Draft: 8/26/24

Cybersecurity (H) Working Group
Chicago, Illinois
August 14, 2024

The Cybersecurity (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met in Chicago, IL, Aug. 14, 2024. The following Working Group members participated: Cynthia Amann, Chair (MO); Michael Peterson, Vice Chair, and Eric Lowe (VA); Bud Leiner (AZ); Chris Erwin (AR); Damon Diederich (CA); Wanchin Chou (CT); Tim Li (DE); Elizabeth Nunes and Matt Kilgallen (GA); Lance Hirano (HI); Daniel Mathis (IA); C.J. Metcalf (IL); Craig VanAalst (KS); Mary Kwei (MD); Jeff Hayden and Jake Martin (MI); Jacqueline Olson and T.J. Patton (MN); Tracy Biehn (NC); Jon Godfread and Colton Schulz (ND); Christian Citarella (NH); Nick Stosic (NV); Gille Ann Rabbin (NY); Matt Walsh (OH); Mike Humphreys and David Buono (PA); Andrea Davenport (WI); and Lela Ladd (WY). Also participating were Sheila Travis and Mark Fowler (AL).

1. Adopted its July 9 Minutes

The Working Group met July 9 (Attachment Three-A). During this meeting, the Working Group took the following action: 1) adopted its May 20, March 27, and Spring National Meeting minutes and 2) heard a presentation from the Federal Bureau of Investigation (FBI) and 10-8 LLC on their approach to cybersecurity incidents.

Chou made a motion, seconded by Schulz, to adopt the Working Group's July 9 (Attachment Three-A) minutes. The motion passed unanimously.

2. Heard a Panel Discussion on the State of the Cyber Insurance Market

Moderated by Commissioner Godfread (ND), the panel, titled "The State of the Cyber Insurance Market: Trends, Challenges, and Opportunities," featured three industry experts: Brent Rieth (Aon), Jamie Schibuk (Arch Insurance), and Shawn Ram (Coalition). Structured in four key areas, the discussion covered 1) market trends, 2) coverage, 3) risk management and claims, and 4) regulatory matters.

Starting with the state of the cyber insurance market, Commissioner Godfread asked Rieth to describe the market and how it has evolved over the past five years. Rieth explained the market evolves with the constant barrage of new and different risks, and insurance companies are trying to navigate developing products and how to do it in a sustainable way on a long-term basis. Addressing the second part of the question, Rieth mentioned how in 2019, the industry observed a significant volume increase of claims connected to ransomware activity where criminals, motivated by monetary gains, attacked companies through the encryption of data and systems, making it difficult for businesses to operate. From 2021 to 2022, the industry saw a dramatic change in how product was priced and an evolution in how it was structured, and in some instances, this meant higher retention levels. An evolution in policy wording around ransomware occurred, as insurance carriers looked to manage the accumulated losses from the 2019 era. Beginning in 2023 and throughout 2024, the pricing environment has increased in competition, as new entrants came into the marketplace, expanding buyer options. Coverage also continues to evolve specifically around the topic of war and the rigorous underwriting process, and how companies are reviewed has become more comprehensive.

Commissioner Godfread opened the question to the remaining panelists. Ram went further back in time back to 2012 which he referred to as the year of the breach in the cyber world, as Target, Home Depot, and other

companies lost hundreds of millions of records. The nature of what cyber insurance was then and continues to be today is focused on the notion of data breach. From an underwriting standpoint, there is an understanding of the amount of records a company has, the resulting impact of a breach, and the cost to remediate. This evolved through more of a focus on business email compromise and security deficiencies, where attack vectors associated with email led to funds being transferred fraudulently to the proliferation of ransomware. Ram said to mitigate the trend of ransomware, the underwriting community emphasized the importance of two-factor authentication, the significance of segmented backups, and a variety of other security measures. The insurance industry helped aid companies around the world to improve their security to maintain insurability, specifically around ransomware, and as security improved, the interest in cyber increased.

Schibuk explained his observations of the shift in underwriting: the level of scrutiny and volume of questions increased. This sophistication in underwriting increased the understanding of what drives claims. He described the emergence of technology to conduct external and internal scans to give a better sense of security posture, which has led to insurers working with the insureds in a more consultative manner.

Referencing the panel's discussion of security package improvements, Amann mentioned reports of a Pakistan-based hacking group that used emojis instead of standard patch language to get around the standard patch security. It was described as "clever on the part of the hackers." Ram explained that Coalition uses a few hundred virtual machines across the world to mimic policyholder technology, reporting over 100 million attacks on these honeypot machines in the previous seven days and giving insights into the mechanisms the cyber actors are utilizing to infiltrate an organization. If there is a concentration of malware, Coalition can develop the decryption cable to help policyholders be prepared.

Commissioner Godfread explained that the cyber market penetration is limited compared to other commercial or personal lines. He asked Ram to explain his opinions on why there is limited penetration and to touch on the biggest impediments to future growth of the market. Ram explained that the Standard & Poor's 500 index (S&P 500) asset class in 1980 would have been focused on tangible property, such as boilers, machinery, and buildings. The same cohort of companies today would be almost exclusively focused on intangible assets, such as intellectual property and trade secrets. Describing the fourth industrial revolution, the digital transformation, Ram said the nature of insurance products has not evolved in the same fashion as asset classes. The nature of impediments revolves around education and a limited understanding of the industry around digital or cyber risk. Ram said this year has been interesting in the world of cyber risk in the United States. In February, Change Healthcare had two-thirds of pharmacists, clinics, and other health-care-related companies impacted by a particular piece of technology. CDK Global impacted 15,000 auto dealerships across North America. Many auto dealerships did not understand the nature of how one piece of software could take down their ability to sell cars and how that could be covered in a cyber insurance policy. He said breaches of this type can improve education among consumers because it helps them understand the risks they might be experiencing.

Accentuating the nuance of the small- and medium-sized entities (SME), he said there is a convergence of misunderstanding of what cyber insurance is and a misunderstanding of what adversaries do. SMEs often believe adversaries are focused on large companies, looking for revenue. Ram said while that may be the greatest impediment, the industry needs to provide education. Schibuk said when using the carrier perspective to look at the low market penetration rates today, projecting outgrowth over a five- to 10-year period results in a fairly sizable marketplace. As the industry grows, continuing to get reinsurers and third-party investors familiar with the cyber risk class will be important. Rieth explained that since cyber is a newer coverage for a lot of companies, it does take work to familiarize them with it and get into a position where they see enough value to purchase the coverage. It is important to consider both the pace at which the risks are changing and the pace at which the

industry can change the product itself. There are some policies that can address systems failure or technology outage; however, it is not understood by every company purchasing, and in some instances, they just purchase the minimum.

Citarella asked the panel to discuss the extent to which the underwriting process is crafted to the needs of the individual and to what extent a loss cost comparison between policies is possible. Rieth described that while there is some level of off-the-shelf policies, there are also a lot of variances across carriers in terms of base level of coverage. This puts pressure on brokers and agents to have knowledge and review the variations in policy wordings and identify needs for improvements, which is not done consistently across segments or geographically if the company is larger.

Chou asked the panel to discuss how cryptocurrencies and artificial intelligence (AI) will affect cyberattack trends. Schibuk explained that the industry has seen threat actors using AI in their applications to scale their operations more efficiently, potentially allowing them to conduct more widespread attacks. Equally, leveraging AI on the defense side, Ram described how Coalition tracks adversarial activity, allowing AI to process the data to aid in developing defensive mechanisms. Regarding cryptocurrencies, Ram suggested that regulations will have an impact on trends, as more organizations refuse to accept the challenges in tracking the money.

Commissioner Godfread asked Ram to discuss some of the common exclusions and how the market is responding. Ram explained how the conflict in Russia and Ukraine has resulted in the war exclusion in cyber, materially impacting the belief of cyber coverage value to some larger companies. These larger companies believe they could be the victim of a nation-state attacker. Additionally, Ram explained there are common exclusions or lack of coverage for items such as funds transfer fraud liability, which can be impactful depending upon the type of company.

Commissioner Godfread asked Rieth to comment on Aon's report of the lack of consistency in the market regarding exclusionary language. Rieth explained how the London marketplace responded to guidelines set by Lloyds of London with 43 variations of compliant wording of one exclusion. This introduced a learning curve for insurers to understand the language being proposed. It also highlighted the concern of accumulating risk that might arise from a nation-state attack.

Inquiring about a federal backstop, Amann asked if it would be viable for a catastrophic event to develop something like the Terrorism Risk Insurance Act (TRIA). Rieth said it would be important to continue to evaluate, working through the process of identifying the risk issues the insurance industry is concerned about. The solvency risk becomes a concern when the risk aggregation is so large. This should allow the insurance carriers to have a more appropriate conversation with reinsurers and the government to determine if a backstop mechanism is feasible.

Commissioner Godfread asked the panelists to give their perspectives on what regulators could do to support the marketplace. Schibuk summarized the discussion's theme as the product's evolution and the efforts that have gone into it. He said regulators should be open to innovation to drive the overall process and use data analysis to reduce risk for the policyholder. Ram suggested a degree of cognizance, being aware of how unique cyber is and how fundamentally different it is from most insurance coverages. The nature of the risks associated with homeowners insurance does not dramatically change within a policy period; however, with cyber, there can be dozens, if not hundreds, of technology updates on existing software during the same period. Ram said ongoing collaboration and regulatory support will help standardize and increase understanding of the product. Rieth said addressing the learning curve by helping to educate companies about the risk issues they face, and mitigation

steps can add value to the partnerships with insurance companies. An ongoing dialogue between the regulatory and private sectors is critical.

Having no further business, the Cybersecurity (H) Working Group adjourned.

SharePoint/NAIC Support Staff Hub/Committees/H CMTE/2024_Summer/WG-Cybersecurity/Minutes-CyberWG081424.docx

Draft: 8/6/24

Cybersecurity (H) Working Group
Virtual Meeting
August 1, 2024

The Cybersecurity (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met August 1, 2024. The following Working Group members participated: Cynthia Amann, Chair (MO); Michael Peterson, Vice Chair (VA); Julia Jette (AK); Bud Leiner (AZ); Mel Anderson (AR); Damon Diederich (CA); Wanchin Chou (CT); Tim Li (DE); Matt Kilgallen (GA); C.J. Metcalf (IL); Daniel Mathis (IA); Shane Mead (KS); Mary Kwei (MD); Jake Martin (MI); T.J. Patton (MN); Tracy Biehn (NC); Colton Schulz (ND); Christian Citarella (NH); Scott Kipper (NV); Gille Ann Rabbin (NY); Don Layson (OH); Jodi Frantz (PA); Bryon Welch (WA); and Andrea Davenport (WI).

1. Adopted its May 29 Minutes

The Working Group met May 29 and took the following action: 1) heard a presentation from the Coalition on the "Effectiveness of Security Controls: A Meta Analysis."

Schulz made a motion, seconded by Chou, to adopt the Working Group's May 29 minutes (Attachment 1). The motion passed unanimously.

2. Heard an Update on Federal Activities Related to Cybersecurity and Cyber Insurance

Shana Oppenheim (NAIC) provided an overview of her federal update, which included: 1) the Cybersecurity and Infrastructure Security Agency's (CISA) Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) Cyber Event Notice Rulemaking; 2) the effect of *Loper Bright Enterprises v. Raimondo* and the overturning of *Chevron* deference on cyber rulemaking policy; and 3) a general overview of federal activity around cyber insurance and cybersecurity.

First, CISA published the notice of proposed rulemaking (NPRM) for CIRCIA in March. Oppenheim said that insurers with $2 million to $47million in revenue and a 500–1,500 employee count will be exempted from this reporting. Insurance companies can act as third-party representatives for covered entities. This means they can submit cyber incident reports on behalf of their clients, provided they have explicit authorization. All other insurers will have to report to CISA within 72 hours of forming a reasonable belief that a covered cyber incident has occurred and 24 hours after paying a ransom. Covered cyber incidents fall into four categories: 1) substantial loss of systems integrity/confidentiality; 2) serious disruption of operations; 3) serious disruption of business; and 4) unauthorized access to non-public information. The reported data is concerned with incident management. CIRCIA requires covered entities to ensure preservation of relevant data and records associated with the reported incidents, and supplemental reports are required for new and different information becoming available.

Oppenheim said that the NAIC provided detailed comments on CISA's proposed rulemaking for CIRCIA. The comments submitted addressed the NAIC's support for clear guidelines, coordination with state insurance regulators, data protection and confidentiality, impact on small and medium-sized entities, and public-private collaboration. These comments reflect the NAIC's commitment to ensuring the CIRCIA rulemaking process results in practical, effective, and fair regulations for the insurance industry.

Second, Oppenheim described the key context of the Supreme Court's decision in *Loper Bright Enterprises v. Raimondo* and its significant implications for federal cyber regulations, particularly in the context of CIRCIA. She

said the ruling eliminates the *Chevron* deference, which previously allowed courts to defer to federal agencies' reasonable interpretations of ambiguous statutes. This change means courts will now independently interpret statutes, potentially leading to more legal challenges against agency rulemaking. CISA's proposed rules under CIRCIA, which require critical infrastructure entities to report cyber incidents, may face increased scrutiny and legal challenges. Oppenheim said that critics, including those in the U.S. Senate, have already raised concerns. The Biden administration is considering changes for the National Cybersecurity Strategy in response to the *Chevron* impact. The decision complicates efforts to enforce security rules on critical infrastructure through executive orders, which relied on broad statutory interpretations. Despite these challenges, the administration plans to proceed with new cybersecurity regulations for the health care sector, even amid opposition from U.S. governors. Oppenheim opined that overall, the *Loper Bright* decision is expected to lead to more rigorous judicial review of federal cyber regulations, potentially slowing down the rulemaking process and necessitating closer collaboration with Congress.

Third, Oppenheim said the discussions around a federal backstop to catastrophic cyber insurance have been quite active in 2024. Across various federal agencies, Congress, and other stakeholders, these efforts are part of a broader initiative to support the existing cyber insurance market and address the increasing risks posed by cyberattacks on critical infrastructure. The Federal Insurance Office (FIO) and CISA have been working together to assess the need for a federal insurance response to catastrophic cyber incidents following a recommendation by a 2022 Government Accountability Office (GAO) report. FIO held a roundtable on this issue in Spring 2024, following the Fall 2023 conference it co-sponsored with NYU Stern's Volatility and Risk Institute (VRI), which brought together industry experts, policymakers, and stakeholders to discuss catastrophic cyber risks and potential federal responses. FIO also partnered with the National Science Foundation (NSF) to establish an industry university cooperative research center to focus on cyber and terrorism insurance. She said the center is trying to provide research that would improve the modeling and underwriting of both terrorism and cyber risks.

Oppenheim said Congress is continuing the discussion of a federal backstop with a hearing to discuss bipartisan support for harmonizing cyber insurance as the market evolves. However, there has not been inclusion of the topic in any legislative language.

Peterson asked if the supreme court opinion will have an impact on a federal organization's ability to take action. Oppenheim said that it would depend on what statute they are attempting to proceed under; CIRCIA could be vague enough that it would need to be amended to give a more specific set of instructions.

Schulz asked about Oppenheim's awareness of discussions to wrap cybersecurity into the Terrorism Risk Insurance Act (TRIA). Oppenheim stated she was not aware of any discussion because it might require amending TRIA. She said the meetings she has attended were more on how to model a cyber backstop and modeling it after TRIA or after the National Flood Insurance Program (NFIP).

Chou offered a reminder of the difference in modeling cyber and terrorism.

Lauren Pachman (National Association of Professional Insurance Agents) offered a comment on the last reauthorization of TRIA in which Congress considered adding cyber terrorism but opted against it. She suggested anticipating the Treasury would have challenges of doing this in the absence of *Chevron*.

Fourth, Oppenheim discussed the federal activity in cybersecurity, starting with the U.S. Securities and Exchange Commission's (SEC's) Cyber Incident Disclosure Rule, implemented last year, which necessitates enhanced reporting for transparency with investors. While CISA is driving for improved federal and public collaboration with a harmonization on reporting rules, Oppenheim added that the SEC's division of corporation finance issued new guidance requiring companies to assess the materiality of ransomware incidents promptly and disclose them on

Form 8-K if deemed material, even if the incident is resolved or a ransom is paid before the reporting deadline. She explained how CISA is trying to get more cybersecurity firms to aid in the event of a severe cybersecurity attack. She said that the CISA director mentioned this could include invoking emergency authorities like the Defense Production Act (DPA) and the National Emergencies Act.

Peterson asked about the federal attitude in response to the recent global information technology (IT) outage caused by CrowdStrike. Oppenheim said while no legislative drafting has surfaced, that could change following the company leadership's hearing at Congress.

Amann discussed the challenges of policy definitions not keeping up with the changing landscape of cyber. She thanked Oppenheim for keeping the Working Group informed on what the federal organizations are saying.

3. Heard a Preview of its Summer National Meeting Plan

Amann told the Working Group about the panel discussion at the Summer National Meeting, during which industry speakers will give their perspectives on the cyber insurance market. This panel is a result of the Working Group's plan to learn from industry experts by inviting them to make presentations to members of the Working Group focusing on actual business practices and less on theory.

4. Discussed Other Matters

Amann reminded the Working Group of the Catastrophe Insurance (C) Working Group's Catastrophe Modeling Primer and asked for participant input. Bubba Aguirre, an investigator in Minnesota, offered his experience investigating cybersecurity events and sharing fraud awareness information with residents. He asked whether other states are investigating cybersecurity incidents reported to them. Peterson offered scheduling a meeting to speak about this topic in a session to provide an update of what other states are doing to address this issue.

Having no further business, the Cybersecurity (H) Working Group adjourned.

SharePoint/NAIC Support Staff Hub/Committees/H CMTE/2024_Summer/WG-Cybersecurity/Minutes-CyberWG080124.docx

Attachment 2

AM BEST | CELEBRATING 125 YEARS

NAIC Cybersecurity Working Group
US Cyber Market Trends & AM Best Cyber Initiatives

Michael Lagomarsino – Senior Director, AM Best
Thomas Mount – Senior Director, AM Best

September 4, 2024

Agenda

- AM Best's Global Cyber Insurance Market Outlook
- Trends in the US Cyber Insurance Market
- AM Best's Ratings Process & Rating Considerations for Affirmative Cyber
- Incorporating Catastrophe Risk & Stress Testing
- AM Best's Cyber Questionnaire
- How Companies Are Managing Cyber Risks
- Q&A

Global Cyber Insurance Market Segment Outlook

Stable Outlook – Positive Signs

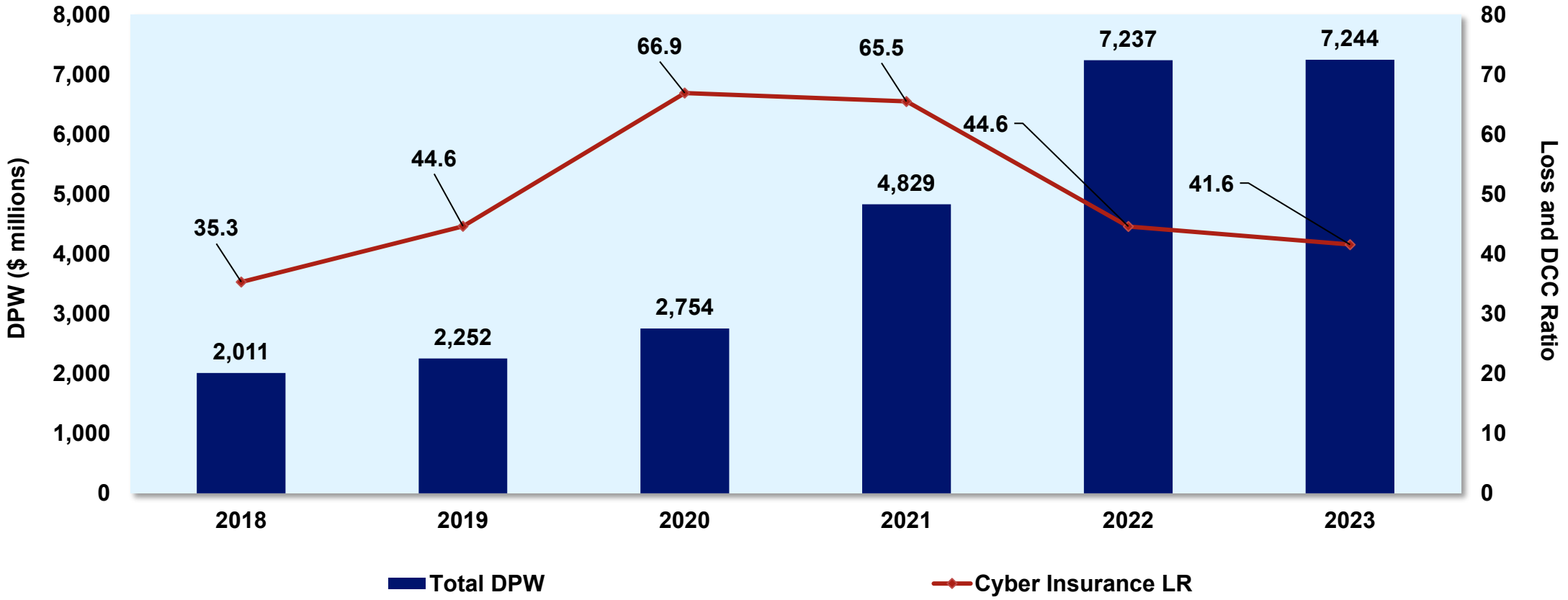
- Greater demand/increasing take up rates
- Continual improvements in cyber hygiene
- Expected profitability over the immediate term
- Improvements in underwriting practices and policy language
- Supportive reinsurance and ILS markets

Stable Outlook – Countervailing Factors

- Increased competition and modest premium growth in US
- Growing sophistication of attacks using AI
- Aggregation risks
- Model risk and divergence among models
- Heavy dependence on reinsurance

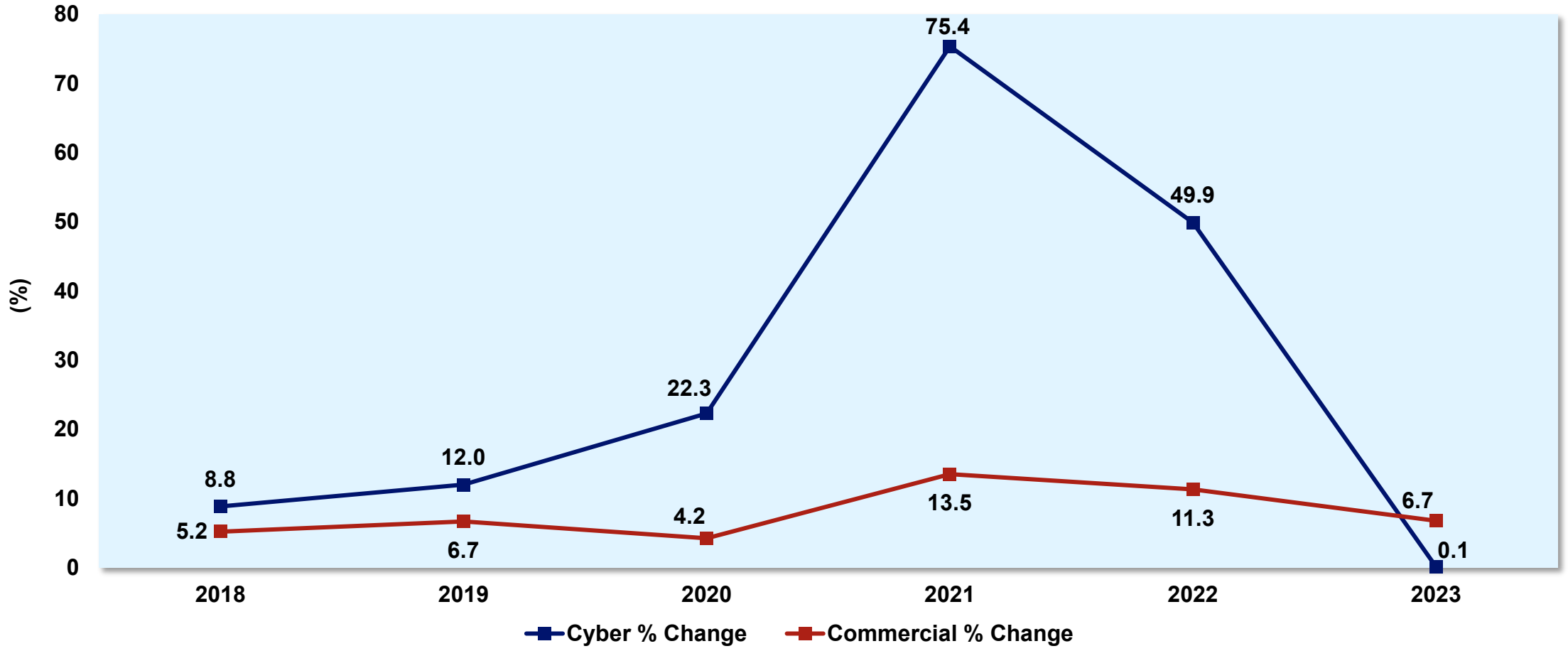
US Cyber Market Overview

Cyber DPW with Loss & DCC Incurred Ratio



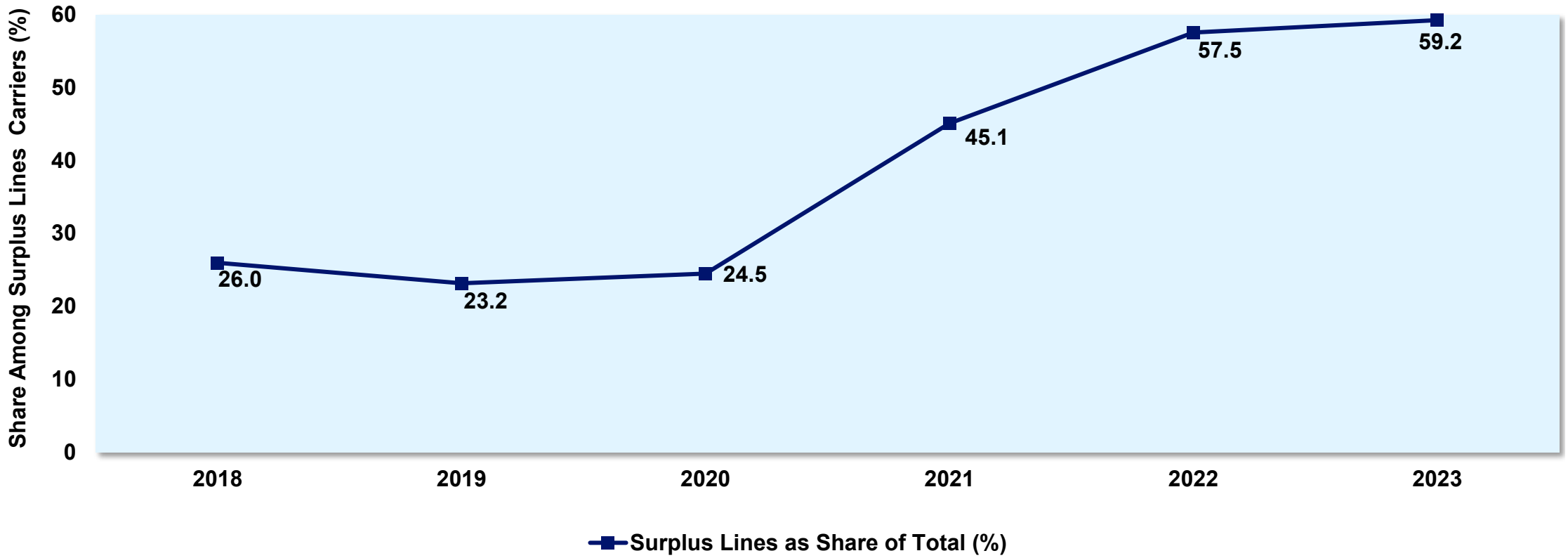
Source: AM Best data and research (based on premium reported as of June 10, 2024)

Changing in DPW – Cyber vs. all Commercial Lines



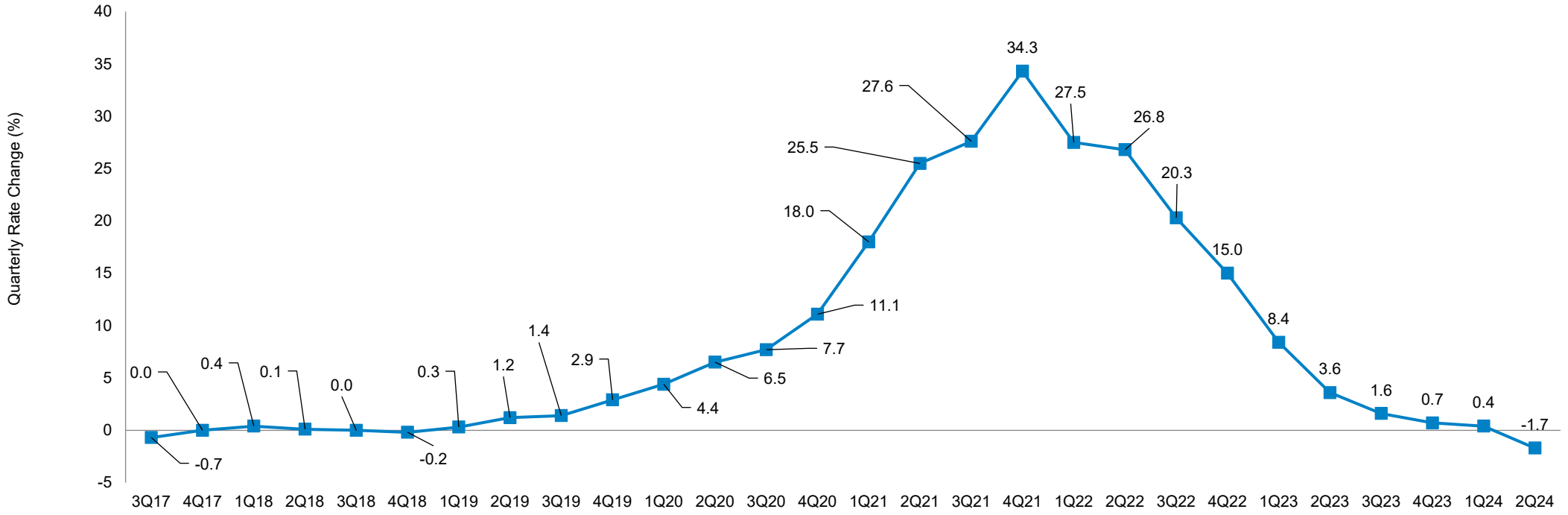
Source: AM Best data and research

Surplus Lines as Share of all Cyber DPW



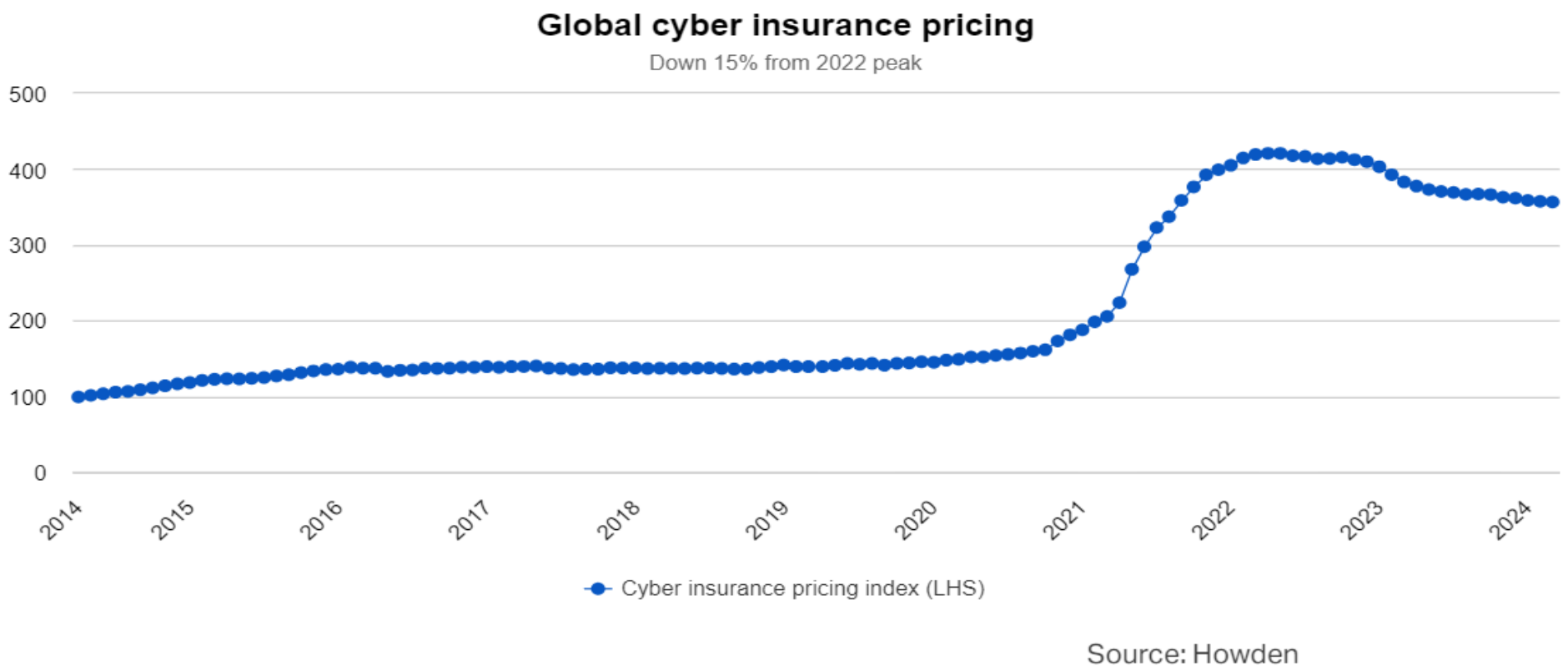
Source: AM Best data and research

US Cyber Insurance Pricing Changes by Quarter (3Q17 – 2Q24)



Source: CIAB

Global Cyber Insurance Pricing (Cumulative Since 2014)



Source: Howden

Top 20 Cyber Writers by DPW ($millions)

Rank			2022	2023	22-23 DPW	Market	% of Cybersecurity DPW		2022 Loss & DCC	2023 Loss & DCC	UW Exp	Est. Comb
###	###	Company Name	DPW	DPW	Chg (%)	Share (%)	Standalone	Packaged	Ratio	Ratio	Ratio	Ratio
1	1	Chubb INA Grp	604.9	573.6	-5.2	7.9	0.0	100.0	53.8	39.1	23.6	62.7
3	2	XL America Companies	527.4	487.2	-7.6	6.7	100.0	0.0	66.2	62.6	24.2	86.8
2	3	Fairfax Financial (USA) Grp	563.0	463.0	-17.8	6.4	100.0	0.0	54.0	51.0	33.7	84.6
6	4	Travelers Grp	315.3	384.9	22.0	5.3	84.7	15.3	34.8	22.4	33.8	56.2
4	5	Tokio Marine US PC Grp	367.6	377.9	2.8	5.2	78.0	22.0	57.8	44.6	29.0	73.6
12	6	Berkshire Hathaway Insurance Grp	228.5	289.3	26.6	4.0	40.3	59.7	48.1	47.1	26.5	73.6
5	7	Arch Insurance Grp	346.4	282.1	-18.5	3.9	88.6	11.4	52.3	58.1	30.0	88.1
7	8	American International Grp	299.0	274.4	-8.2	3.8	100.0	0.0	47.6	79.3	23.3	102.6
10	9	Sompo Holdings US Grp	248.0	262.9	6.0	3.6	100.0	0.0	50.1	44.9	25.5	70.4
208	10	Starr International Grp	0.0	260.0	NA	3.6	47.8	52.2	0.0	0.0	16.0	16.0
11	11	CNA Insurance Companies	228.9	228.4	-0.2	3.2	13.1	86.9	26.5	36.2	28.4	64.6
8	12	Nationwide Property & Casualty Grp	257.3	226.5	-12.0	3.1	93.8	6.2	12.5	27.6	32.8	60.4
9	13	Zurich Insurance US PC Grp	252.5	199.2	-21.1	2.8	72.8	27.2	68.2	63.5	20.0	83.5
15	14	AXIS US Operations	195.7	181.3	-7.4	2.5	88.5	11.5	85.9	73.2	28.7	101.9
13	15	Liberty Mutual Insurance Cos	208.2	178.3	-14.4	2.5	45.6	54.4	57.5	74.0	46.7	120.7
20	16	Hartford Insurance Grp	152.3	174.8	14.8	2.4	14.1	85.9	15.5	11.3	30.5	41.9
17	17	Ascot Insurance U.S. Grp	166.6	174.5	4.8	2.4	52.6	47.4	30.2	30.1	31.9	61.9
24	18	AmTrust Grp	115.9	170.0	46.7	2.3	87.8	12.2	7.6	4.9	36.4	41.3
16	19	Beazley USA Insurance Grp	174.6	149.6	-14.3	2.1	93.7	6.3	19.6	18.3	28.4	46.7
22	20	Intact US Insurance Grp	123.9	144.6	16.7	2.0	87.4	12.6	32.9	18.6	39.1	57.6
		Top 5*	2,378.3	2,286.4	-3.9	31.6	68.7	31.1	54.9	43.5	28.4	71.9
		Top 10*	3,500.2	3,655.2	4.4	50.5	71.1	28.9	53.3	46.4	26.9	73.2
		Top 20*	5,376.2	5,482.4	2.0	75.7	68.6	31.4	47.4	42.2	28.6	70.7
		Total Standalone	5,090.8	4,986.5	-2.0	68.8			47.4	44.3	28.8	73.1
		Total Package	2,146.0	2,257.4	5.2	31.2			47.9	35.5	36.3	71.8
		Total P/C Industry	7,236.7	7,243.9	0.1	100.0	68.8	31.2	44.6	41.6	31.1	72.7

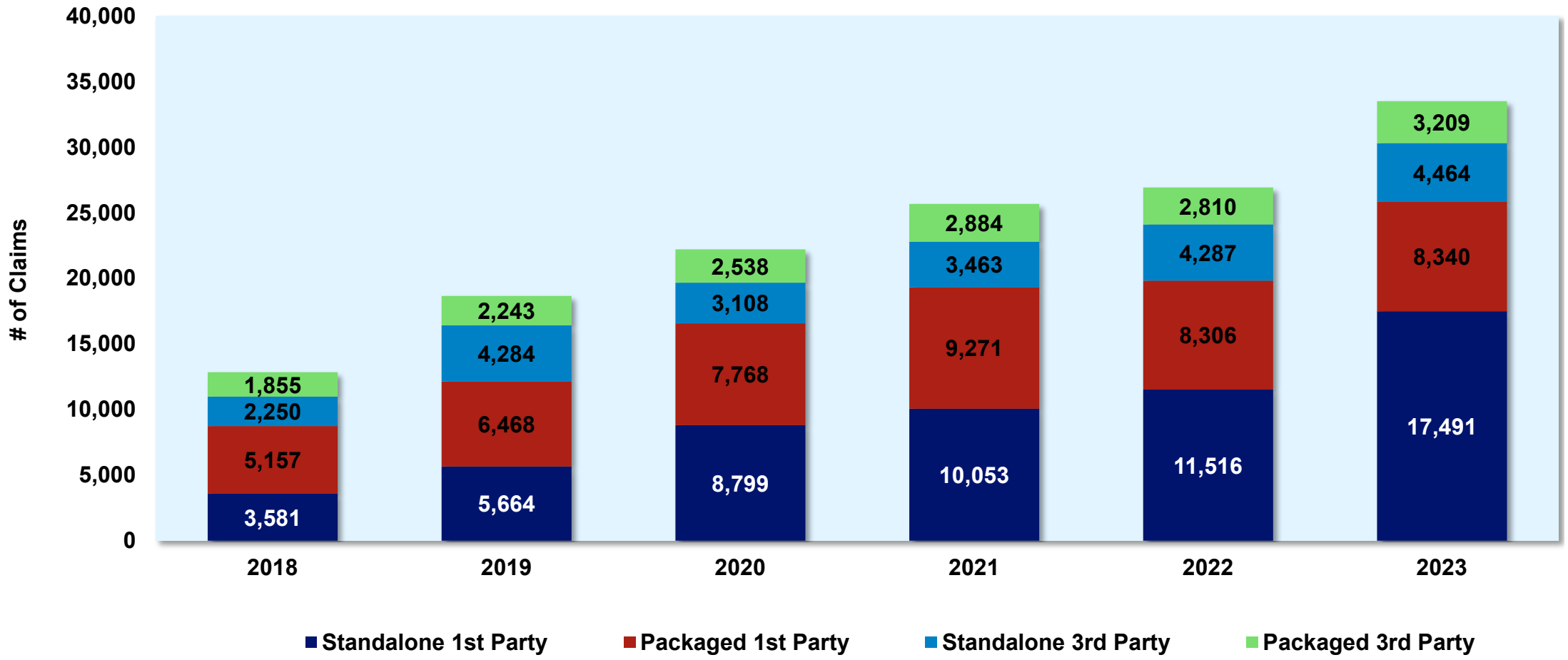
*Ranked by 2023 total standalone and packaged cybersecurity direct premiums written (based on premium reported as of June 10, 2024)

Top 20 Cyber Writers by PIF (thousands)

Company Name	PIF* (thousands) 2022	2023	YoY% Change
Hartford Insurance Grp	629.9	667.4	6.0
American Family Insurance Grp	93.6	349.5	273.2
Erie Insurance Grp	198.3	284.6	43.6
Berkshire Hathaway Insurance Grp	248.3	267.1	7.6
Farmers Insurance Grp	170.8	162.9	-4.6
Tokio Marine US PC Grp	144.8	143.2	-1.1
CNA Insurance Companies	125.6	136.9	9.0
Selective Insurance Grp	114.2	122.8	7.5
Hanover Ins Grp Prop & Cas Cos	110.8	115.5	4.2
Chubb INA Grp	93.5	96.1	2.8
W. R. Berkley Insurance Grp	53.1	89.2	67.8
The Cincinnati Insurance Cos	82.7	78.1	-5.6
Brotherhood Mutual Insurance Co	62.8	67.5	7.5
Travelers Grp	62.2	64.8	4.2
Nationwide Property & Casualty Grp	82.6	58.4	-29.4
Markel Insurance Grp	42.6	53.1	24.6
Federated Mutual Grp	43.7	45.7	4.8
Arch Insurance Grp	44.8	45.6	1.6
United Fire & Casualty Grp	42.7	44.4	4.0
Church Mutual Insurance Grp	38.7	44.3	14.4
Top 5	**1,340.9**	**1,731.6**	**29.1**
Top 10	**1,929.9**	**2,346.1**	**21.6**
Top 20	**2,485.8**	**2,937.1**	**18.2**
Total P/C Industry	**3,914.7**	**4,365.4**	**11.5**

Source: AM Best data and research

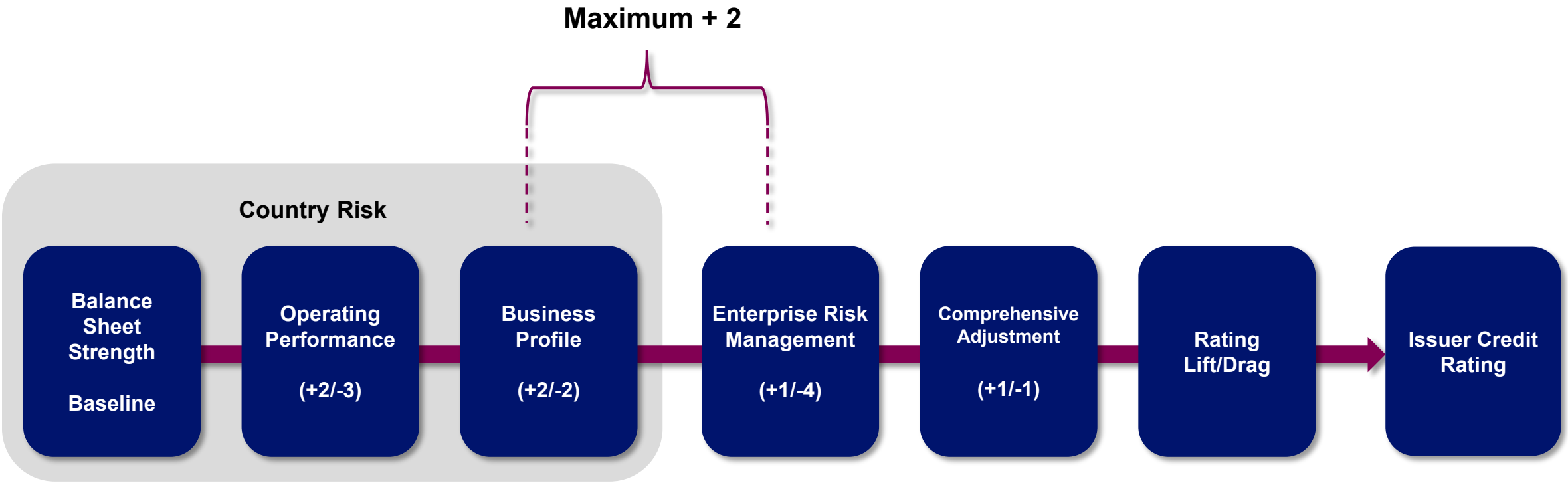
Claims by Policy Type and Claim Type



Source: AM Best data and research

AMB Rating Process & Rating Considerations for Affirmative Cyber

Building Block Approach



Underwriting *affirmative cyber*, where material, impacts multiple building blocks and financial strength.

Rating Considerations for Affirmative Cyber

Balance Sheet Strength	Operating Performance	Business Profile	Enterprise Risk Management
• Risk-adjusted capitalization	• Underwriting & earnings volatility	• Product concentration risk	• Risk appetite & tolerances
• Cyber modelling	• Business plans and assumptions	• High product risk	• Risk aggregation
• Stress testing	• Track record	• Limits offered	• Risk management capabilities
• Reinsurance		• Industries covered	• Stress testing
• Reserve adequacy		• Size of Insured	
• Liquidity		• Management expertise	

US P/C BCAR

BCAR = (Available Capital – Net Required Capital) / Available Capital x 100

Available Capital (AC)
Reported Capital (PHS)
Equity Adjustments:
Unearned Premiums (DAC)
Assets
Loss Reserves
Reinsurance
Equalization/Contingency Reserves
Debt Adjustments:
Surplus Notes
Debt Service Requirements
Other Adjustments:
Future Operating Losses
Goodwill & Intangible Assets
Other

Net Required Capital
Gross Required Capital (GRC):
(B1) Fixed Income Securities
(B2) Equity Securities
(B3) Interest Rate
(B4) Credit
(B5) Loss and LAE Reserves
(B6) Net Premiums Written
(B7) Business Risk
(B8) Potential Catastrophe Loss
Covariance Adjustment
Net Required Capital (NRC)*

***NRC = SQRT [$(B1)^2+(B2)^2+(B3)^2+(0.5*B4)^2$ $+[(0.5*B4)+B5)]^2+(B6)^2$ $+ (B8)^2]$ +B7**

Incorporating Catastrophe Risk & Stress Testing Into the Ratings Process

Why Incorporating Catastrophe Risk & Stress Testing is Necessary?

Effectively managing exposure to catastrophe events is essential to protecting and preserving balance sheet strength

Catastrophes – both natural and man-made – can abruptly impair an insurer

Stress Testing allows AM Best to capture the uncertainties inherent in an insurer's operations and business plans

Catastrophe Risk

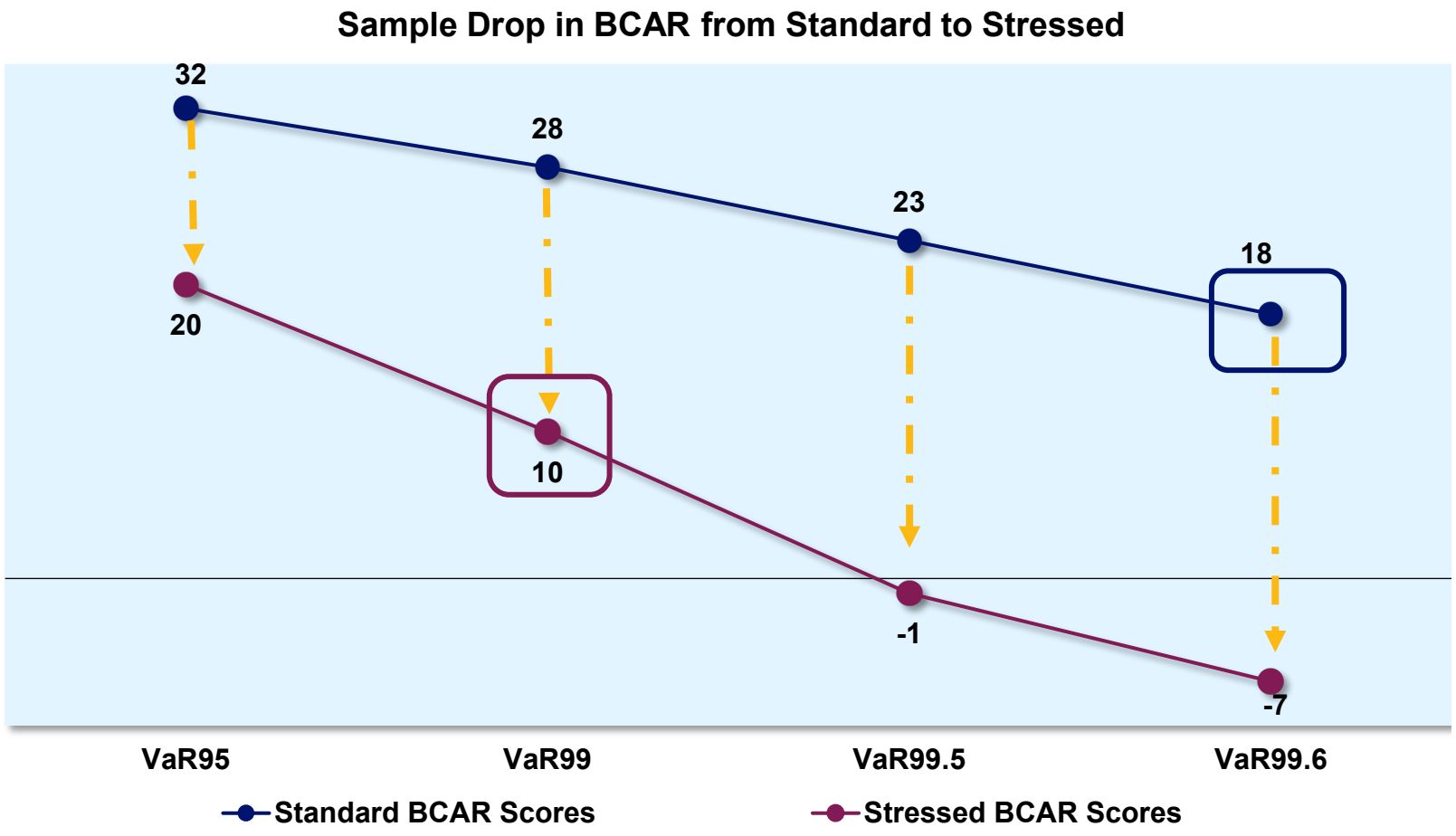
Rating Considerations

- Aggregate exposure
- Concentration of exposures
- Historical losses
- Deterministic scenarios
- Modelled PMLs
- Management's view

Examples

- Natural catastrophes
- Terrorism exposure
- Casualty clash
- Cyber catastrophe
- Pandemic

Stress Testing Risk Adjusted Capital



BCAR Assessment = Very Strong

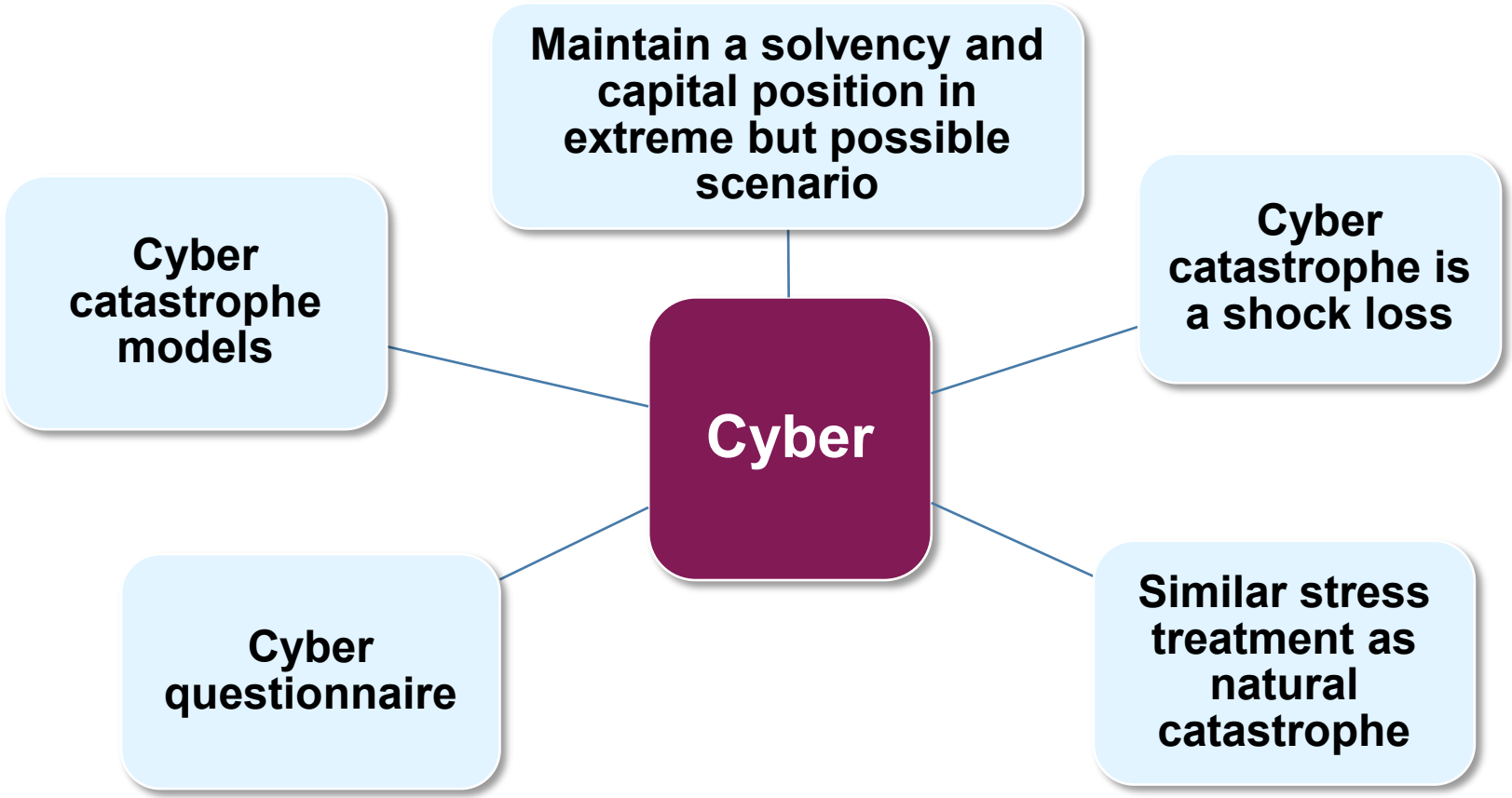
2 level drop

BCAR Assessment = Adequate

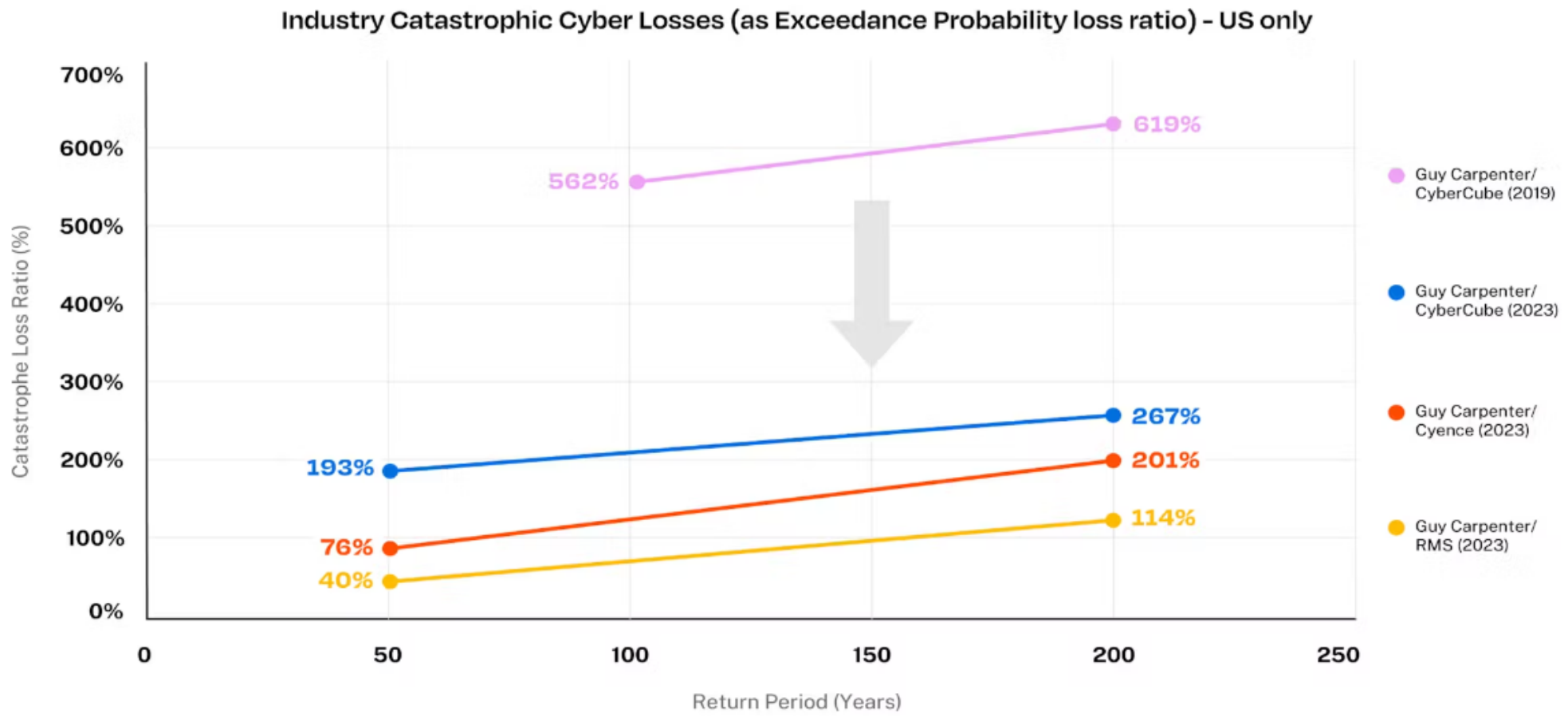
Natural Catastrophe Stress Test

Typical Tolerance for Drop in BCAR Assessment		
Standard BCAR Assessment	**Without Financial Flexibility**	**With Financial Flexibility**
Strongest	**1 Level Drop**	**2 Level Drop**
Very Strong	**1 Level Drop**	**2 Level Drop**
Strong	**1 Level Drop**	**2 Level Drop**
Adequate	**1 Level Drop**	**1 Level Drop**
Weak	**0 Levels**	**0 Levels**

Challenges for Cyber Stress Testing

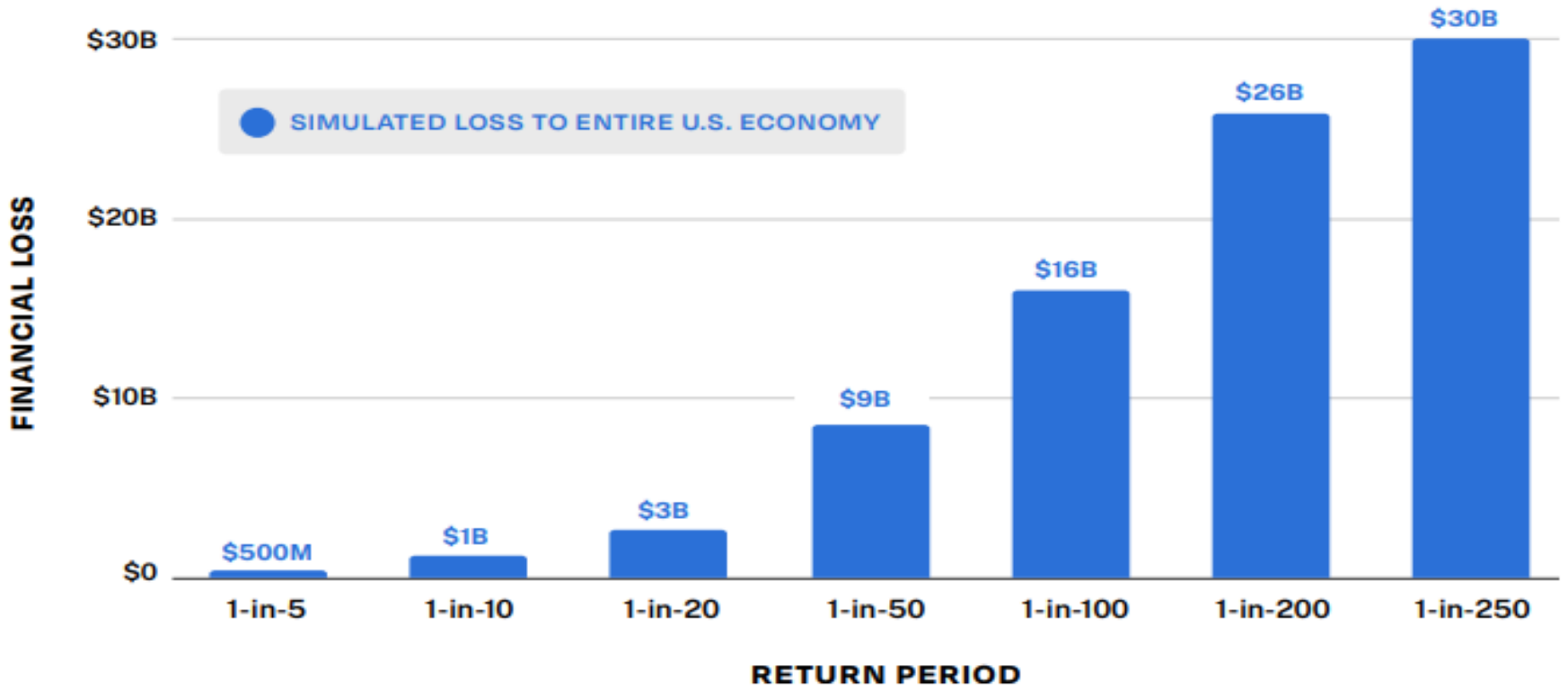


Cyber PMLs



Source: coalitioninc.com

Cyber PMLs



Source: Active Cyber Risk Modeling Report – Coalition Inc 2023

AM Best's Cyber Questionnaire

Cyber Questionnaire – “Why” do we Need It?

Need to assess the potential impact on the rating

Affirmative Cyber is a material risk to the industry

Dramatic Growth in Affirmative Cyber Written

- Historical Growth and Projected Growth
- Greater impact on rating unit operations

Need to quantify and understand impact

- Cyber is not shown as a separate line of business
- Risk profile of cyber portfolio
- Greater exposure to catastrophic loss
- Potential impact of systemic loss/aggregations on balance sheet
- Cyber risk management

Benchmarking

- Better comparisons

AM Best's Cyber Questionnaire

General Questions

- Nature of the portfolio
- Cyber risk appetite and underwriting strategy
- Reinsurance (traditional and non-traditional)
- Use of third parties

Profile & Performance

- Types of cover offered (e.g., 1st party / 3rd party)
- Limits & retention levels (DWP, AWP, CWP, NWP)
- Types of insureds (size / sector) & geographies
- Loss ratios, number of claims paid / reported etc.
- Impact on lines of business results in financial statements

Balance Sheet Items

- PMLs – incl. and excl. attritional losses; gross and net; model vs management's view; impact from any model adjustments
- Deterministic scenarios – description of events, comparison to PMLs
- Stress for BCAR: still use "larger of" (nat cat / terrorism / surety / cyber etc.)

How Companies are Managing Cyber Risks

How Companies are Managing Cyber Risks

- Managing exposure through underwriting and risk transfer
  - Detailed UW application/questionnaire
  - Policy wording (i.e., war exclusions, addressing “silent” cyber)
  - Coverage terms and conditions
  - Utilizing vendor tools
  - Assessing aggregation risk
  - Risk transfer through cyber reinsurance treaties/ILS
- Cyber specialists: real-time exposure monitoring
- Cyber models continue to mature
- Data quality and consistency continue to improve

Q&A

Thank You

Disclaimer

23.MK161AMBRS16x9

Our Insight, Your Advantage™

NAIC NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS

MEMORANDUM

TO: Cynthia Amann, Chair of the Cybersecurity (H) Working Group

FROM: Judy Weaver, Facilitator of the Chief Financial Regulator Forum

DATE: August 16, 2024

RE: Data Security Model Compliance Testing

During its August 12, 2024, meeting, the Chief Financial Regulator Forum discussed whether and how testing for compliance with the Insurance Data Security Model Law (NAIC #668) should be incorporated into full-scope financial condition examinations. In addition, the group discussed whether and how any findings associated with such compliance testing should be communicated across states.

Now that many states have adopted Model #668 or similar requirements (25 as of Spring 2024), as well as the significant amount of overlap between Model compliance testing and what is typically covered in a financial exam IT Review, many states have begun incorporating some compliance testing procedures into their financial examinations. In fact, the IT Examination (E) Working Group has developed a mapping between Model #668 compliance requirements and the IT Review procedures included in the NAIC's *Financial Condition Examiners Handbook* to assist in synchronizing test procedures in this area (see **Attachment A**).

In many cases, states conducting Model #668 compliance test procedures include their findings in a regulator-only management letter as opposed to the public report of examination, due to the sensitivity of IT security topics. Such management letters are generally posted to the regulator-only Financial Examination Electronic Tracking System (FEETS) in iSite+ for sharing with other states.

However, the practices of conducting Model #668 compliance testing procedures and reporting results in a management letter are not consistently applied across all states and are not codified as clear expectations for the lead/domestic state to perform in financial examination guidance.

Additionally, some states may be conducting Model #668 compliance testing procedures on licensed companies through market conduct examinations, given related guidance incorporated into the NAIC's *Market Regulation Handbook*. The lack of clear guidance and expectations for compliance testing and reporting responsibilities has the potential to lead to overlap and duplication of efforts across states and functions.

As the Cybersecurity (H) Working Group is charged with supporting the states with implementation efforts related to the adoption of Model #668, the Chief Financial Regulator Forum is referring these issues for your consideration. For example, questions that could be answered by the Working Group include, but are not limited to, the following:

- Should Model #668 compliance test procedures be incorporated into each full-scope financial condition examination where at least one licensed state has adopted Model #668 or similar requirements?
- Should Model #668 findings be incorporated into regulator-only management letters (or similar communication tools) with the results shared across all licensed states?

Once policy decisions have been made in these areas, we recommend that they be communicated to other relevant NAIC groups for implementation (i.e., IT Examination (E) Working Group, Market Conduct Examination Guidelines (D) Working Group).

If there are any questions regarding the referral, please contact either me or NAIC staff (Bruce Jenson at *bjenson@naic.org*) for clarification. Thank you for your consideration of this important issue.

NOTE: This document is designed as a resource for examiners to use in finding related procedures between the Model Law and Exhibit C. Risk statements and procedures should be customized depending on the situation of the company. This tool should only be used in states that have enacted the *NAIC Insurance Data Security Model Law* (#668). Moreover, in performing work during an exam in relation to the Model Law, it is important the examiners first obtain an understanding and leverage the work performed by other units in the department including but not limited to Market Conduct related work.

Model Law Ref. #	Model Law - General Description	Exhibit C Ref. #	Risk Statement	Control/Test Procedure
D(1)	IT structure/program appropriate to support business activities.	APO 01	IT organizational structure is inadequate to support business objectives.	(Multiple)
D(2)a	Access Controls - Place access controls on Information Systems, including controls to authenticate and permit access only to Authorized Individuals to protect against the unauthorized acquisition of Nonpublic Information;	DSS 05.04	The company's business is threatened by the impact of operational information security vulnerabilities and incidents.	(Multiple)
		APO 10	Third-party service provider risks are not properly assessed, addressed, and mitigated.	The company has a formal process in place whereby: 1) Risk is assessed based on the company's understanding of the third-party service providers information security program as well as by the company's ability to verify elements of the third-party service provider's security program; 2) Based on the company's risk, the company ranks vendors and uses a vendors ranking to determine depth and frequency of review procedures performed related to ongoing vendor relationships; 3) The company determines appropriate access rights, based on the risk assessment and company needs; 4) The company designs specific mitigation strategies, including network monitoring specific to third-party service providers and **access controls**, where appropriate.
D(2)b	Managing Personal Data - Identify and manage the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes in accordance with their relative importance to business objectives and the organization's risk strategy;	APO 03	Enterprise goals may not be met because the data and systems architecture is poorly defined and/or fragmented.	The company has an information architecture model that addresses the creation, use and sharing of data between applications that maintain data integrity, flexibility, functionality, cost-effectiveness, timeliness, security and availability.
		DSS 05.01	The company's business is threatened by the impact of operational information security vulnerabilities and incidents.	(Multiple)
D(2)c	Physical access - Restrict access at physical locations containing Nonpublic Information, only to Authorized Individuals;	DSS 05.05	The company's business is threatened by the impact of operational information security vulnerabilities and incidents.	Procedures are defined and implemented to grant, limit and revoke access to premises, buildings and areas, according to business needs, including during emergencies.
D(2)d	Data encryption - Protect by encryption or other appropriate means, all Nonpublic Information while being transmitted over an external network and all Nonpublic Information stored on a laptop computer or other portable computing or storage device or media;	DSS 05.02	The company's business is threatened by the impact of operational information security vulnerabilities and incidents.	Sensitive data is exchanged only over a trusted path or medium, with controls to provide authenticity of content, proof of submission, proof of receipt and non-repudiation of origin.
		DSS 05.07	The company's business is threatened by the impact of operational information security vulnerabilities and incidents.	The company has an established company-wide IT security baseline and periodically tests and monitors its IT security implementation for compliance with that baseline. Protection against data leaks are implemented
D(2)e	Application Security - Adopt secure development practices for in-house developed applications utilized by the Licensee and procedures for evaluating, assessing or testing the security of externally developed applications utilized by the Licensee;	BAI 01	IT projects may fail to meet business objectives/ERM goals or run over budget in the absence of an effective program and project-management methodology.	A methodology exists to maintain the portfolio of projects that includes identifying, defining, evaluating, prioritizing, selecting, initiating, managing and controlling projects.
		BAI 03.05	Project deliverables fail to meet business objectives due to inadequate design and/or ineffective oversight of implementation.	(Multiple)
		APO 03	Enterprise goals may not be met because the data and systems architecture is poorly defined and/or fragmented.	The company has an information architecture model that addresses the creation, use and sharing of data between applications that maintain data integrity, flexibility, functionality, cost-effectiveness, timeliness, security and availability.
D(2)f	Compliance with Information Security Program - Modify the Information System in accordance with the Licensee's Information Security Program;	BAI 06&07	A lack of proper change management threatens system stability and/or integrity.	The company has a process in place to record, authorize, manage, monitor and implement requests for changes. Procedures exist to ensure documentation is appropriately updated and distributed to affected users and IT staff upon completion of change.
D(2)g	Authentication Procedures - Utilize effective controls, which may include Multi-Factor Authentication procedures for any individual accessing Nonpublic Information;	DSS 05.04	The company's business is threatened by the impact of operational information security vulnerabilities and incidents.	User identities are enabled via authentication mechanisms including multi-factor authentication for remote access, as appropriate based on the sensitivity of the information which may be accessed.
D(2)h	System Monitoring - Regularly test and monitor systems and procedures to detect actual and attempted attacks on, or intrusions into, Information Systems;Regularly test and monitor systems and procedures to detect actual and attempted attacks on, or intrusions into, Information Systems;	DSS 05.07	The company's business is threatened by the impact of operational information security vulnerabilities and incidents.	The company has an established company-wide IT security baseline and periodically tests and monitors its IT security implementation for compliance with that baseline.
D(2)i	Audit Trails - Include audit trails within the Information Security Program designed to detect and respond to Cybersecurity Events and designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Licensee;	DSS 01.03	The quality, timeliness and availability of business data is reduced due to an ineffective data-management process.	IT infrastructure activity is logged with sufficient detail to reconstruct, review and examine operational activities; this activity is monitored on a regular basis.
		DSS 03.01&02	The company has an ineffective problem-management process that increases operating costs and reduces system availability, service levels and customer satisfaction.	The company maintains problem-management policies and procedures, including escalation triggers, with adequate audit trails and analysis to identify, report and classify incidents by category, impact, urgency and priority.
				The company has implemented a problem-management system that identifies and initiates solutions addressing the root cause of the problem and provides adequate audit trail facilities that allow tracking, analyzing and determining the root cause of all reported problems.
D(2)j	Environmental Hazards - Implement measures to protect against destruction, loss, or damage of Nonpublic Information due to environmental hazards, such as fire and water damage or other catastrophes or technological failures: and	DSS 01.04	Inadequate physical and environmental controls may result in unauthorized access and inadequate protection of data.	The data center contains proper physical and environmental controls to protect the equipment, data and personnel located within.
		DSS 04.07	Inadequate continuity management may result in the inability to ensure critical business functions.	All critical backup media, documentation and other IT resources necessary for IT recovery and continuity plans are stored off-site in a secure location.
D(2)k	Information Disposal - Develop, implement, and maintain procedures for the secure disposal of Nonpublic Information in any format.	DSS 05.06	The company's business is threatened by the impact of operational information security vulnerabilities and incidents.	Procedures are in place to ensure that business requirements for protection of sensitive data and software are met upon disposal or transfer of data and hardware (endpoints, mobile devices, network devices, servers, portable media and hard drives).
D(3)	ERM Intergation - Include cybersecurity risks in the Licensee's enterprise risk management process.	APO 12	IT-related enterprise risks have not been integrated into the overall enterprise risk management (ERM) program.	(Multiple)

Model Law Ref. #	Model Law - General Description	Exhibit C Ref. #	Risk Statement	Control/Test Procedure
D(4)	Emerging Threats - Stay informed regarding emerging threats or vulnerabilities and utilize reasonable security measures when sharing information relative to the character of the sharing and the type of information shared; and	DSS 05.07	The company's business is threatened by the impact of operational information security vulnerabilities and incidents.	Threat and vulnerability information received from information-sharing forums and sources (e.g., Financial Services Information Sharing and Analysis Center, etc.) is used in developing a risk profile.
D(5)	Provide cybersecurity training - Provide its personnel with cybersecurity awareness training that is updated as necessary to reflect risks identified by the Licensee in the Risk Assessment.	APO 01	IT organizational structure is inadequate to support business objectives.	Review training programs and schedules to confirm that management and employees are provided with sufficient training to understand the importance of compliance with IT and cybersecurity policies, including awareness of concepts of phishing, malware, and data loss prevention, as appropriate.
E(1)	Require the Licensee's executive management or its delegates to develop, implement, and maintain the Licensee's Information Security Program	APO 01	IT organizational structure is inadequate to support business objectives.	The company's IT management organizational structure, with clearly defined roles and responsibilities, supports business objectives and IT priorities and enables efficient decision making.
E(2)a	Annual reporting of the overall status of the Information Security Program and the Licensee's compliance with this Act	MEA 03	IT processes and IT-supported business processes are not compliant with applicable laws, regulations, and other contractual requirements.	A procedure has been implemented to review and report compliance of IT policies, standards, procedures and methodologies with applicable legal and regulatory requirements.
E(2)b	Annual reporting of material matters related to the Information Security Program, addressing issues such as risk assessment, risk management and control decisions, Third-Party Service Provider arrangements, results of testing, Cybersecurity Events or violations and management's responses thereto, and recommendations for changes in the Information Security Program.	MEA 01	The company does not properly identify and address IT performance and conformance deficiencies.	The company has adopted and implemented a formalized monitoring framework to define the scope, methodology and process to be followed for measuring IT's solution, service delivery and contribution to the company, including tracking corrective actions to address anomolies.
E(3)	If executive management delegates any of its responsibilities under Section 4 of this Act, it shall oversee the development, implementation and maintenance of the Licensee's Information Security Program prepared by the delegate(s) and shall receive a report from the delegate(s) complying with the requirements of the report to the Board of Directors above.	APO 01	IT organizational structure is inadequate to support business objectives.	The company's IT management organizational structure, with clearly defined roles and responsibilities, supports business objectives and IT priorities and enables efficient decision making.
F(1)	A Licensee shall exercise due diligence in selecting its Third-Party Service Provider	APO 10	Third-party service provider risks are not properly assessed, addressed, and mitigated.	The company has a formal process in place whereby: 1) Risk is assessed based on the company's understanding of the third-party service providers information security program as well as by the company's ability to verify elements of the third-party service provider's security program; 2) Based on the company's risk, the company ranks vendors and uses a vendors ranking to determine depth and frequency of review procedures performed related to ongoing vendor relationships; 3) The company determines appropriate access rights, based on the risk assessment and company needs; 4) The company designs specific mitigation strategies, including network monitoring specific to third-party service providers and **access controls**, where
F(2)	A Licensee shall require a Third-Party Service Provider to implement appropriate administrative, technical, and physical measures to protect and secure the Information Systems and Nonpublic Information that are accessible to, or held by, the Third-Party Service Provider	APO 10	Third-party service provider risks are not properly assessed, addressed, and mitigated.	The company has a formal process in place whereby: 1) Risk is assessed based on the company's understanding of the third-party service providers information security program as well as by the company's ability to verify elements of the third-party service provider's security program; 2) Based on the company's risk, the company ranks vendors and uses a vendors ranking to determine depth and frequency of review procedures performed related to ongoing vendor relationships; 3) The company determines appropriate access rights, based on the risk assessment and company needs; 4) The company designs specific mitigation strategies, including network monitoring specific to third-party service providers and **access controls**, where appropriate.