



Cyber Insurance Deep Dive: Best Practices and Q&A

- Brian Mahon
- Certified Insurance Counselor
- Cyber COPE Insurance Certification
- 302.275.4591 bmahon@ehdinsurance.com

Agenda

- 1. CYBER THREAT LANDSCAPE**
- 2. CYBER INSURANCE 101**
- 3. BEST PRACTICES**
- 4. Q&A**



CYBER THREAT LANDSCAPE



EXTON | LANCASTER | PITTSBURGH | WYOMISSING

Cyber Threat Landscape (Who)

TYPES OF BAD ACTORS

- APT
- Organized Crime
- Industrial Spies
- Hackers
 - Script Kiddies
 - Worm/Virus Writers
 - Black & White Hat
- Hacktivists
- Insiders



Cyber Threat Landscape (Why)

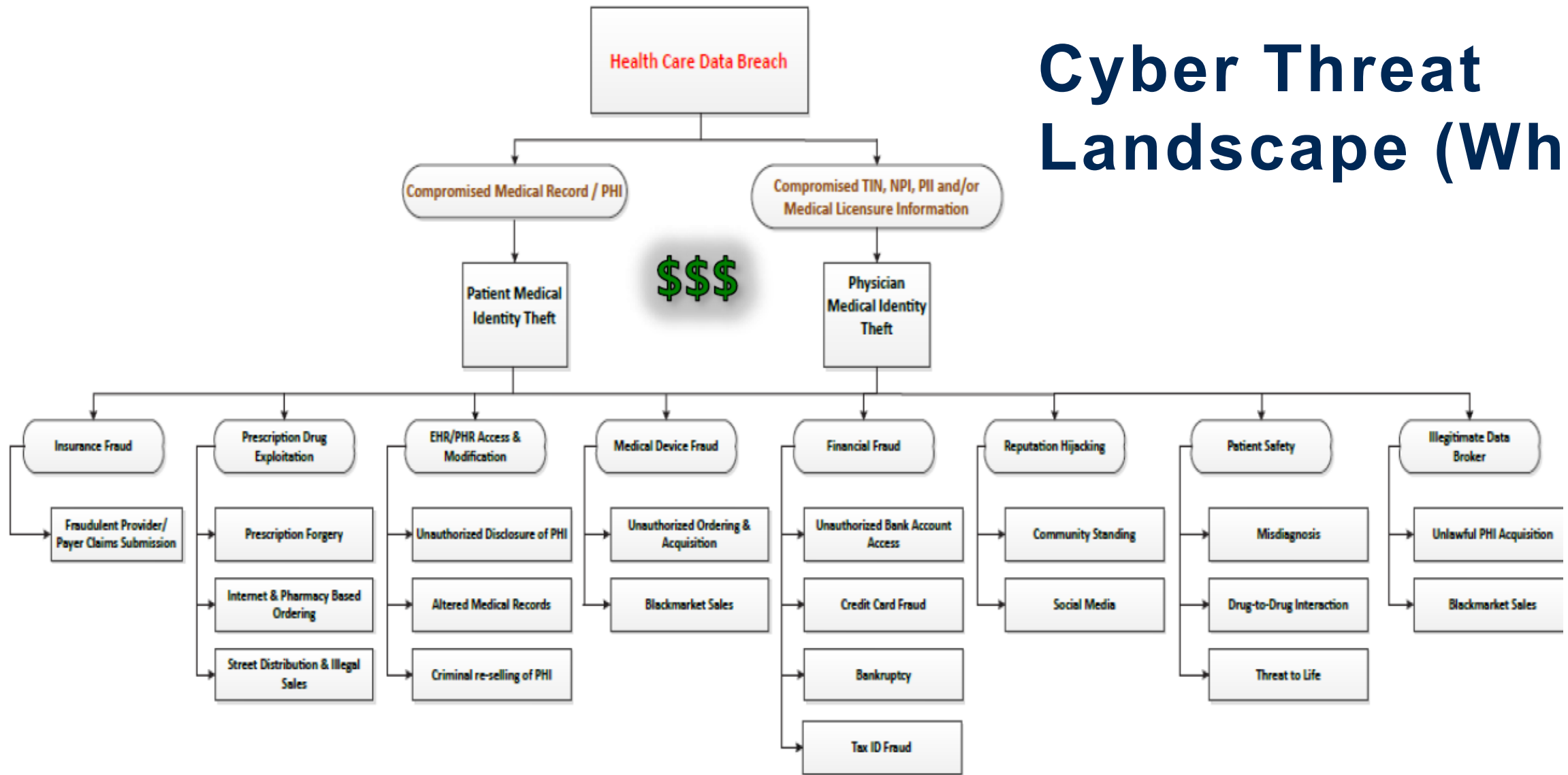


Image Source: Allegheny Digital



Cyber Threat Landscape (How)

Phishing

- \$150 avg cost per record
- 75% Organizations
- 96% Email

Ransomware

- ¼ Victims Pay
- 11s – How Often in 2021
- 51% of Surveyed Business
- 78K Avg Ransom

DDoS Attack

- 150% Increase in 2020
- \$120K - \$2M Costs
- 106 Per Day Average
- 16 DDoS a minute

Insider Threat

- 62% Negligent Insiders
- 43% of Reported Security Incidents
 - \$775,800 Costs

Funds Transfer

- W-2 Fraud
- 815% Increase in 1.5 Y
- \$8.3M reported 1/2018 – 6/2019

Cyberattacks now cost companies \$200,000 on average, putting many out of business

PUBLISHED SUN, OCT 13 2019-10:30 AM EDT | UPDATED MON, MAR 9 2020-11:37 AM EDT



Scott Steinberg
@AKEYNOTESPEAKER

SHARE    

- Forty-three percent of cyberattacks are aimed at small businesses, but only 14% are prepared to defend themselves, according to Accenture.
- These incidents now cost businesses of all sizes \$200,000 on average, reveals insurance carrier Hiscox.
- More than half of all small businesses suffered a breach within the last year.
- Sixty percent will go out of business within six months of being victimized.
- Cyber crime will cost businesses \$5.2 trillion worldwide within five years --- Accenture.

<https://www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html>



2023 FBI Cyber Crime Report

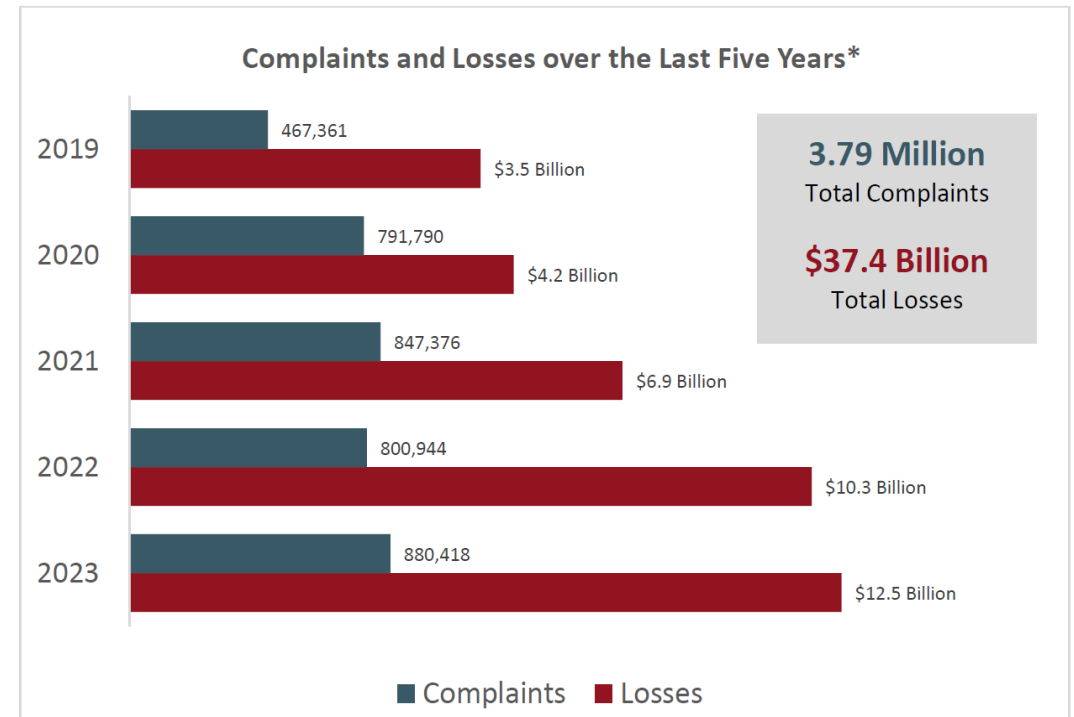
Losses Attributed to Subjects per Destination State*

| Rank | State | Loss |
|------|--------------|-----------------|
| 1 | California | \$1,450,468,117 |
| 2 | New York | \$659,190,424 |
| 3 | Florida | \$460,557,456 |
| 4 | Texas | \$436,917,629 |
| 5 | Washington | \$197,573,721 |
| 6 | New Jersey | \$162,556,627 |
| 7 | Pennsylvania | \$161,290,998 |
| 8 | Illinois | \$160,429,405 |
| 9 | Arizona | \$143,931,864 |
| 10 | Georgia | \$138,867,559 |

IC3 COMPLAINT STATISTICS

LAST FIVE YEARS

Over the last five years, the IC3 has received an average of 758,000 complaints per year. These complaints address a wide array of Internet scams affecting individuals across the globe.³



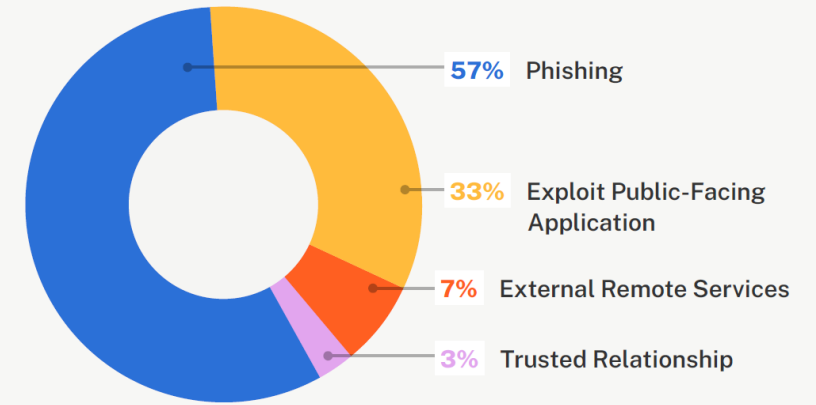
Industry Spotlight: Healthcare

\$10.1 million

Average total cost of a **data breach** for healthcare organizations¹

Cyber Claims in the Healthcare Industry by Attack Vector

KEY INSIGHT — Phishing isn't associated with one event type; it's simply how attackers get into a system. Once inside, they can pursue all sorts of malicious activities, which is why **phishing is the leading attack vector for all cyber claims.**



Source: Coalition forensics survey data

Claims Insights

It's just a little security incident. How bad could it be?

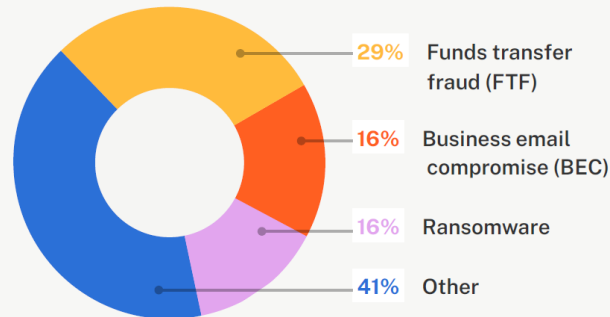
\$134,000

Average cost of a cyber insurance claim for healthcare organizations

Claim Examples

| ORGANIZATION | EVENT TYPE | LOSS |
|-------------------------------|---------------------------|-----------|
| Patient-Centered Medical Home | Funds Transfer Fraud | \$500,000 |
| Behavioral Health Services | Business Email Compromise | \$125,000 |
| Medical Equipment | Ransomware | \$275,000 |

Cyber Claims by Event Type



Source: Coalition claims data

KEY INSIGHT — Although it's not the leading event type, the average ransomware loss for organizations in the healthcare industry is nearly \$355,000.

UNIQUE EXPOSURES

- PHI
- EMR SYSTEMS
- IOT MEDICAL DEVICES
- PAYMENT PROCESSING
- TELEMEDICINE
- END OF LIFE HARDWARE/SOFTWARE
- PATIENT PORTALS
- BIOMETRIC DATA

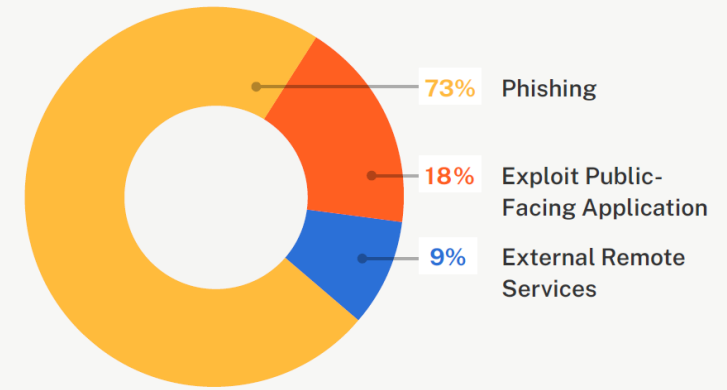
Industry Spotlight: Non-Profit

\$2.6 million

Average total cost of a **data breach** for nonprofit organizations¹

Cyber Claims in the Nonprofit Industry by Attack Vector

KEY INSIGHT — Phishing isn't associated with one event type; it's simply how attackers get into a system. Once inside, they can pursue all sorts of malicious activities, which is why **phishing is the leading attack vector for all cyber claims.**



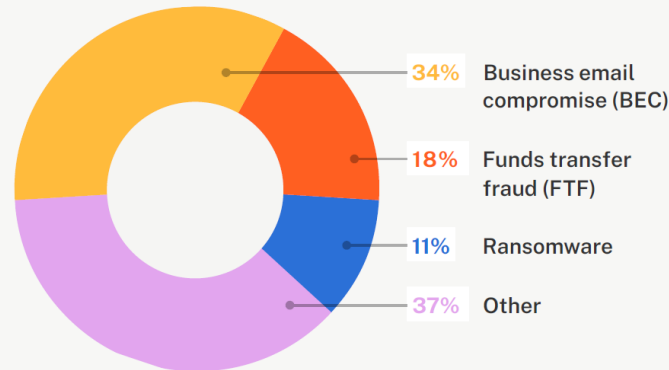
Source: Coalition forensics survey data

Claims Insights *It's just a little security incident. How bad could it be?*

\$110,000

Average cost of a cyber insurance claim for nonprofit organizations

Cyber Claims by Event Type



Source: Coalition claims data

KEY INSIGHT — Although it's not the leading event type, the average ransomware loss for nonprofit organizations is more than \$365,000.

Claim Examples

| ORGANIZATION | INCIDENT | LOSS |
|-----------------------|---------------------------|-----------|
| Veterans Charity | Funds Transfer Fraud | \$125,000 |
| Social Services | Business Email Compromise | \$155,000 |
| Rehabilitation Center | Ransomware | \$962,000 |

UNIQUE EXPOSURES

- **SOCIAL MEDIA**
- **DMS**
- **ONLINE FUNDRAISING**
- **PII (DONORS, BOARD MEMBERS & VOLUNTEERS)**
- **CASE MANAGEMENT**
- **GRANT APPLICATIONS**

Industry Spotlight: Public Entity



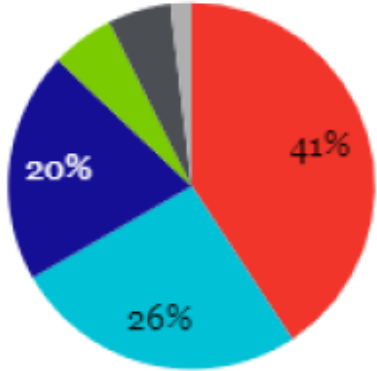
\$2.3 million

Average cost of a data breach for a public sector entity

UNIQUE EXPOSURES

- TAX PAYER DATA (PFI, PII, PHI)
- CLASSIFIED DOCUMENTS
- LIMITED TECHNOLOGY/IT SECURITY BUDGET
- APT/HACKTIVIST TARGETS
- INSIDER THREAT

Actions Causing Cyber Incidents Since 2009
Global, Public Entity and \$25.1M to \$150M

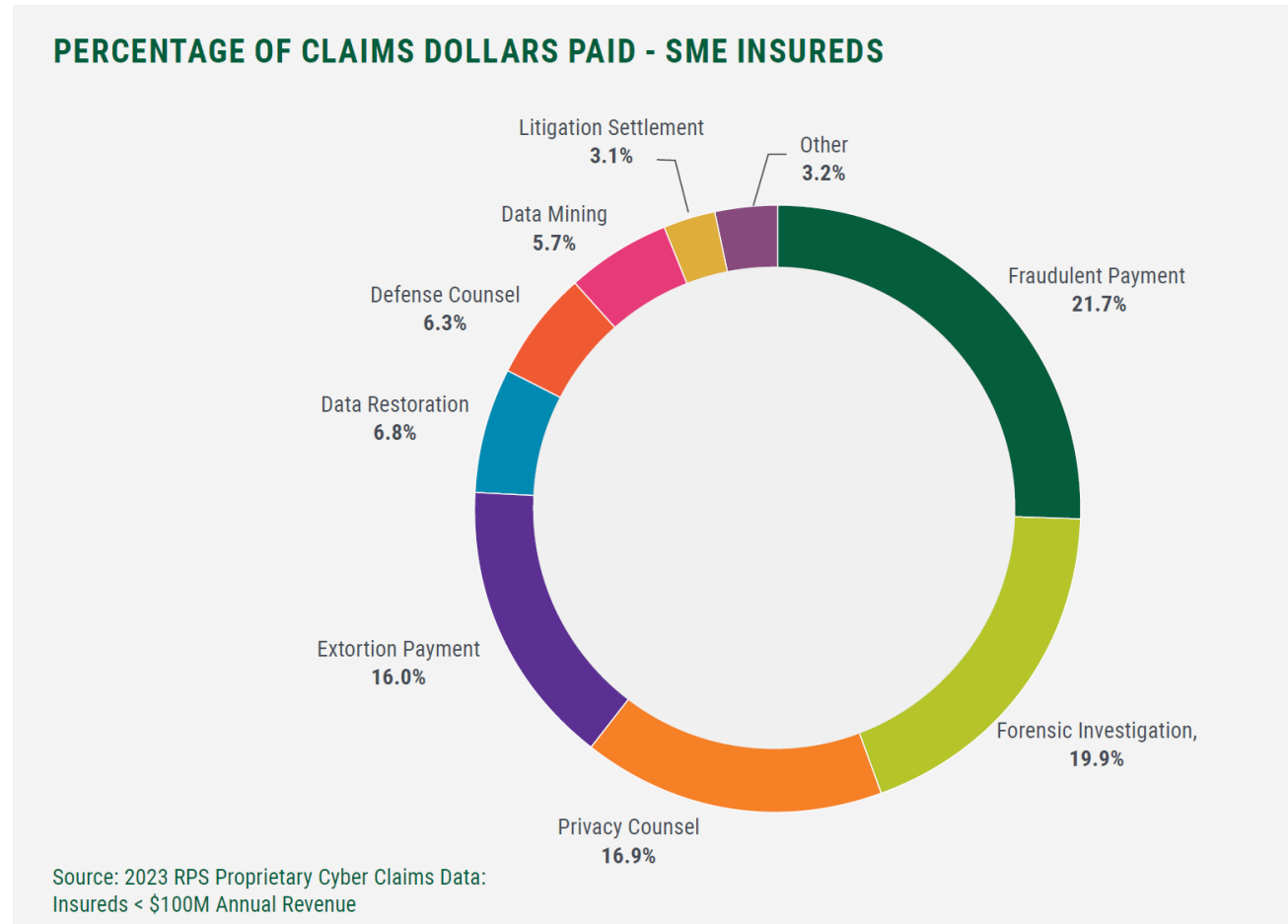
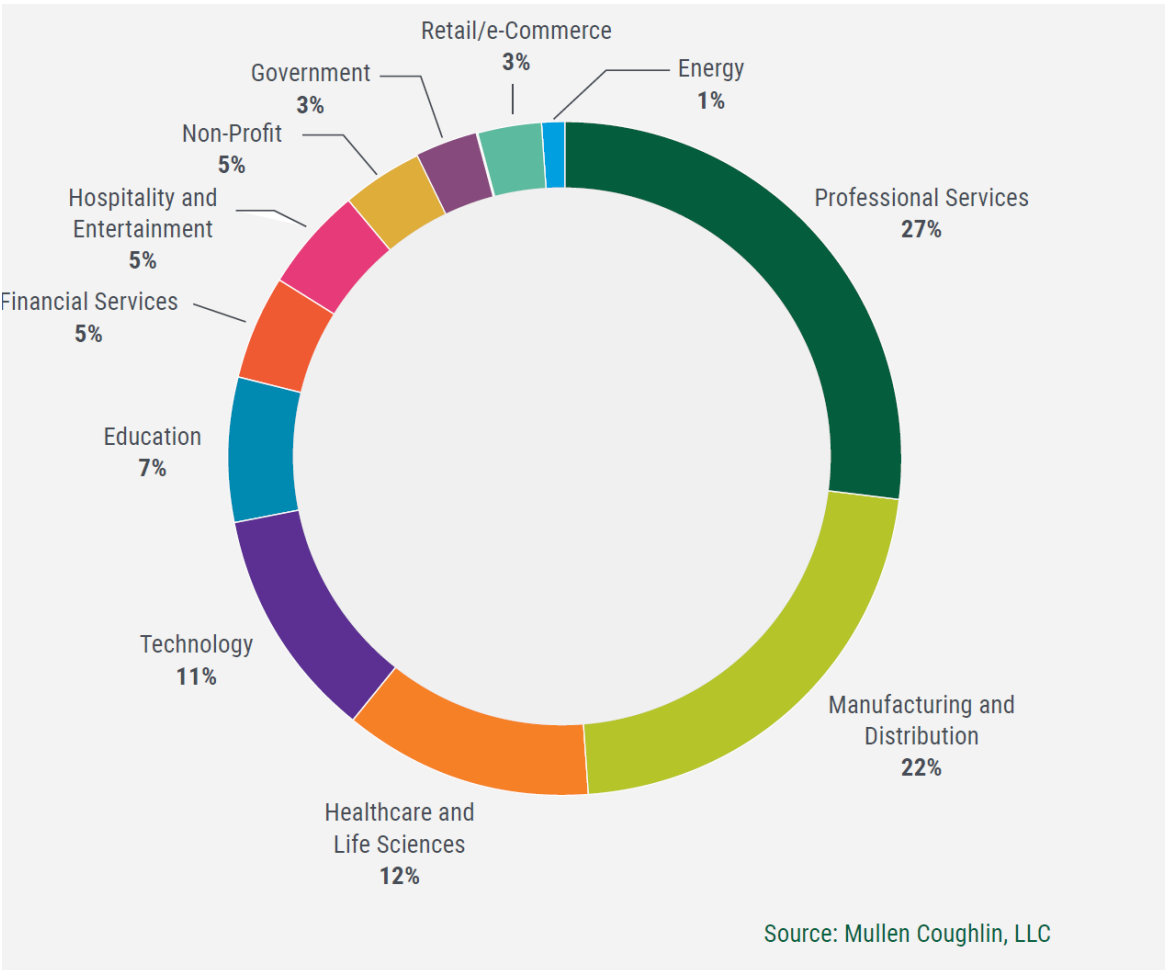


* The data set contains negative or zero value.

Your Selections vs. Overall

| | |
|----------|-------|
| Error | 4% ▼ |
| Hacking | 1% ▼ |
| Malware | 1% ▼ |
| Misuse | 1% ▼ |
| Physical | 3% ▼ |
| Social | 15% ▲ |
| Unknown | 4% ▼ |

Ransomware Activity by Industry

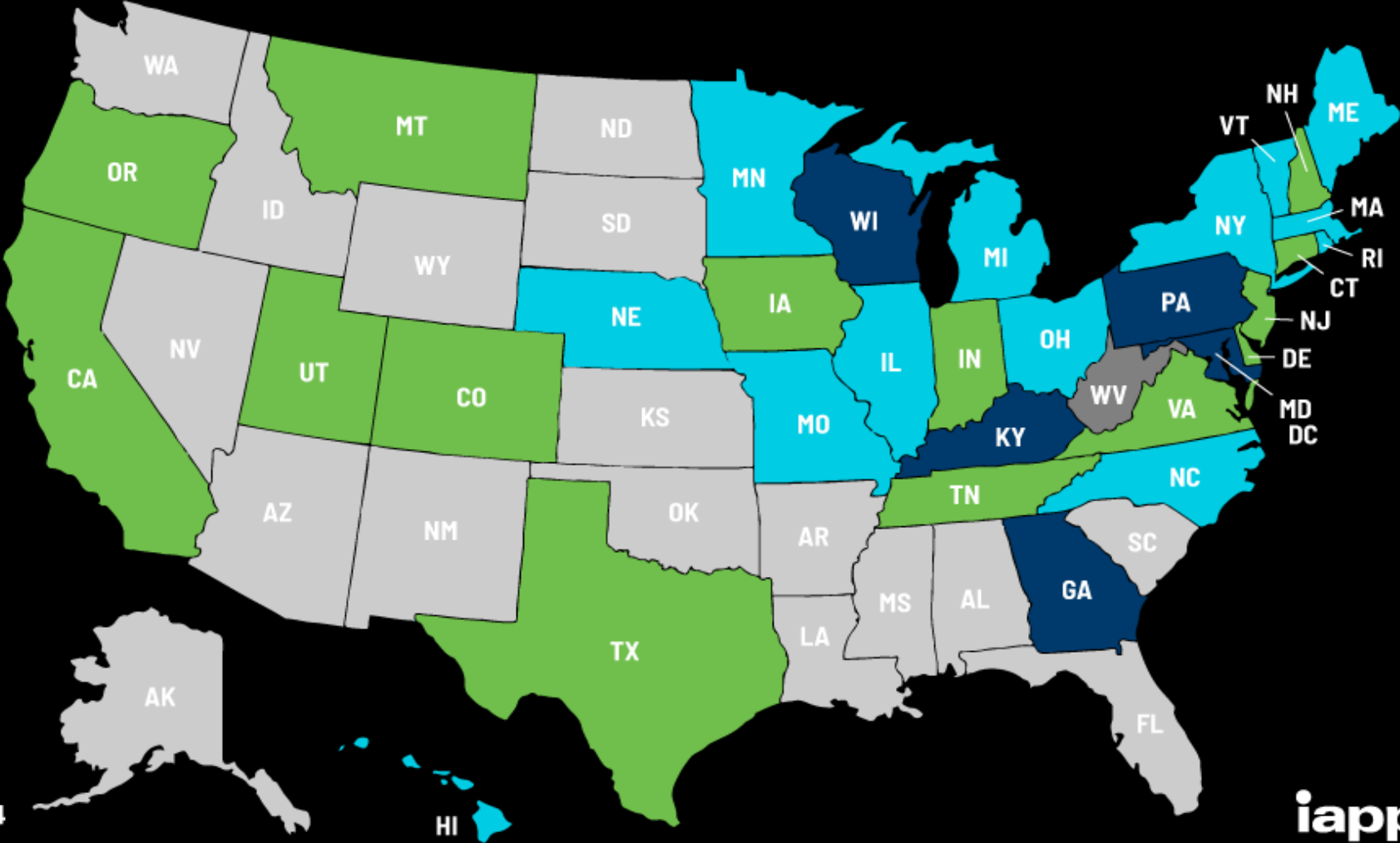


Increased Privacy Laws = Increased Need for Cyber Insurance

US State Privacy Legislation Tracker 2024

Statute/bill in legislative process

- Introduced
- In committee
- In cross chamber
- In cross committee
- Passed
- Signed
- Inactive bills
- No comprehensive bills introduced



Last updated 22 March 2024



Cyber Threat Landscape

PA BREACH OF PERSONAL INFORMATION NOTIFICATION ACT

- Applies to: Any state agency, political org, individual or business in PA that maintains, stores, or manages computerized PI data of PA residents
- PI includes: first & last name in combo with SS#, DL#,DL, bank/credit/debit card numbers in combo with credentials
- Obligated to Notify
- **Fines Calculated: \$1,000 X**
- **[# of individuals who should have been notified]**



Pennsylvania Attorney General Sues Uber Over Data Breach

By [Rahul Mukhi](#) & Kal Blassberger on March 14, 2018

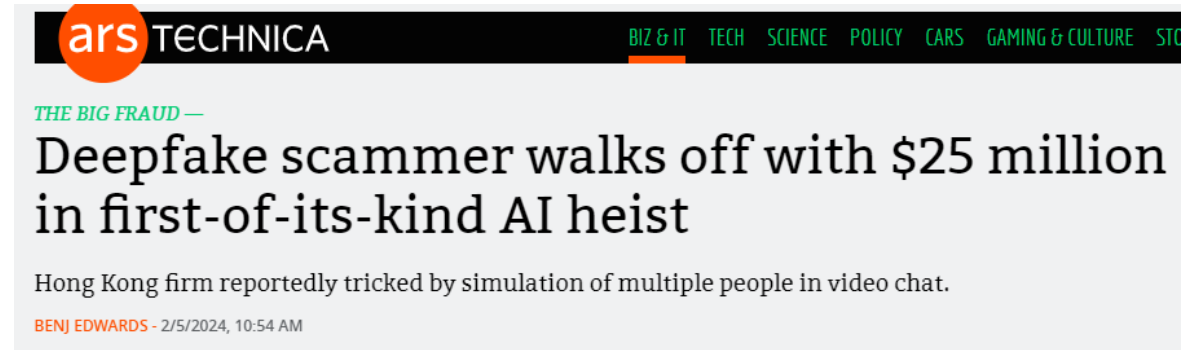
POSTED IN [BREACH NOTIFICATIONS](#), [CYBERSECURITY](#)

Last week, Pennsylvania's Attorney General sued Uber for allegedly failing to provide timely notice to its drivers that their personal identifying information ("PII") had been compromised in a data breach in 2016. The lawsuit seeks **\$13.5 million** in penalties against Uber—\$1,000 for each of the 13,500 Pennsylvanian Uber drivers whose driver's license information [was accessed by hackers](#). The complaint alleges that, in violation of Pennsylvania's data breach notification law,^[1] Uber failed to provide notice "without

Generative AI & Cyber Security



3.4M Talent Gap for Skilled Cybersecurity Professional



Global Cyber Incident Growth

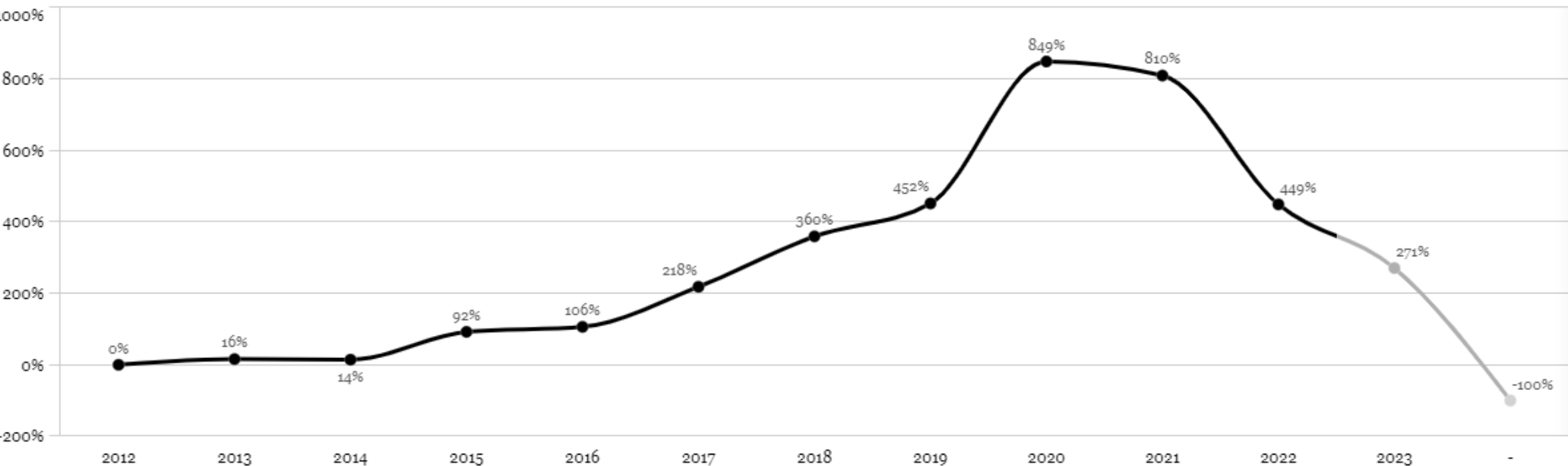
Industries

Revenue Size

Global Incident Growth Compared to 2012*

Global, All Industries, All Revenue Sizes

Industry



Select an Industry for Comparison

Overall

* Please note - this data is indexed against the base line year of 2012 and current year shown in grey is a projection.



CYBER INSURANCE 101



EXTON | LANCASTER | PITTSBURGH | WYOMISSING

What is Cyber Insurance?



**POST-BREACH
V.S.
PRE-BREACH**



Cyber Liability Terminology

STRUCTURE

| |  |  |  |
|---|---|---|---|
| VALID UNTIL | 05/20/23 | 05/20/23 | 05/05/23 |
| ADMISSION STATUS | Non-Admitted | Non-Admitted | Admitted |
| ISSUING INSURER | CFC Underwriting Limited | North American Capacity, Arch... | Clear Blue Insurance... |
| AM BEST RATING Financial strength rating | A (Excellent) | A+ (Superior) A- (Excellent) | A- (Excellent) |
| AGGREGATE LIMIT Maximum amount paid by the insurance company for the duration of the policy | \$1,000,000 | \$1,000,000 | \$1,000,000 |
| RETENTION The same as a deductible, the amount of a claim you pay | \$2,500' | \$10,000' | \$10,000' |

Cyber Liability Terminology

FIRST PARTY

| | | | | | |
|----------------------|--|-------------|-------------|-------------|-------------|
| FIRST PARTY COVERAGE | NOTIFICATION COSTS Cost to notify affected individuals after a data breach | \$1,000,000 | \$1,000,000 | \$1,000,000 | \$1,000,000 |
| | BREACH COSTS INSIDE/OUTSIDE Will the breach costs erode the aggregate limit (inside) or are separate (outside) | Outside | Outside | Inside | Inside |
| | BUSINESS INTERRUPTION Covers lost profits incurred due to not operating | \$1,000,000 | \$1,000,000 | \$1,000,000 | \$1,000,000 |
| | BI WAITING PERIOD Minimum duration of business interruption before coverage starts | 8 hours | 8 hours | 8 hours | 8 hours |
| | CONTINGENT BUSINESS INTERRUPTION Losses from an interruption in 3rd party computer services or software | \$1,000,000 | \$1,000,000 | \$100,000 | \$1,000,000 |
| | DATA RECOVERY The cost of recovering lost data | \$1,000,000 | \$1,000,000 | \$1,000,000 | \$1,000,000 |
| | EXTORTION/RANSOMWARE Covers damage and ransom payments from an attack | \$1,000,000 | \$1,000,000 | \$500,000 | \$1,000,000 |
| | BRICKING When computers and electronic hardware are damaged beyond repair | \$1,000,000 | \$1,000,000 | \$1,000,000 | \$1,000,000 |



Cyber Liability Terminology

THIRD PARTY

| | | | | | |
|----------------------|--|-------------|-------------|-------------|-------------|
| THIRD PARTY COVERAGE | NETWORK SECURITY AND PRIVACY LIABILITY Third party liability costs | \$1,000,000 | \$1,000,000 | \$1,000,000 | \$1,000,000 |
| | PCI Covers fines or penalties imposed by banks or credit card companies | \$1,000,000 | \$1,000,000 | \$1,000,000 | \$1,000,000 |
| | REGULATORY In case you're fined by regulators (e.g., for breaching consumer privacy) | \$1,000,000 | \$1,000,000 | \$1,000,000 | \$1,000,000 |
| | MEDIA When your content triggers legal action against you (e.g. - libel, plagiarism) | \$1,000,000 | \$1,000,000 | \$0 | \$1,000,000 |



Cyber Liability Terminology

CYBER CRIME

| | | | | | |
|-------------|--|------------------------|------------------------|------------------------|------------------------|
| CYBER CRIME | COMPUTER FRAUD Covers funds or property stolen resulting from a hack | \$250,000 ¹ | \$250,000 ¹ | \$100,000 ¹ | \$250,000 ¹ |
| | FUNDS TRANSFER FRAUD When a criminal deceives a bank/institution to transfer funds | \$250,000 ¹ | \$250,000 ¹ | \$100,000 ¹ | \$250,000 ¹ |
| | SOCIAL ENGINEERING When cyber criminals deceive a business to transfer funds willingly | \$250,000 ¹ | \$250,000 ¹ | \$100,000 ¹ | \$250,000 ¹ |



Pre Incident Service Providers



Loss Mitigation Services: Partner Contacts

| Company | Primary Service Capability |
|-----------------------|--------------------------------|
| BitSight | Network Security |
| Cofense | Security Education & Awareness |
| CrowdStrike | Endpoint Security |
| Dashlane | User Account Security |
| Fidelis Cybersecurity | Response Planning |
| FireEye | Security Operations |
| NetDiligence | Network Security |
| RSM | Compliance |
| Skillbridge | Security Education & Awareness |
| StealthBits | User Account Security |

6 FREE CYBERSECURITY RISK MANAGEMENT SERVICES

\$6,000 Market Value

Evolve teamed up with specialist cybersecurity experts to help strengthen, improve, and protect your organization. Each Evolve policyholder has the benefit of using the following services at no additional cost:



EVOLVE MGA'S MOBILE APP

THREE CRUCIAL RISK MANAGEMENT SERVICES FOR POLICYHOLDERS + MORE

- **24/7 Dark Web Monitoring**
 - Our mobile app monitors the Dark Web around the clock, alerting you of any stolen credentials tied to your organization in real time.
- **Network Deep Scanning**
 - We continuously scan your network for surface vulnerabilities like exposed RDP ports, notifying you if we uncover risks that are leaving your business exposed to hackers.
- **Phishing Simulation Campaigns**
 - Educate your staff and gain valuable organizational insights by running simulated phishing campaigns designed to challenge your employees' cyber awareness.

In addition to these risk management tools, our app allows insureds to directly message our forensic experts, and even notify a claim directly in the app.



BLACKFOG

ON DEVICE RANSOMWARE PROTECTION

BlackFog's data exfiltration prevention technology stops ransomware! After your trial, meet with BlackFog's VP of Threat Intelligence who will analyze the findings and present you with your customized threat report.



NINJIO

EMPLOYEE CYBERSECURITY AWARENESS VIDEO TRAINING

4 minute "gamified" video episodes on real breaches that train your employees on how to avoid falling victim to hack attacks. Actively train up to 25 employees with this educational software.



CONTROL CASE

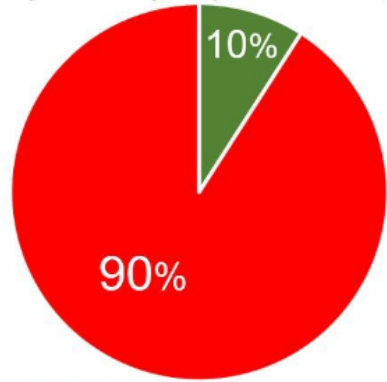
PRIVACY REGULATORY BODY COMPLIANCE AUDIT

Control Case provides a 30 minute consultation to identify if your business' sensitive information properly complies with foreign, federal, state, & private privacy regulatory laws.



Insurer Cyber Risk Services

Only 10% of policyholders use provided risk services



- Using Additional Services
- Not Using Additional Services

Post Incident Service Providers

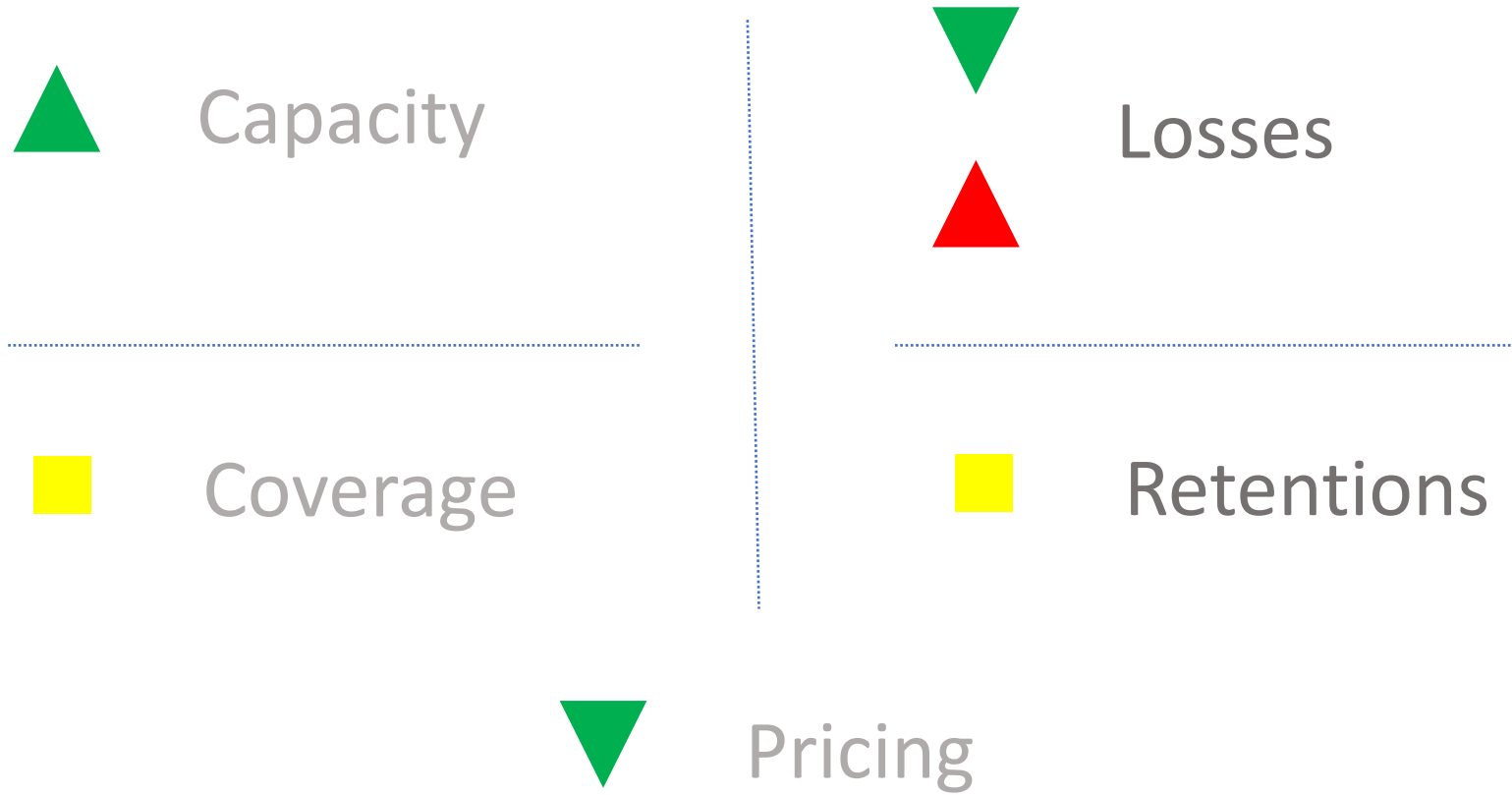
| Company | Primary Service Capability |
|-----------------------|----------------------------|
| BakerHostetler | Response Coach |
| Borden Ladner Gervais | Response Coach (Canada) |
| Cipriani & Werner | Response Coach |
| Fasken Martineau | Response Coach (Canada) |
| Marshall Dennehey | Response Coach |
| Mullen Coughlin | Response Coach |
| Norton Rose Fulbright | Response Coach |

| | |
|--------------------|-----------------------------|
| KPMG | Computer Forensics (Canada) |
| Kroll | Computer Forensics |
| LEVICK | Public Relations |
| NPC | Notification |
| RSM | Computer Forensics |
| Stroz Friedberg | Computer Forensics |
| The Ackerman Group | Extortion |
| TransUnion | Notification |
| Verizon | Computer Forensics |

| | |
|----------------------------------|-----------------------------|
| Allclear ID | Notification |
| Ankura (acquired Navigant Cyber) | Computer Forensics |
| CGI | Computer Forensics (Canada) |
| Charles River Associates | Computer Forensics |
| Cooley LLP | Legal Counsel |
| CrowdStrike | Computer Forensics |
| Crypsis | Computer Forensics |
| Cyintelligence | Computer Forensics |
| Davis Wright Tremaine | Legal Counsel |
| Edelman | Public Relations |
| Epiq | Notification |
| Equifax | Notification (Canada) |
| Experian | Notification |
| Fidelis Cybersecurity | Computer Forensics |
| FireEye | Computer Forensics |

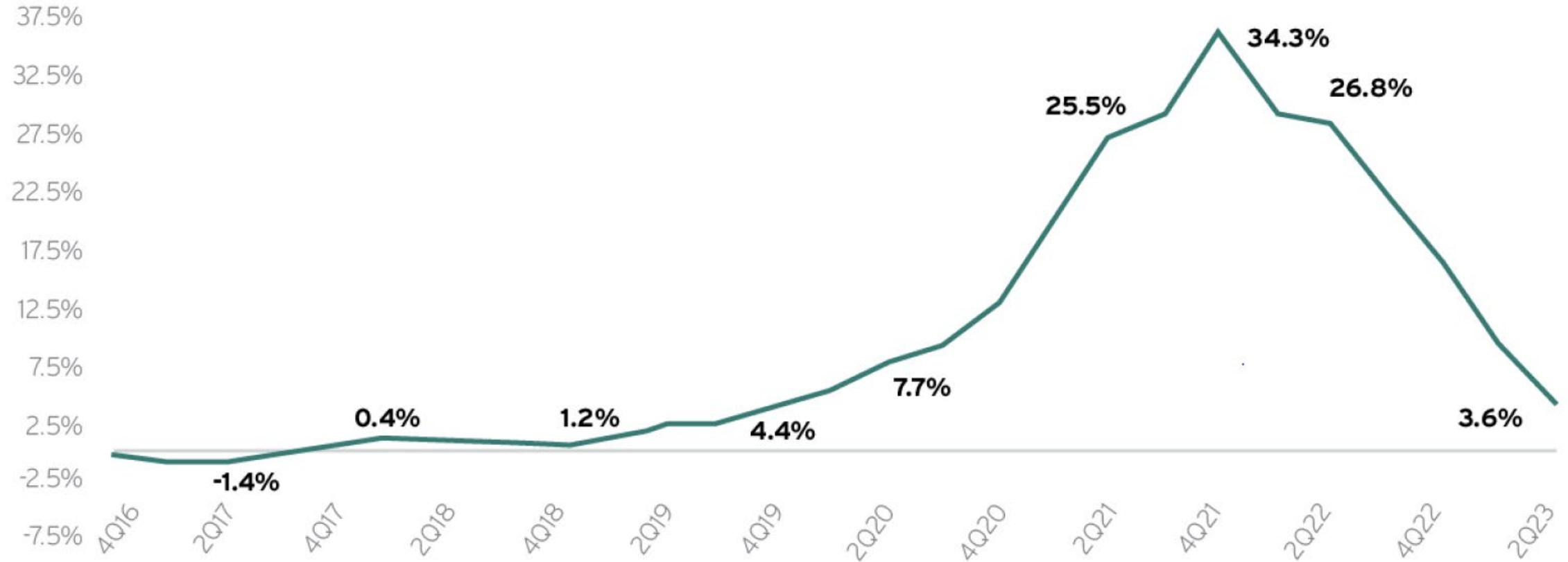


2024 Q1 Update State of the Cyber Insurance Market



2024 Cyber Insurance Premium Outlook

Premium Change for Cyber, Q4 2016–Q2 2023



Source: Council of Insurance Agents & Brokers

2024 Price Prediction:

0% to +15%


2024 Cyber Insurance Coverage Updates

NOT ALL CYBER POLICIES CREATE EQUAL

1. Cyber Crime (Phishing/Funds Transfer Fraud)
2. Ransomware/Extortion
3. Neglected Software
4. Bricking/Hardware Replacement/Betterment
5. Crypto-Jacking

| | | Company Name | | |
|---|--|---|------------------|-------|
| | | Tech E&O/Cyber Insurance Comparison Checklist | | |
| | | Policy Term | | |
| | | EHD | | |
| | | Manage Risk. Maximize Performance. | | |
| What is this? | Option 1 Carrier | Option 2 Carrier | Option 3 Carrier | Notes |
| CYBER LIMITS | | | | |
| Policy Aggregate Limit | The maximum the policy will pay in a given period | | | |
| Deductible | The amount the named insured pays in the event of a claim to activate policy limits | | | |
| Co-insurance | Percentage of a Covered loss that is paid by carrier (The higher the percentage, the more a covered loss will be p | | | |
| Waiting Period | How long the insured must wait for coverage to trigger (The shorter the better) | | | |
| Annual Estimated Policy Premium | The Annual Estimated Cost of the Policy | | | |
| Defense Costs Limits | Are legal claim defense costs included within the policy outside, or submitted? | | | |
| Cyber Crime Coverage | Pays for any claims resulting from electronic funds trans impersonation, phishing, social engineering or electroni identity fraud | | | |
| AM Best | Financial Strength Guide rated from A++ to D | | | |
| Admitted or Non Admitted | Admitted is backed by a state guarantee fund, non admi carriers are not. | | | |
| Coverage Trigger | Policies are written on one of the following to determin what policy period triggers coverage : (Occurrence, Clai Made, or Claims Made & Reported) | | | |
| 1st Party Security Breach Expense/Privacy Notification Expense | Typically includes the costs to notify affected parties, investigate cause of breach, may provide identity theft protection or credit monitoring | | | |
| 1st Party Business Income & Extra Expense | Pays for loss due to an interruption to the named insured computer system resulting from a cyber-related event. | | | |
| 1st Party Contingent Business Interruption/dependent entity | Pays for loss due to an interruption to the named insur key supplier or other dependt parties' computer system resulting from a cyber-related event | | | |
| 1st Party Extortion Threat, Ransom Payment or Rewards Payment | Pays for loss due to an extortion threat. Extortion threat where a business's computer system is being held host typically with a message demanding payment in exchan for system restoration | | | |
| 1st Party Public Relations/Reputational Harm/Crisis Management Expense | Pays for cost of a PR firm to protect/restore named ins reputation tdue to negative publicity resulting from a cy event | | | |
| 1st Party Replacement/Restoration of Electronic Data/Cyber Vandalism | Typically pays for the cost to replace or restore the nam insured's electronic data which has been destroyed or corrupted as a result of a cyber event | | | |
| 3rd Party Privacy Liability | Pays for claims from a third party in the event of a relea non-public information in violation of a person's right to privacy, often Personal Financial Information, Protected health Information or Personally Identifiable informatio | | | |
| 3rd party Content/Web Publishing/Multi Media Liability | Typically provides broader "digital coverage" for Person Advertising Injury Liability, which covers 3rd party claim infringement or violation of another's copyright, title, si trademark, trade name, trade dress, service mark, or see name, unauthorized use of images or music, disparagmei defamation, libel, slander, and wrongful imprisonment o detainment | | | |
| 3rd Party Security Breach Liability/Information Security/Network Breach Liability | Pays for claims resulting from 3rd party liability resultin from responsibility of a virus, security breach, or transmi of malicious code. | | | |

June 2021



THE BETTERLEY REPORT

CYBER/PRIVACY INSURANCE MARKET SURVEY—2021

*Ransomware Claims Are a Huge Problem—
How Long Will Insurers Be Able To Continue this Coverage?*

Richard S. Betterley, LIA
President
Betterley Risk Consultants, Inc.

Highlights of this Issue

- Difficult Renewals Expected
- Insurers Report on How They Treat Ransomware Retentions
- Pandemic-Related Coverage Enhancement and Exclusions Insights from 21 Insurers
- Rates Are Increasing, and Maximum Limits Are Decreasing—Ransomware Is a Huge Problem
- New Insurers Added: Celerity Pro and Resilience
- Insurers Removed from Survey: The Hartford

Next Issue

August 2021

Private Company Management Liability Insurance Market Survey



Neglected Software Endorsement

It is agreed that the **Policy** is amended as follows:

- Item 4 of the Declarations is amended by adding the following:

| Period of Neglect | Coinsurance | Limit of Insurance per Policy Period |
|----------------------|-------------|---|
| 0 – 45 days | 0% | \$<LIMIT01> |
| 46 – 90 days | 5% | \$<LIMIT02> |
| 91 – 180 days | 10% | \$<LIMIT03> |
| 181 – 365 days | 25% | \$<LIMIT04> |
| Longer than 365 days | 50% | \$<LIMIT05> |

MORE CITRIX BLEED CASUALTIES —
Xfinity waited 13 days to patch critical Citrix Bleed 0-day. Now it's paying the price
Data for almost 36 million customers now in the hands of unknown hackers.
DAN GOODIN · 12/19/2023, 6:14 PM

Brian Mahon, CIC, CCIC · You
Certified Cyber Insurance Counselor
3mo · 🌐

The "IT Guy Asleep at the Wheel" endorsement strikes again!

This time, quite close to home, to a large telecom company based out of #philly While they weren't the only ones affected by the "#CitrixBleed" Vulnerability, let me explain...

https://lnkd.in/eBfPPP_z

You may not realize this, but there is an entire underground industry built off discovering, selling/buying, and utilizing "#zeroday exploits" which is a type of vulnerability that is a new/unknown ...see more

👍 8 2 comments · 1 repost

Like Comment Repost Send

📊 446 impressions View analytics

Add a comment...



How do Cyber Underwriters Rate my Cyber Insurance Policy?

- 1. Industry**
- 2. Revenue**
- 3. Type & Amount of Data**
- 4. Loss History**
- 5. IT Controls**



2023 Cyber Security Control Requirements for Cyber Insurance Underwriting

RED

Minimum standard of security required for underwriters

- Multifactor authentication (MFA) for employee email
- MFA for remote access
- MFA for privileged accounts/privileged access
- Offsite (preferably offline) backups of critical data.
- Deploy an endpoint detection and response (EDR) solution on all managed endpoints (Underwriter requirements for EDR solutions depends largely on the insured's revenue)
- Create an audited written plan for patching critical software and hardware
- Employee cybersecurity training, including phishing simulations

AMBER

Requirements over and above red—more attractive to underwriters

- Strong email filtering tools
- Privileged access account security measures
- End-of-life (EOL)/unsupported software and hardware segregated from the network, with plans to decommission in a timely fashion (This can be classified as “Red” for some underwriters)
- Cyber-incident disaster recovery/incident response plan, and segmentation of your computer network by operational function, data classification and operational risk
- Local domain control turned off on all owned managed endpoints

GREEN

Requirements over and above amber—most attractive to underwriters

- Password management
- Detailed asset footprint of particular service accounts with domain credentials, services and monitoring
- Security information and event monitoring (SIEM) tool
- Data loss prevention (DLP) tool
- Follow an information security framework
- Maintain a 24/7 Security Operations Center (SOC) internally or externally

MDR



Managed detection and response is an outsourced cyber protective service that combines advanced technology and human knowledge to actively seek, detect, monitor and respond to cyber threats.

At-Bay acknowledged the impact of MDR by saying an "MDR solution could help prevent or mitigate the losses of more than 50% of cyber insurance claims"



More Scrutiny on Recommended IT Security Policies

External-Facing

Website Privacy Policy

Website Terms of Use

Internal-Facing

Data Security Policy

Data Breach Response Policy

Data Classification Policy

Document Retention/Destruction Policy

Acceptable Use Policy

BYOD Policy

Remote Access Policy

Credit Card Handling Policy

Vendor Selection/Management Policy

Wire Transfer Policy

IT-Facing Policies

Physical Security Policy

Asset Management Policy

Change Management Policy

Password Policy

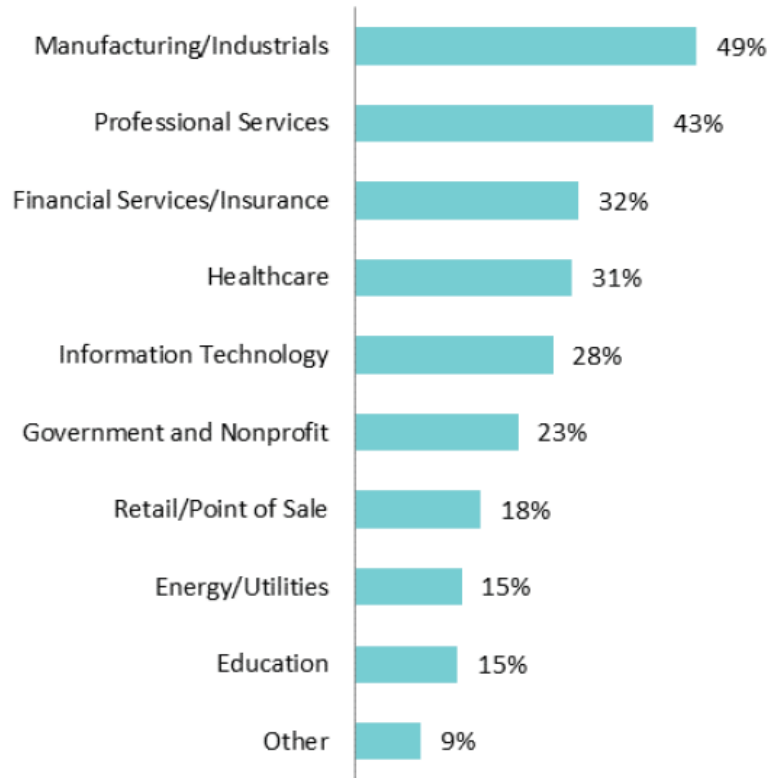
Backup Policy

Website ADA Accessibility Policy



Cyber Insurance by Industry

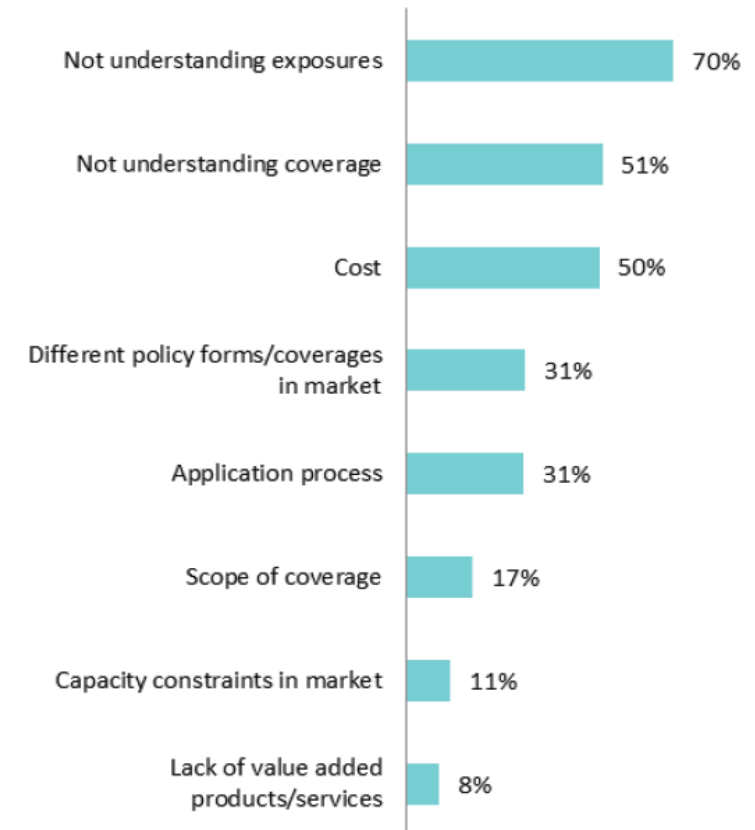
What industries brought the most new-to-market buyers of standalone cyber insurance?



What is the top driver(s) of new/increased cyber insurance sales?



What are the biggest obstacles to writing/selling cyber insurance?



TIPS, TRICKS, BEST PRACTICES, Q&A



EXTON | LANCASTER | PITTSBURGH | WYOMISSING

Cyber Insurance Application Process

1. **How are you mitigating risks?**
2. **Be as thorough and descriptive as possible**
3. **Use an addendum if necessary to further explain any “no” answers**
4. **Explain and describe any updates that have been performed or are expected to be performed**

Travelers Wants Out of Contract With Insured That Allegedly Misrepresented MFA Use

By Chad Hemenway | July 12, 2022



Email This | Subscribe to Newsletter



[Travelers Wants Out of Contract With Insured That Allegedly Misrepresented MFA Use \(insurancejournal.com\)](https://www.insurancejournal.com)



Tips for Cyber Insurance Buyers

- 1. Work with insurance professionals that understand cybersecurity**
- 2. Work with IT professionals that understand cyber insurance**
- 3. Start early**
- 4. Take advantage of pre-incident loss control services offered by current carriers**
- 5. Put the 365/24/7-incident response hotline # from your policy in your cellphone**
- 6. Invest in IT controls, like security/awareness training, pen tests, MDR, MFA etc. (See slide 30)**
- 7. Invest in IT processes and procedures (see slide 32)**



Incident Response Best Practices

- 1. Do not be afraid to call insurance carrier**
 - 1. (notice of circumstance versus a claim)**
- 2. Get Panel Providers Pre-Approved**
- 3. Do not destroy logs (crime scene)**
- 4. Do Act Fast**
- 5. Do Reference Incident Response Plan**
- 6. Do Communicate frequently with DBRP Team**



How to Evaluate Your Cyber Insurance Agent

Basics

1. Licensed
2. Credentialed
3. Reviews & Complaints
4. AM Best

Advanced

1. Service timeline
2. Technology
3. Industry Specific Knowledge

Questions to Ask

1. How many cyber insurance policies do you write?
2. Have you been Involved in any cyber claims?
3. What proactive services will you offer to keep me out of trouble?

<https://www.brianmmahon.com/post/is-my-insurance-broker-agent-good-how-to-evaluate-your-insurance-agent-broker-in-the-internet-age>



Cyber Insurance Carrier Tiers

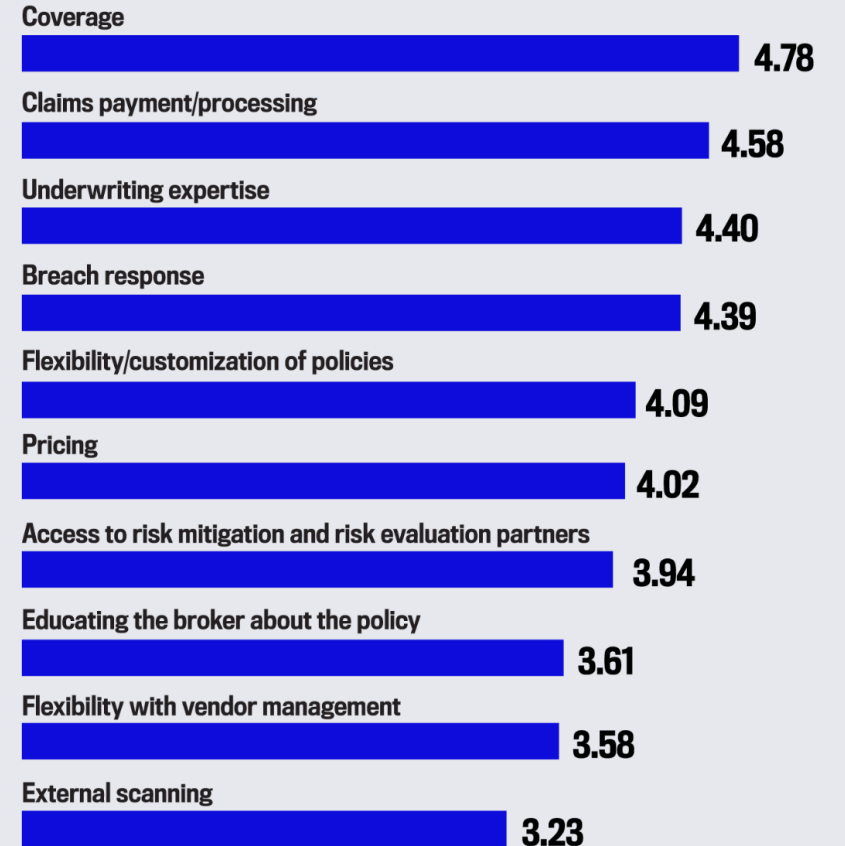


TOKIO MARINE



MOST IMPORTANT ATTRIBUTES RATED BY BROKERS WHEN PLACING A CYBER POLICY

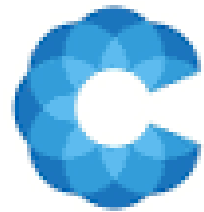
1 = not at all important, 5 = very important



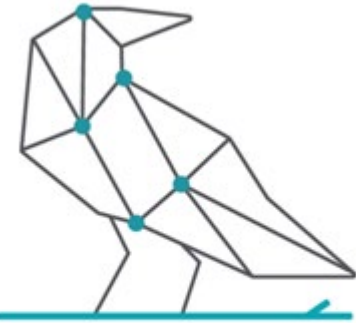
<https://www.insurancebusinessmag.com/us/>

Cyber Insurance Carrier Tiers

at
— bay



Coalition®



CORVUS



Q&A – Thank You!



Cyber Insurance Deep Dive: Best Practices



- Brian Mahon
- Certified Insurance Counselor
- Cyber COPE Insurance Certification
- 302.275.4591 bmahon@ehdinsurance.com

