



ProWriters

Professional & Management Liability Insurance

Introduction to Cyber Insurance in 2023

Introduction

- The history of cyber insurance
- Client exposures for certain industries
- A dissection of cyber insurance coverage
- Cyber underwriting
- Claims and incident response
- The state of the market in 2023 and beyond
- Providing guidance to clients
- Q&A
- Closing remarks

The History Cyber Insurance - The Late 90's

- The first cyber / internet policies start to appear in the market.
 - Many take credit for writing the first cyber policy.
- Some of the first stand alone products only covered liability from a Hack of a 3rd Party.

The History Cyber Insurance - Early 2000's

- Later versions covered breaches occurring at the insured.
 - They had many exclusions:
 - Rogue Employee
 - Regulatory
 - Fines & Penalties
 - No First Party Coverage

The History Cyber Insurance - Mid 2000's

- Added Coverage for 1st Party
 - Cyber Business Interruption
 - Cyber Extortion
 - Network Asset Damage
- Added sublimit for HIPAA Liability

The History Cyber Insurance - CA Security Breach Information Act

- Effective July 1, 2003
- Requires a business or agency that conducts business in CA to notify affected residents of CA of any breach if personal information was or is reasonably believed to have been accessed by an unauthorized person.

The History Cyber Insurance - CA Security Breach Information Act cont.

- Personal Information means an individuals first or last name in combination with a Social Security number, drivers license number; or account, credit or debit card number in connection with an access code or password.

The History Cyber Insurance - The results

- Many states follow in adding similar laws.
- This resulted in new coverages being offered.
- New 1st Party Coverages:
 - IT Forensics, PR, Credit Monitoring / Repair, Customer Notification.
- New 3rd Party Coverages:
 - Regulatory Defense & Fines / Penalties

The History Cyber Insurance - Late 2000's

- Many of the new coverage's offered were only available with strict sub-limits.
- This made excess placements difficult.
- Each carrier had a very different appetite
- Each carrier had different hot button issues
- Each carrier had very different views on Cyber Risk.

The History Cyber Insurance - 2010's

- The number of carriers with stand alone products has grow north of 50 into the 60's
- 2014 – Year of the retail Breach
- 2015 – Year of the Healthcare Breach
- Products continue to evolve
- Carriers have changing appetites in response to breaches

The History Cyber Insurance - State of the Market in 2016

- Leading carriers in a better position than those with small market share.
- Pricing is still volatile.
- Coverage terms still differ greatly.
- Movement towards providing more Risk Management Services with the policy.

The History Cyber Insurance - State of the Market in 2016 cont.

- There are many differences between small business and large accounts.
 - As far as the right market
 - As far as the number of questions asked
 - Broad Coverage vs. Narrow / Skinny coverage
- Real expertise is hard to come by.

The History Cyber Insurance - State of the Market in 2017-2020

- Significant market growth
 - Large risks expanding coverage and limits
 - Smaller risks starting to buy policies
 - More services available for SME business
- New Entrants – Insuretechs launch

The History Cyber Insurance - State of the Market in 2021 - 2023

- The market hardens
 - Reinsurance rates go up
 - Capacity shrinks and dries up for poor risks
 - Carriers focus on mandatory controls
 - New services, new automation, security scans are prevalent
- Comparative rating goes mainstream

Client Exposures for certain industries

- All businesses, but here are some of the top classes:
 - Technology risks
 - Transportation and warehousing
 - Retail trade
 - Manufacturing
 - Public administration
 - Professional services
 - Healthcare & social assistance
 - Accommodation and food services
 - Entertainment & recreation
 - Education

Client Exposures for certain industries - Who is at risk?

- Any business that uses computers / technology
- Businesses that hold healthcare or credit card data
- Any business that would be harmed by a disruption to their computers and tech enabled parts of their business
- Any business with consumer data
- Any business that uses computer make payments – wires, ACH, checks, etc.
 - Email is a gateway to social engineering events

A Dissection of cyber insurance coverage

- 1st Party
 - IT Forensics
 - Customer Notification
 - Call Centers
 - Credit Monitoring
 - Ransomware
 - Business Interruption (Dependent, System Failure)
 - Network Asset Damage
 - Crime & Social Engineering
- 3rd Party
 - Defense and Indemnity from customers (Network Security / Privacy Liability)
 - Defense and Indemnity from regulators (Breaches, Privacy Law Violations like GDPR)
 - Defense and Indemnity for PCI Fines & Assessments
 - Media Liability
- Vendor Panel
- Cyber Risk Management Services

Cyber underwriting

- Applications
- Ransomware supplements
- What type of data does an insured have?
- How much data does an insured have?
- What kind of controls do they have around the data?
- What are the impacts from a business interruption event?

Claims & Incident Response

- Data breach
- Regulatory investigations
- IT forensics
- Ransom payments

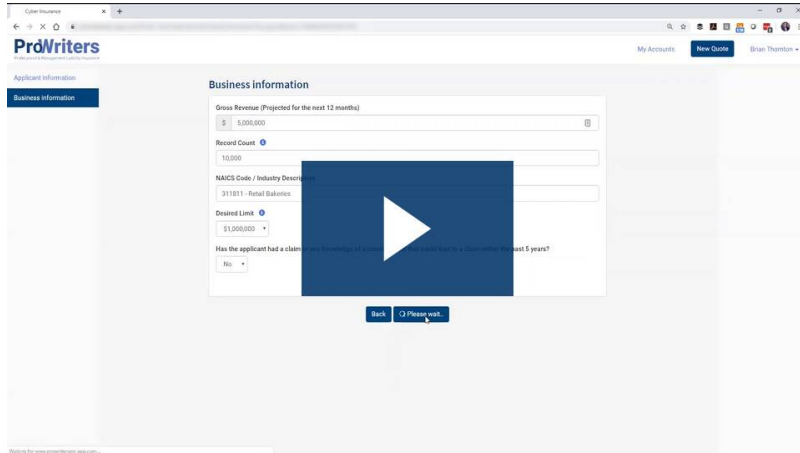
The state of the market in 2023 and beyond

- Significant claims
- Capacity reductions
- Policies being non-renewed
- Major price increases 50% on larger accounts / 20% on smaller business
- Classes that are impossible to place (Municipalities, Casinos, Schools, MSPs)
- Declinations related to controls, lack of MFA, Endpoint Protection
- Cyber risk management services

Providing guidance to clients – Cyber Risk Management

- Focus on cyber risk management, what can a client do to manage and improve their cyber risk posture?
 - Enable Multi Factor Authentication – for email, remote network access, privileged users
 - Cloud based backups / segregated backups – enables clients to get back up and running sooner
 - Add a secure email gateway (SEG) – Barracuda, Proofpoint, Mimecast
 - Dual authorization for fund transfer
 - Call to confirm payments prior to transfer
 - Don't call the number on the invoice or in an email
 - Use a password manager
 - Added email and website security – DMARC (Domain-based Message Authentication, Reporting, and Conformance) SPF (Sender Policy Framework)
 - Employee training / awareness
 - **Add a cyber insurance policy**
- Partner with an expert

Demo



The screenshot shows a web browser window with the ProWriters logo and navigation links. The 'Business Information' form is displayed with the following fields:

- Gross Revenue (Projected for the next 12 months): \$ 5,000,000
- Record Count: 10,000
- NAICS Code / Industry Description: 511011 - Retail Electronics
- Desired Limit: \$1,000,000
- Has the applicant had a claim and/or knowledge of a claim that was paid or is a claim within the past 5 years?: No

A video player overlay is centered on the form, featuring a large white play button on a dark blue background. Below the video player are 'Back' and 'Next' buttons. The 'Next' button is highlighted with a mouse cursor.

[Professional & Management Liability Services | ProWriters](#)

Questions?

- Questions?

Closing Remarks

- Get educated
- Partner with experts
- Address the exposure, it is not going away

Thank you

- Contact us with any questions
- info@prowritersins.com

Or

- Brian Thornton
- Brian.Thornton@prowritersins.com
- (w) 484-321-2342
- (m) 610-701-1484