



AUGUST 7-8, 2024
BRIEFINGS

Strengthen Cybersecurity by Leveraging Cyber Insurance

Speaker: Bridget Quinn Choi Esq. of Woodruff Sawyer, Cyber Broker



WOODRUFF
SAWYER

Bridget Quinn Choi

Current Role: Head of Product for Woodruff Sawyer

Experience: Attorney, Cyber Consultant/DFIR, Claims, and Underwriting

Contact: bchoi@woodruffsawyer.com





black hat[®]

USA 2024



WOODRUFF SAWYER

We are champions for your success.



Privately Held

Service-first and resource-rich



Nationwide & Worldwide

12 US offices; Assurex & IBN presence on 6 continents



Worldclass Service

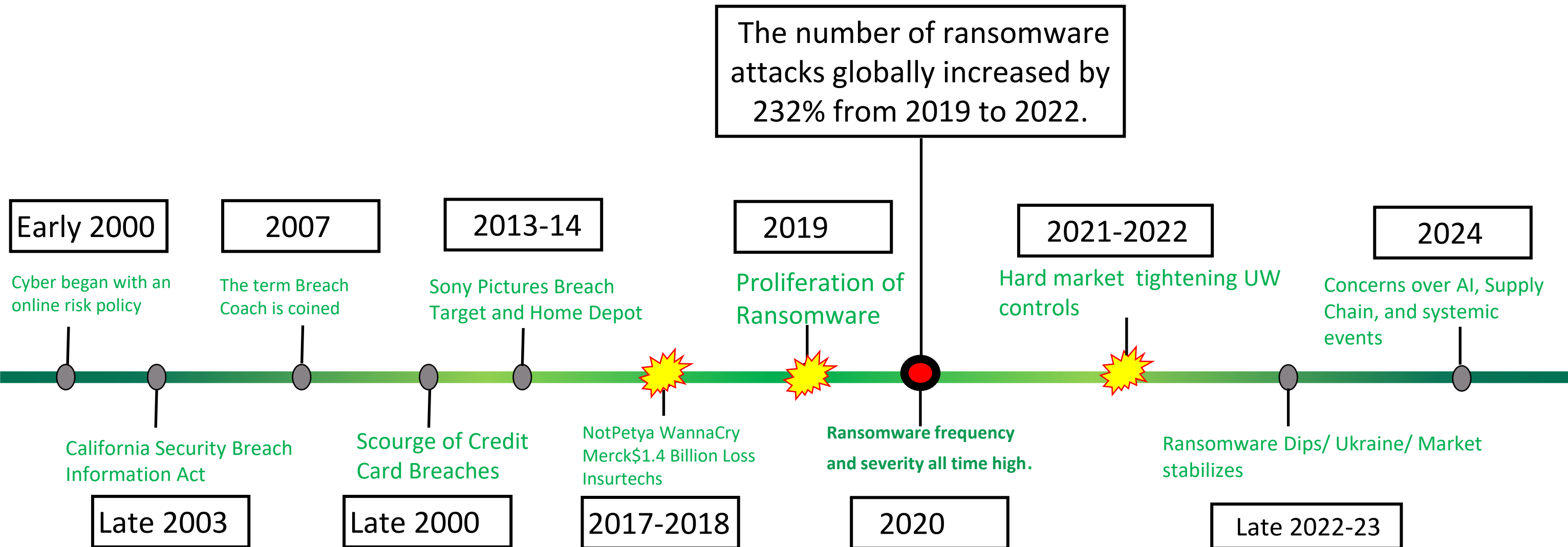
Service ranked world-class by NPS client satisfaction survey



Comprehensive

Cyber, D&O, P&C, Benefits, Private Client

Cyber Insurance Industry Timeline



Roles and Relationships



Policyholder

- Numerous stakeholders including CEO, CISO, RM, GC, audit committee, board
- Different perceptions of what cyber insurance is and how it works
- Varying lines of communication and decision-making hierarchy



Broker

- Represents the policyholder in the insurance marketplace
- May not always have the upper hand in coverage negotiations (depending on market conditions)
- Should (ideally) be able to act as a translator between InfoSec and Underwriting



Insurance Carrier

- Determines policy terms, conditions, pricing, and exclusions (to be managed and improved by broker)
- Does substantial work vetting and QA on IR panel vendors
- Will (usually) govern policy response and payment during and after an incident



Incident Response Panel

- Pre-approved breach counsel, DFIR, PR, and restoration firms
 - Exceptions need approval
- Serve two masters: policyholder and insurer
- Best possible chance to reduce litigation and regulatory risk

Dynamic cyber risk demands coverage that can keep apace with the risk

2020 RANK	2019 RANK	GROUP NAME	DIRECT WRITTEN PREMIUM	LOSS RATIO W/DCC	MARKET SHARE
1	1	CHUBB LTD GRP	\$404,144,104	61%	14.7%
2	2	AXA INS GRP	293,025,192	98.2%	10.6%
3	3	AMERICAN INTRNL GRP	228,424,711	100.6%	8.3%
4	4	ST PAUL TRAVELERS GRP	206,817,208	85.5%	7.5%
5	5	BEAZLEY GRP	177,746,192	47.9%	6.5%
6	6	AXIS CAPITAL GRP	133,549,784	46.2%	4.8%
7	7	CNA INS GRP	119,612,168	105.7%	4.3%
8	10	FAIRFAX FINANCIAL	108,687,558	55.7%	3.9%
9	11	HARTFORD FIRE 7 CAS GRP	102,864,503	25.4%	3.7%
10	8	BCS INS GRP	86,582,699	59.1%	3.1%
11	14	TOKIO MARINE HOLDINGS INC GRP	78,160,355	51.1%	2.8%
12	12	SOMPO GRP	72,588,641	114.1%	2.6%
13	13	ZURICH INS GRP	64,430,818	40.4%	2.3%
14	9	LIBERTY MUT GRP	41,856,727	30%	1.5%
15	18	APOLLO GLOBAL MGMT GRP	39,338,993	29.6%	1.4%
16	15	BERKSHIRE HATHAWAY	37,366,878	25.8%	1.4%
17	19	MARKEL CORP GRP	29,736,405	38%	1.1%
18	28	EVEREST REIN HOL INC	28,173,404	48%	1%
19	17	CINCINATTI FNCL GRP	24,888,476	24.6%	0.9%
20	25	SWISS RE GRP	23,654,519	42.6%	0.9%

- The top 20 groups in the cyber insurance market reported direct loss ratios in the range of 24.6% to 114.1%. The loss ratio for 2020 for the top 20 groups averaged 66.9%, up from 44.6% in 2019.
- During 2020, the top 10 U.S. groups wrote almost 68% of the cyber insurance market.
- The top 20 U.S. groups writing standalone and package cyber insurance combined are listed in the table.

How to make your insurance work for you?



Partnerships

- DarkWebIQ
- EDR Discounts
- Consultant Discounts on resilience planning and assessments
- Free ransomware readiness briefings or how to get budget out of a CFO



Broker

- Use modeling platforms to give you benchmarking for breach costs
- Consultants on staff that help guide you to broader coverage for less premium
- Cyber maturity benchmarking
- Free threat intel
- Free advisory services
- Platforms that can both help provide a baseline, benchmarking, and validations
 - Spektrum
 - Safeonline



Insurance Carrier

- Threat intelligence
- Attack Surface management
- Notification of CVE
- Active remediation of exploits
- Premium discounts for implementing or upgrading key tooling or planning
- Premium discounts for validation points
- Inhouse security consultations and services
- Inhouse IR services
- Inhouse resilience services packaged with a policy
- Inhouse EDR packaged with a policy



Incident Response Panel

- Free or discounted IRPs
- Free or discounted tabletops
- Free or discounted privacy assessments
- 0 dollar IR retainers
- Experience of handling 1000's of incidents a year
- Teams that have efficiency on their mind not selling something
- Teams that understand the insurance triggers and can help you get the most out of your policy
- Vetted and tested

Cyber Insurance Trends We're Watching



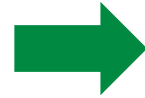
Heightened Cyber Extortion Controls



Nice to Have → Need to Have
Continued ransomware attacks are driving the need for new and improved defenses.



Artificial Intelligence Impact on Risk



AI enhancing capabilities of cyber adversaries and cyber defenders alike.
Underwriters seek clarity on use of AI tools internally and in service offering and its impact on privacy and professional liability.



Evolution of Privacy Regulations



More States join U.S. privacy law landscape (CA, VA, CO, TX, DE, OR...)
Insurers underwrite and charge for non-breach privacy coverage as regulations and enforcement activity expand, with a focus on data collection practices (collection, retention, scope)

Cyber Market Update



INCREASING CAPACITY

- New entrants to the market
- Existing carriers deploying \$10M limits more frequently
- Global insurers deploying capital to US market



STABLE PRICING

- Premiums renewing at flat or slightly reduced pricing from last 2 years
- New placements may experience lower premiums than comparable renewals
- Poor controls continue to experience increases



STABLE COVERAGES

- Limited new restrictions on cyber coverage
- Developing strategies around war, systemic risk, non-breach privacy incidents, and supply chain risk
- Shrinking ransomware restrictions
- Poor controls continue to see restricted coverage



STRINGENT UNDERWRITING

- Laser focus on ransomware resilience & disaster recovery especially for OT/ICS
- Dependent business interruption and system failure—largely sublimited / “Systemic risk” exclusions
- Non-breach privacy (GDPR, CCPA, BIPA) data collection and sharing practices are extremely critical
- Biometric data collection and security is highly scrutinized
- No tolerance for exposures in Russia, Belarus, or Ukraine

Critical Underwriting Areas of Focus



Multi-factor authentication in place for **all** remote access, external email, and privileged or admin accounts



Culture of training and awareness around phishing emails and risk reduction for all employees, including healthy click rates



EDR/MDR/XDR (endpoint detection) in place across 100% enterprise, including servers with proper configuration and monitoring



A strong patching cadence



Segmented, tested, proven, and protected backups for all critical systems, including telephony and network switch configurations



Reduced or well managed "unsavory" data collection practices like pixel tracking, cookies, and ad tech as well as privacy policy for data collection



Reduced, eliminated, or PAM-protected service accounts and admin accounts in the domain



Demonstration of resilience planning: IRP, BC and DR planning testing, with executive tabletop

Coverage Pitfalls to Avoid



Excluded claims arising out of sunsetted or unsupported software



Wrongful data collection, failure to delete, or other elevated privacy statute-related claims



Excluded claims arising out of a failure to maintain the security posture declared at the point of binding



Exclusions for claims or suits arising out of unlawful collection or wiretapping



Overly broad-reaching systemic or widespread event exclusions



Extremely narrowed coverage for biometric claims and class action suits



Cyberattacks resulting from a failure to implement a specific patch or security fix



A carve back in the definition of extra expense for patching of a vulnerability

No cyber insurance case study vs. a well managed incident through insurance

