 2.6 terabytes of data, which is more than the Edward Snowden NSA leaks in 2013 and the U.S. diplomatic cables released by WikiLeaks in 2010 combined. A consortium of investigative journalists combed through the documents to reveal the firm's involvement in creating over two hundred thousand shell corporations set up for tax evasion purposes and resulted in the resignations of Iceland Prime Minister David Gunnlaugsson and Jose Manuel Soria, the Minister of Industry for Spain. In March of 2018, the Mossack Fonseca law firm announced it was closing, blaming economic and reputational damage caused by the document leak.

In March of 2016, the Wall Street Journal reported that hackers had broken into two prominent New York law firms, Cravath, Swaine & Moore and Weil Gotshal & Manges, stealing the emails of partners. It was revealed that the hack had been perpetrated by three Chinese citizens in order to obtain information about mergers and acquisitions that were in the works. The hackers used the information they obtained to buy shares in the target companies and made more than four million dollars in profit off trades. The United States attorney general was quoted as saying "[This case] should serve as a wake-up call for law firms around the world: you are and will be targets of cyber hacking, because you have information valuable to would-be criminals."

These are only two recent examples of cyber attacks that have yielded devastating results for law firms; however there are doubtless many others that have gone unreported with equally dramatic results.

III. Cyber Coverage Gaps in Traditional Insurance Policies

As of June 2016, only 11 percent of lawyers responding to an ABA Technology Survey indicated that their firm had obtained cyber liability insurance.[6] Unfortunately, too many law firms may be relying upon traditional insurance policies, particularly lawyer's professional liability ("LPL") and commercial general liability ("CGL") insurance policies. While the coverage that these types of policies provide remain relevant for law firms for the risks that they insure, these two types of policies, however, will likely not provide sufficient coverage for cyber risk and security breach liability.[7] Significant gaps exist in both LPL and CGL policies as to both first-party and third-party liability (damages incurred by clients or employees). In the few court cases that have considered CGL coverage for damages from security breaches and hacked data, the courts have generally held that the breach and loss of electronic data is not damage to "tangible property" and have not found coverage for the damages incurred by the breached companies.

[6] "Cyber Insurance for Law Firms", Jeffrey A. Franklin, Vol. 33 No. 3 GP Solo 3, pg. 1.
[7] *Id*., pg. 2.

Also, as the ISO started providing endorsements for CGL policies in 2014 that specifically exclude coverage for liability based on the loss or damage of electronic data, it could be expected that GCL policies will increasingly limit coverage for security breach liability. In addition, other recent court cases have found that breach of privacy incidents are not covered under a CGL's personal and advertising injury coverage as that coverage is limited to when the insured publishes information and does not apply to a hacker's dissemination of stolen data and information. As a result, there are serious gaps in both LPL and CGL insurance for cyber risk and security breach liability for law firms and other businesses.

In the **first-party situation** for a law firm, where the law firm seeks to insure damages that it may incur from a security breach, the kind of gaps that are recognized in LPL policies (CGL policies cover third-party liability discussed below) include coverage for damages and costs regarding the following: [8]

- Theft or destruction of the law firm's data and information
- Cyber extortion or ransomware threats
- Business interruption
- Lost income
- Remediation -- restoration or re-creation of data, information and electronic business assets such as proprietary software and files
- Credit monitoring
- Investigations and forensics into the source, method and extent of damages
- Crises and public relations management
- Extra expenses.

With regard to a law firm's **third-party** liability (from clients or employees) from a privacy or security breach, the gaps that are currently recognized in LPL and CGL policies include damages and costs associated with:

- Fines and penalties from regulatory actions (privacy laws)
- Privacy notification
- Credit monitoring
- Business interruption
- Intellectual property infringement (copyright, trademark, etc.)
- Reputational damage (slander, libel, disparagement of products, etc.)
- Crisis and public relations management
- Remediation -- recovery/re-creation of data
- Investigations and forensics
- Extra expenses.

The same gaps exist for other types of businesses, especially those that hold electronic consumer information, which exposes them to increased risk of fines and penalties for

[8] *Id.*

insufficient security surrounding their computer and electronic data systems. Given the recent Facebook hearings on Capitol Hill, it can be expected that privacy legislation and regulation for electronic data and information will be increasingly considered and passed by both state and federal lawmakers. This, in turn, will likely increase the necessity for adequate cyber risk and security breach insurance by companies holding sensitive and confidential client and/or consumer information.

IV. The Scope of Cyber Insurance Coverage Currently Available

The previous discussion concerned the gaps in traditional insurance policies for cyber risk and security breach liability for law firms and other businesses. This discussion will focus on what coverages are currently available to protect a law firm for damages and costs associated with cyber risk and security breach liability. From the outset, it is important to note that the cyber insurance that is currently offered by insurance companies is far from uniform. While some policies appear to take the familiar format of insuring clauses, exclusions and definitions, etc., in reality, they can be significantly different than the more familiar LPL and CGL policies. Some of the more important differences include:

- Most cyber risk and security breach liability policies currently include **elements of both first-party and third-party insurance** and thus are considered "mixed" or "package" policies rather than pure first-party or third-party policies. This involves the use of different types of insuring clauses and both insurers and insureds have found that policies that cross-reference terminology (e.g., definitions) between the different parts of the policy has resulted in complications and ambiguities in some cyber risk and security breach liability policies.

- Most cyber policies are **stand-alone policies**, however, it should be noted that the ISO has created both stand-alone "Cyber Risk Solutions" policies but also a set of "Businessowners Cyber Endorsements" that provide "optional cyber-related endorsements and complementary manual rules and loss costs" in a three-tiered approach (first-party endorsement is tier one; third-party endorsement is tier two; and tier three adds coverage for extortion threats; business income, extra expense and website publishing liability). The ISO's cyber risk and security breach liability policies are the topic of another paper in this seminar. The ISO is not alone in offering endorsements to other business-related policies, such as CGL policies to expand the coverage provided to businesses, however, the efficacy of "grafting" a cyber risk and/or security breach liability endorsement onto a CGL that insures significantly different risks has yet to be fully evaluated. It might be foreseen, however, that unless there is a significant benefit for businesses, e.g., cost savings, for such an "endorsement" approach; it may be safer for businesses that have significant exposure to obtain a comprehensive cyber risk and security breach liability policy. In other words, as the field matures and the risks and damages are more clearly assessed, quantified and regulated, it may become clear that cyber risk and security breach liability insurance is as different from LPL or CGL as say, automobile insurance, and the attempt to meld the two via endorsement(s) might only increase the risk of gaps and unnecessarily complicate the use of necessary terminology

and the interpretation of that terminology. As noted, however, this will no doubt become clearer as the field matures.

- **Standardization has not yet evolved** for cyber risk and security breach policies – policies from different companies incorporate different types and scope of insured risks/perils, insuring clauses, different types and numbers of definitions and terminology, different exclusions and conditions, and different investigation and cooperation requirements.

- Most cyber insurance reporting is on a **claims made basis** (rather than on an occurrence basis) that requires both the breach and the claim reporting to occur within the effective policy period which can be problematic as companies have often not learned of some security breaches until well after the fact; however, retroactive coverage appears to be an option in some policies.

- **Cost varies widely** for a cyber risk and security breach liability policy between insurance companies which is attributable to the newness of the risk and the lack of statistical data that underwriters traditionally use to assess and categorize risk, probabilities and associated scope of damages in cost calculations. Until the cyber risk and security breach liability insurance market matures, costs between policies will not easily be compared and costs are likely to fluctuate. Factors that will influence cost include: a firm's risk management practices including network and computer security, personnel safeguards, vendor management, liability limit and deductibles, claims history and firm footprint (exposure to local versus international risks, the latter will likely include a greater need for compliance under various jurisdiction's privacy regulatory frameworks)[9].

- **Very limited comparative reviews have been undertaken by insurance professionals or coverage attorneys** of the various cyber policies which are increasingly coming onto the market making it difficult for businesses and others to compare coverages and costs.

- **Increasing governmental regulation** in the privacy area may increase the potential for liability and damages.

[9] "Everything you need to know about cyber liability insurance but never knew to ask", JoAnn L. Hathaway, 95-DEC Mich. B.J. 42, December 2016, p. 1-4.

Given the general characteristics listed above and the variance between policies, cyber insurance nevertheless generally covers the following:

Common Cyber Coverages[10]	
First Party Coverages: Costs and expenses the insured incurs due to a security breach or security failure	
Privacy or personal information breach or security breach	Costs (direct and extra expense) to respond to a data breach (known as an incident or event response), including forensic and legal investigation, legally required breach notification, credit monitoring, call center and public relations (reputation) costs. Some policies may provide coverage for theft of firm and client trust funds (cyber crime).
Digital asset replacement costs	Costs to replace, restore, re-create or re-collect digital assets corrupted or destroyed by a security breach. The biggest variation between carriers appears to be in breach remediation coverage and carriers may negotiate coverage. Cost savings may be obtained by using carrier designated service providers.
Extortion and ransomware threats and rewards	Expenses and ransom and reward payments to resolve a credible extortion threat to: • Launch or continue a computer security attack on the insured; • Release, improperly use or destroy personal or confidential corporate information
Network or Business interruption loss	Lost income and extra expenses due to interruption of service of a computer system through a security breach or attack. Some policies include contingent/dependent business income loss coverage.
Other coverages that may be available	• Social engineering fraud loss • PCI-DSS assessment fines and costs (failure to comply with PCI Data Standards) • Telecommunications hacking
Third Party (Liability) Coverages:	
Privacy liability coverage (Personal information breach or security breach)	Defense costs, settlements and judgments resulting from civil suits from clients or employees (other than by regulators) for negligence in allowing or failing to prevent the unauthorized use, access or disclosure of protected personal, private or confidential information or violation of privacy laws regarding the maintenance, protection, use or disclosure of protected personal information. Client losses may include notification costs, credit and identity monitoring; business interruption, digital asset

[10] Table is modified from the American Bar Association's Business Law Section - Spring Meeting 2018 "Cyberinsurance: Coverage, Claims and Cross-Border Concerns," John Black, pg. 1; some modifications are from "Cyber Insurance: A Last Line of Defense When Technology Fails", Latham & Watkins Insurance Coverage Litigation Practice, April 15, 2014.

	replacement and extra expenses similar to those listed above in the first-party coverages. *Considerations include*: the nature of the triggers (failure to protect confidential information versus a cause of breach and whether the breach was "intentional" or not (inadvertent); some policies include coverage for a firm's failure to disclose a breach in accordance with privacy laws.
Regulatory proceeding liability	Defense costs from federal or state regulatory agency investigations or proceedings arising from a privacy breach. Some policies also cover fines, penalties and consumer redress funds. Not all policies provide regulatory proceeding liability. *Considerations include*: <u>when</u> the duty to defend is triggered – some policies follow the traditional necessity of a "suit" but some provide coverage from an initial governmental inquiry such as a civil investigative demand; there are different coverage considerations for civil versus criminal investigations.
Network security liability	Defense costs, settlements and judgments from third party claims for acts, errors or omissions in computer system security or customer record security or confidentiality. Some policies also cover transmission of viruses or malicious code.
Other coverages that may be available	• Multimedia and advertising liability coverage (may cover losses related to libel, slander, defamation and other media torts as well as copyright, trademark and patent infringement). This can also include losses from information posted to social networking sites. This coverage generally does not include civil or criminal fines. • Technology professional services • Contingent bodily injury/property damage

In order to determine what types of cyber coverage is appropriate for a law firm, the cyber risks that a given law firm faces must be affirmatively reviewed, identified and assessed. Only through this process may a law firm identify necessary and optional coverages that will protect the law firm as a "last line of defense" against cyber attacks and incidents. Usually the first analysis that should be undertaken is what type of client (or other third party) information does a law firm maintain on its computer systems. Depending on the type of practice, law firms often maintain sensitive client information including a variety of data "types" governed by privacy regulations such as personally identifiable information (PII) or protected health information (PHI). In order to protect itself from a breach of these types of data a law firm may wish to obtain broader regulatory coverage with higher limits. Also law firms may also wish to obtain broader "conduit liability" coverage[11]. Conduit liability refers to an insured's losses where it is held partially or fully responsible for a third-party hacker's data breach as the hacker uses

[11] eDiscovery for Corporate Counsel, Chapter 17: Crisis Management: Electronic Data and Cyber Security Considerations, § 17:8: "Risk management – Will a cyber insurance policy fill the gaps and protect an organization from first-party losses and third-party losses arising from a cyber breach?", Fernando M. Pinguelo, Angelo A. Stio III, and Hasan Ibrahim, January 2018 Update, pg. 1.

the insured's system as a "conduit" to access the system of a third party. In that case, such conduit liability coverage may be advisable.[12]

One particularly notable concern for law firms and other businesses that maintain proprietary client information on their computer systems is that cyber liability coverage often is limited to the breach of "personal information" rather than confidential corporate information such as trade secrets. A law firm should ensure that any cyber risk and security breach liability policy will cover potential losses that are applicable to the type of client data and information that the law firm maintains. Also, to the extent that firms maintain client or other third-party credit card information, coverages should include broad payment card information (PCI) coverage.

An effective way to ascertain what coverages may be needed and to compare cyber risk and security breach liability policies for a given type of practice is to:

- Identify the cyber risks unique to your practice or organization;
- Identify the third-party network or computer security requirements the firm maintains and what government privacy regulatory requirements apply to the law firm;
- Identify one or more appropriate policy(ies) in terms of scope and coverage that affirmatively address and provides coverage for the identified risks;
- Compare different cyber insurance policies and quotes by reviewing the wording of the policy and any endorsements applicable to each identified risk;
- Prepare to negotiate coverages and changes dependent on your firm's identified risks.

Law firm cyber risk and security breach liability insurance can be obtained from various sources and companies. As just one example, as of February 2017, cyber insurance is available through the American Bar Association underwritten by Chubb Limited. An ABA article on its website notes that this insurance includes "cyber coverage for a firm's own expenses, such as network extortion, income loss and forensics, associated with a cyber-incident as well as for liability protection and defense costs. The coverage can be tailored to meet a law firm's unique needs and also includes Chubb's loss mitigation services both before an incident and following an incident."[13]

V. The Evolving Cyber Marketplace

Early cyber-related coverages were drafted during the '90s when cellular phones were shrinking in size (though they were still primarily mobile phones, not the hand-held computers of today), people had to access the internet through a dial-up, Amazon was a website that only sold books, and society was staring down the year 2000 and the "Millennium Bug". These early insurance products typically provided third-party liability only for threats concerning

[12] *Id.*

[13] "ABA begins offering cyber liability insurance to lawyers, law firms of all sizes", Feb. 28, 2017, <www.americanbar.org/news/abanews/aba-news-archives/2017/02/aba_begins_offering.html>; last accessed on April 19, 2018. The Chubb policy referenced has not been reviewed nor is it endorsed by the author.

unauthorized access, network security and virus transmittal, and were often written as endorsements to Errors & Omissions (E&O) policies for entities in the technology sector.[14] Other early buyers of cyber coverage were typically entities in the health care, banking and retail industries, which collected considerable amounts of health-related, financial or consumer information.[15]

It was not until the mid 2000's that cyber insurance carriers began adding basic first-party coverage to their cyber policies. This expansion of coverage was driven in part by the onset of state data breach notification laws, beginning with California in 2002, which require an entity that has been subject to a data breach to notify their customers of the breach and follow the mandated steps for remediation.[16] The initial offerings of first-party coverage typically included cost reimbursements for the forensic investigation of the breach, the use of a public relations firm, customer credit monitoring and notification of the breach. Usually these first-party coverages were offered on a sublimit basis, which may have ranged from $5,000 to $100,000, depending on the policies total limit of insurance.

A. Market Growth

Industry experts predict that cyber insurance will continue to be one of the leading growth areas as respects premium volume in the U.S. property and casualty insurance market. 2016 U.S cyber premium increased by more than 34% over the prior year to reach $1.3 billion, and is forecasted to grow to $20.0 billion by 2020. [17]

The U.S. currently accounts for an estimated 80% of the global cyber insurance premium volume,[18] in large part due to the increased awareness of cyber attacks brought on by numerous high profile data breaches and the higher level of cyber regulation which has been enacted in this country. The remaining 20% is spread between Europe and Asia.[19]

European demand for cyber coverage is expected to rise with the coming implementation of Europe's new framework for data protection laws, the General Data Protection Regulation (GDPR) in May 2018. This new data privacy regulation is intended to provide greater protections to individuals by establishing 1) new rights for people to access the personal information that businesses have on them, 2) obligations for improved data management by

---

[14] "Cyber Insurance 101: The Basics of Cyber Coverage", Lauri Floresca, Woodruff Sawyer Insights, June 19, 2014.
[15] "Cyber Insurance: Considerations for Businesses", Teri Cotton Santos, Risk and Insurance Management Society, Inc., 2017 https://www.rims.org/RiskKnowledge/RISKKnowledgeDocs/2017-Cyber-Ins-Considerations-for-Business_3212017_14345.pdf.
[16] https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.82
[17] "A.M. Best Special Report: U.S Cyber Insurance Market Topped $1 Billion in 2016; More Writers Move to Standalone Policies", A.M. Best, June 26, 2017, Retrieved from http://www3.ambest.com/ambv/bestnews/presscontent.aspx?refnum=25414&altsrc=9.
[18] "Cyber Insurance Market Outlook", Miriam Wilbert and Benno Kroger, Munich RE, Jan. 19, 2018, Retrieved from https://www.munichre.com/topics-online/en/2018/01/cyber-insurance.
[19] *Id.*

businesses, and 3) a new structure of fines for noncompliance.[20] Similar to what the wave of new cyber regulations that spread across the U.S did to drive some of the increased activity in the domestic cyber insurance market, it is anticipated that the GDPR will incite more businesses in Europe to look toward the risk transfer mechanism and cyber policies to protect them from some of these exposures.

In addition to the increase in cyber regulation and the constant media coverage of one major data breach after another, there are other factors which may further drive the demand for cyber insurance. There is a continuing shift in attitude among corporate decision makers toward cyber insurance and its place within the overall risk management program. Whereas cyber insurance was previously considered to be unnecessary, it is being increasingly viewed as a valuable component in a comprehensive risk management program, to work in conjunction with an entity's security software, employee data management training and practices, and event response to manage cyber risks. In addition, a growing number of companies are contractually requiring their business partners to secure cyber insurance. For example, an increasing number of clients predominately from the financial and health care sectors are requiring their law firms to purchase certain minimum limits of cyber insurance.[21]

B. Top Cyber Insurance Writers

While the number of insurers offering cyber products has increased substantially in recent years to over 130, the market is dominated by a small number of insurers. In 2016, the top three insurers of cyber coverage held a combined market share of over 40%, with the top 15 accounting for approximately 83% of the market.[22]

The following are the top 10 writers of cyber insurance based on written premium as of 2016:[23]

1. American International Group
2. XL Group
3. Chubb
4. Travelers
5. Beazley
6. CNA
7. Liberty Mutual
8. BCS Insurance
9. AXIS Insurance Group
10. Allied World

---

[20] "What is GDPR? The Summary Guide to GDPR Compliance in the UK", Matt Burgess, Wired, May 8, 2018 Retrieved from http://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018

[21] "Protecting Firm Assets with Cyber Liability Insurance", Eileen Garczynski, Business Law Today, Sept. 5, 2016, Retrieved from https://www.americanbar.org/publications/blt/2016/09/05_garczynski.html

[22] "Cyber Insurance Premium Volume Grew 35% to $1.3 Billion in 2016", Insurance Journal, June 23, 2017, Retrieved from https://www.insurancejournal.com/news/national/2017/06/23/455508.htm

[23] *Id.*

C. Challenges Facing Insurers and Policyholders

A Fitch Ratings report in 2017 cited the following challenges that insurers and policyholders face:[24]

- **Limited historical data** creates difficulty in pricing cyber coverage.
  Insurers rely on credible actuarial data when developing pricing for their products. The difficulty they face regarding cyber-related loss data and predictive modeling is that the underlying exposure keeps changing. As cyber security evolves, so do the methods and targets of hackers. It is difficult to develop meaningful loss projections for future cyber risks, some of which may not even be contemplated today.[25] As such, rates remain variable, and at times appear to be based more on market competition rather than being actuarially derived.[26]

- **The nature of cyber-risk and the wide variety of potential cyber events** add to challenges in quantifying risk aggregations and catastrophe loss potential.

- **Insurers that lack cyber-underwriting expertise**, poorly manage their risk accumulations, or fail to recognize loss potential from "silent" cyber-exposure in their traditional commercial insurance products could face pressure on earnings, capital, or even ratings, if large loss scenarios emerge as the market expands.

- **Unduly large cyber-risk aggregations** of specific insurers may not become evident until after a large or catastrophic cyber-event.

- **A lack of standardized policy language** and terms can also lead to meaningful differences in individual insurers' product offerings, which is a source of confusion and uncertainty for policyholders.

An example of the lack of policy standardization comes from a review of policy forms from three of the top ten cyber insurance writers. Policy A contains 41 defined terms, while policies B and C contain 59 and 53 defined terms, respectively. Of these defined terms, only seven are common to all three coverage forms, and they are the generic terms that do not have

---

[24] "Cyber Insurance – Risks and Opportunities (Globaln Non-Life Insurer Underwriting Exposures Examined", Fitch Ratings, Sept. 27, 2017.

[25] "the Evolving Cyber Insurance Market: How IT Companies, Financial Institutions, and Other Nontraditional Players Can Offer Cyber Insurance Coverage to Their Customers", Robert M. Fettman, Hogan Lovells Publications, Nov. 14, 2017, Retrieved from http://www.hoganlovells.com/en/publications/how-it-companies-financial-institutions-and-other-nontraditional-players-can-offer-cyber-insurance-coverage-to-their-customers.

[26] "The Need Is Not Standard. Can the Product Become So?", Joseph S. Harrington, The Rough Notes Company, Inc., Oct. 26, 2017, Retrieved from http://roughnotes.com/can-cyber-insurance-standardized/.

anything material to do with the cyber coverage being provided: Application, Claim, Insured, Loss, Policy Period, Pollutants and Subsidiary.

Another example of the inconsistent language among cyber policy forms can be seen in how each of the three policies referenced above define "computer virus".

Policy A refers to computer virus as a malicious code under its "security failure" definition:

> *"**Security Failure**" means the following occurring on or after the Retroactive Date and prior to the end of the Policy Period:*
> *(1) A failure or violation of the security of a Computer System including, without limitation, that which results in or fails to mitigate any unauthorized access, unauthorized use, denial of service attack, or receipt or transmission of a malicious code;*
> *(2) Failure to disclose an event referenced in Sub-paragraphs (1) above in violation of any Security Breach Notice Law*
> *"Security Failure" includes any such failure or violation, resulting from the theft of a password or access code from an insured's premises, the Computer System, or an officer, director or employee of a Company by non-electronic means.*

Policy B also refers to computer virus as a malicious code, but under its "computer virus" definition, which is referenced under the "computer violation" definition, which in turn appears under the "computer system disruption" definition:

> ***Computer System Disruption** means the actual and measurable interruption, suspension or failure of a Computer System resulting directly from:*
> *1. A Computer Violation; or*
> *2. An intentional attack of a Computer System with protocols or instructions transmitted over the internet or another computer communication network, which triggers the use of a Computer System's resources to the extent that the capacity of those resources to accommodate authorized users of such Computer System is depleted or diminished,*
> *Provided that the Insured Organization is the specific target of such Computer Violation or intentional attack.*
>
> ***Computer Violation** means:*
> *1. The introduction of a Computer Virus into a Computer System; or*
> *2. Damage to, or destruction of, computer programs, software or other electronic data stored within a Computer System by a natural person, including an Employee, who has (a) gained unauthorized access to a Computer System, or (b) authorized access to a*

Computer System but uses such access to cause such damage or destruction.

Computer Virus *means any malicious code which could destroy, alter, contaminate, or degrade the integrity, quality, or performance of:*

1. *Electronic data used, or stored, in any computer system or network; or*
2. *A computer network, any computer application software, or a computer operating system or related network.*

Policy C refers to it as unauthorized data under its "cyber-attack" definition:

Cyber-attack *means the transmission of fraudulent or unauthorized Data that is designed to modify, alter, damage, destroy, delete, record or transmit information within a System without authorization, including Data that is self-replicating or self-propagating and is designed to contaminate other computer programs or legitimate computer Data, consume computer resources or in some fashion usurp the normal operation of a System.*

C. Increased Use of Exclusions

Certain elements of a cyber-related claim may be found under various policies falling under other lines, such as crime, property, commercial general liability or lawyers professional liability. However, industry experts predict that more insurers will be utilizing cyber exclusions to carve out any possible coverage from their more traditional policy forms,[27] thereby pushing the coverage on to specific cyber endorsements or stand-alone policies.

D. Continued Migration toward Stand-Alone Cyber Policies

According to a joint PartnerRe and Advisen Cyber Insurance Market Trends 2017 Survey,[28] the market is seeing a clear shift from cyber insurance endorsements to stand-alone policies, which is expected to continue. Survey respondents indicated that cyber insurance endorsements may be a good way to introduce the coverage to the new buyer, however since they tend to have more restrictive coverage and insufficient limits, they are not seen as an appropriate long-term solution.

E. More First-Party Coverage Being Purchased

[27] "A Guide to Cyber Risk", Allianz Global Corporate & Specialty, Sept, 2015, pg. 21, Retrieved from http://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf.

[28] "2017 Survey of Cyber Insurance Market Trends", PartnerRe, Oct. 2017, Retrieved from https://partnerre.com/wp-content/uploads/2017/10/PartnerRe-2017-Survey-of-Cyber-Insurance-Market-Trends.pdf.

An increasing number of cyber insurance buyers have been expanding their coverage appetite to include more first-party coverages, and this trend is expected to continue. More policies for small to mid-sized accounts are including coverage for business interruption and dependent business interruption, along with the other cost reimbursement type first-party coverages.[29] Some of the key concerns driving this demand are the loss of income due to a computer system shutdown, potential loss of future business, public relations services needed to repair any reputation damage, internal and social engineering risks, and cyber extortion.[30]

F. Continued Lack of Standardization

Among the more traditional lines of insurance such as CGL, Property, and Workers Compensation, there is a fair amount of standardization among the court tested insuring agreements, exclusions and defined terms found within the coverage forms and endorsements, especially among those insurers who use standard Insurance Services Office, Inc. (ISO) and National Council on Compensation Insurance (NCCI) forms as their base. For example, there is a reasonable expectation that the defined term "products-completed operations hazard" will have a very similar meaning across most CGL policies, that loss or damage caused by wear and tear will be excluded under commercial property policies, and workers compensation policies, though established by state statutes, will pay for the medical costs associated with an employee's work-related injuries and illnesses. The same cannot be said of the language and terms for cyber insurance, and many industry experts feel that standardization is still a ways off.

The insurance marketplace has seen new types of losses emerge before, such as those related to toxic mold and silica which surged during the early 2000's. However, once these types of losses appeared, it did not take long for the marketplace, aided by consistent court rulings, to define these exposures and formulate amended policy language to reinforce their coverage stance. For cyber related claims, court rulings, like the variation in policy language, are all over the map.

Cyber insurance buyers may be applying some pressure on the market to standardize the general types of cyber and data breach coverages being offered, however what is absent is a strong push to standardize the policy language, which varies greatly. The general coverage intent amongst the large cyber writers may be becoming more similar, however inconsistencies in policy language could reveal stark differences as to what is covered and excluded. This is in large part due to the evolving nature of cyber risks. In order to keep up with a constantly expanding cyber environment, policy language will need to continue to evolve as well. Early cyber policies were drafted to address the specific needs of a very different environment, one which was not comprised of the technological advances being utilized and pioneered today. As such, cyber writers, for the foreseeable future, are expected to continue to utilize proprietary forms which they can amend as the need arises, as opposed to relying on industry standard forms.

---

[29] "The Need Is Not Standard. Can the Product Become So?", Joseph S. Harrington, The Rough Notes Company, Inc., Oct. 26, 2017, Retrieved from http://roughnotes.com/can-cyber-insurance-standardized/.
[30] *Id.*

VI. ISO Cyber Program and CGL Amendments

Insurance Services Office, Inc. (ISO), an advisory and rating organization servicing the property and casualty insurance industry, provides services including advisory loss costs, manual rules and policy forms to its participating insurers. Many insurers elect to use ISO industry standard policy forms in their entirety for the traditional lines of insurance, or utilize them as a benchmark when developing proprietary forms.

Since 2001, as part of an effort to clarify coverage intent regarding cyber-related exposures, ISO made several important amendments to their Commercial General Liability (CGL) policy forms in order to exclude cyber-related coverage:

- 2001: Changes to the CGL Coverage Form:
    - Amended the definition of "property damage" to clarify that "electronic data is not tangible property." The amendment went further to state that "electronic data means information, facts or programs stored as or on, created or used on, or transmitted to or from computer software, including systems and applications software, hard or floppy disks, CD-ROMs, tapes, drives, cells, data processing devices or any other media which are used with electronically controlled equipment."
    - Added three exclusions affecting internet related coverage under Coverage B - Personal and Advertising Injury Liability:

        Exclusion j. Insureds in Media and Internet Type Businesses
        Exclusion k. Electronic Chatrooms or Bulletin Boards
        Exclusion l. Unauthorized Use of Another's Name or Product

- 2004: Added exclusion p. Electronic Data under Coverage A – Bodily Injury and Property Damage to complement the 2001 changes. This exclusion broadly excludes coverage for "damages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data."

Leading up to 2014, ISO determined that damages arising from so-called data breach liability (unauthorized publication of private information) are not contemplated within the coverages and rate structure afforded by the CGL coverage form. Furthermore, first-party expenses stemming from a data breach (notification costs, forensic expert costs, fines and penalties, public relations costs, etc.) also fall outside the scope of coverage. As such, ISO

introduced several mandatory and optional exclusionary endorsements which build upon the Electronic Data exclusion.[31]

- **CG 2106 0514** – Exclusion – Access or Disclosure of Confidential or Personal Information and Data-Related Liability – With Limited Bodily Injury Exception

- **CG 2107 0514** – Exclusion – Access or Disclosure of Confidential or Personal Information and Data-Related Liability – With Limited Bodily Injury Exception Not Included

- **CG 2108 0514** – Exclusion – Access or Disclosure of Confidential or Personal Information (Coverage B Only)

It is essential to be familiar with these changes because not all jurisdictions and insurers implement these amendments at the same time. While some insurers have adopted the most recent CGL policy form and exclusionary endorsements, thus carving out these exposures from their coverage intent, others have not, and therefore may be providing "silent", unintentional cyber-related coverage.

Since 2005, in order to address first and third-party cyber/data breach exposures of commercial enterprises, ISO developed three cyber insurance programs for their member insurers to use. Each program is designed for a specific market segment based on a commercial entity's size.

- **Information Security Protection Endorsement – Businessowners Program**
  Small businesses, insuring agreements are offered in three tiers, aggregate limit up to $100,000

- **Commercial Cyber Insurance Policy**
  Small to medium sized businesses, aggregate limit up to $1 million.

- **Information Security Policy**
  Large commercial entities, government and nonprofit organizations, financial services and media companies, aggregate limit up to $50 million

The programs offer similar insuring agreements and are subject to nearly identical exclusions. Third-party coverages are written on a claims-made basis, and defense expenses reduce the policy aggregate.

[31] "Cyber Loss Exposures – No Longer Breaching the CGL", Paul W. Burkett, Insurance & Risk Management Knowledge Alliance, June 18, 2015, Retrieved from https://irmka.scic.com/2015/06/18/cyber-loss-exposures/.

A. ISO Cyber Insuring Agreements[32]

First-Party Coverages

- **Security Breach Expense**
  Expenses incurred to establish whether a security breach has occurred; investigate the cause and scope of a security breach; notify parties affected by a security breach, including overtime salaries paid to staff; cover fees and costs of the insured hiring a company to operate a call center; and reimburse the insured for post-event credit-monitoring costs for victims of the breach

- **Replacement or Restoration of Electronic Data**
  Expenses incurred to replace or restore electronic data or computer programs affected directly by a virus

- **Business Income and Extra Expense**
  Actual loss of business income and/or extra expenses incurred because of the interruption of the insured's e-commerce activities resulting directly from a virus or extortion threat

- **Extortion Threats**
  Ransom payments and other expenses incurred resulting directly from threats to send a virus to a computer system; disseminate the insured's proprietary information; inflict ransomware or other types of viruses to destroy, corrupt, or prevent normal access to the computer system; or publish clients' personal information

- **Public Relations Expense**
  Expenses incurred to restore the insured's reputation after being subject to negative publicity resulting directly from a virus or security breach

Third-Party Coverages

- **Website Publishing Liability**
  Liability arising from an infringement of another's copyright, title, slogan, trademark, trade name, trade dress, service mark, or service name; defamation against a person or organization; or violation of a person's right to privacy

- **Programming Errors and Omissions Liability**

---

[32] "ISO's Cyber Insurance Program", ISO Cyber Risk Solutions, July 2016, Retrieved from https://www.verisk.com/siteassets/media/downloads/iso-cyber-insurance-program.pdf.

Liability arising from programming errors or omissions that ultimately disclose clients' personal information held within the computer system

- **Security Breach Liability**
  Liability arising from the unauthorized disclosure of client's personal information held within a computer system or in nonelectronic format; transmission of a virus to a third party by e-mail or other means

B. ISO Cyber Policy Exclusions

- Lightning, earthquake, hail, or any other acts of nature
- War
- Dispersal of biological or chemical materials, nuclear reaction or radiation
- Bodily injury or physical damage of tangible property, including loss of use
- Any indeterminable failure, malfunction or slowdown of a computer system, or inability to access or manipulate electronic data
- Any disruption in normal computer function due to insufficient capacity to process transactions
- Any disruption of internet service or external telecommunication network
- Any failure, reduction or surge of power
- Any violation of the Racketeer Influenced and Corrupt Organizations Act (RICO), or similar provisions of any federal, state or local law
- Any failure of any satellite
- Any oral or written publication of material, if done by an insured or at an insured's direction with knowledge of its falsity
- Liability assumed by contract or agreement
- Any patent or trade secret violation
- Pollution
- Any claim or suit which was pending or existed prior to the policy period
- Any actions related to the insured's practices as an employer, including refusal to employ, termination, demotion, etc.
- Any cyber incident, extortion threat, security breach or wrongful act that any insured became aware of prior to the policy effective date
- Any cyber incident, extortion threat, security breach or wrongful act which was reported under any policy of which this policy is a replacement
- Any criminal, dishonest, malicious or fraudulent acts committed by an insured, except for dishonest, malicious or fraudulent acts committed by an employee which give rise to a claim under the Security Breach Expense and Security Breach Liability insuring agreements
- Any action brought by any governmental authority or regulatory agency, except when covered under the Security Breach Liability insuring agreement
- Any costs associated with upgrading a computer system, regardless of the reason
- Any claim brought by one insured against another

- Contract fines, penalties or assessments, including Payment Card Industry (PCI) fines, penalties or assessments

The ISO cyber programs provide member insurers access to standardized policy forms for a growing and critical market. These programs may facilitate take-up rates, especially among the lower exposure, smaller commercial first-time cyber insurance buyers. However, for entities with a higher level of cyber exposure, such as law firms, a more robust policy form from one of the larger cyber writers may be more appropriate. Large cyber writers may be more inclined to negotiate policy terms based on the commercial entity's cyber risk profile, and their policies tend to have broader insuring agreements, less ambiguous definitions, and higher limits. Some of these policies, like Chubb's cyber policy which was recently endorsed by the American Bar Association, are specifically designed to work in conjunction with the Lawyers Professional Liability policy.