Marsh

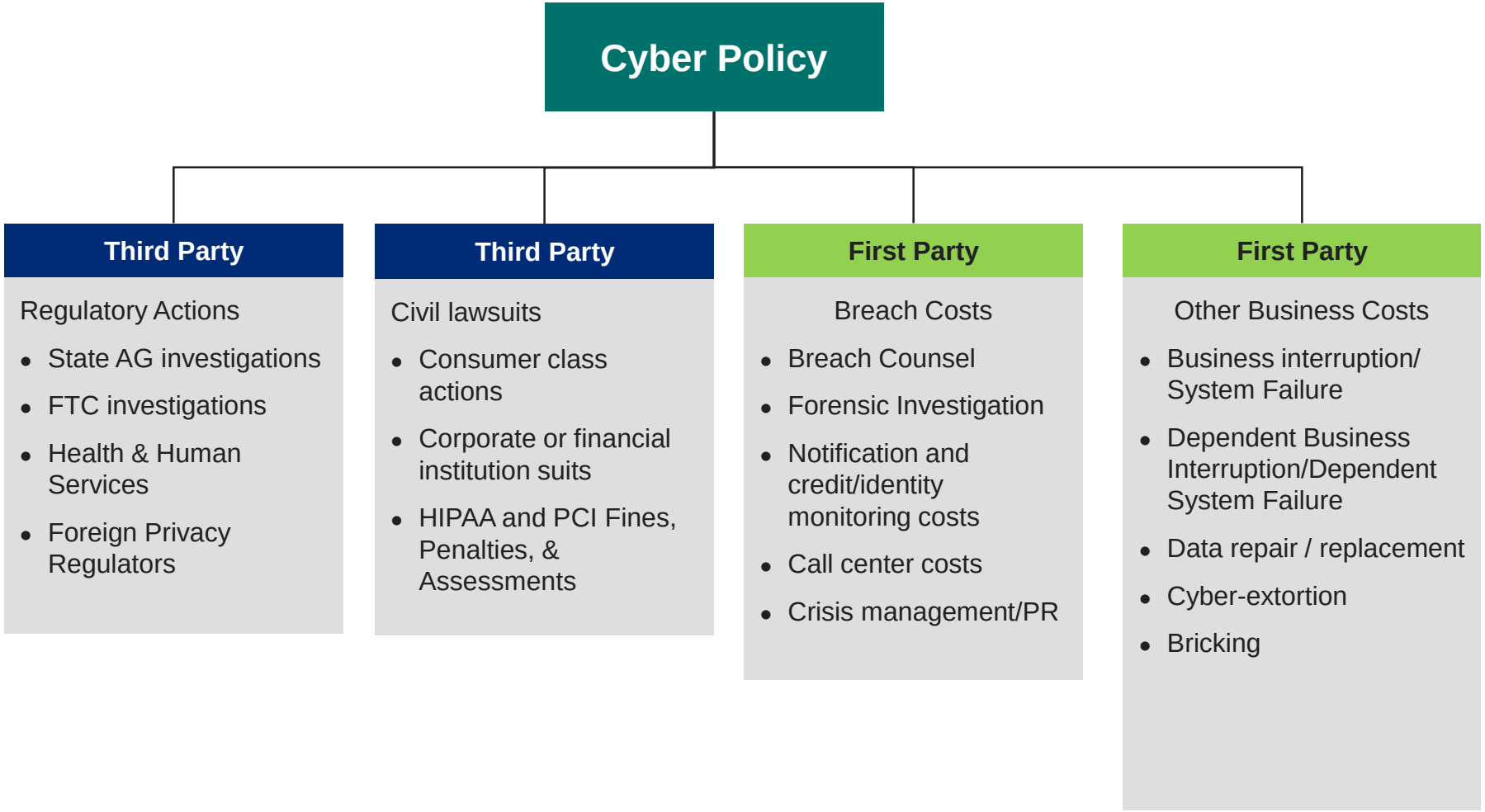
Marsh McLennan Agency

2022 NC Primary Care Conference

Cyber Insurance Market Update

May 2022

Cyber Insurance Coverage Structure



Macro Cyber Trends: Insurance Market Challenges

Ransomware: Amplified underwriting scrutiny; controls based risk selection

Market Contraction/ Aggregation concerns: Reduction in limits deployed; significantly higher price for limits (reinsurance cost); capital is now selectively deployed

Coverage: Scope of coverage being scrutinized due to unexpected frequency and severity of losses, deteriorating profitability

Premium/Pricing: Rating models revised to factor in higher frequency and severity of losses, faster claim payments (short tail and also long tail) as well as systemic (widespread) events (e.g. Log4j)

Underwriting authority: Increased awareness of aggregated cyber incidents and supply chain risks by management at insurance companies has led to slow decision making, little underwriting authority, and no flexibility by underwriters

Macro Cyber Trends: Cyber Market Dynamics

Frequency and severity of claims drives a rapid shift in the marketplace

Soft cyber market

2015 - 2018

- Profitable product with loss ratios < 50% each year
- Increase in available capital from new entrants each year
- Flat to decreasing rates – supply outpaced demand

Claims start to impact

2019

- Product still profitable for long term players; but claims pick up and loss ratio for several insurers > 100%
- Insurers scrutinize their portfolios and approach to underwriting
- Uptick in the price of risk remains modest for many

Claims accelerate

2020

- Ransomware drives significant increase in claims activity and losses
- Insurers challenged to profitably underwrite to their portfolio and the scope of the product
- Price of risk starts to rise

Insurers adjusting

2021

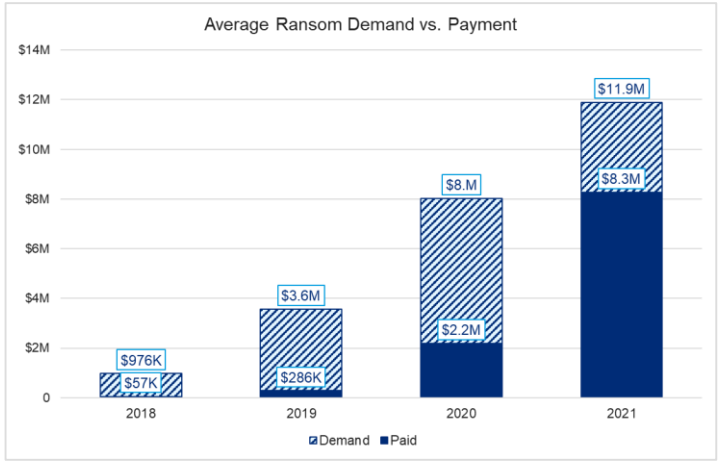
- Ransomware continues to drive losses
- Some insurers exit cyber market; others evolve underwriting to focus on security controls that are correlated to loss mitigation
- Material increases in the price of risk, including significantly higher CAT loads informed by modelling

2022 Cyber Risk Environment

Dominated by ransomware, regulations & supply chain cyber risk

Increasing controls drive improved outcomes, but drive more focus on ransomware sophistication:

- **42% of ransomware victims had viable backups in 2021** – up from 23% in 2020 – meaning more companies were able to avoid paying ransoms.



- **The difference between the average ransom demanded ($11.9M)** and the **average ransom paid ($8.3M)** is decreasing as sophistication has grown (aided by data exfiltration) and threat actors more effectively attack targets.
  - Large insurer: $40M paid
  - Oil pipeline: $4.4M paid
  - Infrastructure: $50M demanded
  - Food manufacturer: $11M paid
  - Chemical distribution:$4.4M paid
  - Tech hardware: $50M demanded

Systemic risk concerns intensify:

- **Aggregation** exposure is a concern for underwriters
- **Systemic loss** – possible cyber risks:
  - Common vulnerabilities – in hardware or software
  - Common dependencies – vendors (such as cloud providers) and software
- **Cyber/digital supply chain vulnerabilities** are driving increased scrutiny: SolarWinds, Accellion, Microsoft Exchange, Kaseya & Log4j

Privacy regulations evolve; patchwork approach remains:

- **GDPR** fines are growing (~$27M BA, ~$24M Marriott, ~$41M H&M)
- **CCPA** (California Consumer Privacy Act) and similar legislation (i.e. VA CDPA) allow for private rights of action with per consumer statutory damages and require additional compliance efforts
- **BIPA** (IL Biometric Information Privacy Act) litigation is expensive and is on the rise with increased use of biometric identifiers, especially for employee access – driving additional underwriting questions. 45 states have existing / pending biometric privacy legislation.

Sources: Coveware Ransomware Blog & MMC Cyber Analytics Center

Top Cybersecurity Controls

The key to insurability, mitigation, and resilience

Preparation for the underwriting process:

1. Start early! Without positive responses in the top 12 control categories, coverage offered and insurability may be in question.
2. Evaluate your cybersecurity maturity by reviewing required applications – where improvements are needed, leverage MMA's Cyber Resiliency Network
3. Expect more rigorous underwriting and more detailed questions from underwriters.

Multifactor authentication for remote access and admin/privileged controls

Endpoint Detection and Response (EDR)

Secured, encrypted, and tested backups

Privileged Access Management (PAM)

Email filtering and web security

Patch management and vulnerability management

Cyber incident response planning and testing

Cybersecurity awareness training and phishing testing

Hardening techniques, including Remote Desktop Protocol (RDP) mitigation

Logging and monitoring/network protections

End-of-life systems replaced or protected

Vendor/digital supply chain risk management

Note: Each insurance carrier has their own specific control requirements that may differ by company revenue size & industry class. For more on the Cyber hygiene see: Cyber hygiene controls critical as cyber threats intensify (marsh.com)

US Cyber – All Industries

Q1 2022 Market Conditions

Rate Ranges

- Q1 Average Total Program increase of +109.9%
- Q1 Median Total Program increase of +81.7%
- Q1 rate ranges do not include renewals with changes in limits
- 30.2% of clients reduced their total limits in Q1

Client Experience

- 66.5% of clients increased their retention in Q1
- 8.0% of clients increased their total limits in Q1
- Insureds are still being pushed to increase retentions and/or reduce total limits purchased to manage overall premium increase

Coverage/Capacity

- Capacity contraction continues with many carriers managing down to $5M or $10M on any single risk
- Ransomware, contingent business interruption, and privacy regulatory coverage restrictions are common.
- Introduction of territorial exclusions due to Russia/Ukraine conflict
- Increase of non-concurrencies in towers

Condition Drivers

- Baseline cybersecurity controls are a requirement to securing broad coverage
- Insurer concerns regarding the potential for correlated cyber losses is significant and growing
- Insurers continue to set new price per million metrics on all accounts and across all industries

Looking Ahead

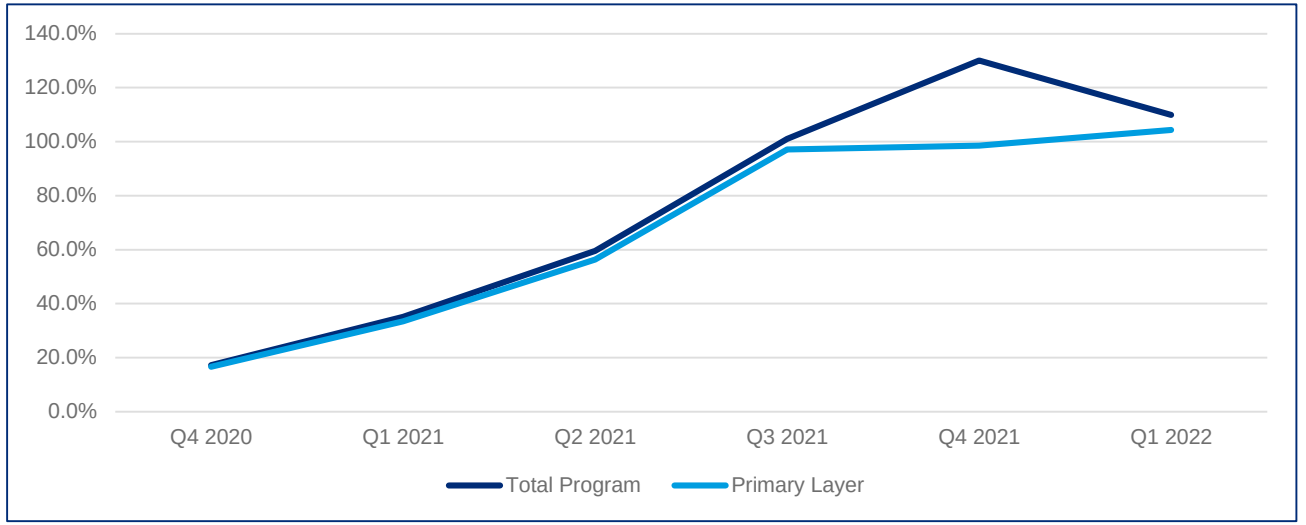
- Insureds are continuing to invest in cybersecurity improvements
- Premium rates are still increasing but at a decreasing rate and will continue throughout H2 2022
- Captives are increasingly being contemplated as a complementary component of cyber risk transfer strategies & solutions

Cyber Market Conditions

Q1 2022 – All Industries

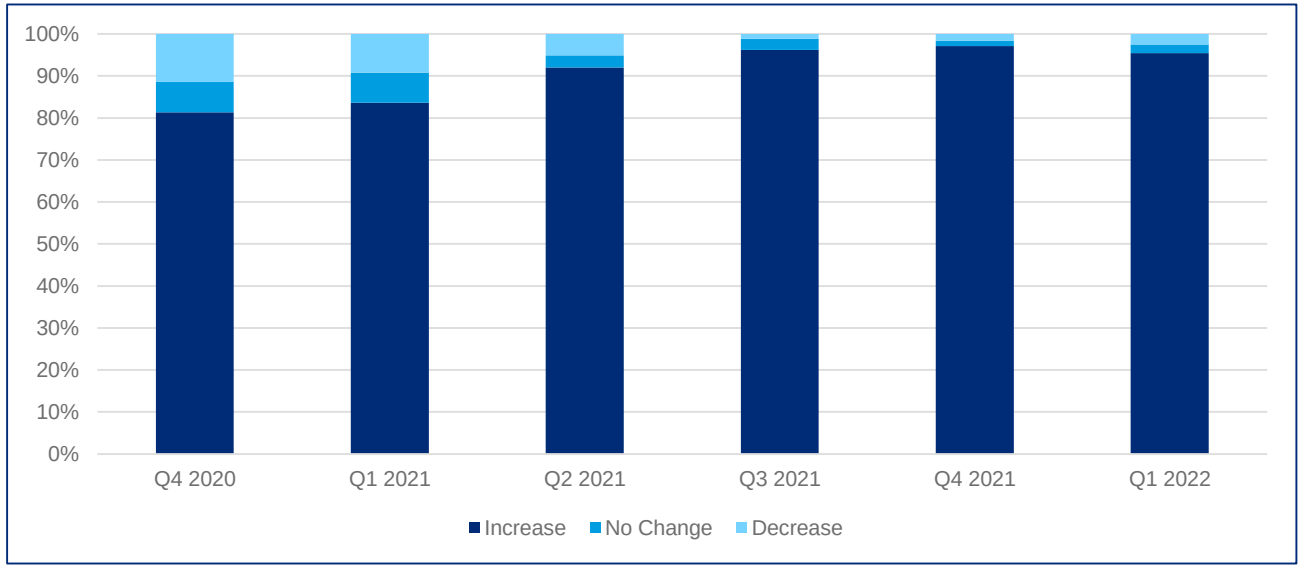
Rate Trends

	Q1 2022	Trend
Average Primary	+104.3%	▲
Median Primary	+78.6%	▲
Average Total Program	+109.9%	▼
Median Total Program	+81.7%	▼



Percent of Clients with Pricing Changes

	Q1 2022	Trend
Increase	95.4%	▼
No Change	2.1%	▼
Decrease	2.5%	▼



US Cyber – HealthCare

Q1 2022 Market Conditions

Rate Ranges

- Q1 Average Total Program increase of +119.8%
- Q1 Average Primary increase of +102.0%
- Q1 Median Total Program increase of +115.4%
- Q1 Median Primary increase of +88.5%
- Rate ranges do not include renewals with changes in limits

Client Experience

- 67.9% of clients increased their retention in Q1
- 25.6% of clients reduced their total limits in Q1
- 12.8% of clients increased their total limits in Q1

Coverage/Capacity

- Capacity contraction has accelerated with most carriers managing down to $5M on any single Healthcare risk and prefer attachment point excess of $50M for larger risks
- Some insurers are either non-renewing or have limited appetite to underwrite risks in this industry segment
- Healthcare remains a high hazard class of business with Health Tech and Health Systems viewed as the riskiest

Condition Drivers

- The high frequency and severity of ransomware claims in the healthcare industry is the top trend affecting the market
- Health Systems may operate numerous end of life devices that serve a specific function in the delivery of care to patients. Carriers are concerned with endpoints that can no longer be supported by patches and updates
- M&A activity in the industry remains high with no signs of slowdown in 2022. Carriers are becoming more focused on target company IT Security controls and the parent orgs plans for IT Security oversight, management and integration.

Looking Ahead

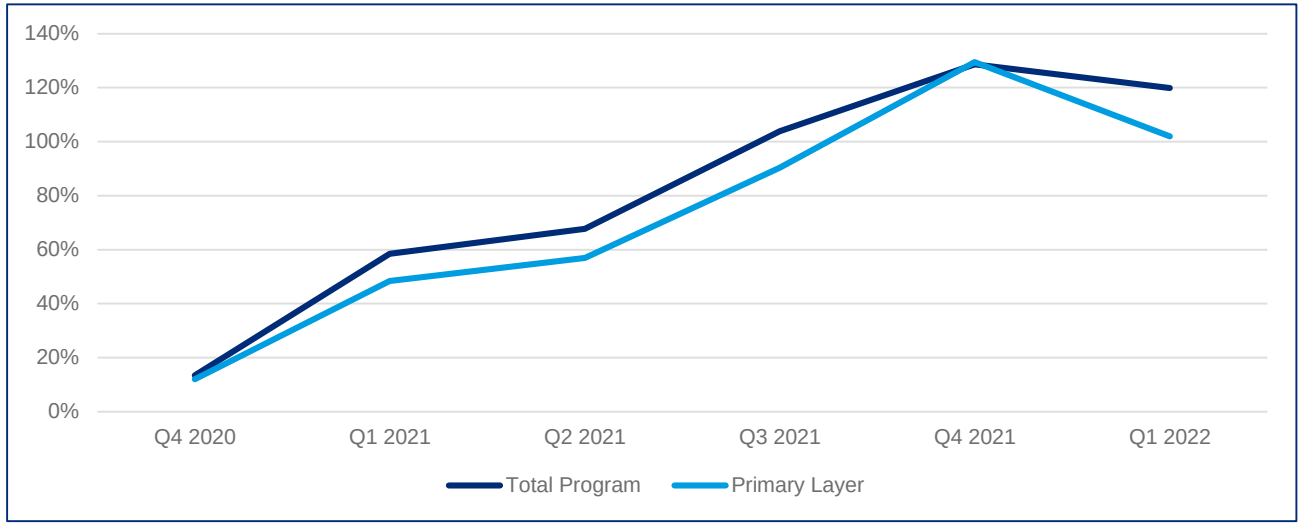
- Healthcare continues to be viewed as a particularly challenging class of business
- Underwriting scrutiny will continue to increase with greater scrutiny and oversight on key IT security controls.
- Premium rates are still increasing but at a decreasing rate and will continue throughout H2 2022

Cyber Market Conditions

Q1 2022 – HealthCare

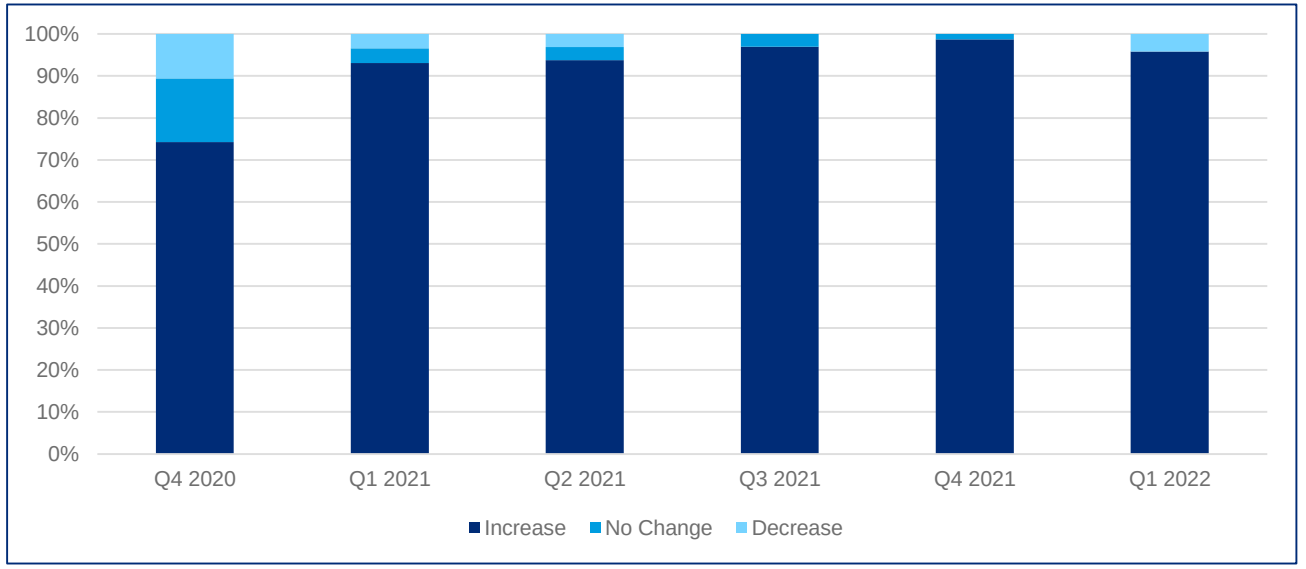
Rate Trends

	Q1 2022	Trend
Average Primary	+102.0%	▼
Median Primary	+88.5%	▼
Average Total Program	+119.8%	▲
Median Total Program	+115.4%	▲



Percent of Clients with Pricing Changes

	Q1 2022	Trend
Increase	95.8%	▲
No Change	0%	▲
Decrease	4.2%	▲



Cyber Insurance Market Snapshot

Favors Buyer | Neutral | Favors Insurers

Claims & Rates

Claims frequency and severity remains high driven by ransomware. Ransomware, systemic risk & regulations continue to drive concern.

Losses have accelerated pricing pressure even on loss free accounts with good controls. Excess pricing is increasing faster than primary, compounding increases. Expect increases to continue into 2022.

December 2021 Cyber Premiums:

+154%

Avg increase all renewals*

*All renewals include limits changes.

Structure & Coverage

Insurers are aggressively managing global capacity & increasing SIRs. Distressed classes & large towers may see capacity challenges.

Some insurers imposing more restrictive coverage on ransomware, contingent business interruption (systemic risk), regulatory cover (biometric information), etc.

December 2021 Cyber Renewals:

32% reduced limits

7% increased limits

68% increased SIRs

Driven by insureds minimizing increases & less available capacity.

Underwriting

Full application & responses to ransomware Q's are required; carriers using 3rd parties to externally scan environments.

Also expect inquiries on recent supply chain events including Log4j, biometric info, & operational technology.

12

Key Controls & Best Practices are now viewed by carriers as essential

Marsh McLennan Agency Team

Bryan Beasley

Consultant – Non-Profit Practice Group Leader

336-209-6466

Bryan.Beasley@marshmma.com

Russell James

Consultant – Financial Practice Group Leader

919-397-6675

Russell.james@marshmma.com