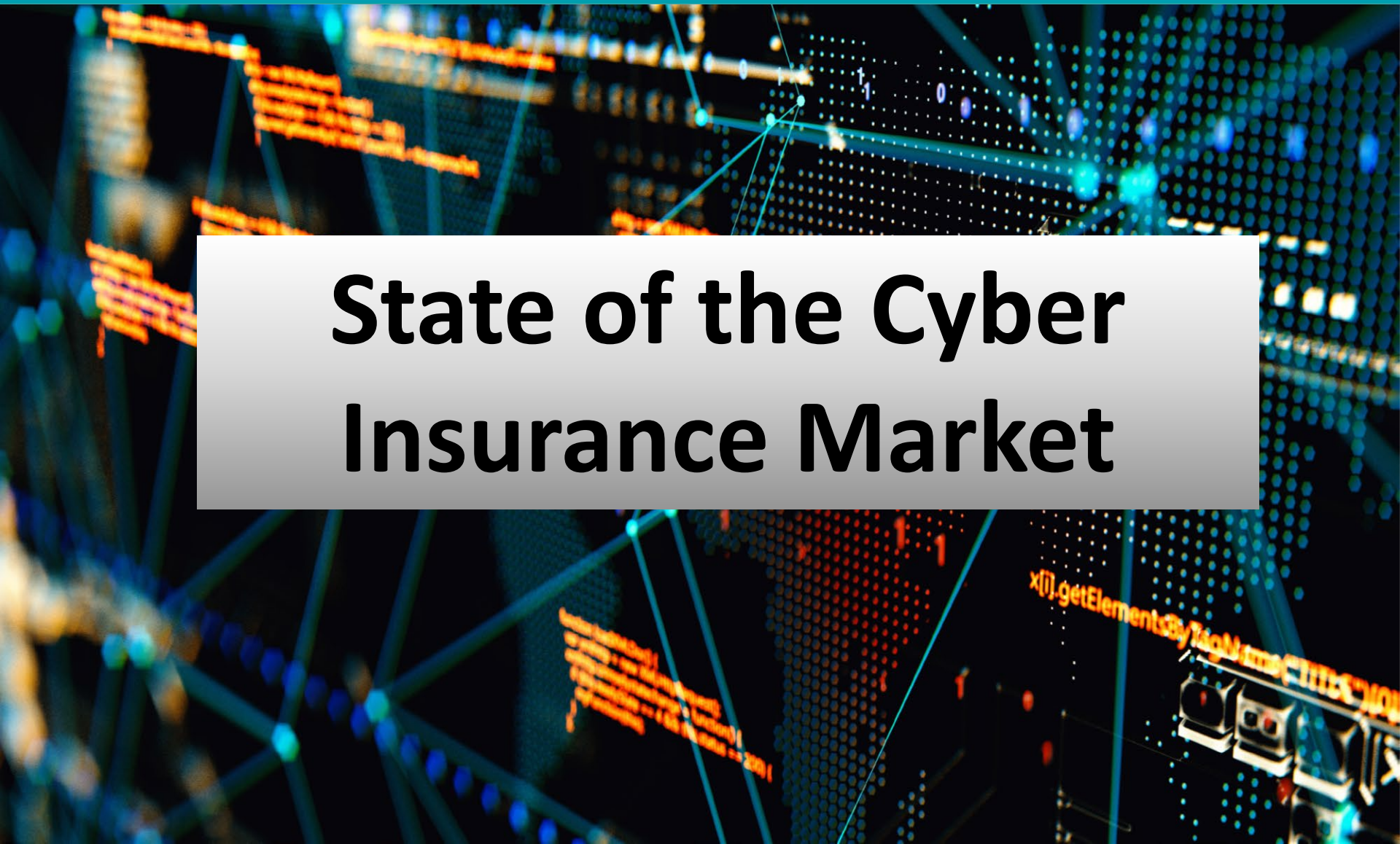
2023 WEBINAR SERIES



State of the Cyber Insurance Market

2023 WEBINAR SERIES

Agenda

- Agenda
- Cyber Market Update
- Public Entity Cyber Market Update
- Security Controls Guidelines Update
- New War Exclusions
- Going Forward

2023 WEBINAR SERIES

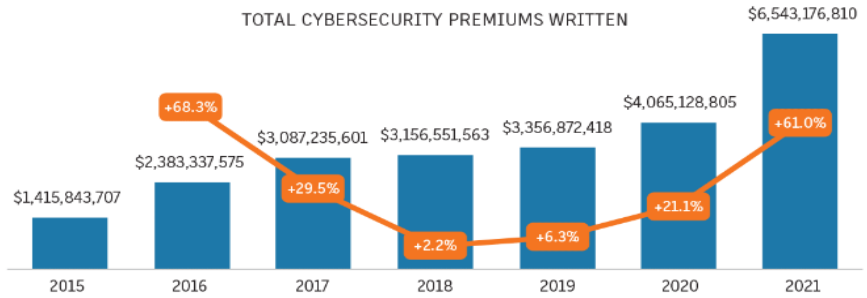
Cyber Market Update

2023 WEBINAR SERIES

Cyber Market Update

CYBER INSURANCE MARKET*

The total U.S. market for cybersecurity insurance increased 61.0% to $6.5 billion in 2021 from $4.1 billion in 2020.



*U.S. domiciled insurers and alien surplus lines insurers

LARGEST CYBER INSURERS

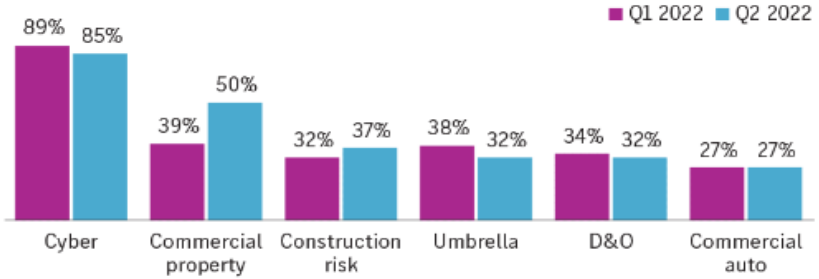
The top 10 U.S. groups wrote 57.4% of the cyber insurance, totaling $2.8 billion in 2021.

2021 rank	2020 rank	Company	Direct written premium	Market share
1	1	Chubb Ltd.	$473,073,308	9.8%
2	8	Fairfax Financial Holdings Ltd.	$436,447,801	9.0%
3	2	Axa Insurance Group	$421,013,729	8.7%
4	11	Tokio Marine Holdings Inc.	$249,785,218	5.2%
5	3	American International Group Inc.	$240,613,748	5.0%
6	NR	Travelers Cos. Inc.	$232,276,831	4.8%
7	5	Beazley Insurance Co. Inc	$200,877,555	4.2%
8	7	CNA Financial Corp.	$181,382,785	3.8%
9	NR	Arch Capital Group Ltd.	$171,944,995	3.6%
10	6	Axis Capital Holdings Ltd.	$159,059,212	3.3%

Source: National Association of Insurance Commissioners

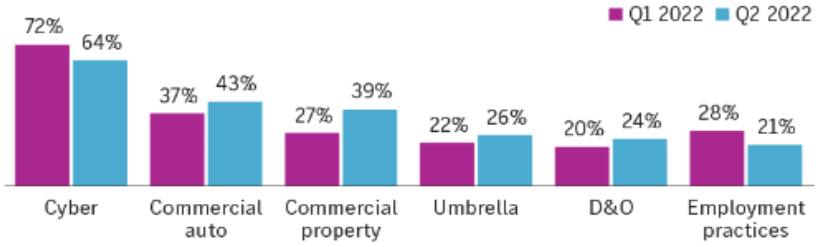
DEMAND INCREASE

Demand was again highest for cyber insurance in Q2 2022, with 85% of brokers noting they had seen an increase in demand for that particular line.



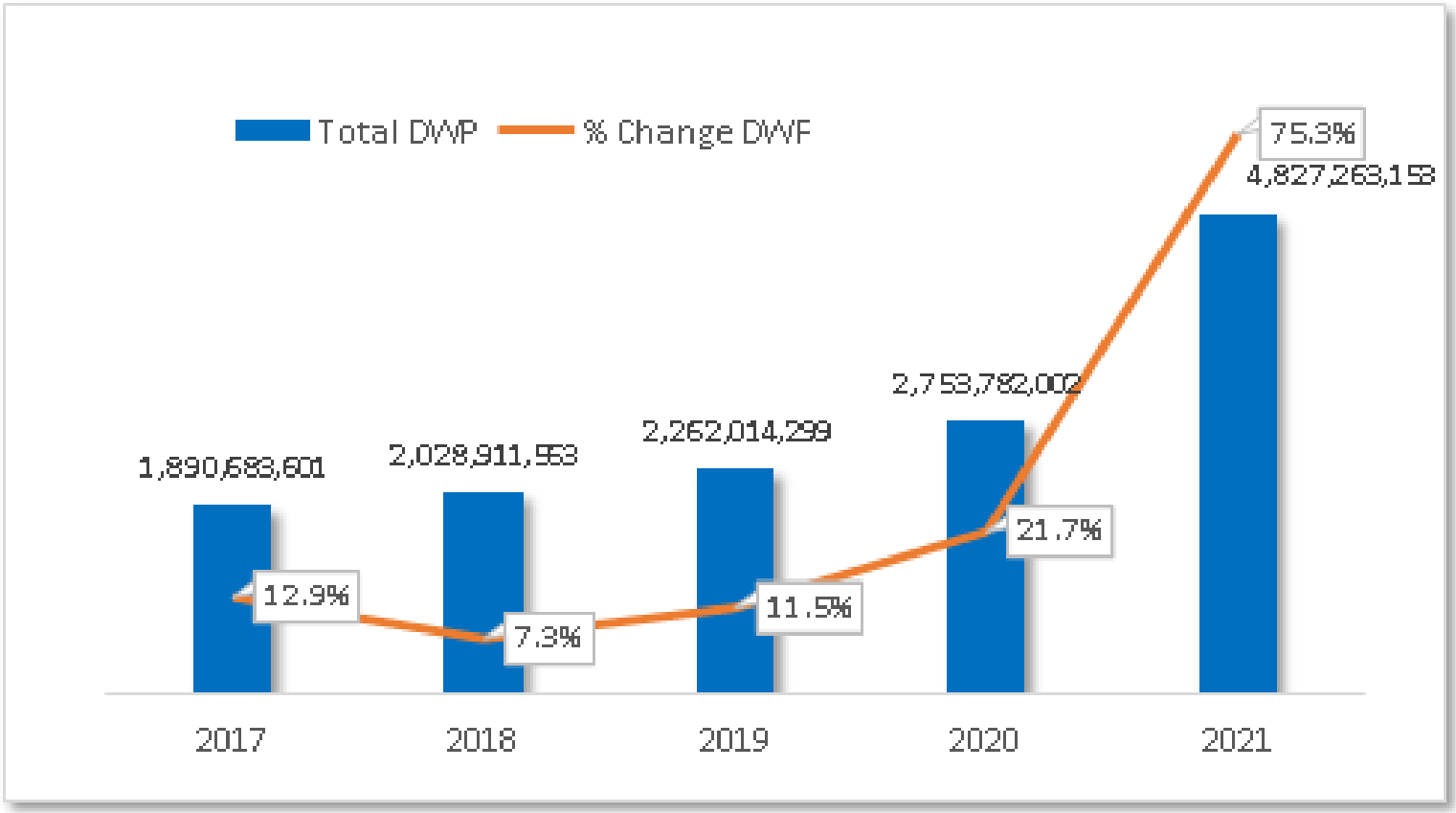
CLAIMS INCREASE

The number of cyber claims has been on a downward trend for the past few quarters, with the number of brokers reporting an increase in claims decreasing from a high of 81% in Q4 2021 to 64% in Q2 2022.



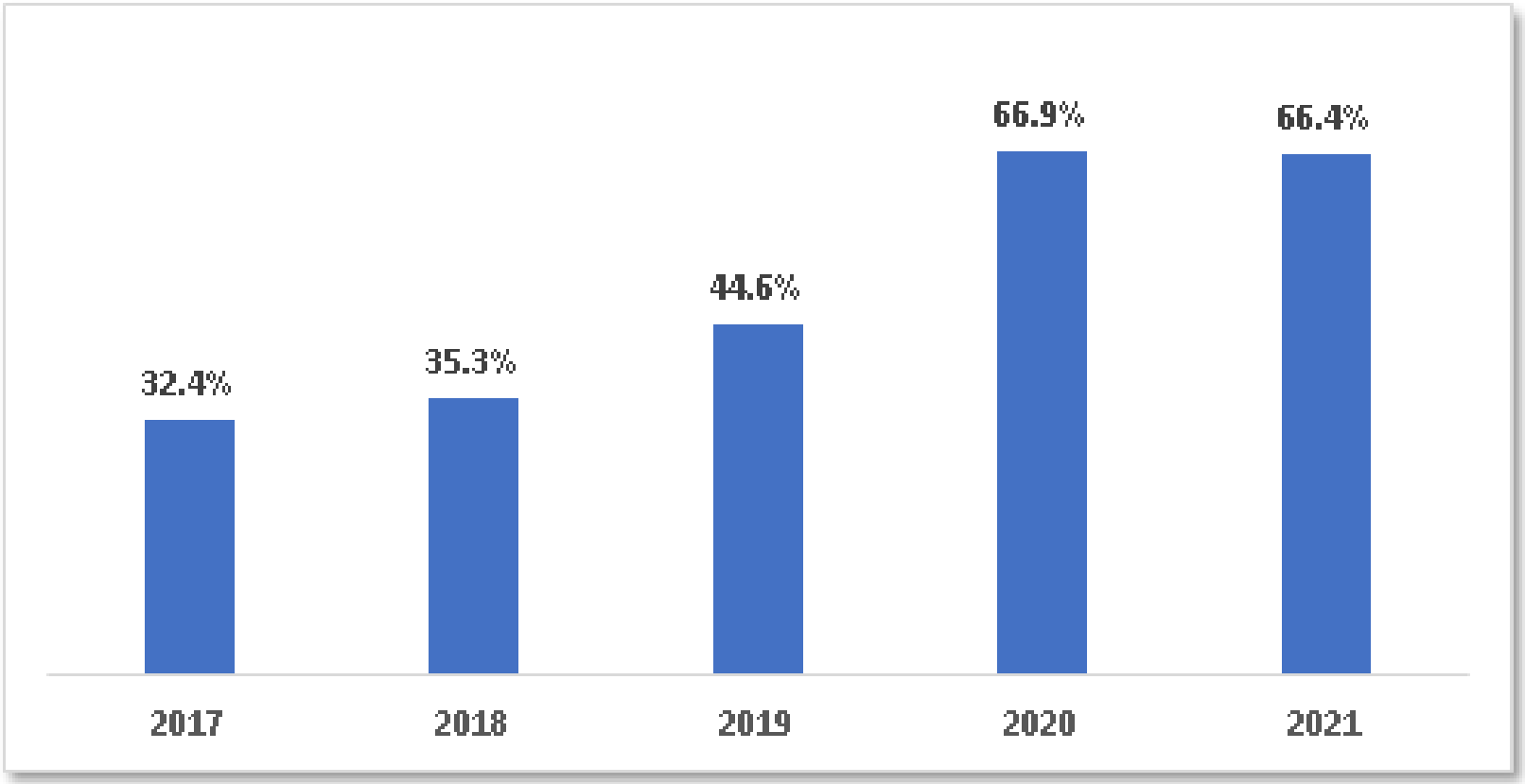
Source: Council of Insurance Agents and Brokers

Cyber Market Update – U.S. Industry Standalone Premiums



Source: National Association of Insurance Commissioners

Cyber Market Update – U.S. Industry Loss Ratios



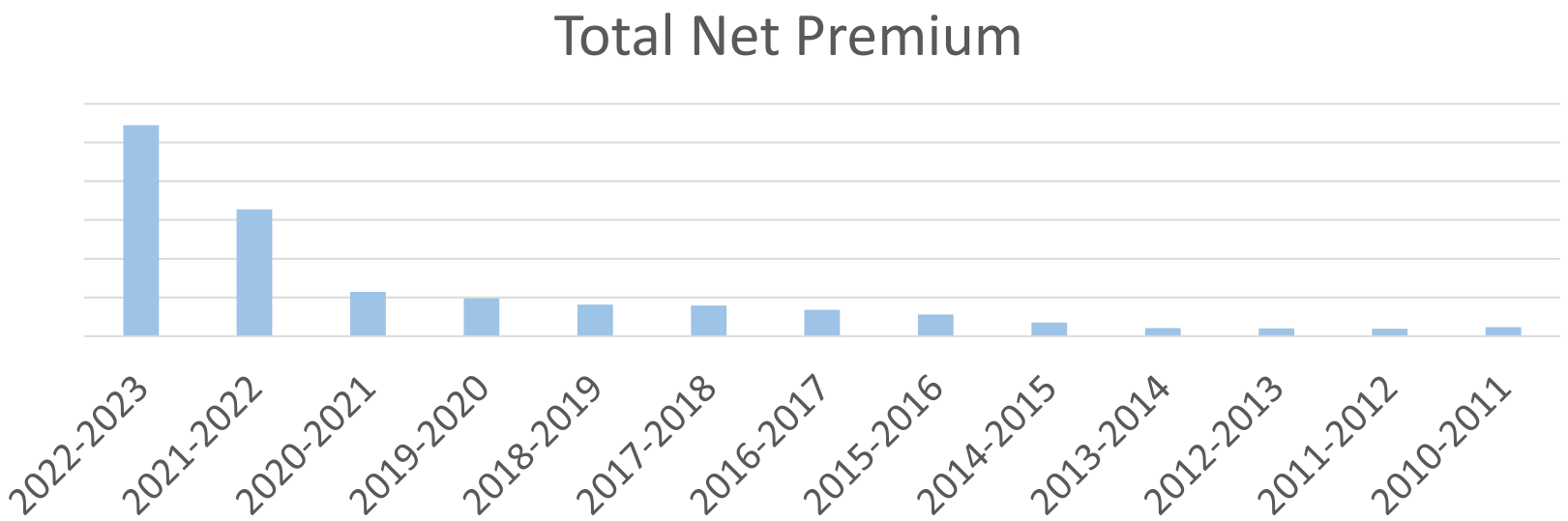
Source: National Association of Insurance Commissioners

2023 WEBINAR SERIES

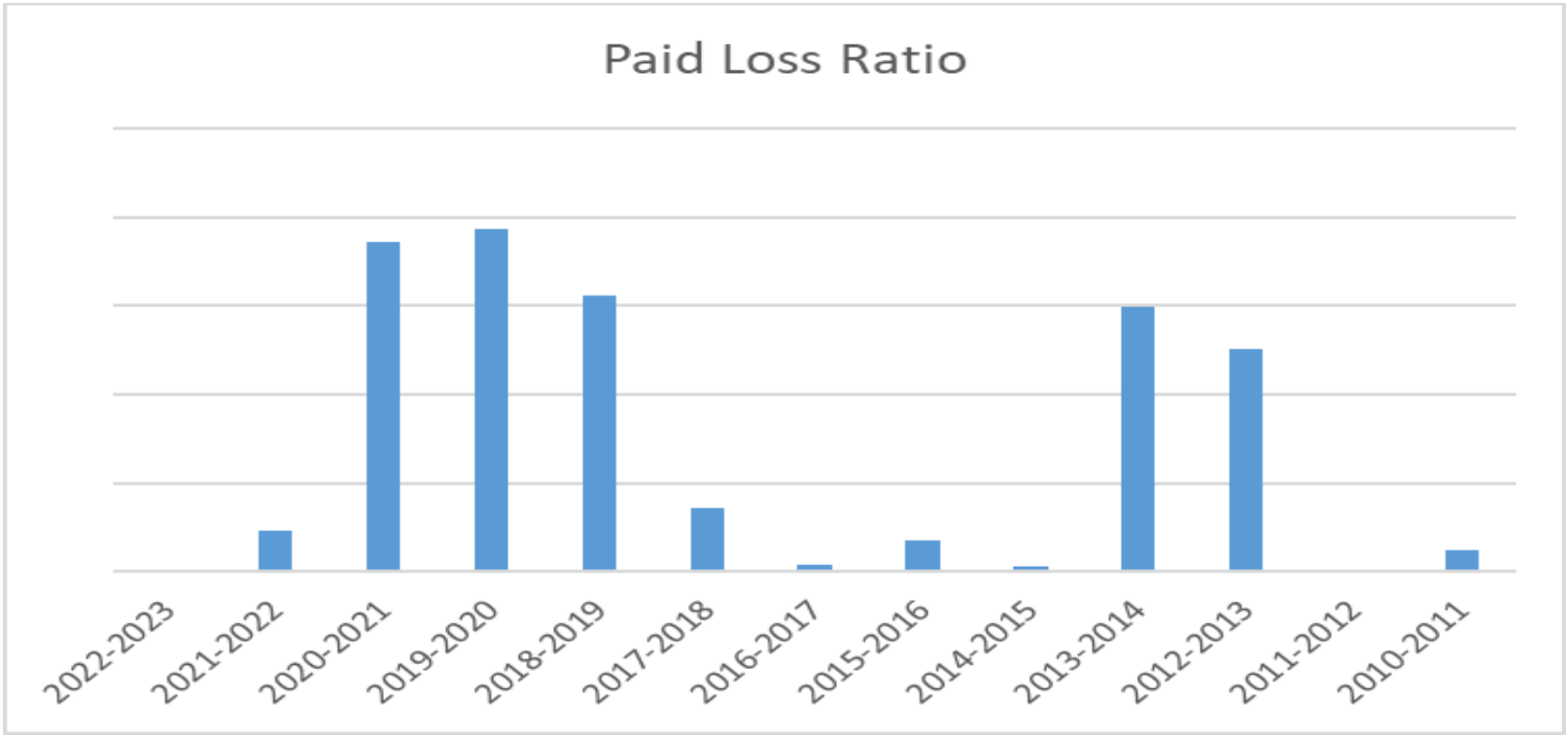
Public Entity Cyber Market Update

2023 WEBINAR SERIES

Public Entity Cyber Market Update



Public Entity Cyber Market Update



2023 WEBINAR SERIES

Security Controls

2023 WEBINAR SERIES

Security Controls Guidelines Update

MFA 100% implemented for remote access and privileged user accounts.

Minimum: MFA implemented for access to email (e.g. enforced via Office 365. Note, if using O365, enabling Advanced Threat Protection is also a recommended standard).

Minimum: MFA enforced for access to "privileged user accounts" (i.e., the information technology department).

End-point protection, detection, and response product implemented across enterprise.

Minimum: an End-Point Protection (EPP) solution in place.

- Preferred: an End-Point Detection & Response (EDR) solution in place (Now considered a minimum on medium-large sized organizations)

If Remote Desktop Protocol connection enabled, the following are implemented:

Minimum: MFA-enabled VPN is used for access to any Remote Access software.

- Network level authentication enabled

Security Controls Guidelines Update

Backups

Minimum: regular backups are (i) in place, (ii) successful recovery is tested, (iii) backups are stored separately (i.e. 'segregated') from the primary network, (iv) encrypted, and (v) protected with anti-virus or monitored on a continuous basis.

- Tested at least twice per year
- Ability to bring up within 24-72 hours – less time for critical operations (4-8 hours)

Planning & Policies

Minimum: Tested (rehearsed) Incident Response, Disaster Recovery & Business Continuity plans are in place.

- Incident Response Plan
- Disaster Recovery Plan
- Business Continuity Plan

Training

Minimum: training and regular simulated phishing exercises for all users.

- Social Engineering Training
- Phishing Training
- General Cyber security training
- Training of account team staff on fraudulent transactions

Security Controls Guidelines Update

Patching

Minimum: Critical & high severity patches installed within 30 or fewer days, optimally within 1-7 days for critical & high severity patches regarding active exploits.

Miscellaneous

- Plan or have adequate measures in place to protect end of life software
- Sufficient IT Security budgets and dedicated security personnel, carriers generally like to see 10% of total IT spend go to security but this will differ based on organization size.
- Email Security controls in place
- Privileged Access Management. A PAM solution is now considered a minimum on medium-large sized insureds
- Service Account Management. What controls are in place to protect against loss from a compromised service account?

2023 WEBINAR SERIES

War Exclusion

New War Exclusions

Why?

- Not actually a result of the current Ukraine Crisis
- Original Lloyd's War Exclusion was released on 1st January 1938
- Lloyd's committee formed post the Mondalez/Zurich property policy claim
- 4 New Lloyd's Market Association War Exclusions
- Looking to create clarity
- Looking to create consistency

New War Exclusions

		WORST			BEST
		Clause 1 (LMA 5564)	Clause 2 (LMA 5565)	Clause 3 (LMA 5566)	Clause 4 (LMA 5567)
1.	Excludes any cyber operation (whether or not in the course of war?)	Yes	No	No	No
1.	Excludes retaliatory cyber operations between specified states (China, France, Germany, Japan, Russia, UK, USA)?	N/a	Yes	Yes	Yes
1.	Excludes cyber operations that have a major detrimental impact on functioning of a sovereign state?	N/a	Yes	Yes	Yes
1.	Provides full limit cover for cyber operations other than (2) and (3) above?	N/a	No	Yes	Yes
1.	Disapplies (3) above for direct or indirect effect on a bystanding cyber asset?	N/a	No	No	Yes

New War Exclusions

- Currently not widely used
- The recent Lloyd's bulletin stating that Insurers must exclude Cyber War and Cyber attacks that have a major detrimental impact on the functioning of a state (by its impact on an essential service in that state), or on the security or defense of a state.
- A push to use the LMA exclusions
- 4 is the best
- Look to exclude events that have a detrimental effect on a nations digital infrastructure (i.e., Amazon Web Services) or key services relied upon by a nation such core financial services utilities

2023 WEBINAR SERIES

Going Forward

Potential Expectations

- More capacity
  - Existing Carriers
  - Managing General Agencies
  - “Exotic” Products
    - Catastrophe Bond
- Continued losses
- Continued demand for product
- More technical expertise/consulting/analytics
- Potentially a temporary easing up in security controls requirements
- Potentially government intervention

2023 WEBINAR SERIES

Q & A