

Understanding Cyber Insurance: Why Arbitration May Make Sense for your Policy

Daniel B. Garrie, Esq., Co-Founder, Law & Forensics, Mediator, Arbitrator, and e-Discovery Special Master, JAMS

Kevin Szczepanski, Partner & Cybersecurity Team Co-Leader, Barclay Damon LLP

Joshua Mooney, Partner, Kennedys Law

Andrew Nadolna, Arbitrator and Mediator, JAMS

(c) 2022 Lexeprint Inc. All Rights Reserved.

Speakers



Daniel B. Garrie, Esq.
Co-Founder, Law & Forensics
Mediator, Arbitrator, and Special Master, JAMS



Kevin Szczepanski
Partner & Cybersecurity Team Co-Leader
Barclay Damon LLP



Joshua Mooney
Partner
Kennedys Law



Andrew Nadolna
Arbitrator and Mediator
JAMS

(c) 2022 Lexeprint Inc. All Rights Reserved.

Disclaimer



This is not legal advice, nor should it be considered legal advice.



This presentation and the comments contained therein represent only the personal views of the participants, and do not reflect those of their employers or clients.



This presentation is offered for educational and informational uses only.

(c) 2022 Lexeprint Inc. All Rights Reserved.

Agenda

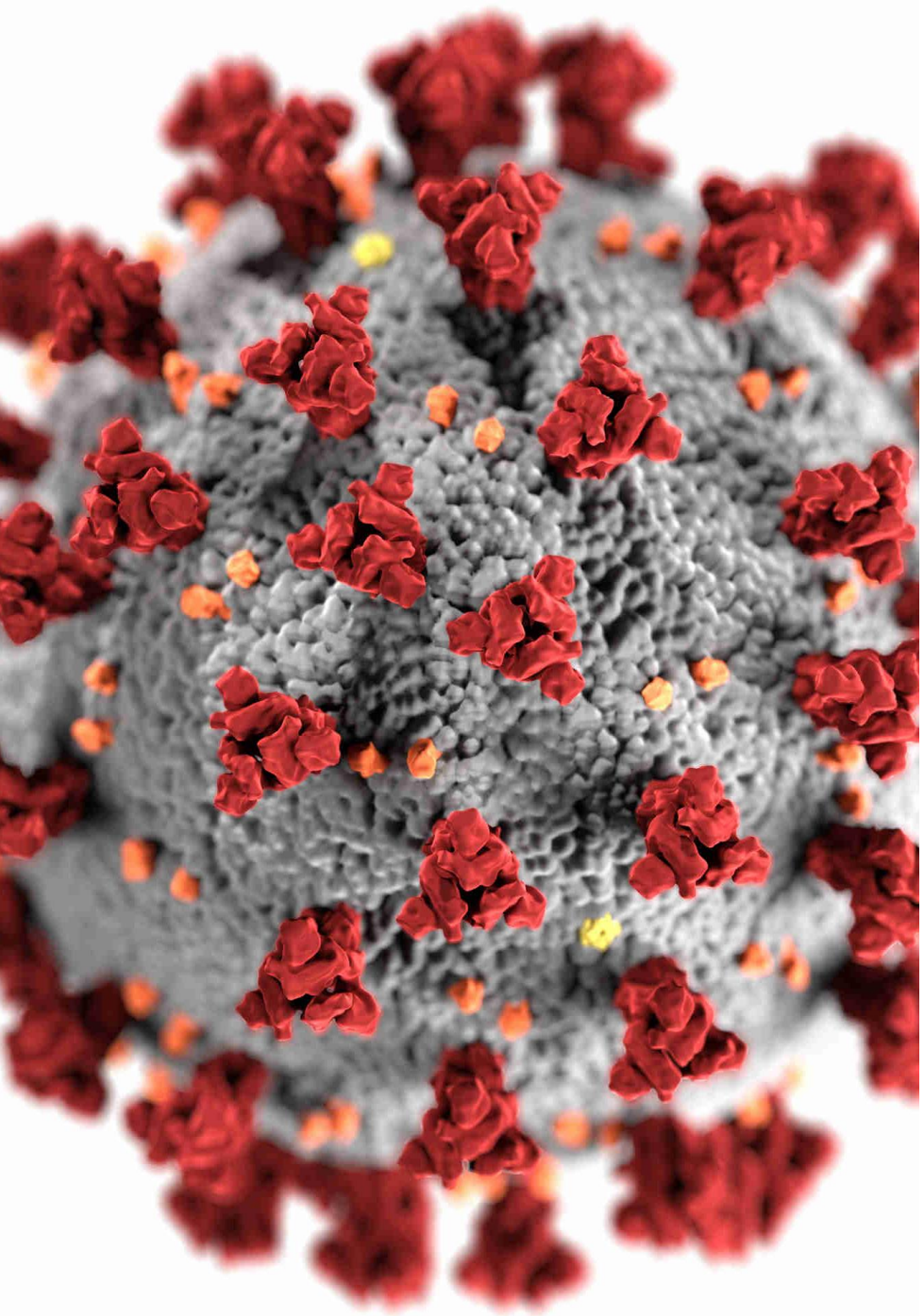
- The Growing Need for Cyber Insurance
- Cyber Insurance Overview
- Types of Insurance Policies
- Arbitration Overview
- Why is Arbitration Better than Litigation in Resolving Cyber Disputes?
- Attorneys' 4 Tips to Cyber Insurance

(c) 2022 Lexeprint Inc. All Rights Reserved.



The Growing Need for Cyber Insurance

(c) 2 int Nig d.



COVID-19 Increased the Need for Cyber Insurance

- The ongoing COVID-19 pandemic has resulted in an increased interest and demand to secure cyber liability insurance coverage.
- As more people continue to work from home, there has been an increased volume of phishing, ransomware or other social engineering scams.
- Additionally, businesses have recognized that cyber-related losses are most likely excluded under the traditional general liability and property policies. As a result, they have started to focus on analyzing potential exposures and cyber risk management.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Increased Demand for Cyber Insurance

- However, as a result of this demand, the cyber insurance market is competitive as they work to offer coverages that meet businesses' needs.
- As insurance carriers gain experience from responding to voluminous cyber claims, they are able to offer guidance on preventing cyber incidents. E.g., Employing technical security practices and internal back-up and recovery policies.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Why is Cyber Insurance Needed?

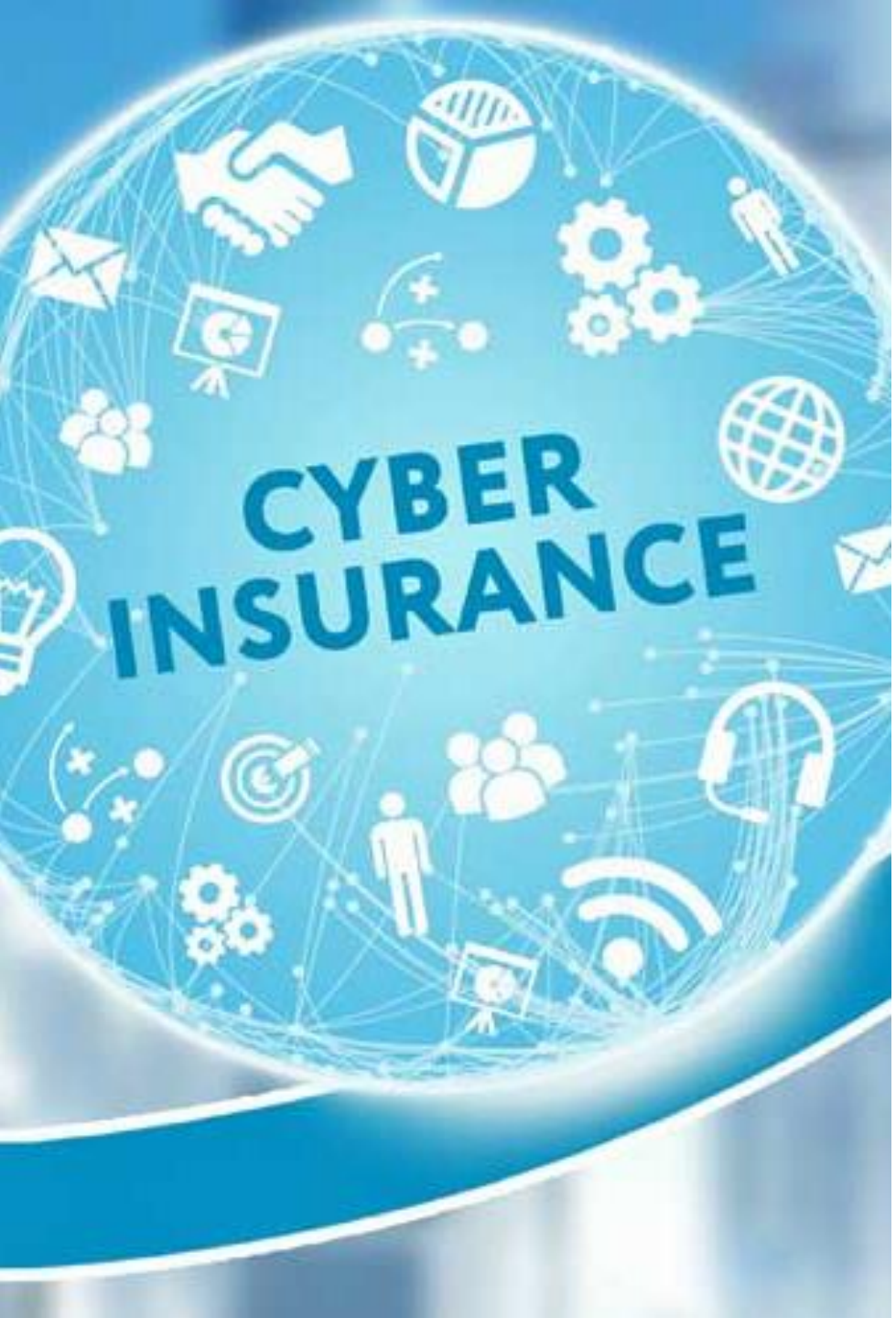
- According to IBM, the average global cost of a data breach is $4.24 million. Data breach costs increased from $3.86 million in 2020.
- A data breach in the U.S. costs a company on average **$8.19 million**, an increase from **$7.91 million** in 2018. This is twice the global average!
- IBM also reported that customer PII was the most common and most expensive type of record lost or stolen in a data breach incident.
- **Data breaches are the costliest in the United States and the Middle East.**

(c) 2022 Lexeprint Inc. All Rights Reserved.



Cyber Insurance Overview

(c) 2022 Lexeprint Inc. All Rights Reserved.



Cyber Insurance in 2022

- Before the COVID-19 pandemic, cyber insurers were tightening their underwriting guidelines. They were asking for more details to better understand the risk that they were insuring.
- Companies looking for cyber insurance this year can expect a more rigorous underwriting process.
- The COVID-19 pandemic has highlighted a few areas of concern as not all cyber insurance policies are created equally. As many employees worked from home, insureds were advised to review the definitions within their cyber policies to ensure that 'work from home' employees on personal computers were covered.

(c) 2022 Lexeprint Inc. All Rights Reserved.

Potential Threats that Cybersecurity Insurance Covers

Threats within an organization may include:	Social engineering
	Lost mobile devices
	Improper handling of PII
	Unintentional disclosure
	Rogue employees
	Coding inaccuracies
	Human error

(c) 2022 Lexeprint Inc. All Rights Reserved.



What is Cyber Insurance?

- Cyber insurance generally covers your business' liability for a data breach, identity theft, personal data theft, or loss of other data involving sensitive customer information.
- Cyber insurance can help you recover from a data breach or identity theft by offsetting costs that pile up in the aftermath of an attack, as well as mitigate your cyber risk.
- Cyber insurance can reimburse for costs associated with business interruptions and extra expenses due to a cyber attack.

(c) 2022 Lexeprint Inc. All Rights Reserved.



What Does Cyber Insurance Cover?

- First-Party and Third-Party risks.
- Respond to “bad actors” both inside and outside the insured corporation.
- Provide cover for fines & penalties (where allowed by law).
- Cover intangible risks – loss and damage to non-physical “property”.
- Costs associated with operational disruptions due to a cyber-attack; including Ransomware attacks.
- Include costs associated with Media/Electronic content liability.

(c) 2022 Lexeprint Inc. All Rights Reserved.

Top Cyber Insurance Providers of 2020 and 2021

CoverWallet

Hiscox

AIG

HSB

Liberty Mutual

XL Catlin

Hackinsure

Chubb

CNA

Beazley

(c) 2022 Lexeprint Inc. All Rights Reserved.



Types of Insurance Policies

(c) 2022 Lexeprint Inc. All Rights Reserved.



Types of Cyber Policies

- Cyber Insurance is split between First Party Coverage and Third-Party Coverage types.
- Policies can either be purchased as a basic endorsement added onto a general liability policy, or they can be purchased as a "stand-alone" policy.

(c) 2022 Lexeprint Inc. All Rights Reserved.



First-Party Coverage

- This will usually cover forensic investigations or remediation.
- Covers costs of determining (but not always eliminating) the cause of loss of data.
- FPC will sometimes, but not always, cover the repair or replacement cost of the lost data.
- Most policies will NOT cover damage to other property/equipment resulting from loss of data or network downtime.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Third-Party Coverage

- Third-Party Coverage covers:

1. Regulatory actions arising from breaches, including:
   - Privacy notification costs;
   - Costs of notifying third parties potentially affected by breach; and
   - Civil litigation including defense costs.
2. Often includes costs of call centers and credit/identity monitoring:
   - Costs of retaining privacy counsel;
   - Payment card industry fines and penalties; and
   - Sometimes, but not always, covered.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Stand-Alone

- A “stand-alone” insurance product is one that is designed to provide insurance protection for a specific risk or cost and afford an insured coverage for a particular concern.
- Stand-alone policies usually provide the broadest coverage.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Endorsements

- Cyber Risk "Endorsements" are insurance policies that may be purchased along with traditional insurance and provide coverage specifically geared toward cyber risks.
- Cyber endorsements are not as comprehensive as a true separate cyber policy, but they are more cost effective.

(c) 2022 Lexeprint Inc. All Rights Reserved.

What to Look for When Advising a Client on Cyber Insurance?

- Policy Type: Is it stand-alone or an extension of existing policy?
- Deductibles: compare.
- Beware of applicability of coverage and potential sub-limits.
- Attack Scope: any attack affecting company or only targeted attacks.
- Attack Vectors: network vs. social engineering.
- Time Frames: APT's and spear phishing take time; is there time period for applicable coverage.
- Consider cross-over with other policies such as crime, K&R and Property; address potential Silent Cyber Issues.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Arbitration Overview

(c)2022 Lexegy, Inc. All rights Reserved.



What is Arbitration?

- Arbitration, a form of alternative dispute resolution (ADR), is a technique for the resolution of disputes outside the courts. The parties in a dispute refer it to arbitration by one or more persons (the "arbitrators", "arbiters" or "arbitral tribunal"), and agree to be bound by the arbitration decision (the "award").
- A third-party reviews the evidence in the case and imposes a decision that is legally binding on both sides and enforceable in the courts.

(c) 2022 Lexeprint Inc. All Rights Reserved.



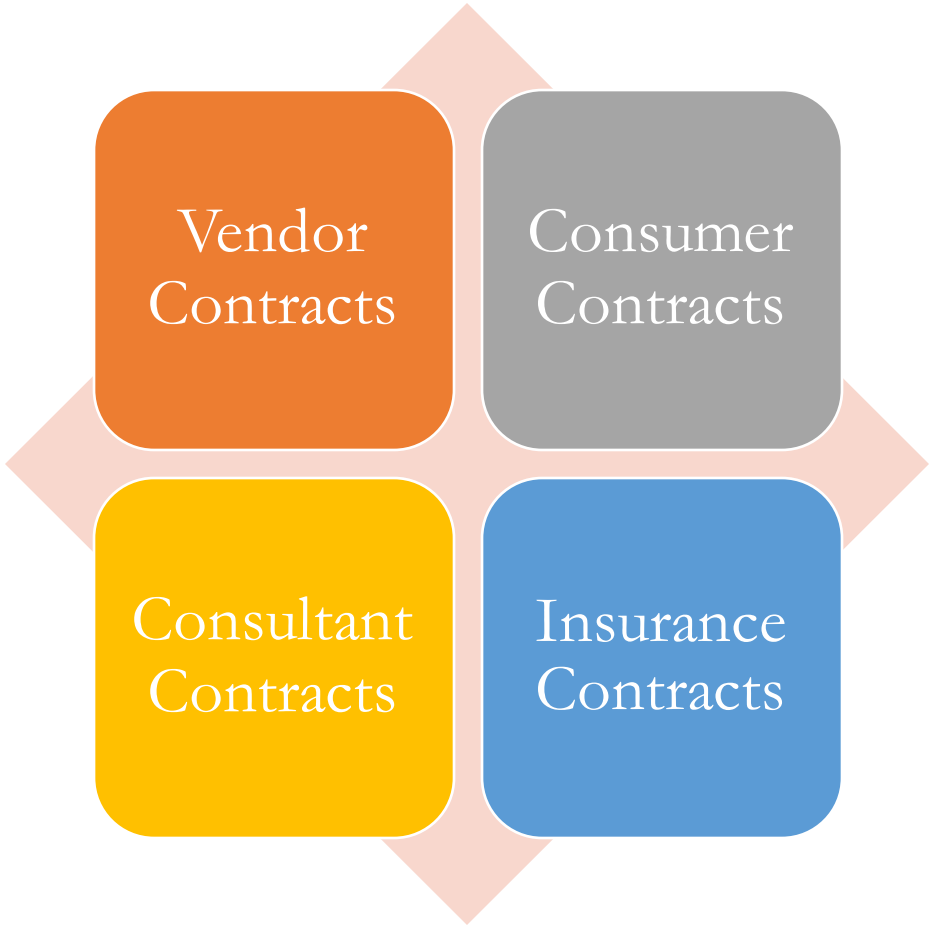
Using Arbitration to Resolve Cyber Issues

- In addition to addressing third-party risks, companies should look for ways to limit the costs of resolving their disputes.
- Litigation can be a costly, time consuming, and unpredictable process.
- Arbitration clauses allow companies to mitigate those costs and risks, by controlling the dispute resolution process.

(c) 2022 Lexeprint Inc. All Rights Reserved.

(c) 2022 Lexeprint Inc. All Rights Reserved.

Arbitration Clauses in Contracts That Might Be Implicated in Data Breach Disputes





Why is Arbitration Better than Litigation in Resolving Cyber Disputes?

(c) 2022 I



Arbitration Over Litigation: Procedural Ease

- In arbitration, a party trades the formal procedures of a courtroom for the simplicity, informality, and expedition of arbitration:
  - [T]he fact finding process in arbitration usually is not equivalent to judicial fact finding. The record of the arbitration proceedings is not as complete; the usual rules of evidence do not apply; and rights and procedures common to civil trials, such as discovery, compulsory process, cross-examination, and testimony under oath, are often severely limited or unavailable. … And as this Court has recognized, '[a]rbitrators have no obligation to the court to give their reasons for an award.'… Indeed**, it is the informality of arbitral procedure that enables it to function as an efficient, inexpensive, and expeditious means for dispute resolution.**
  - *Alexander v. Gardner-Denver Co.,* 415 U.S. 36, 57-58 (1974).

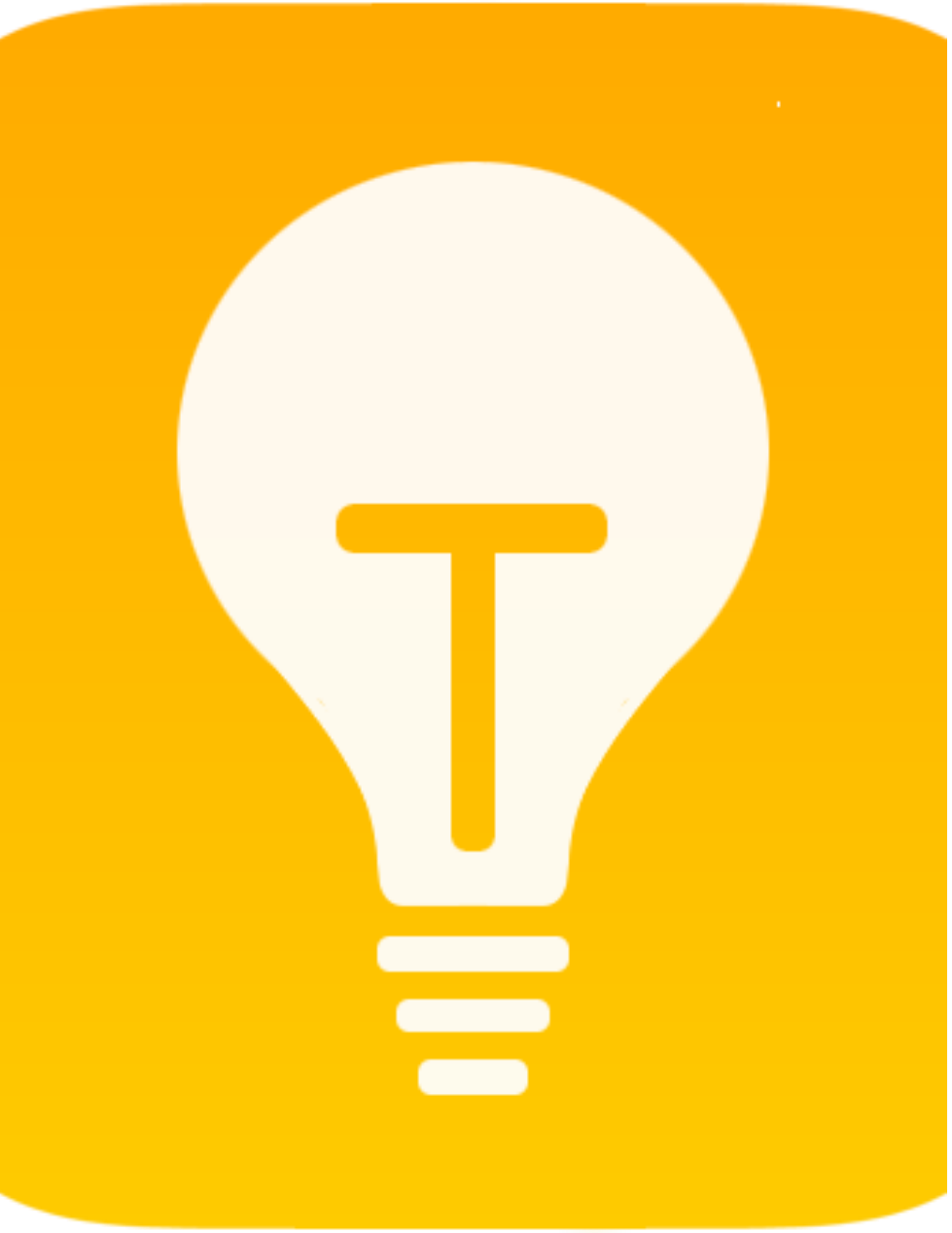
(c) 2022 Lexeprint Inc. All Rights Reserved.



Arbitration Over Litigation: Time, Money & Discovery

- Arbitration can save anywhere from a handful of months to several years.
  - Reducing dispute duration results in huge reductions in legal, discovery, and court fees.
- While parties are free to define the scope of discovery in their agreements, every set of form rules contains a narrower scope of discovery than civil litigation.
- The arbitrator also has increased flexibility and discretion vis-à-vis a federal judge when dealing with discovery disputes.
- Keeping the dispute out of the courtroom allows for reduced media/publicity.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Attorneys' 4 Tips to Cyber Insurance

- If you do not know if you have cyber insurance, chances are, you do not have it.
  - It is essential that you meticulously review your cyber insurance options and not simply lock into whatever an insurance broker is selling as a premium coverage.
- Read the policy in its entirety!
- Exclusions can be cruel.
  - It is important to review your policy to determine what it really covers.
- Do not wait until a breach occurs to negotiate!
  - Better coverage can always be negotiated. You may want to ask for lower retentions and higher sub limits.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Questions?

(c) 2022 Lexeprint Inc. All Rights Reserved.

Contact Us



Daniel B. Garrie
Email: daniel@lawandforensics.com
dgarrie@jamsadr.com
Phone: 855-529-2466
URL: www.lawandforensics.com



Kevin Szczepanski
Email: kszczepanski@barclaydamon.com
URL: https://www.barclaydamon.com/



Joshua Mooney
Email: Joshua.Mooney@kennedyslaw.com
Phone: (267) 479-6706
URL: https://kennedyslaw.com



Andrew Nadolna
Email: anadolna@jamsadr.com
URL: www.jamsadr.com

(c) 2022 Lexeprint Inc. All Rights Reserved.



Daniel B. Garrie, Esq.
Law & Forensics – Co-founder
JAMS – Mediator, Arbitrator, eDiscovery Special Master
Contact:
W: (855) 529-2466
E: daniel@lawandforensics.com
URL: www.lawandforensics.com

LAW & FORENSICS
A Global Legal Engineering Firm

B.A., Computer Science, Brandeis Uni.
M.A., Computer Science Brandies Uni.
J.D., Rutgers School of Law

Daniel Garrie is the Co-Founder of Law & Forensics LLC, Head of Computer Forensics and Cyber Security Practice Groups and has been a dominant voice in the computer forensic and cybersecurity space for over 20 years. Prior to Daniel's legal career, he successfully built and sold several technology start-up companies. Since co-founding Law & Forensics LLC in 2008, Daniel has built it into one of the leading boutique cybersecurity forensic engineering firms in the industry. Daniel has both a Bachelor's and a Master's Degree in computer science from Brandeis University, as well as a J.D. degree from Rutgers Law School. Daniel has led forensic teams in some of the most visible and sensitive cyber incidents in the United States.

Daniel regularly testifies as an e-discovery, cybersecurity and computer forensic expert witness, authoring forensic expert reports on multi-million-dollar disputes. His ability to perform complex investigations and effectively communicate the results to a jury has made him one of the most sought-after experts in the country. His testimony has been pivotal in a number of cases. Since 2008, Daniel has served as a Neutral and Special Master and in 2016, he joined JAMS as one of the organization's youngest Neutrals. At JAMS, Daniel serves as an Arbitrator, Forensic Neutral, and technical Special Master with a focus on cybersecurity, cyrptocurrency, and complex software and technology related disputes.

Daniel is well-published in the cybersecurity space, Editor-in-Chief of the Journal of Law & Cyberwarfare, author of more than 200 articles and books including, "Understanding Software, the Internet, Mobile Computing, and the Cloud. A guide for Judges", published by the Federal Judicial Center. He has been recognized by several United States Supreme Court Justices for his legal scholarship and is a trusted source and a thought leader for cybersecurity articles and opinions, being cited over 500 times to date.

© 2022 Lexeprint Inc. All Rights Reserved.



Kevin Szczepanski
Partner & Cybersecurity Team Co-Leader – Barclay Damon LLP

Contact:
E: kszczepanski@barclaydamon.com
URL: https://www.barclaydamon.com/

BARCLAY DAMON LLP

A trial and appellate lawyer who primarily concentrates his practice on insurance-coverage litigation and cyber risks, Kevin has extensive experience litigating directors and officers (D&O), errors and omissions (E&O), and property and casualty (P&C) coverage under both primary and excess policies. He has served as both lead settlement and trial counsel in highly sensitive business and coverage disputes. He also advises clients on insurance-policy drafting and underwriting issues.
As co-leader of the Cybersecurity Team, Kevin represents businesses facing first- and third-party losses due to data breaches, service interruptions, theft, and other cyber threats. He also counsels clients on contract drafting and coverage for cyber risks and represents them in liability and coverage disputes.

(c) Law and Forensics 2016. All Rights Reserved



Joshua Mooney
Kennedys Law – Partner
Contact:
E: Joshua.Mooney@kennedyslaw.com
W: (267) 479-6706
URL: https://kennedyslaw.com

Kennedys

Josh is the firm's head for US Cyber and Data Privacy and is based in Philadelphia.

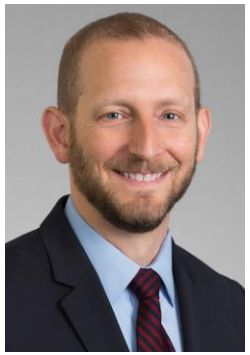
Josh advises clients on a wide array of data privacy and security, including breach response, compliance under such laws as CCPA, HIPAA, New York's DFS Cyber Regulation and the SHIELD Act, and BIPA, and big data usage and licensing. Josh also advises on cross-border data transfers and implementation of privacy and security protocols.

In addition, Josh represents insurers in media and cyber liability coverage matters. He has litigated at trial and appellate levels throughout the country, winning two cases involving matters of first impression before the United States Court of Appeals for the Third Circuit, and litigating one of the first cyber coverage matters in the Commonwealth of Pennsylvania.

Josh is an integral part of Kennedys global 24/7 breach response services and data privacy services, coordinating responses in North America and managing notification requirements worldwide. Josh also is a key member of Kennedys global privacy services.

Josh regularly writes and lectures on cybersecurity and data privacy and coverage issues. He has guest-lectured on cyber law and insurance at Temple University Fox School of Business and Rutgers Law School, and has been quoted in The Wall Street Journal, S&P Global Market Intelligence, Law360, Business Insurance, Claims Journal, and Compliance Week. He also served as an editor for a working group of X9, an ANSI-accredited standards developing organization, to develop a universal standard for data protection and data breach notification in the financial services industry.

Currently, Josh is a former Vice Chair of the ABA TIPS Cybersecurity and Data Privacy Committee, and is the founding Chair and current Co-Chair of the Cybersecurity and Data Privacy Committee for the Pennsylvania Bar Association. He is also a founding member of The Oxford & Cambridge Society of Philadelphia, and has been selected by Cambridge in America and the University of Cambridge as an official alumnus contact for the Commonwealth of Pennsylvania.



Andrew Nadolna
JAMS – Arbitrator and Mediator

Contact:
E: anadolna@jamsadr.com
URL: www.jamsadr.com

Andrew S. Nadolna, Esq. comes to JAMS with 25 years of experience in the insurance industry as a claims executive and litigator. Mr. Nadolna brings a unique perspective of settlement to JAMS. He is a luminary in the insurance industry and Bar and brings a pragmatism to settling complex cases, particularly where coverage is at the heart of the dispute.

Mr. Nadolna spent 17 years in leadership positions at AIG, including most recently 5 years as Global Head of Casualty Claims for AIG Property Casualty where he was responsible for an organization of 1800 people that paid roughly $9B per year in claims throughout the U.S., Canada, the U.K. and continental Europe, Australia, Singapore, and Hong Kong. His oversight at AIG included hundreds of thousands of claims worldwide involving general liability (including umbrella and excess at all layers), pollution, mass tort, medical malpractice, personal and advertising injury, and construction defect, as well as workers compensation, Defense Base Act, employers' liability, and commercial auto.

Mr. Nadolna has significant experience with nearly every form of insurance claim under almost every form of liability policy including primary and excess policies (all layers), occurrence, claims made, integrated occurrence, occurrence reported, Bermuda and London forms, fronted deductible, and other complex risk transfer arrangements. He has settled cases himself with a wide range of people from severely injured plaintiffs to risk managers and general counsels of Fortune 100 companies. Mr. Nadolna's broad experience allows him to understand the varying perspectives of the parties, providing an environment conducive to settlement. He is keenly aware of the risks of litigation and his expertise offers both plaintiffs and defense a distinctive perspective on resolving some of the most complex matters.

As a litigator, Mr. Nadolna focused on insurance coverage analysis and litigation involving issues of coverage for Superfund sites, toxic torts, construction defect, errors and omissions, and intellectual property. He also defended attorney malpractice, product liability, and general and auto liability cases.A sought after speaker on complex insurance topics, Mr. Nadolna has participated in speaking engagements for several organizations including ARIAS-U.S., ABA, DRI, IADC, RIMS, the Advisen Casualty Insights Conference, and others.

(c) Law and Forensics 2016. All Rights Reserved

DATA BREACHES (/BLOG/SEARCH/DATA-BREACHES)

How Much Does a Data Breach Cost in 2021?

by Chris Brook (https://digitalguardian.com/author/chris-brook) on Wednesday August 4, 2021

The cost of data breaches continues to rise; according to this annual report, the global shift to remote work is partly to blame.

When all is said and done - after the incident response, after the forensic analysis, after the victims have been notified – how much does a data breach truly cost in in 2021?

If the numbers in IBM's annual **Cost of a Data Breach Report (https://www.ibm.com/security/data-breach)** are to be believed, the figure
ıt up over the last 12 months, an increase that's largely being attributed to
COVID-19 pandemic's effect on organizations and their ability to respond to
a breaches.

year's final total - $4.24 million per incident on average - is actually the
ıest figure since the report, which is carried out annually by the Ponemon
itute and sponsored by IBM, originated 14 years ago. The number is a 10
percent increase over **last year's (https://digitalguardian.com/blog/what**

percent increase over last year's (https://digitalguardian.com/blog/what-does-data-breach-cost-2020) total, $3.86 million per incident on average.

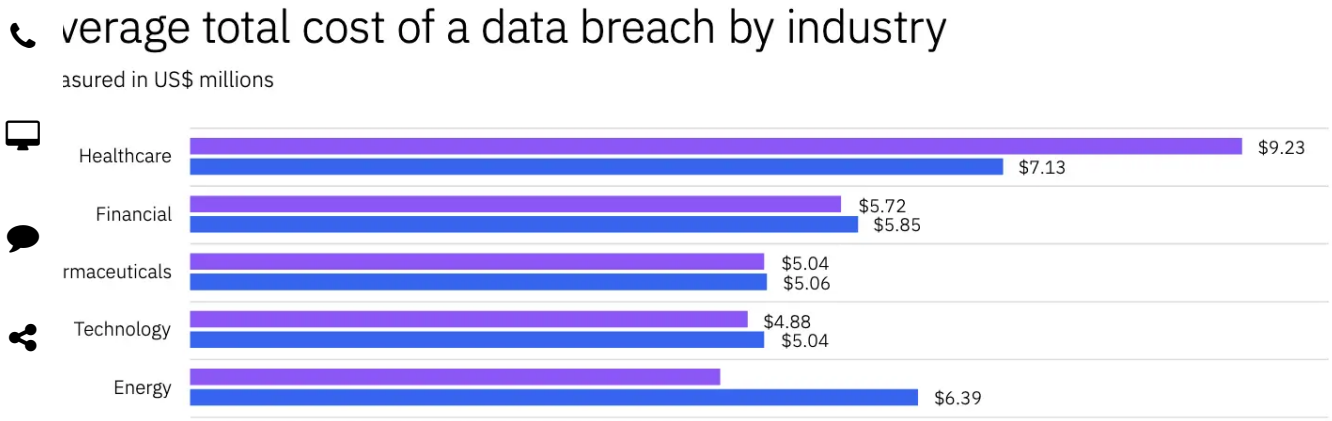
One of the report's clearest takeaways is that COVID-19 and the shift by many companies worldwide to a distributed workforce had a direct effect on the cost of a data breach. The report looked at breaches at 537 organizations from May 2020 to March 2021 and found that those that acknowledged that remote work was a factor in their breach suffered a higher loss ($4.96 million) compared to those who didn't ($3.89 million) – a 15 percent difference.

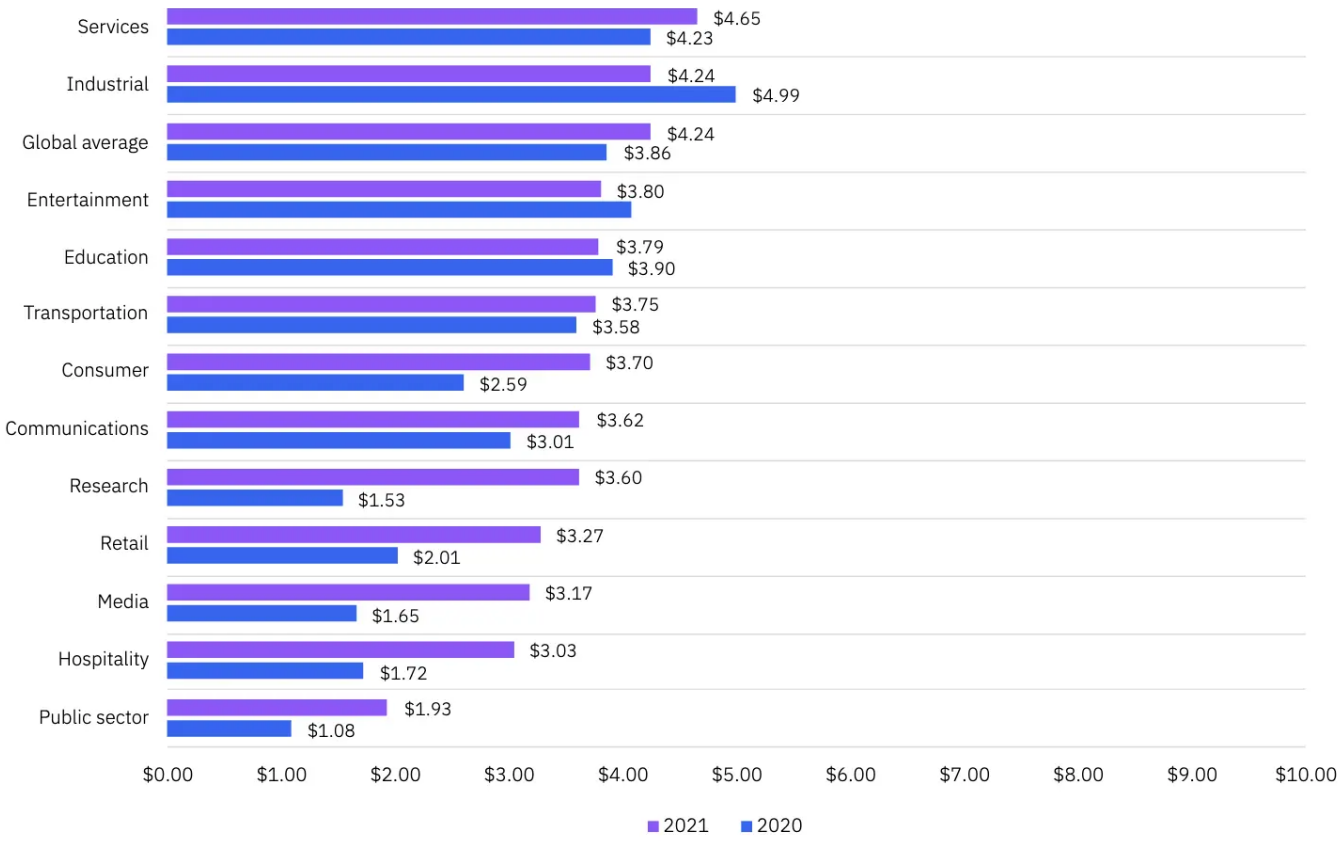
Of course that $4.24 million figure is an average; the actual figure for companies depended on a series of variables. Were there compliance failure? Was ransomware the culprit? Where was the company located? What industry did the company operate in?

For many of these questions, the story remains the same.

Healthcare organizations continued to be the costliest industry to recover from a data breach. $9.23 million on average, more than double the cost on average of a data breach this past year. The total is a more than $2 million costlier than a healthcare data breach last year suggesting things have gotten worse at hospitals and healthcare facilities, many which were hit by ransomware, especially last fall.

Figure 4





Speaking of ransomware, it should not be a huge surprise that ransomware breaches again were more expensive than other types of breaches. Those types of attacks cost businesses between $4.62 and $4.69 million on average, with much of the sum likely attributed to downtime, lost business, and the costs accrued by having to rebuild systems from backups if not from scratch entirely.

Lost business, according to the report, accounts for 38 percent of a data breach's total cost, roughly $1.59 million. Detecting the breach in the first place runs companies around $1.24 million while responding to the breach after its happen costs around $1.14 million.

last year, most breaches (44%) involved sensitive customer personally
ıtifiable information, or PII. What's notable is that this figure is actually a big
ɔ from last year in which a whopping 80% of breaches included customer
Anonymized customer data and intellectual property were the second and
d most common type of record breached last year.

Figure 6

Types of records compromised

Percentage of breaches involving data in each category

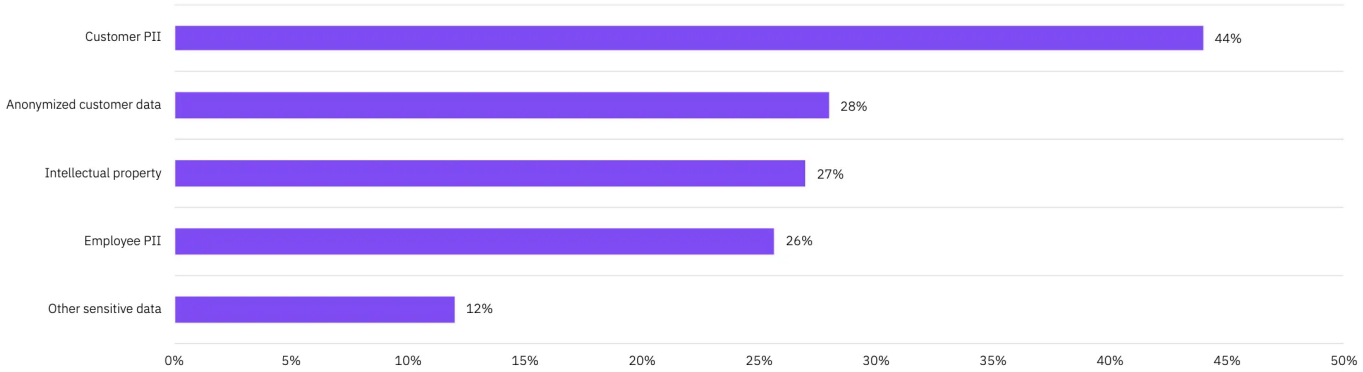
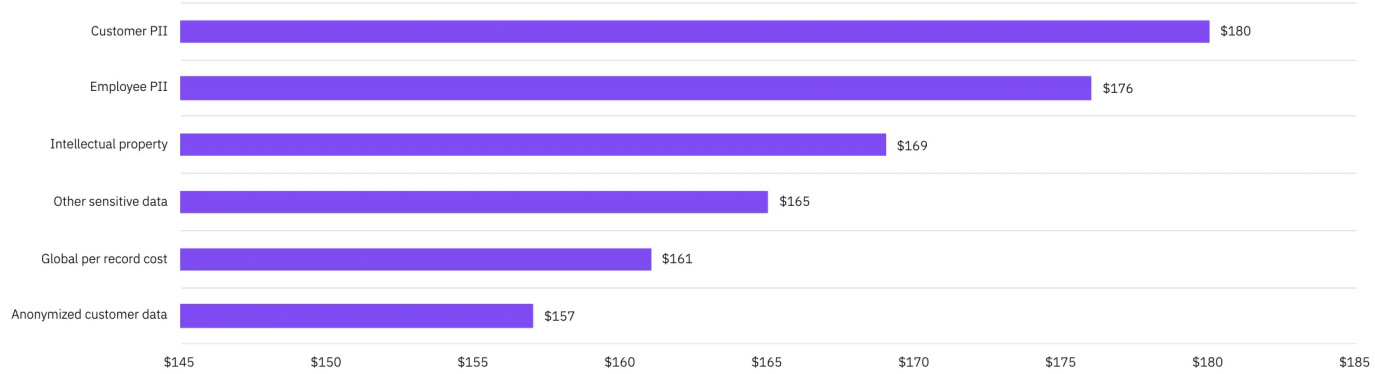


Figure 7

Average cost per record by type of data compromised

Measured in US$



Like years past, its seemingly taking longer than ever for organizations to identify and contain a data breach, 287 days, more than three quarters of a year. According to the report, it's taking 212 days to identify and 75 to contain a breach, that’s longer than any period over the last five years. For comparison,

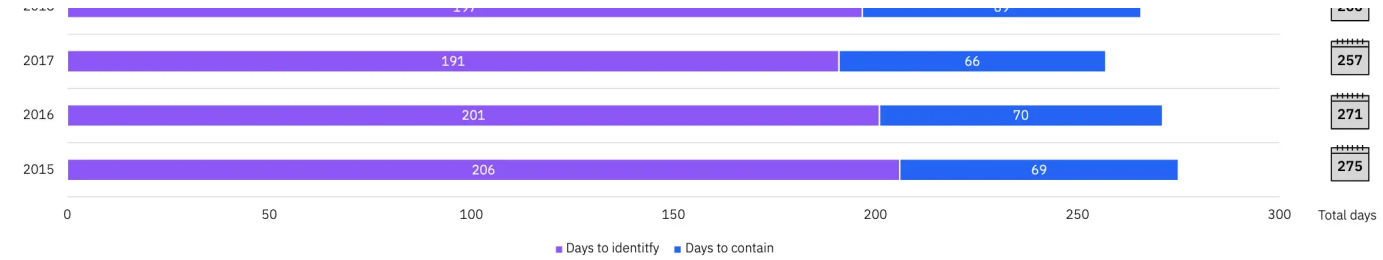
year it took on average 207 days to identify and 75 days to contain.

9

erage time to identify and contain a data breach

ıred in days

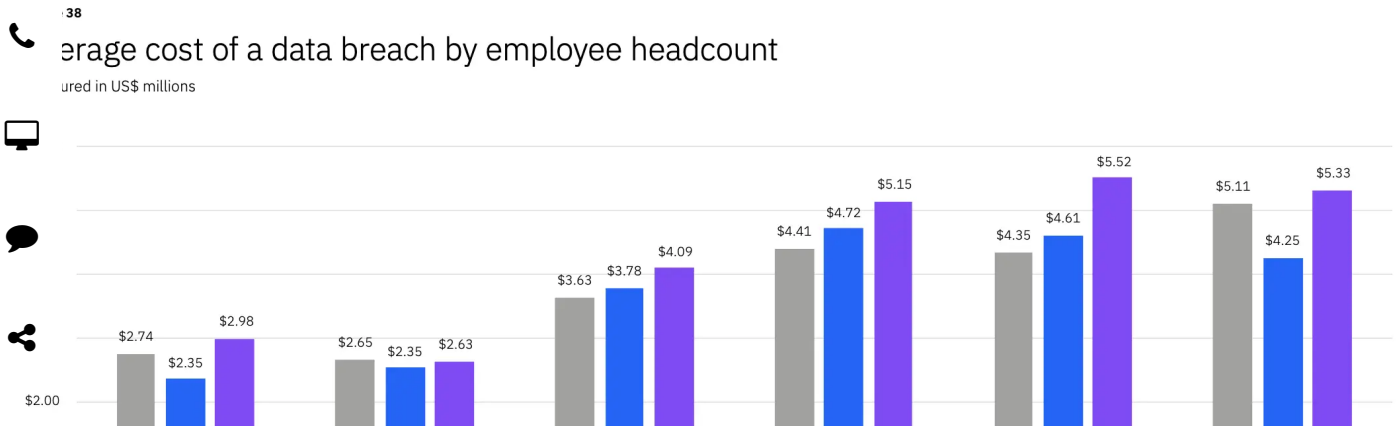


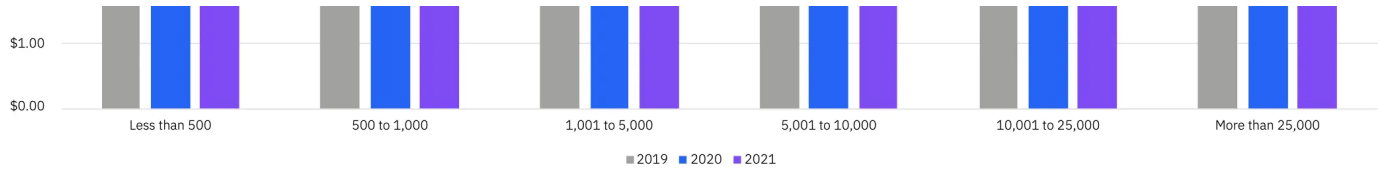


Companies that embraced modern security solutions, like a hybrid cloud setup, in which some resources are overseen in-house and some via cloud-based services, saved money for the most part.

According to the report, companies that experienced a cloud-based data breach that had a hybrid cloud lost $3.61 million on average while those that had a public cloud or private cloud lost between $4.80 and $4.55 million on average. Organizations with a zero trust strategy in place, encryption, some form of security analytics, or employed artificial intelligence incurred lesser data breach costs too. While the amount jumps around, the solutions saved companies - at least those consulted for the report - between $1.25 million and $1.49 million.

For those curious, the report breaks down a number of additional vectors - how much breaches cost companies with an incident response team in place vs. no incident response team, the average cost of a data breach based on the size of an organization, and how much it cost companies who experienced what IBM and Ponemon call "high level compliance failures."





For those interested, it's worth digging into **the report (https://www.ibm.com/security/data-breach)** in its entirety to get the full scope.

Tags: **Data Breaches (/blog/search/data-breaches)**

Recommended Resources

The Definitive Guide to Data Classification

(https://info.digitalguardian.com/ebook-definitive-guide-to-data-classification.html)

- Why Data Classification is Foundational
- How to Classify Your Data
- Selling Data Classification to the Business

GET THE EBOOK (HTTPS://INFO.DIGITALGUARDIAN.COM/EBOOK-DEFINITIVE-GUIDE-TO-DATA-CLASSIFICATION.HTML)

Gartner Report: How to Overcome Pitfalls in Data Classification Initiatives

(https://info.digitalguardian.com/analyst-report-gartner-overcome-pitfalls-data-classification.html)

- How to simplify the classification process
- Why classification is important to your firm's security
- How automation can expedite data classification

Why Arbitration Clauses May Make Sense in Cyber Insurance Policies

By Andrew S. Nadolna, Esq., Adrienne Publicover, Esq. and Daniel B. Garrie, Esq.

I. INTRODUCTION

Arbitration tends to work best when both parties buy into the process from the beginning. Alternatively, the process often works poorly when one party feels that arbitration was imposed on them.[1]

In the commercial insurance context, arbitration can sometimes feel imposed, even to sophisticated policyholders.[2] This comes about through mandatory arbitration clauses in form policies that are usually non-negotiable, and includes domestic, excess and surplus lines London and Bermuda policies.[3] Also, policyholders may perceive elements of unfairness in the arbitration process created by such clauses.[4] But arbitration does not have to be either imposed or unfair in the insurance context. There are circumstances where policyholders may actually want to be part of a confidential arbitration, particularly when the dispute involves a core business process that has failed.[5] A policyholder may wish to avoid publicity over the presence or absence of insurance coverage for such a loss, and they may want confidentiality over documents and testimony that pertain to that business failure. Cyber breach is a case in point.

In this Article, we will argue that policyholders should ask for an arbitration clause in their cyber policies and negotiate over the terms. We will also argue that insurers should offer more options in this space. In this regard, modular arbitration clauses can prove useful for both sides and lead to an effective dispute resolution mechanism for dealing with what may turn out to be a flood of cyber coverage disputes.[6]

We will start with a discussion of the principal objections policyholders often have to mandatory arbitration clauses. Then we will discuss why some of these objections may cut differently for policyholders with cyber risks. Finally, we will discuss some of the options the cyber insurance marketplace could offer.

II. POLICYHOLDER OBJECTIONS

The first policyholder objection concerns the fundamental nature of arbitration. Like other arbitrations, insurance arbitrations are decided by a private tribunal through a confidential process and produce (mostly) confidential results.[7] There is no jury. There is no judge who will write and potentially publish an opinion. And there is only a lim-



ANDREW S. NADOLNA, ESQ.



ADRIENNE PUBLICOVER, ESQ.



DANIEL B. GARRIE, ESQ.

This article originally appeared in the *Cardozo Journal of Conflict Resolution*, Vol. 19:43.

ited avenue for appeal on narrowly circumscribed grounds.[8] Generally, there is also no media coverage.[9]

Policyholder lawyers have argued that confidentiality gives the insurance company license to take more extreme positions than it would in court.[10] While there isn't data to support or refute this assertion, it is an enduring policyholder concern.[11] In our experience, extreme positions are rarely rewarded, as arbitrators can get as frustrated as judges and juries do with overreaching. But there is no doubt that a public process creates leverage that usually benefits the policyholder.

For example, litigation risks of creating adverse precedent in a published opinion that may impact language that the insurer or even the insurance industry has used over and over is a significant piece of leverage that does not exist in arbitration.[12] This "portfolio risk" is one of several ways in which policyholder lawyers may increase pressure on insurers to settle insurance coverage disputes.[13] Arbitration eliminates the risk. Each arbitration ruling stands on its own. Other arbitration panels will not know about the rulings and cannot cite to them as precedent.[14]

Second, policyholders may view the pool of potential insurance arbitrators as skewed toward those with significant insurance industry experience.[15] This can come about through specific requirements in the arbitration clause, i.e., specific educational, professional or occupational requirements.[16] It can also come about just through the arbitration selection process.[17]

In three-person panels, each side will pick an arbitrator they like, and the two chosen arbitrators will pick a third person.[18] Inevitably, the third person will likely have some connection with the industry and some inside knowledge that may be seen as a predisposition or bias.[19] This may simply mean that arbitrators drawn from this pool are not likely to view a coverage dispute in the same way that a judge or jury or other non-insurance expert would.[20] When coupled with the fact that insurance companies are often repeat customers with insurance arbitrators, while policyholders usually are not, this may be a significant risk. While many policyholder lawyers are skilled at finding arbitrators more likely to lean their way (policyholders are usually not repeat customers for arbitrators, but policyholder law firms are), this can be a difficult task, especially when arbitration clauses require arbitration in London or Bermuda, and the panel to comprise former insurance company executives, as some clauses do.[21]

Third, relief in an arbitration may be more limited than what can be obtained in court.[22] This can be accomplished by limiting or eliminating the possibility of recovering attorneys fees, limiting punitive damages, or interest on the amount in dispute.[23] Limiting relief can also be accomplished by limiting the availability of extracontractual or bad faith damages[24] or through a choice of law provision.[25] In these situations, insurers often choose New York law, which has been viewed specifically as insurer friendly for a long time, including on issues concerning allowing policyholders to recover attorney's fees and bad faith damages.[26] From the perspective of affording leverage or increasing the risk to insurers, litigation provides more potential leverage for policyholders to bring to bear maximum risk to insurers.

Fourth, the rules of interpretation are often changed in the arbitration clause. Common law rules require interpretations in favor of the policyholder where there is ambiguity (*contra proferentum*). Arbitration clauses may be altered to allow for something closer to an interpretation that assumes equal bargaining power between the parties.[27] In court, a tie goes to the policyholder.[28] In arbitration, a tie may go either way. Also, such clauses may limit the introduction of parole or extrinsic evidence to aid in policy interpretation, a tactic that can work in impacting the outcome.[29]

Fifth, in most arbitration clauses each party generally bears their own cost, at least initially.[30] This means each party pays for arbitrator time.[31] In a three-person panel, this means each party pays its own selected arbitrator as well as a portion of the umpire. For one-person arbitration, the sides will split the fees. To compound the problem, many arbitrations, particularly in London, have a loser-pays rule, so if the policyholder arbitrates and loses, it could be out of pocket quite a lot of money.[32] The American court system, in contrast, is nearly free.[33] Other than some minimal filing fees,

court personnel and juries are paid by tax dollars, and the "American Rule" prevents most fee shifting in litigation.[34] So a policyholder faces significant potential expenses it otherwise would not face in court.[35]

Sixth, companies purchasing large limits through a tower made up of multiple insurers may face different arbitrations with different insurers at different levels, thereby having to litigate and relitigate coverage as it moves up the tower, rather than having everything handled in a single consolidated lawsuit in court.[36]

In addition to all of these objections, additional evidence that arbitration clauses may be one-sided exists in the form of state statutes, in nearly half of the states, which forbid the use of mandatory arbitration clauses in some or all insurance contracts.[37] These laws coexist with a strong federal policy in favor of arbitrating disputes, as codified in the Federal Arbitration Act, 9 U.S.C. sections 1–16 (2001), and state statutes in nearly every state making agreements to arbitrate future disputes valid.[38] In the state of Washington, the Washington Supreme Court has held that mandatory arbitration clauses are unenforceable even in the excess and surplus lines market, where insurers are more lightly regulated.[39] Given the risk of unenforceability, most insurers in the cyber context are resorting to some form of optional arbitration clause.

III. WHY CYBER RISKS MAY BE DIFFERENT

Litigation over ADR clauses in cyber policies is already happening.[40] If one of the purposes of arbitration is to obtain a more cost-effective resolution of a dispute, litigation over the dispute resolution method defeats that purpose and thereby defeats other purposes of arbitration as well.[41] It may be useful to step back and consider the policyholder objections in the cyber context, particularly in the context of a marketplace that may be amenable to negotiation around arbitration clauses.

The first policyholder objection is the private and confidential nature of the process.[42] There is no judge, no jury, only a limited avenue of appeal and no media coverage. Depending on the specific nature of the coverage dispute, these objections may actually benefit a cyber policyholder. Cyber coverage disputes could involve an exchange of sensitive or confidential information.[43] There could be discovery about the cyber-defenses employed by the policyholder, including weaknesses in its systems.[44] There could be discovery about due diligence in choosing what systems to implement.[45] Also, the policyholder may not want to have media coverage about the extent of its available insurance when it is in the midst of dealing with defending a class action arising out of a breach.[46] Nor would the policyholder want a public court ruling that its defenses are inadequate, or misrepresented, or not properly thought through, so the lack of a written ruling and the circumscribed appellate opportunities might be welcome.[47] Depending on the type of coverage defense asserted, discovery relevant to that issue could lead to the exchange of damaging information about internal processes and procedures and cyber-defenses, adequacy of funding for cyber-defense, quality of decision-making processes and existence of other vulnerabilities in systems that the policyholder would not want documented in public court filings.[48] Although this could potentially be addressed in court filings under seal, that is still more risky than a truly confidential arbitration process.[49] Many hacks also lead to lengthy class action litigation. The class would be following any public insurance dispute with interest and looking for the opportunity to get at any information exchanged in the insurance dispute that was not part of the discovery in the class action.[50] Sometimes, there are regulatory proceedings as well. Regulators also closely follow insurance coverage action.[51]

Also, arbitration provides the policyholder with the opportunity to make some very creative arguments that would not go over as well in court as they might to a sophisticated panel. Such considerations would need to be weighed against the loss of leverage that happens in arbitration because the insurer no longer faces portfolio risk. If the arbitration is optional and the policyholder gets to choose, these objections may be considered and evaluated before arbitration is invoked.

The second policyholder objection is concerned with the pool of potential arbitrators. In the cyber security context, London and Bermuda arbitrations, with their pool of highly technical arbitrators

with some distance from the U.S. litigation environment, may be a plus. It is possible arbitrators may be more sympathetic to the nature of cyber risks and the challenges policyholders face in securing appropriate coverage and dealing comprehensively with the risks both from a cyber and a risk management perspective compared to judges and juries. The policyholder may want a level of expertise with both policy language and technical cyber issues in its decision makers.[52] Cyber policies have not really hardened into standard forms yet, so there is little benefit to looking to court precedents for rules of decision.[53] And it seems that those cases that do get litigated usually lead to the policy form changing yet again, which limits the precedential value of those cases that do get decided.[54]

Also, when policy language is not yet standardized, it may help to have decision makers who read policies frequently and can compare how the language in cyber policies matches up to policies that have endured more testing and modified to adjust for lessons learned.

Similarly, judges and juries may have lower tolerance for flaws in cyber security approaches, even when just considering insurance coverage, but cyber experts may have a much better sense of the feasibility of preventing the kind of thing that happened from happening again based on technology as it existed at the time.[55] In addition, it is possible to negotiate into the arbitration clause what any panel would look like.[56] So, for example, it may be possible to insist on at least one arbitrator with corporate board experience who has been in a position to deal with cyber-related exposures and understand the trade-offs that are being made.[57]

The third and fourth objections do not change much in a cyber context. If the arbitration clause eliminates or reduces the policyholder's ability to obtain attorney's fees and/or bad faith damages in the event it prevails, this is a reduction of leverage for the policyholder.[58] The only question here is whether keeping this leverage is worth the downside risks that go along with litigation, including loss of confidentiality, potential media exposure and possibly less sympathetic decision makers. Also, in a negotiable marketplace, there may be ways to deal with these issues. Perhaps insurers would consider including both attorney's fees and bad faith damages to procedural protections, adequate evidentiary standards and perhaps caps on punitive damages.[59] And, of course, choice of law provisions can be negotiated and need not always be New York or other forums supportive of insurance companies.

The fifth objection also presents no unique cyber considerations. The cost of arbitration plays out differently than litigation. If the arbitration is set up and conducted appropriately, the costs of arbitrators, while expensive, will be more than offset by the reduced spend on litigation.[60] Even if the arbitration is more expensive, the policyholder may be paying for a kind of expertise that ensures it will receive a fairer hearing and potentially a more sympathetic ear than it might get in court.[61]

The sixth objection also presents no unique cyber circumstances. But given the flexibility in the marketplace, it would seem wise to discuss the possibility of all carriers in a tower signing on to an arbitration clause that provides for consolidation of arbitrations, at least as to common issues.

IV. WHAT THE MARKETPLACE MAY BEAR

Given the potential that cyber policyholders may want an arbitration option and the likelihood that they will not want arbitration in all instances and certainly would not want it to be mandatory, what are some of the possibilities?

Many carriers already offer a limited optional arbitration clause that requires both parties' consent to move forward.[62] Most of these clauses have a general reference to some existing set of arbitration rules, whether AAA, JAMS or others. This is helpful but may cause either side to try to game the incident and closely evaluate risks and rewards of either approach.[63] If one side clearly wants an arbitration, the other may go the other way, sensing that some advantage will be lost if it agrees.[64]

But arbitration clauses may involve a situation where a modular approach is preferable. By modular, we simply mean a clause with different elements that can be chosen and combined in different ways. There are lots of potential choices.[65] In terms of triggering arbitration, you can require both parties' consent, or you can have one way

mandatory—this would give the policyholder the right to invoke and proceed with arbitration, and the insurer would have no right to object. In either case, the insurer gains from secrecy and confidentiality, and avoids appeal and media; this may be sufficient for insurers to sign on to this approach. But depending on what other provisions are in the arbitration clause, the insurer may have additional reasons for liking this approach. Other choices in this modular approach could be a variety of choice of law options (including New York, the law of the policyholder's principal place of business and other states with some nexus to insured operations); varieties of fee shifting and potential damage options, including bad faith subject to caps; different arbitrator requirements in terms of background and perhaps even fully neutral panels (as suggested under ARIAS neutral rules); and different rule and discovery options.[66]

V. CONCLUSION

The cyber market is broad and deep with lots of insurers, and pricing is relatively low compared to the risks.[67] Competition is intense.[68] Policyholders can and are negotiating policy language.[69] Arbitration clauses should be a part of this discussion. Once you take away arbitration as an imposed concept and policyholders have the opportunity to view it as an option that may inure to its benefit, the dialogue will be much different. Given the importance of cyber security to most businesses, the ongoing media coverage, published opinions and jury verdicts may not be what the C-suite wants. Even smaller companies may be harmed by continuing publicity around cyber attacks.[70] Consider this: You've been hacked. Regulators are coming your way. A class action may be filed at any moment. You are in internal crisis mode utilizing the services of a breach coach, and your teams are in high alert. Then you get a reservation of rights letter or a partial disclaimer from your insurance company, and your counsel tells you that you might also face a declaratory judgment action in federal court. If you don't have an arbitration clause, would you want to try negotiating one now?

Better to have that option in place before a crisis happens.

ANDREW S. NADOLNA, ESQ. *is a JAMS mediator and arbitrator based in New York City. Before becoming a neutral, he was a senior claims executive at AIG for over 15 years. Before that, he was an insurance coverage attorney in private practice. He can be reached at* **anadolna@jamsadr.com**.

ADRIENNE PUBLICOVER, ESQ. *is a JAMS neutral based in Northern California. She has counseled domestic insurers and brokers, as well as the London market, in litigation matters in state and federal courts throughout the country. She can be reached at* **apublicover@jamsadr.com**.

DANIEL B. GARRIE, ESQ. *is a JAMS neutral who serves as an e-discovery special master, technical special master, forensic neutral and mediator/arbitrator with a focus on complex software and business litigation, e-discovery disputes, privacy and data breach matters, trade secret theft and intellectual property litigation. He can be reached at* **dgarrie@jamsadr.com**.

ENDNOTES

1. The cost involved in compelling a recalcitrant party to arbitrate has the potential to significantly increase the overall cost of the proceeding. *See* Nat'l Union Fire Ins. Co. of Pittsburgh v. Beelman Truck Co., No. 17-CV-2946, 2017 U.S. Dist. LEXIS 111136 (S.D.N.Y. July 17, 2017) (appointing an umpire; the first trip to court involved arbitrability).

2. Joshua Gold, ANDERSON KILL P.C., *Insurance Policy Arbitration Clauses: Perils and Considerations for Policyholders,* CORPORATE COUNSEL (Dec. 2007), https://www.andersonkill.com/webpdfext/CorporateCounsel-December2007.pdf; Peter A. Halprin, ANDERSON KILL P.C., *Arbitration in Insurance Coverage Disputes: Pluses and Minuses,* POLICYHOLDER ADVISOR (2014), https://www.andersonkill.com/webpdfext/publications/PHA/PDF/Arbitration-in-Insurance-Coverage-Disputes-Pluses-and-Minuses.pdf.

3. Rich Lewis, REED SMITH, *A Quick and Dirty Guide to London Insurance Arbitrations,* POLICYHOLDER PERSPECTIVE, (June 4, 2009), https://www.policyholderperspective.com/2009/06/articles/insurance-coverage/a-quick-and-dirty-guide-to-london-insurance-arbitrations/; Leon Kellner & Vivek Chopra, PERKINS COIE LLP, *Bermuda Form Arbitration: A Policyholder Perspective,* GETTING THE DEAL THROUGH (July 2, 2014), https://gettingthedealthrough.com/area/16/article/28741/insurance-reinsurance-bermuda-form-arbitration-policyholder-perspective; Joshua Gold & Peter A. Halprin, ANDERSON KILL P.C., *Cyber Insurance Disputes: Will Arbitration Clauses be a Battleground?,* POLICYHOLDER ADVISOR, (2016), https://www.andersonkill.com/Custom/PublicationPDF/PublicationID_1362_Cyber-Insurance-Disputes-Will-Arbitration-Clauses-be-a-Battleground.pdf.

4. Gold, *supra* note 2; Edmund M. Kneisel & Richard English Dolder, *Arbitration Clauses in Insurance Policies: A Primer for the Construction Professional,* in 2004 CONSTRUCTION LAW UPDATE 223 (Neal J. Sweeney, ed., 2004), *available at* http://kilpatricktownsend.com/~/media/Files/articles/2012/CH-5_CLUP_2004.ashx.

5. Gold, *supra* note 2; John G. Nevius & Peter A. Halprin, ANDERSON KILL P.C., *Arbitration of Insurance Coverage Disputes: A*

Policyholder's Definitive Survival Guide, MONDAQ (Dec. 21, 2010), http://www.mondaq.com/unitedstates/x/118608/Insurance/Arbitration+of+Insurance+Coverage+Disputes+A+Policyholders+Definitive+Survival+Guide.

6. Carrie E. Cope & Ian Reynolds, *"Breaking Bad" in Cyberspace: A Challenge for the Insurance Industry,* 7296 EMERGING ISSUES (LexisNexis, 2015).

7. Mark Chudleigh & Neil Thomson, I*nsurance Arbitrations: Confidentiality Versus Consistency,* INS. L. BLOG: LEXOLOGY (Aug. 30, 2016), https://www.lexology.com/library/detail.aspx?g=3a23ae16-bd30-4e6c-874f-7335f03f032b.

8. Del. Coal. for Open Gov't, Inc. v. Strine, 733 F.3d 510, 518 (3d Cir. 2013). However, appeals from arbitration rulings seem to be increasing, although not with much success, other than impinging on confidentiality.

9. Jill I. Gross & Barbara Black, *When Perception Changes Reality: An Empirical Study of Investors' Views of the Fairness of Securities Arbitration,* 2008 J. DISP. RESOL. 349 (2008).

10. *See* Gold, *supra* note 2.

11. *Id.*

12. *Id.*

13. *Id.*

14. *Strine*, 733 F.3d at 518. See also Drennen v. Certain Underwriters at Lloyd's of London, 563 B.R. 756 (Bnkr. S.D.N.Y. 2016) (discussing insurance coverage dispute).

15. Stephen J. Choi et al., *The Influence of Arbitrator Background and Representation on Arbitration Outcomes,* 9 VA. L. & BUS. REV. 43 (2014) (discussing correlation of outcome with the background of the arbitrators in securities arbitration). *See also* Gold, *supra* note 2; Halperin, *supra* note 2; Strine, 733 F.3d at 518.

16. *See, e.g.,* ARIAS U.S., RULES FOR THE RESOLUTION OF U.S. INSURANCE AND REINSURANCE DISPUTES, R. 6.2 (2014), http://www.arias-us.org/wp-content/uploads/2016/09/ARIASU.S.-Rules.pdf ("The arbitrators and umpire shall be persons who are current or former officers or executives of an insurer or reinsurer and shall be ARIAS-certified as of the date of their appointment."). *See, e.g.,* Nat'l Union Fire Ins. Co. of Pittsburgh v. Beelman Truck Co., No. 17-CV-2946, 2017 U.S. Dist. LEXIS 111136 (S.D.N.Y. July 17, 2017) (on limiting clauses).

17. *Beelman Truck Co.,* 2017 U.S. Dist. LEXIS 111136, at *3.

18. These proceedings are referred to as "Tripartite Panels." The third arbitrator is intended to act as a neutral "umpire," whereas the other two unilaterally appointed arbitrators generally act on behalf of the party that appointed them. Stephen C. Rogers, *Can Tripartite Arbitration Panels Reach Fair Results?,* 19 A.B.A. SEC. SOLO, SMALL FIRM & GEN. PRAC. DIV. 6 (2002), https://www.americanbar.org/content/newsletter/publications/gp_solo_magazine_home/gp_solo_magazine_index/rogers.html.

19. MITCHELL L. LATHROP, INSURANCE COVERAGE FOR ENVIRONMENTAL CLAIMS (1990).

20. Commonwealth Coatings Corp. v. Cont'l Cas. Co., 393 U.S. 145 (1968) (disclosure is the key to avoiding the appearance of bias).

21. ARIAS U.S, *supra* note 16; *Beelman Truck Co.,* 2017 U.S. Dist. LEXIS 111136, at *4.

22. Gold, *supra* note 2; Halperin, *supra* note 2.

23. Gold, *supra* note 2; Halperin, *supra* note 2.

24. Gold, *supra* note 2; Halperin, *supra* note 2.

25. Gold, *supra* note 2; Halperin, *supra* note 2.

26. Gold, *supra* note 2; Halperin, *supra* note 2.

27. Gold, *supra* note 2; Nevius, *supra* note 5.

28. Newport Assocs. Dev. Co. v. Travelers Indem. Co., 162 F.3d 789 (3d Cir. 1998).

29. Gold, *supra* note 2; Nevius, *supra* note 5.

30. Bradford v. Rockwell Semiconductor Sys., 238 F.3d 549, 556 (4th Cir. 2001).

31. R. Brian Tipton, *Allocating the Costs of Arbitrating Statutory Claims Under the Federal Arbitration Act: An Unresolved Issue,* 26 AM. J. TRIAL ADVOC. 325, 361 (2002).

32. Walter Olson & David Bernstein, *Loser-Pays: Where Next?,* 55 MD. L. REV. 1161 (1996).

33. *See* N.Y. ST. UNIFIED CT. SYS., *Filing Fees,* NYCTS.GOV, https://www.nycourts.gov/forms/filingfees.shtml).

34. Dixon v. Comm'r, 91 T.C.M. (CCH) 1086 (2006).

35. *See generally* Theodore Eisenberg & Geoffrey P. Miller, *The English Versus the American Rule on Attorney Fees: An Empirical Study of Public Company Contracts*, 98 CORNELL L. REV. 327 (2013).

36. Insurance towers are created by combining multiple different insurers with different policies, setting up base insurers and upper "excess policy" insurers. This protects the company against bankruptcy of any individual insurer. Some Direct and Officer liability insurance companies are so specialized that they offer only excess, upper floor insurance. *See* Richard Squire, *How Collective Settlements Camouflage the Costs of Shareholder Lawsuits,* 62 DUKE L.J. 1 (2012).

37. *See State Laws Regulating Arbitration in Insurance Contracts,* PUB. CITIZEN (May 24, 2017), https://www.citizen.org/article/state-laws-regulating-arbitration-insurance-contracts-0.

38. Federal Arbitration Act, 9 U.S.C. § 1–16 (1925). *See, e.g.,* N.Y. C.P.L.R. § 7501 (1963) ("A written agreement to submit any controversy thereafter arising or any existing controversy to arbitration is enforceable without regard to the justiciable character of the controversy and confers jurisdiction on the courts of the state to enforce it and enter judgment on an award.").

39. Dep't of Transp. v. James River Ins. Co., 292 P.3d 118 (2013). *But see,* United Nations Convention on the Recognition & Enforcement of Foreign Arbitral Awards, *opened for signature* June 10, 1958, 330 U.N.T.S. 38 (entered into force June 7, 1959) (enforcing the clause due to the international nature of the contract, regardless of state statutes).

40. *See, e.g.,* New Hotel Monteleone, LLC v. Certain Underwriters at Lloyd's of London, No. 2:16-CV-00061 (E.D. La. Aug. 17, 2016) (subscribing to Ascent Policy No. ASC14C000944); Columbia Gas. Co. v. Cottage Health Sys., No. CV-15-03432, 2015 U.S. Dist. LEXIS 93456 (C.D. Cal. July 17, 2015).

41. If mandatory arbitration is always preceded by a challenge as to its enforceability, the combined cost of both proceedings may well warrant a foregoing of mandatory arbitration. Therefore, the prima facie enforceability of arbitration agreements is of paramount importance, and can be secured significantly easier if both parties negotiate and agree to mandatory arbitration.

42. *See* Gold, *supra* note 2.

43. *See* Music Grp. Macao Commer. Offshore, Ltd. v. Foote, No. 14-CV-03078, 2015 U.S. Dist. LEXIS 81415 (N.D. Cal. 2015) (regarding disclosure of extensive documentation).

44. *See In re* Anthem Data Breach Litig., 162 F. Supp. 3d 953 (N.D. Cal. 2016) (alleging insufficient security measures).

45. *See In re* Heartland Payment Sys., Customer Data Sec. Breach Litig., 834 F. Supp. 2d 566 (S.D. Tex. 2011).

46. Lili Dai et al., *The Governance Effect of the Media's News Dissemination Role: Evidence from Insider Trading,* 53 J. ACCT. RES. 331 (2015).

47. The effect of a public court ruling against a defendant exceeds purely legal considerations. By giving plaintiffs multiple chances to obtain such a ruling, the public court system has significant disadvantages for defendants vis-`a-vis the circumscribed appellate opportunities available to arbitration. *See* Matt Levine, *There Will Always Be Stock-Drop Lawsuits,* BLOOMBERG (June 23, 2014), https://www.bloomberg.com/view/articles/2014-06-23/there-will-always-be-stock-droplawsuits.

48. Public documentation of these issues increases the likelihood that affected companies will be the subject of related litigation. See Christopher P. Skroupa, *Shareholders Sue Companies for Lying About Cyber Security,* FORBES (Oct. 27, 2016), https://www.forbes.com/sites/christopherskroupa/2016/10/27/exposing-litigation-the-hidden-risks-of-cyber-breach/#66a16baf31a1.

49. Lisa R. Hasday, *Think Before You Seal*, A.B.A. SEC. LITIG. (Dec. 27, 2011), https://apps.americanbar.org/litigation/litigationnews/top_stories/122111-sealed-case-files.html.

50. *In re* Heartland Payment Sys., 851 F. Supp. 2d 1040 (S.D. Tex. 2012) (involving disclosure of data security breach followed directly by class action comprising over one-hundred million plaintiffs).

51. Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches,* 105 MICH. L. REV. 913 (2007).

52. *Id.*

53. Jennifer Gordon, *Like a Bad Neighbor, Hackers are There: The Need for Data Security Legislation and Cyber Insurance in Light of Increasing FTC Enforcement Actions,* 11 BROOK. J. CORP. FIN. & COM. L. 183, 184 (2016) ("Interpretations of cyber insurance policies are still in their infancy.").

54. Michael A. Tomasulo & Scott N. Godes, *The Cybersecurity Playbook: Helping Clients Evaluate Their Cyber Risks, in* UNDERSTANDING DEVELOPMENTS IN CYBERSPACE LAW: LEADING LAWYERS ON ANALYZING RECENT TRENDS, CASE LAWS, AND LEGAL STRATEGIES AFFECTING THE INTERNET LANDSCAPE 157 (2012).

55. Gregg A. Paradise, *Arbitration of Patent Infringement Disputes: Encouraging The Use of Arbitration Through Evidence Rules Reform,* 64 FORDHAM L. REV. 247 (1995) ("Judges and jury members who lack technical expertise often are overwhelmed and confused by such material and lack the background to resolve the conflicting assertions.").

56. BERTHOLD H. HOENIGER, COMMERCIAL ARBITRATION HANDBOOK 1–11 (rev. ed. 1991) ("Since arbitration is a creature of contract, the possibilities for custom tailoring are almost endless.").

57. AM. ARB. ASS'N, COMMERCIAL ARBITRATION RULES AND MEDIATION PROCEDURES, 15 (2016).

58. Gold, *supra*, note 2.

59. Panoche Energy Center, LLC v. Pacific Gas & Electric Co., 1 Cal. App. 5th 68 (Cal. App. 1st Dist. July 1, 2016). "Arbitration is foremost a creature of contract. Arbitration's consensual nature allows the parties to structure their arbitration agreement as they see fit." *Id.* at 93 *quoting* Bunker Hill Park Ltd. v. U.S. Bank Nat'l Assn., 231 Cal. App. 4th 1315, 1326 (Cal. App. 2d Dist. Nov. 26, 2014). *See also* Baker v. Sadick, 162 Cal. App. 3d 618 (1984) (allowing arbitration to consider issues of punitive damages).

60. According to statistics furnished by the American Bar Association, arbitration takes, on average, sixteen months less than civil cases in district courts. Edna Sussman & John Wilkinson, *Benefits of Arbitration for Commercial Disputes,* 2012 A.B.A., SEC. DISPUTE RESOL. 3 (2012), https://www.americanbar.org/content/dam/aba/publications/dispute_resolution_magazine/March_2012_Sussman_Wilkinson_March_5.authcheckdam.pdf.

61. Studies show that a majority of respondents believe arbitration is superior to litigation. Furthermore, arbitrators may work full time and have a significantly lower caseload than traditional judges, allowing them to devote unlimited time to a single case. DOUGLAS SHONTZ ET AL., RAND CORP., INST. FOR CIV. JUST., BUSINESS TO BUSINESS ARBITRATION IN THE UNITED STATES: PERCEPTIONS OF CORPORATE COUNSEL (2011), http://www.rand.org/content/dam/rand/pubs/technical_reports/2011/RAND_TR781.pdf.

62. *See, e.g.,* CYBEREDGE®, CYBER LIABILITY INSURANCE, AIG.

63. David Sherwyn, *Because It Takes Two: Why Post-Dispute Voluntary Arbitration Programs Will Fail to Fix the Problems Associated with Employment Discrimination Law Adjudication,* BERKELEY J. EMP. & LAB. L., March 2003, at 1.

64. Samuel Estreicher, *Saturns for Rickshaws: The Stakes in the Debate over Predispute Employment Arbitration Agreements,* 16 OHIO ST. J. ON DISP. RESOL. 559 (2001).

65. Because arbitration agreements are created by contracts founded on mutual assent, the parties have wide latitude to decide the structure, form, and substance of arbitration processes. With sufficient negotiations, both parties can obtain terms that protect their core interests, without acting to the detriment of the other party.

66. 66 HOENIGER, *supra* note 56. ("[S]ince arbitration is a creature of contract, the possibilities for custom tailoring are almost endless.").

67. Richard S. Betterley, *Cyber/Privacy Insurance Market Survey,* BETTERLEY REPORT (2016), http://betterley.com (on file with author).

68. AGCS ALLIANZ, A GUIDE TO CYBER RISK: MANAGING THE IMPACT OF INCREASING INTERCONNECTIVITY (2015), http://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/Cyber RiskGuide.pdf.

69. Rene Siemens & David Beck, *How to Negotiate Cyber Insurance,* LEXISNEXIS (Jan. 24, 2013), https://www.lexisnexis.com/legalnewsroom/insurance/b/cyberinsurance/archive/2013/01/24/how-to-negotiate-cyber-insurance.aspx?Redirected=true.

70. Matt Mansfield, *Cyber Security Statistics—Numbers Small Businesses Need to Know,* SMALL BUS. TRENDS (Jan. 3, 2017), https://smallbiztrends.com/2017/01/cyber-security-statisticssmall-business.html.

This article was originally published in the Policyholder Advisor, *Volume 25, Issue 2 (March/April 2016)*

ANDERSON KILL
POLICYHOLDER ADVISOR
The Policyholder Law Firm



Cyber Insurance Disputes: Will Arbitration Clauses be a Battleground?

By Joshua Gold and Peter A. Halprin

Commercial insurance companies are marketing cyber risk policies with messages such as, "Just about any organization that uses technology to do business faces cyber risk." In response to such risk, insurance companies are offering scores of "cyber" insurance products that get tweaked regularly and vary greatly in quality and terms. That lack of uniformity foretells coverage disputes — and litigation over insurance coverage for cyber claims began to emerge recently.

In such cases, the dispute resolution mechanism may pose an important threshold issue. Some cyber insurance policies may purport to require a mediation before litigation can be commenced,[1] while others may have no dispute resolution clause at all. Still others may attempt to bind the policyholder to use mandatory arbitration in the event of a coverage dispute. Mandatory arbitration has its advantages and disadvantages,[2] and a policyholder should be aware of the implications of such provisions before agreeing to them.

In some cases, a mandatory arbitration clause in the policy may prove unenforceable. Some states have laws barring arbitration of insurance disputes, and establishing such a state as the venue for a dispute may enable a policyholder to obtain its day in court. If the dispute involves a foreign entity, however, insurance companies will likely argue that the Federal Arbitration Act and related law preempt state anti-arbitration statutes, rendering arbitration mandatory.

State Anti-Arbitration Provisions: Preemption and Reverse Preemption

Nearly half the states have laws imposing some form of limitation on the enforceability of mandatory arbitration provisions in insurance disputes.[3] The McCarran-Ferguson Act leaves regulation of insurance to the states, providing that "[n]o Act of Congress shall be construed

---

Joshua Gold is a shareholder in the New York office of Anderson Kill and co-chair of the firm's Cyber Insurance Recovery Group. Mr. Gold's practice involves matters ranging from international arbitration, data security, directors and officers insurance, business income/property insurance, commercial crime insurance and marine insurance disputes. He has been lead trial counsel in multiparty bench and jury trials, and has negotiated and crafted scores of settlement agreements including coverage-in-place agreements.
(212) 278-1886 | jgold@andersonkill.com

Peter A. Halprin is an attorney in Anderson Kill's New York office. His practice concentrates in commercial litigation and insurance recovery, exclusively on behalf of policyholders. Mr. Halprin also acts as counsel for U.S. and foreign companies in domestic and international arbitrations. He is a member of the Chartered Institute of Arbitrators and earned a Postgraduate Diploma in International Commercial Arbitration at Queen Mary, University of London.
(212) 278-1165 | phalprin@andersonkill.com

Attorney Advertising

to invalidate, impair, or supersede any law enacted by any state for the purpose of regulating the business of insurance." Accordingly, state laws limiting mandatory arbitration provisions in insurance disputes are generally enforced. McCarran-Ferguson therefore "reverse preempts" federal law to the extent a federal law invalidates, supersedes, or impairs the state law that regulates the business of insurance. *See, e.g., Riverview Health Institute v. Medical Mutual of Ohio* (6th Cir. 2010).

Reverse preemption generally does not apply however, when a "foreign element" is involved. Such cases are generally subject to the United Nations Convention on the Recognition and Enforcement of Foreign Arbitral Awards (also known as the New York Convention). See, e.g., Safety National Cas v. Certain Underwriters at Lloyd's, London (5th Cir. 2009); ESAB Group v. Zurich Ins. (4th Cir. 2012). The New York Convention, to which more than 130 countries including the United States are parties, provides for mutual recognition and enforcement of arbitral awards by contracting states, and limits the defenses that may be raised in opposition to the confirmation of an award.

To assess whether the New York Convention applies to an arbitration agreement, the following four-factor test is applied: (1) whether a written arbitration agreement between the parties exists, (2) whether the arbitration agreement provides for arbitration in the territory of a signatory of the New York Convention, (3) whether the relationship between the parties involves a commercial subject matter, and (4) whether the relationship between the parties is something other than entirety domestic. See, e.g., Murphy Oil USA, Inc. v. SR Int'l Bus. Ins. Co. (W.D. Ark. Sept. 20, 2007).

Thus, assuming the factors point in favor of applying the New York Convention to a dispute, courts are likely to find that the application of the New York Convention trumps McCarran-Ferguson and applicable state anti-insurance arbitration statutes. The general rationale, as set forth in *Murphy Oil*, 2007 U.S. Dist LEXIS 69732, is as follows:

> To allow parties to international agreements to rely on state-law defenses to render arbitration clauses unenforceable would damage the fabric of international commerce and trade and would diminish the willingness of foreign businesses and individuals to enter into international commercial agreements. The Supreme Court has given much deference to principles of international comity in its treatment of international agreements to arbitrate as distinct from domestic agreements.

Of course, there are exceptions to every rule, and one such exception comes in the form of a Kentucky appellate court decision denying a motion to compel arbitration, based in large part on the fact that the insurance company was not truly "foreign." *See Scott v. Louisville Bedding Co., 404 S.W.3D 870* (Ky Ct. App. July 2013) (a Swiss entity was not "foreign" when it conducted all of its business in Texas).

Mandatory Arbitration in Cyber Policies: *New Hotel Monteleone*

Early this year, a suit was filed that may be the first cyber coverage dispute to involve the enforceability of an arbitration clause. In *New Hotel Monteleone, LLC v. Certain Underwriters at Lloyd's of London, Subscribing to Ascent Policy No. ASC14C000944 et al.*, a hotel sued Lloyd's of London in Louisiana state court for failing to make payments under a CyberPro policy following a cyber attack. According to the initiatory pleading, the cyber attack resulted in a security breach such that "payment card numbers allegedly were compromised and were no longer confidential." Following the attack, the hotel was held liable for multiple types of losses and received a demand for damages from a payment card processor. The crux of the coverage dispute appears to be the limit of liability applicable to the dispute and, relatedly, the scope of a Payment Card Industry Fines or Penalties Endorsement.

The insurance company removed the action from state court to federal court and then moved to dismiss or, in the alternative, compel arbitration (pursuant to the policy's arbitration clause) and stay the court action. In their moving papers, Lloyd's argued that the arbitration agreement in the insurance policy was subject to the New York Convention. Because, according to Lloyd's, the New York Conven-

tion applied, a Louisiana state law that barred the enforcement of arbitration agreements in insurance policies could not overcome the force of the international treaty.

Lloyd's motion was not adjudicated as the parties agreed to stay the federal case and refer the matter to alternative dispute resolution. The case, however, demonstrates that even in the cyber insurance arena, policyholders should review and understand dispute resolution provisions prior to purchase. Further, those policyholders purchasing "layered" cyber insurance programs should also check their excess "follow form" cyber policies to see if their terms are truly follow-form in actuality. While a primary cyber policy may be devoid of an arbitration provision, it is possible that one or more excess policies in the tower contain their own dispute resolution clauses including one calling for binding arbitration in the United States or perhaps even abroad.

Policyholders should also be aware that there are means of challenging such provisions after a coverage dispute arises, but that the presence of a foreign element will complicate such a challenge.

ENDNOTES

[1] *Columbia Cas. Co. v. Cottage Health Sys.,* Case No. CV 15-03432, 2015 U.S. Dist. LEXIS 93456 (C.D. Cal. Jul. 17, 2015).

[2] *See* Peter A. Halprin, "Arbitration in Insurance Coverage Disputes: Pluses and Minuses." *Policyholder Advisor* (Jan. 6, 2015).

[3] *See* Public Citizen, "State Laws Regulating Arbitration in Insurance Contracts," http://www.citizen.org/congress/article_redirect.cfm?ID=6560

About Anderson Kill

Anderson Kill practices law in the areas of Insurance Recovery, Commercial Litigation, Environmental Law, Estate, Trusts and Tax Services, Corporate and Securities, Antitrust, Banking and Lending, Bankruptcy and Restructuring, Real Estate and Construction, Foreign Investment Recovery, Public Law, Government Affairs, Employment and Labor Law, Captive Insurance, Intellectual Property, Corporate Tax, Hospitality, and Health Reform. Recognized nationwide by Chambers USA for Client Service and Commercial Awareness, and best-known for its work in insurance recovery, the firm represents policyholders only in insurance coverage disputes — with no ties to insurance companies and has no conflicts of interest. Clients include Fortune 1000 companies, small and medium-sized businesses, governmental entities, and nonprofits as well as personal estates. Based in New York City, the firm also has offices in Ventura, CA, Philadelphia, PA, Stamford, CT, Washington, DC, and Newark, NJ.

The information appearing in this article does not constitute legal advice or opinion. Such advice and opinion are provided by the firm only upon engagement with respect to specific factual situations.
©2016 Anderson Kill P.C.

New York, NY • Ventura, CA • Philadelphia, PA • Stamford, CT • Washington, DC • Newark, NJ

The 10 Best Cyber Insurance Providers for 2022

Learn more about cyber insurance with rankings, financial ratings and frequently asked questions about cyber insurance for businesses.

Updated on December 29th, 2021

The SMB Guide is reader-supported. When you buy through links on our site, we may earn an affiliate commission. Learn more (https://www.thesmbguide.com/editorial-policy)

Updates:

Updated 12th of June 2020

We added comparisons between the leading cyber insurance providers, as well as further details about CoverWallet, Hiscox, and AIG.

Cyber insurance is a type of liability insurance (https://www.thesmbguide.com/small-business-liability-insurance) that protects your business in the event of a cybersecurity breach. Since so much important information is now stored on computers, cyber insurance is an increasingly popular type of coverage.

Our Pick



Coverwallet (https://go.thesmbguide.net/coverwallet-our-pick)

Small Business Insurance

Get Free Quote (https://go.thesmbguide.net/coverwallet-our-pick)

(https://go.thesmbguide.net/coverwallet-our-pick)

- ✓ Available 24/7.
- ✓ Competitive rates.
- ✓ Receive quotes in minutes.

Why We Chose CoverWallet, Hiscox, & AIG:

CoverWallet (https://www.thesmbguide.com/coverwallet) offers a wide range of business insurance, including commercial property insurance, cyber liability, medical malpractice, commercial auto insurance, professional liability, and umbrella insurance. CoverWallet customers can purchase and manage all necessary business insurance on one platform.

CoverWallet's cyber insurance insures your sensitive data from both internal and external cyber attacks. It provides coverage for a wide range of breaches, including loss of digital assets, business interruption, cyber extortion, and cyber terrorism.

Hiscox (https://www.thesmbguide.com/hiscox-reviews) offers worldwide cyber liability coverage to protect, businesses with optional coverage for business interruption resulting from a cyber disruption, cyber crime, and more. Hiscox also provides clients with useful breach response resources so that they'll know exactly how to respond in the event of a cyber breach.

AIG (https://www.thesmbguide.com/aig) is one of the most well-known insurance providers in the United States. AIG offers a variety of cyber insurance solutions, and their cyber experts will help clients to analyze threats and mitigate their risk with the best possible coverage.

Things to Consider When Evaluating Cyber Insurance Providers:

1. Evaluate the sensitivity of your company's data and the risks you face, as well as the data security rules and regulations that your particular business needs to be compliant with.
2. Consider the policy options, the incidences the different options cover and any limitations on coverage or responses to a data breach.
3. Read reviews and ask for references to see how quickly a provider responds to a data breach.

Best Cyber Insurance Providers:

Our Ranking	Company	A.M. Best Rating	Review
1.	CoverWallet (https://www.thesmbguide.com/coverwallet)	A	Offers an intuitive dashboard where you can file claims 24/7 but some customers have reported slow response times from customer service.

2.	Hiscox (https://www.thesmbguide.com/hiscox-reviews)	A+	Offers industry-specific coverage with 24/7 claims filing but some of their products are only available online.
3.	AIG (https://www.thesmbguide.com/aig)	A	Cyber insurance limits up to $100 million with 24/7 claims filing but they only offer 3 different policy options.
4.	HSB (https://www.munichre.com/hsbcanada/en.html)	A++	Assists with recovering from damage done to data and systems caused by cyber attacks. Company is based in Canada.
5.	Liberty Mutual (https://www.thesmbguide.com/liberty-mutual-cyber-insurance)	A	Offers resources for managing cyber risks but has an annual limit of $50,000.

6.	XL Catlin (https://axaxl.com/)	A	Offers a wide range of insurance products to a variety of industries.
7.	Hackinsure (https://hackinsure.frontrowinsurance.com/)	Not rated.	Offers fast online applications and purchases. Only available to Canadian residents.
8.	Chubb (https://www.thesmbguide.com/chubb-cyber-insurance)	A++	Offers a wide range of cyber insurance policies but lacks live support.
9.	CNA (https://www.thesmbguide.com/cna-reviews)	A	Offers customized coverage options and special services but lacks live chat support.

10.	Beazley (https://www.beazley.com/usa.html)	A	Offers a wide range of insurance products aside from cyber insurance in several countries.

Pros and Cons:

Pros

- Receive financial compensation in the event of a cyber attack that disrupts essential systems.
- Lost data due to a cyber breach may be able to be recovered through the insurance claim process.
- Your business will be able to afford continued service to customers despite a cyber disruption.

Cons

- Not all cyber insurers offer global coverage.
- Rates may be high for companies that do not meet certain security standards.
- Cyber insurance does not limit or prevent cyber-attacks.

Cyber Insurance Comparisons:

CoverWallet vs. Hiscox:

CoverWallet is a complete online insurance marketplace the sells cyber insurance from a number of different providers, including Hiscox, while Hiscox itself is an insurance provider that sells their own coverage options exclusively. Hiscox has flexible cyber insurance options, but small businesses may find more affordable rates by using CoverWallet.



CoverWallet vs. AIG:



AIG offers advanced cyber insurance coverage with tailored threat assessment services, which CoverWallet does not have. However, small businesses can use CoverWallet to obtain competitive cyber insurance quotes from dozens of providers, which could result in finding a more affordable solution than AIG.



AIG vs. Hiscox:

Hiscox's cyber insurance includes coverage for liability, extortion, business interruption, and data recovery. Hiscox also has optional coverage for cybercrime, cyber deception, and social engineering. AIG has all of the same options, plus a 24/7 cyber claims hotline where customers can get advice from network experts.



FAQs:

What is the price range for cyber insurance coverage?

The price of your cyber insurance policy depends on the size of your business and the risks that are unique to your industry. Contact an insurance provider for a cyber liability insurance quote.

What is the AM Best rating?

AM Best rates the financial status of insurance providers. The insurer's financial status reflects its ability to pay out cyber liability claims.

How do I know if my business needs cyber liability insurance?

Consider the dynamics of your business. Do you use computers or mobile devices? Do you store information on those computers? Is the data that you store (https://www.thesmbguide.com/cloud-services) critical to your operations or sensitive to your clients? If you answered yes to any of these questions, you should consider cyber security insurance.

LEXOLOGY

The Coronavirus Pandemic Creates Increased Demand for Cyber Liability Insurance

Newmeyer Dillion

USA | May 28 2020

As a result of the ongoing COVID-19 (commonly referred to as the Coronavirus) pandemic, there has been increased interest and demand to secure cyber liability insurance coverage. With the increase of volume of businesses that have switched to some form of a work from home structure, there has also been an increased volume of phishing, ransomware or other social engineering scams, as well as concerns over data related to COVID-19. Further, businesses have realized that cyber-related losses are most likely excluded under traditional general liability and property policies, and have focused in on analyzing potential exposures and cyber risk management.

On the positive side, the cyber insurance market is competitive with carriers working to offer coverages to meet businesses' needs. Unlike other coverages, cyber liability insurance carriers offer guidance on preventing cyber incidents, such as employing technical security practices and internal back-up and recovery policies. This knowledge is based on experience gained from insurers' responding to voluminous cyber claims. And these preventative measures work in conjunction with policy coverages in the event of a cyber claim.

However, there still can be a number of limitations included in cyber liability policies and coverage varies greatly amongst policies. There is no standard form of cyber insurance coverage and it is important to keep in mind that the specific terms and conditions of the insurance policy itself will dictate whether there is coverage or not for a particular loss. As we have recently noted, areas of coverage concerns may include:

- Limited or no coverage for cyber incidents arising from computer hardware that it is not owned by the insured, such as employee's personal laptops, tablets and other devices.
- Limited or no coverage for social engineering claims such as funds transfer fraud situations.

Why Does This Matter For Businesses

- If you are considering securing a cyber liability insurance policy, have the form policy as well as applicable endorsements reviewed by an experienced cyber insurance coverage attorneys that can identify and understand all available coverages and limitations.
- Such a review should be conducted without delay and prior to binding coverage to confirm that you will actually have the coverage you want to secure during this pandemic.
- Once a cyber liability policy is bound, have the issued policy as well as other company insurance policies reviewed by an experienced cyber insurance coverage attorney to understand how all insurance policies interact with one another and identify potential coverage gaps.
- For California businesses, ensure that any cyber liability policies addresses requirements related to the

California Consumer Privacy Act of 2018 (CCPA) (effective January 1, 2020, with the July 1, 2020 date for enforcement action quickly approaching.

Newmeyer Dillion - Jeffrey M. Dennis and Heather H. Whitehead

Powered by
LEXOLOGY.