MarshMcLennan Agency

OALA
Ohio Assisted Living Association

2025 Spring Conference

May 14, 2025

Dr. Louis DeWeaver – Cyber Security Consultant
Jake Pease CIC, CEAL, CEHCH— Vice President

Agenda

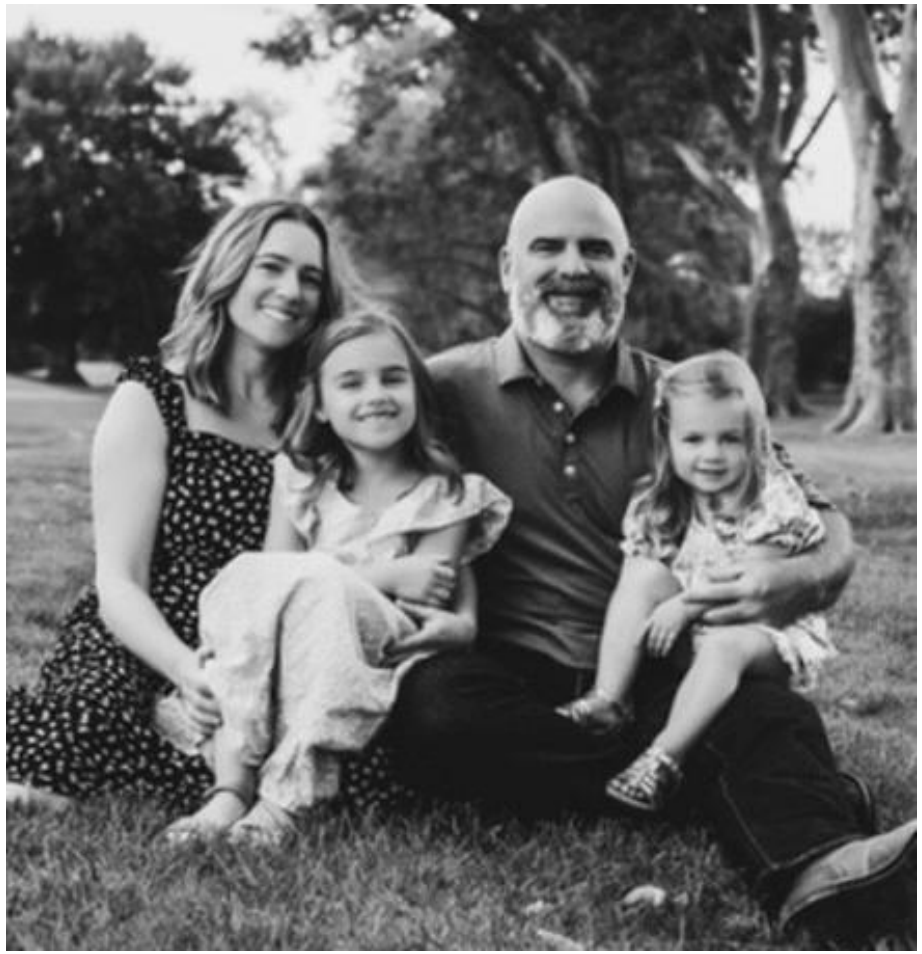
- Speaker Introductions
- Insurance Market Update
- Cyber Liability – Network Security

Jake Pease – Vice President, MMA - CIC, CEAL, CEHCH

For the past 15 years Jake Pease has partnered with healthcare providers to protect their assets and improve their profitability so they may focus on providing care to their staff and patients. He takes pride in educating himself on market changes, developing relationships built on trust, and identifying areas for growth. Prior to MMA, Jake led the healthcare and aging service provider practice at one of the nation's largest independent insurance brokerage firms. Jake crafts traditional programs, alternative strategies for clients in the form of risk retention groups and captive formation. Jake sources solutions for employee benefits and retirement planning, and key person buy sell arrangements.

Jake is a graduate of Baldwin Wallace University. He holds his Certified Insurance Counselor (CIC), Certified Executive for Assisted Living (CEAL), and Certified Executive Homecare and Hospice (CEHCH) designations. Jake is an active presenter with Ohio Council for Home Care & Hospice (OCHCH), Ohio Assisted Living Association (OALA) Ohio Healthcare Association (OHCA), and LeadingAge Ohio. He instructs Insurance 101 for LNHA-CORE.

Jake resides in Westlake Ohio with wife Ashley, daughters Priscilla and Vivian. A lifelong Clevelander Jake is a vested sports fan, crummy golfer, and landscaping enthusiast. In free time he is with his girls smiling and having adventures.



Senior living team overview

100+

Combined years insuring senior living organizations

400K+

beds/units insured across the U.S.

125+

dedicated senior living insurance professionals

80+

senior living insurance carriers

1,500+

Clients nationwide

$750M+

In premiums placed annually

Senior Living

captive insurance company and TPA

How we minimize risk and maximize health

Our holistic approach to risk services:

Innovative program design | Compliance | Wellness | Safety | Claims | Risk transfer | Positive measurable results

Our risk management goal:

1 Create value for clients 3x revenue received

2 Use analytics to change our clients' loss portfolio

3 Provide specialized senior living risk management team

Insurance Market

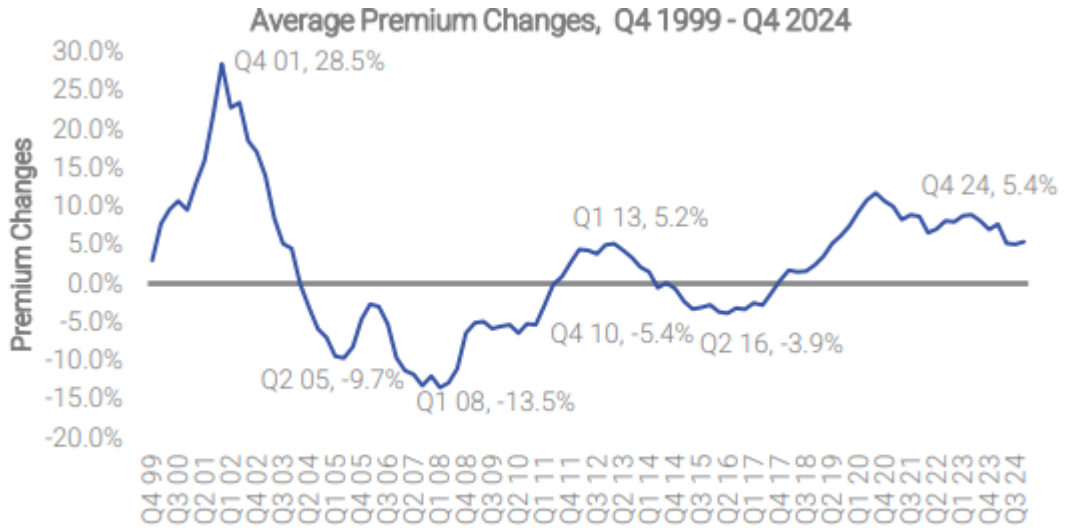
Market conditions

HARD vs. SOFT Market

What drives the volatility?

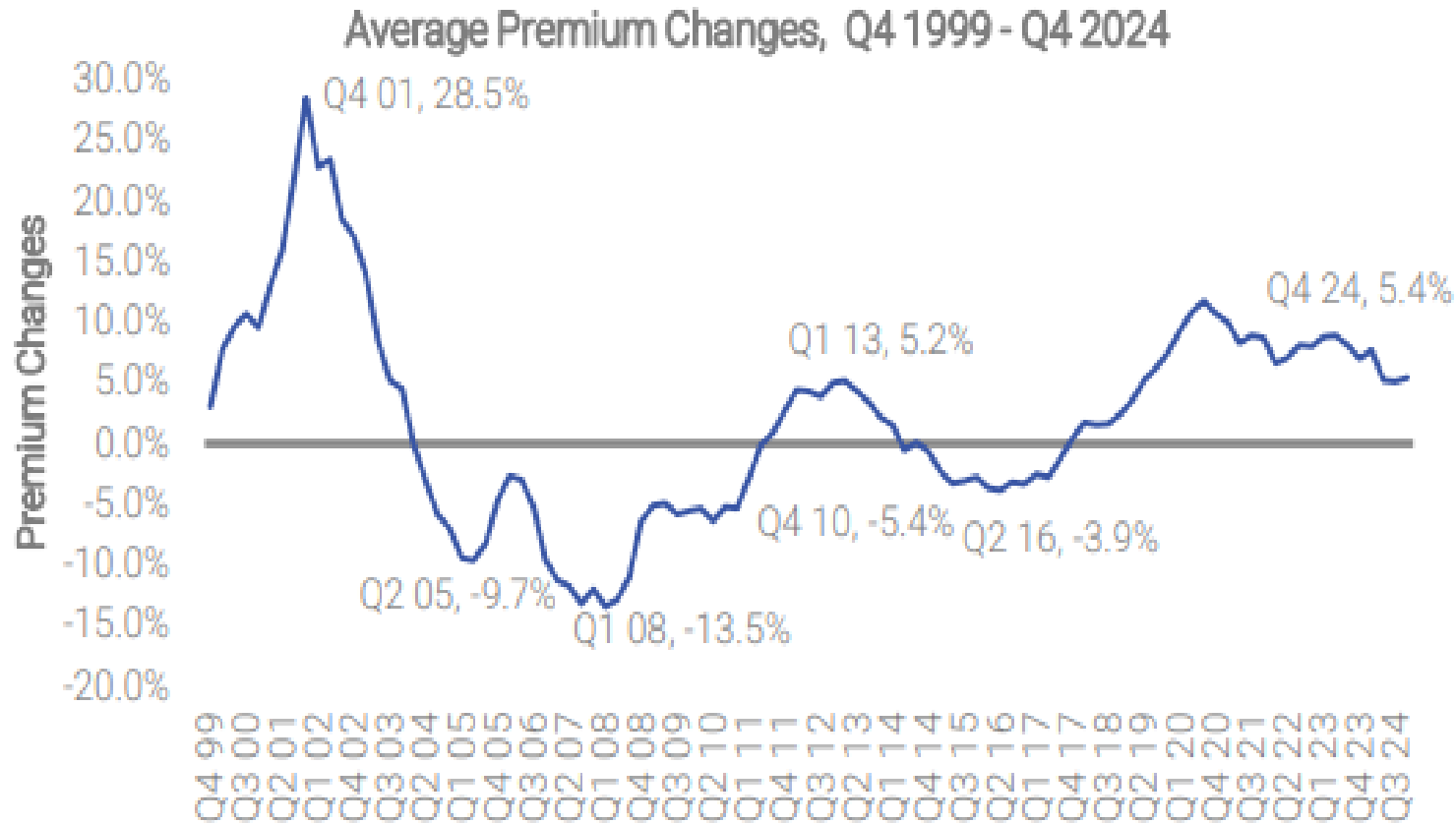
- Carrier profit
- Losses (Frequency – Severity)
- Classes of business (High or Low Risk)
- Underwriting posture
- Legislation / Jurisdiction
- Restoration costs (inflation)
- Social Inflation (verdict $ awards)
- Third Party Litigation Funding
- General inflation (labor material)

The end of 2024 came with no real change in current market conditions. Q4 was the 29th consecutive quarter of premium increase. Premiums across all account sizes continued to climb at an average of 5.4%. Broker respondents reported challenges like less capacity or more information requests from carriers. Liability remains a key focus heading into 2025 as reinsurance capacity plays critical role, as loss development continues.



Source: The Council of Insurance Agents & Brokers

Market conditions



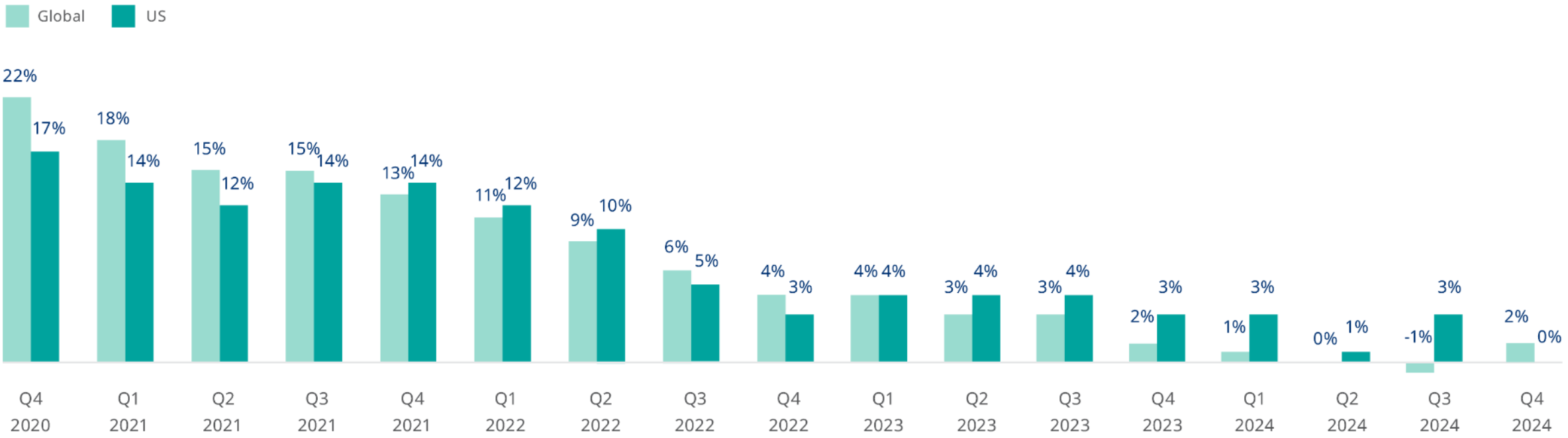
Source: The Council of Insurance Agents & Brokers

Market conditions

Q4 2024 market observations

The global composite rate tracked in the Marsh Global Insurance Market Index decreased by 2% in Q4. U.S. commercial insurance prices were flat in the fourth quarter of 2024. The overall decrease in the global index came despite an elevated risk landscape, with 2024 insured natural catastrophe losses totaling almost $130 billion, the fifth consecutive year in which the industry total has topped $100 billion.

U.S. composite insurance pricing change



Source: Marsh Specialty and Global Placement

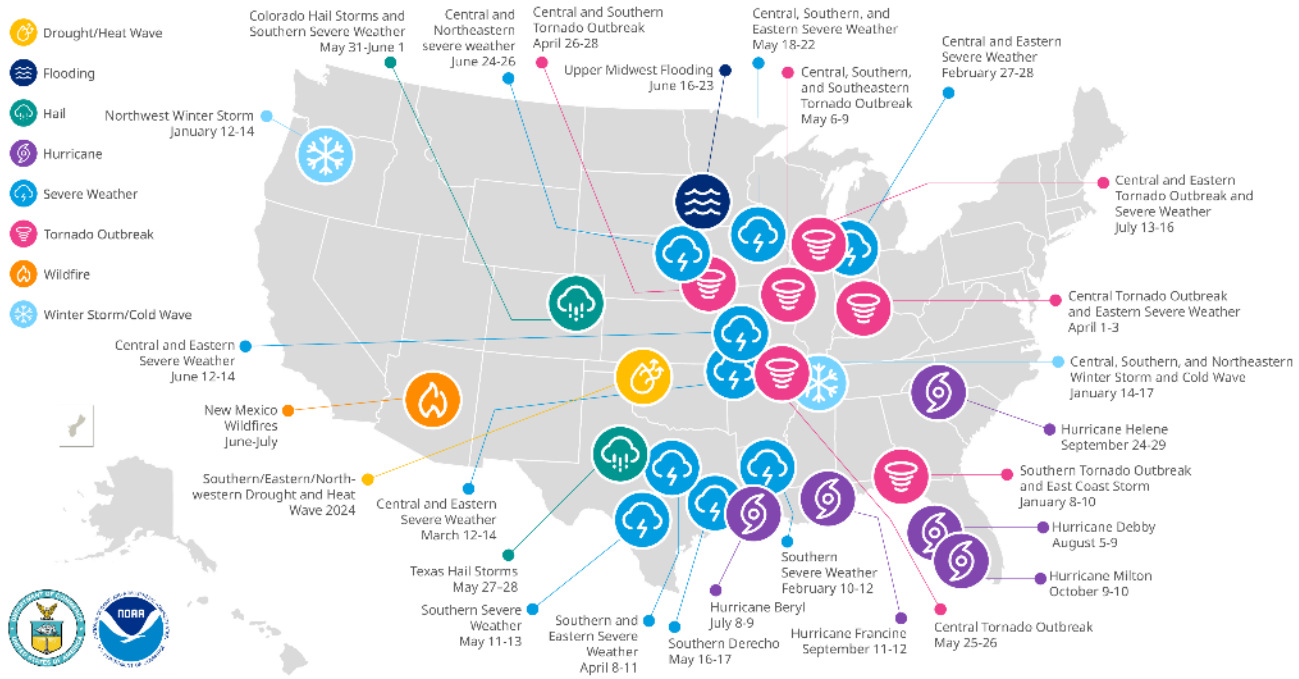
Property

Property coverages

- Property rates continued to stabilize through Q4 2024. Although hurricanes Helene and Milton caused significant destruction, they ended up being Q3 and Q4 earnings hits, respectively, rather than market-changing events.
- Initial insured loss estimates are in the range of $35 billion to $55 billion from the recent devastations caused by numerous California wildfires.
- The market remains bifurcated in that rate reductions can still be achieved on shared and layered programs by restructuring capacity and bringing in new markets that are aggressively looking to write business.
- In the single-carrier space, the market is more measured, with incumbents typically seeking modest rate increases.

Property coverages

The billion-dollar weather and climate disasters tracked by NOAA in 2024 resulted in 27 confirmed events in the U.S., with losses exceeding $1 billion.



This map denotes the approximate location for each of the **27 separate billion-dollar weather and climate disasters that impacted the United States in 2024.**

Overall, these events resulted in the deaths of 568 people and had significant economic effects on the areas impacted.

The 1980–2024 annual average is 9.0 events (CPI-adjusted); the annual average for the most recent five years (2020–2024) is 23.0 events (CPI-adjusted).

MMA can help your organization implement optionality, helping you understand alternative risk options such as structured solutions, parametric insurance, catastrophe bonds, and more.

Casualty aka Liability

Casualty coverages

Headwinds remain in the casualty marketplace as reinsurers become more selective and insurers re-evaluate their adverse development reserve positions.

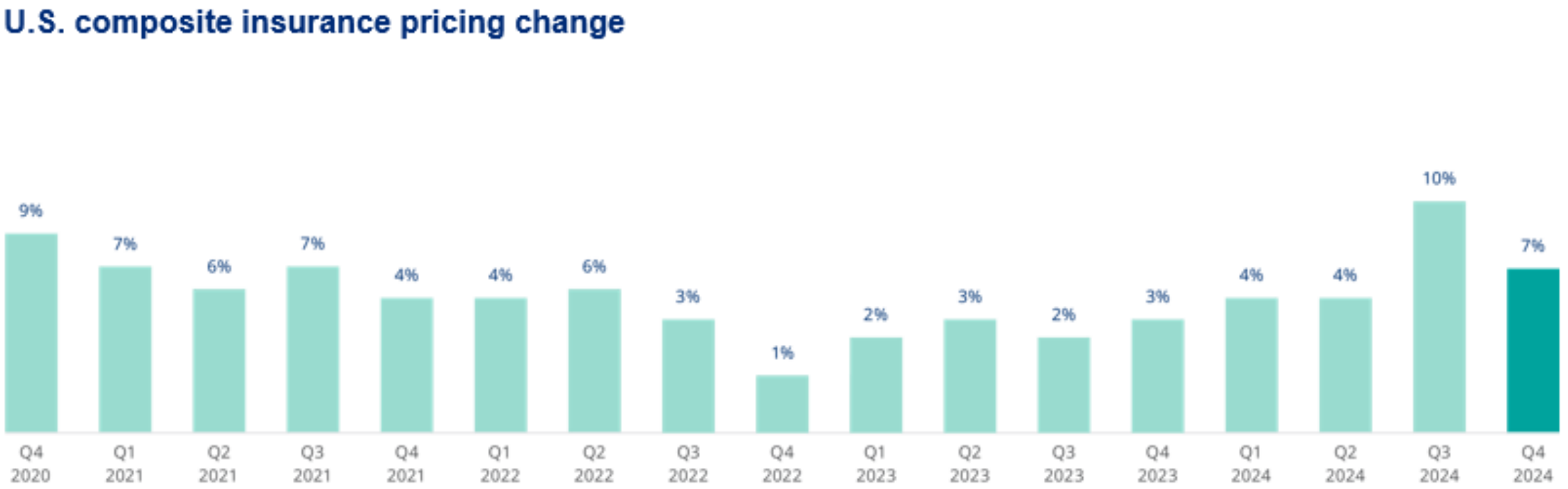
There's a good chance that **rate increases** are here to stay for the foreseeable future.

Primary coverage layer increases have been lagging behind the excess and umbrella layers in an unsustainable way.

There is some optimism around **new capacity** entering the market, and innovative solutions are likely to result from these novel market participants.

Liability continued

MMA Business Insurance U.S. Market Observation



Casualty coverages

Rate trends

Automobile/fleet

Average rate increases were between **5%** to **15%**, with higher double-digit increases for businesses with heavy trucks and/or adverse claims experience.

General liability

Rate increases are averaging from flat to single-digit percentages, and higher for risks with losses and/or product liability exposures. Flat renewal pricing can be achieved in some instances.

Umbrella/excess

The Marsh Global Insurance Market Index shows risk-adjusted rates increasing by **15%** compared to **21%** in the prior quarter. Where there was no program structure change, rates increased by **9%** and **20%**, respectively.

Workers' compensation

Rates generally remained flat or in negative territory, with decreases of around **-3%.**

Liability trends affecting healthcare

- Healthcare margins have been impacted by the pandemic but are improving. However, long-term challenges persist. Underwriting is cognizant of risk impacted by fiscal challenge.
- Greater labor and supply expenses, as well as rising patient acuity are a challenge.
- Private equity growing in healthcare adds to regulatory scrutiny of pricing and care.
- In senior care good risks should find stable to slightly favorable insurance pricing as carrier competition is finally increasing post pandemic. However, risks with adverse loss history or in litigation-prone venues will be challenged.
  - *As losses continue to outpace premiums, underwriters would like to obtain renewal increases. However, market competition overall is instead producing flat premiums to single digit decreases and this trend is expected to continue into 2025. Premium pressure is not being driven by new capacity but, rather, increased competition (particularly on larger accounts) as established markets try to increase market share. The exception is excess liability, where capacity continues to be limited, and care facilities can expect to see umbrella increases of 30% or more.*

Liability trends affecting healthcare (cont.)

- Reinsurers continue to push for SAM limitations or exclusions. As a result, primary markets are pulling back on limits and/or offering coverage only via a limited supplemental abuse endorsement. Obtaining affirmative coverage for SAM in excess layers is difficult. Underwriters also maintain their push for hired and non-owned auto exclusions.
- As more carriers without tailored healthcare forms enter the market, buyers and retailers should be cautious about lower premiums that may signal limited coverage or financial risk from newer, less established carriers. They must also evaluate if a carrier is financially stable and has a strong track record for paying claims.

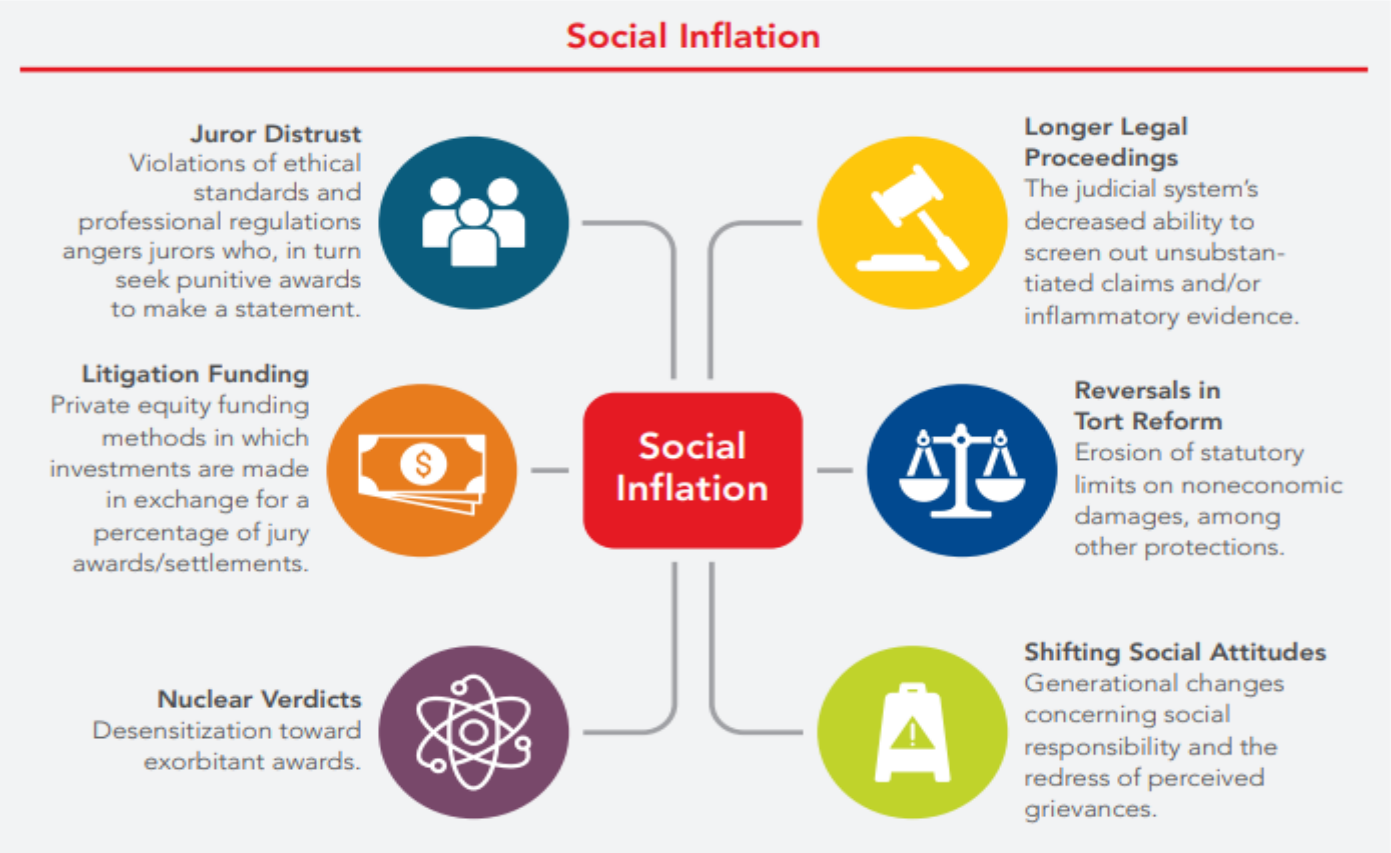
Additional impacts affecting clients

- As in other sectors, social inflation is leading to increased severity of claims and higher losses, driving costs up significantly and keeping pricing and terms from improving even more. The list of litigation hotbeds for healthcare providers continues to grow as states that used to be less litigious are now becoming more active. Cuyahoga, Hamilton, & Franklin. The 3 C cities.
- In this environment, the concern is that carriers chasing market share will not be able to sustain pricing, and insureds will be faced with steep increases, which can be harder on a care providers business than long-term stable pricing and good historic relationship with a carrier.

Liability cost drivers

Social Inflation, Third Party Litigation Funding, Nuclear Verdicts

- Social Inflation – driven by societal and legal factors that lead juries to award higher amounts especially in healthcare cases on negligence, abuse, neglect, or wrongful death

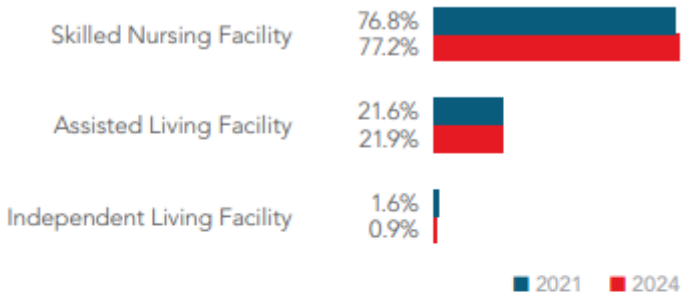


CNA – Claim report 2024

Closed Claim Analysis – Trends by Bed Type

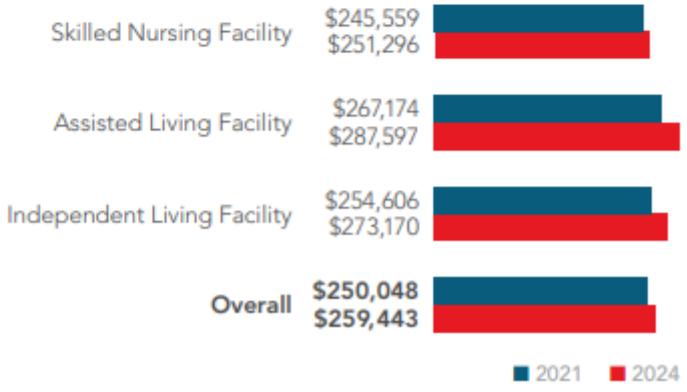
1 Distribution of Closed Claims by Bed Type

Closed Claims with Paid Indemnity of ≥ $10,000



2 Average Total Incurred by Bed Type

Closed Claims with Paid Indemnity of ≥ $10,000



Top 5 Highest Severity Allegations

1 **$384,088** Resident abuse

2 **$312,107** Failure to move resident to higher level of care

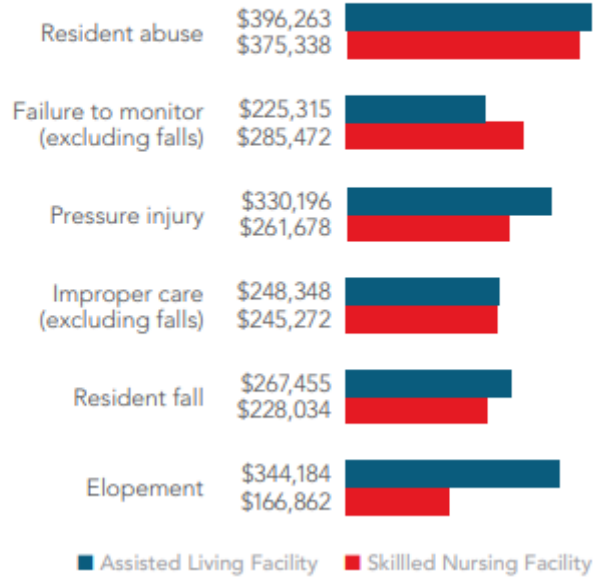
3 **$311,480** Failure to follow physician's order

4 **$306,373** Medication error

5 **$303,883** Elopement

8 Average Total Incurred for Top Allegations by Bed Type

Closed Claims with Paid Indemnity of ≥ $10,000



Cybersecurity and data privacy

Cybersecurity and data privacy

Rate trends

According to the Marsh Q4 2024 U.S. Cyber Insurance Index, rates decreased by an average of **5%** in Q4 2024, with larger reductions for risks that demonstrate year-over-year improvements in security controls.

Insurers remain concerned about the potential for catastrophic and systemic cyber losses. Underwriters closely scrutinize the aggregation of exposures, emerging privacy compliance risks, and supply chain risks.

Competition continues to accelerate, with rates decreasing, and many carriers are willing to increase capacity and provide options for lower deductibles and self-insured retentions.

The maturing cyber market remains competitive, with increased capacity, which leads to a positive experience for insureds, as rate reductions and enhancements to coverage have remained available, including higher limits and lower retentions.

Policy wording continues to evolve, with some carriers imposing updated exclusions related to war, privacy regulations, and data collection.

Cyber claim trend insights

Insider threats and employee re-education

- Arete, one of our Cyber Resiliency Network partners, released its Q3 2024 Crimeware report, highlighting trends in ransom demands and payments. Most notable is the lower percentage (29%) of organizations making ransom payments in Q3, suggesting that companies are better prepared to respond to ransomware or extortion attacks.
- According to various studies and reports, **it is estimated that anywhere from 70% to 90% of cyber incidents can be attributed to human error.** This means security risks that originate from within an organization, typically involving employees, contractors, or business partners who have inside information regarding the organization's security practices, data, and computer systems.

To mitigate insider threats, organizations must prioritize:

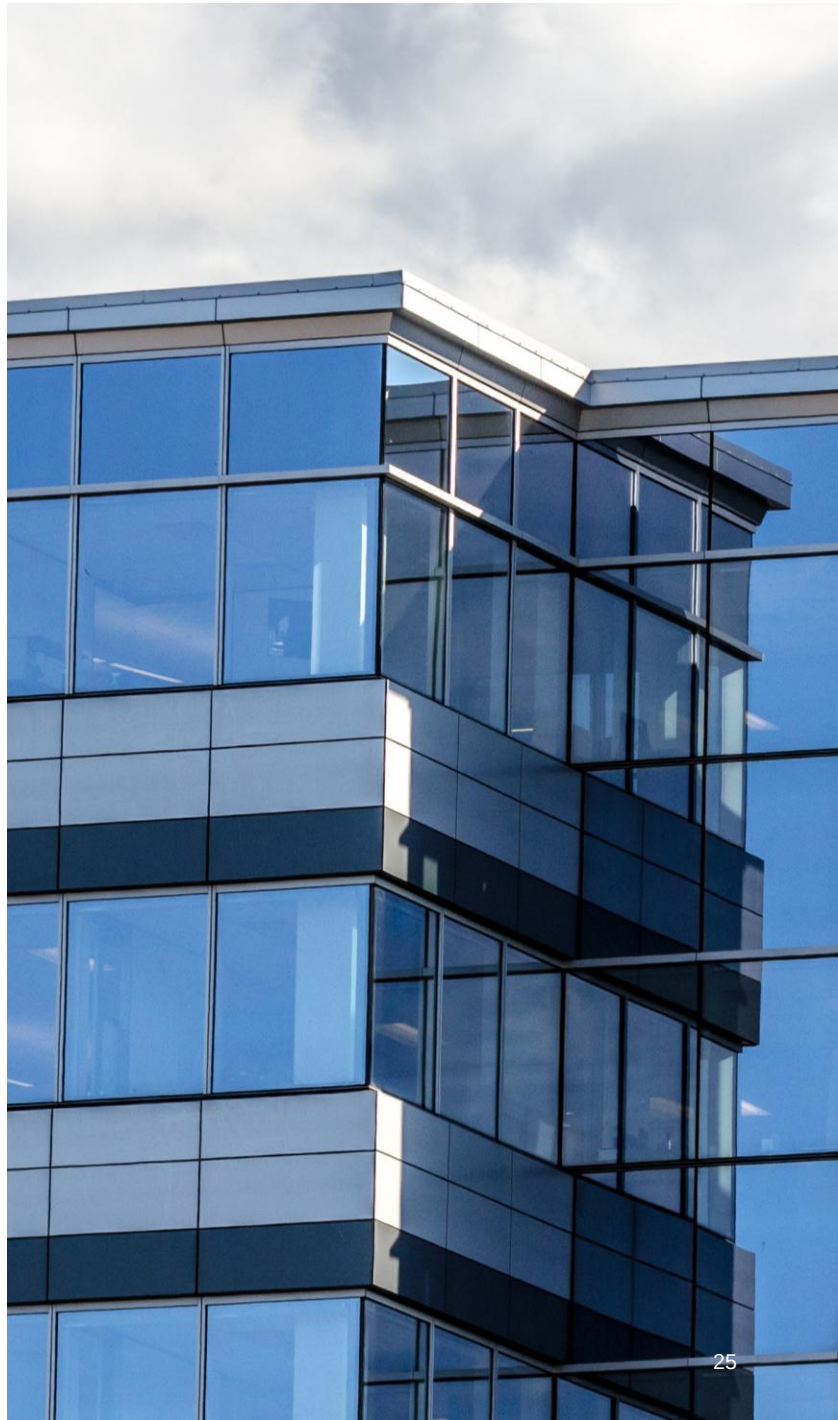
- **Regular training programs:** Implementing ongoing training sessions
- **Clear communication of policies:** Ensuring that all employees are familiar with the organization's security policies
- **Simulated phishing exercises:** Conducting regular simulated phishing attacks
- **Feedback mechanisms:** Establishing channels for employees to provide feedback on security practices
- **Role-specific training:** Tailoring training programs to specific roles within the organization

Safeguarding business continuity and resiliency: finding a path to adaptability

We are monitoring impacts from presidential executive orders in the U.S. that could affect commercial insurance buyers in several ways:

Regulatory changes	Economic policies	Climate and environmental policies
Litigation environment	Market stability	Cybersecurity and data privacy

Marsh McLennan Agency is here to help you navigate these changes. We can explore alternative risk solutions with you and use informed analytics to support your insurance-buying decisions.



Clinical Zero Trust – Cyber Security in Healthcare

Louis DeWeaver, Cyber Security Consultant

Meet Dr. DeWeaver

Dr. Louis DeWeaver

Cyber Security Consultant

I am currently employed as a Cyber Security Consultant at Marsh McLennan Agency (MMA), where I leverage over twenty years of industry experience. I obtained an Associate of Applied Science degree in Information Technology and Computer Network Systems in 2009, followed by a Bachelor of Science degree in Information Systems Security in 2011. In 2016, I further advanced my education by earning a Master of Science degree in Information Assurance, with a concentration in Cybersecurity. Most recently, in 2021, I completed my academic pursuits with a Doctor of Computer Science degree, also focusing on Cybersecurity.

In addition to my educational qualifications, I actively participate as a member of the MITRE Engenuity ATT&CK® Evaluations Community Advisory Board. I have achieved success in various Capture The Flag (CTF) and cybersecurity competitions, with notable recognition for winning the ONCD (Office of the National Cyber Director) Badge Challenge at DEFCON 31 (2023) and DEFCON 32 (2024). Furthermore, I have shared my knowledge and insights as a speaker at numerous conferences, including BlackHat, DefCon, GrrCon, and several other events outside the cybersecurity domain.

Yes, cyberattacks can have deadly consequences

RANSOMWARE FALLOUT DIRECTLY CONTRIBUTED TO AT LEAST 42 US DEATHS.

In any ransomware event, there's the data impact. The real risks–particularly for healthcare–are also measured in operational impacts and lives.

The University of Minnesota Twin Cities - School of Public Health studied real-world impacts to hospitals and patient care caused by ransomware events between 2016 and 2021[1].They found:

20%

Patient care throughput dropped by 20% across the first week of a ransomware attack.

1 in 4

While only 5% of US hospitals were directly affected by ransomware during the study's timeframe, an additional 20% of hospitals suffered ripple effects when patients were transferred or diverted from the victim hospitals to surrounding hospitals.

0.5-1%

A typical hospital lost between 0.5 and 1% of their total annual revenue as a direct result of a single ransomware attack.

2-3 wks

Hospitals averaged two to three weeks for a return to typical patient care levels following a ransomware attack.

42-67 deaths

The fallout from ransomware attacks directly contributed to the deaths of between 42 and 67 patients[2].

These attacks aren't just affecting data, businesses, or individual privacy anymore. There's direct evidence cyberattacks are a life and death issue.

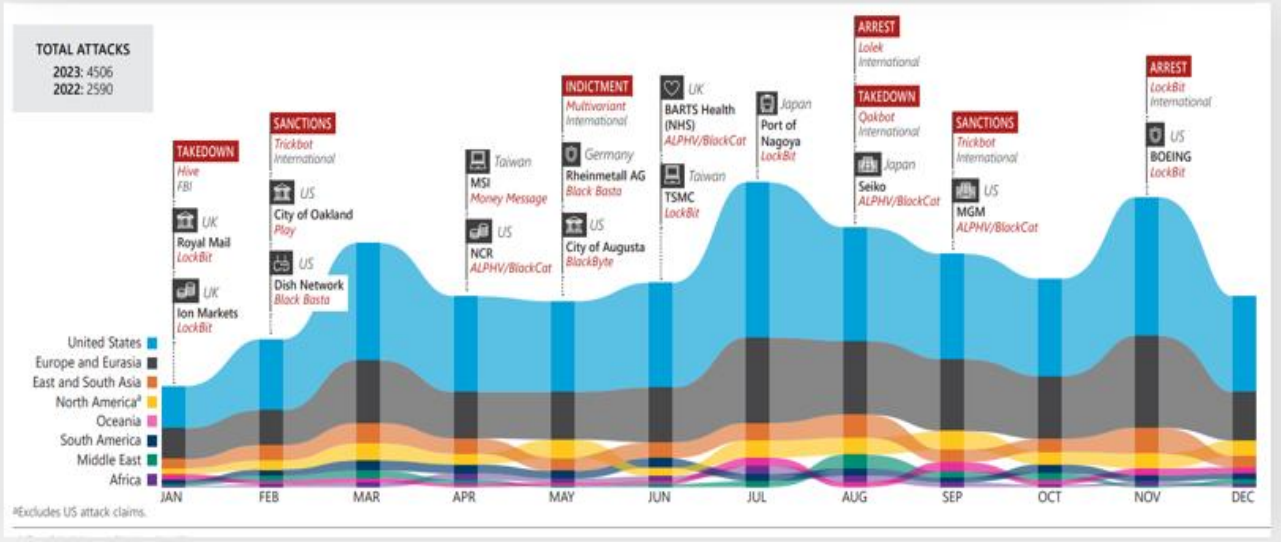
THE HIPAA JOURNAL

Become HIPAA Compliant » HIPAA News » HIPAA Compliance Checklist Latest HIPAA Updates » HIPAA Training » About Us »

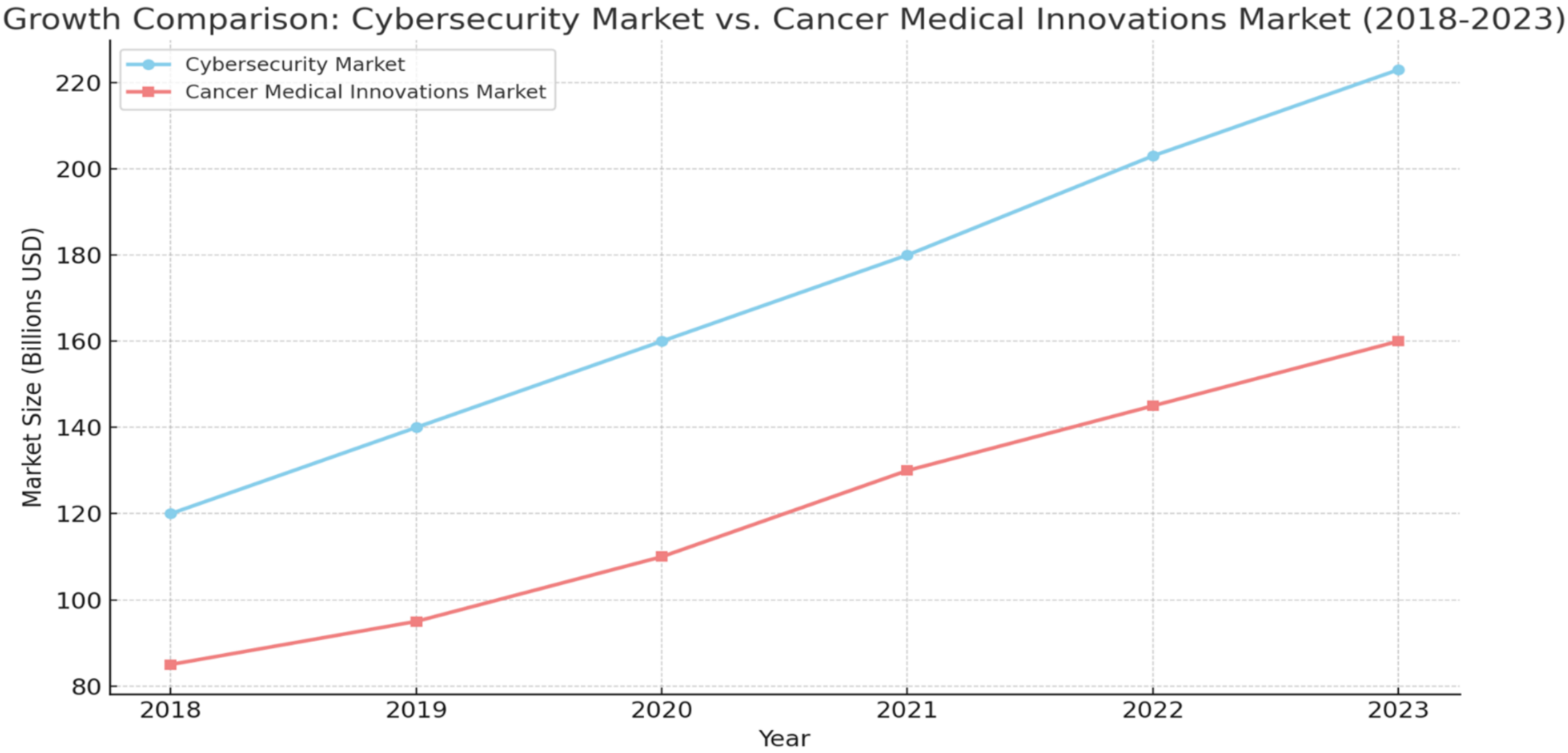
At Least 141 Hospitals Directly Affected by Ransomware Attacks in 2023

Posted By Steve Alder on Jan 4, 2024

Last year was a particularly bad year for ransomware attacks. According to an analysis by the



We have invested more for cyber than to cure cancer!



Your cybersecurity solutions will not protect you

Move to zero trust

(What is zero trust)

Created in 2010 by John Kindervag (Forrester)

Shift from castle and moat security model to zero trust approach in order to address current IT environments and workplaces

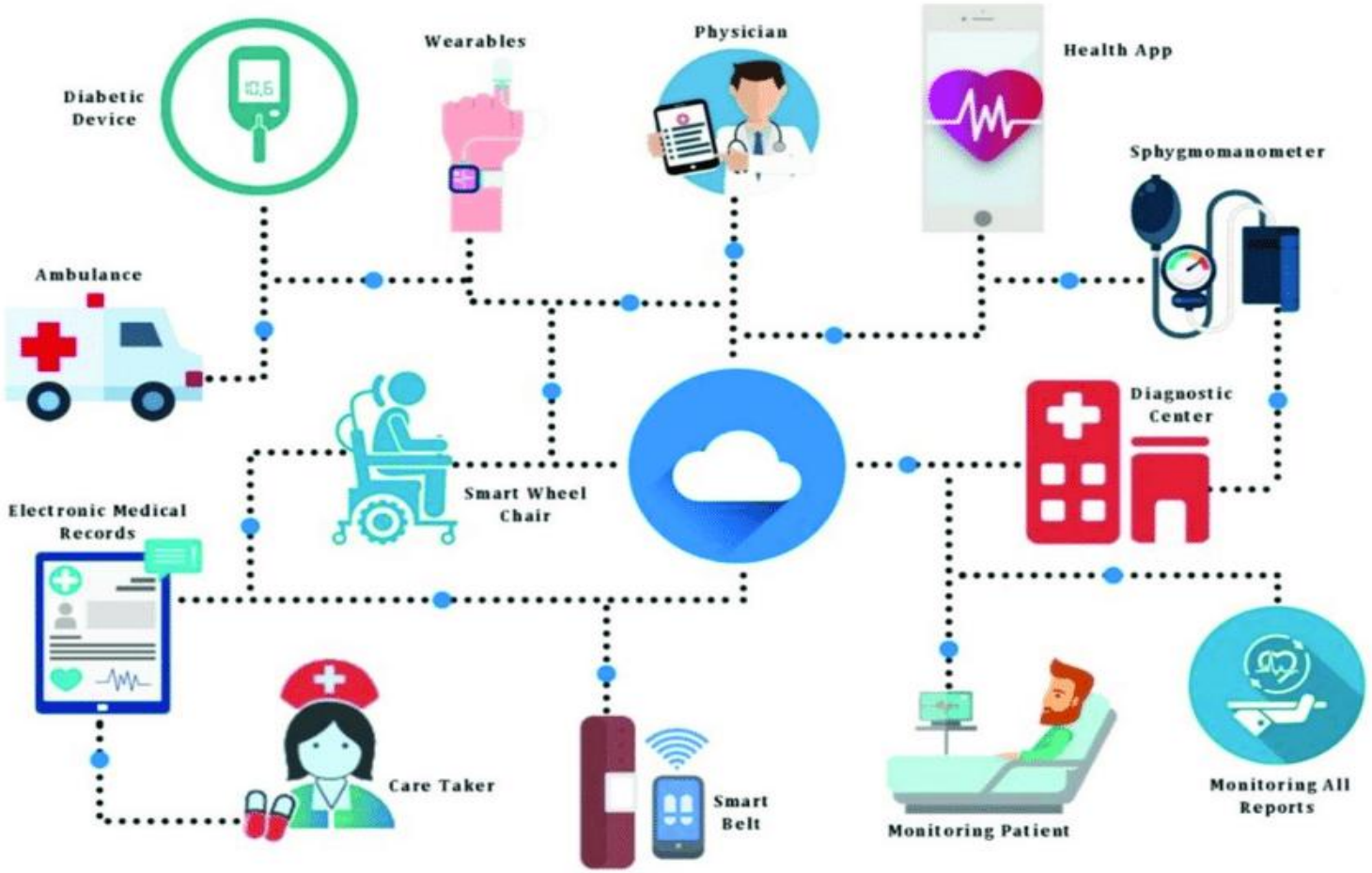
None of the following should ever be trusted by default, regardless of the location each is operating from, either inside or outside the security perimeter:

- Devices
- Users
- Workloads
- Systems

1. Every device should be treated as a threat vector
2. Anything that cannot be verified is denied access

Why implement zero trust?

Given the interconnected nature of the future with IoMT devices, augmented reality, robotics and more, it is clear that the current perimeter-based security model that most healthcare organizations use will no longer be effective. To stay ahead of these trends, healthcare organizations must continue to invest in the basics while making a fundamental shift from the castle-and-moat approach to a Zero Trust model.



Clinical zero trust

When the principles of Zero Trust are applied to the healthcare setting, that is Clinical Zero Trust. The difference between implementing Zero Trust in a healthcare setting is that instead of just protecting devices and data, the goal of Clinical Zero Trust is also to protect the physical workflows of care delivery, including the people and processes responsible.

Five phases to advance your organization's Clinical Zero Trust strategy:

Solution #1: Identify your assets: Gain a deep understanding of your clinical environment and the connected devices.

Solution #2: Define your network: Mapping the usage of each device uncovers important information about how devices talk to one another, including which devices they communicate, how, when, and why.

Solution #3: Design a strategy: Your organization has a unique risk tolerance and any Clinical Zero Trust strategy should be molded to the needs and requirements of your healthcare system.

Solution #4: Monitor the environment: Once your individualized policies are in place, it's time to monitor the environment and see the impact of your enforced policies.

Solutions #5: Automate your processes: If you've taken the time to make modifications to your policies and processes after monitoring and improving them, then at some point you will have found the proper architecture for your aims and objectives. Automating these procedures is the final step to achieving your best possible Clinical Zero Trust strategy for your environment.

Back to the basics

Here's a breakdown of why these basics are so important:

- **Cyber Hygiene:** Practicing good "cyber hygiene" is the foundation of strong cybersecurity.
- **Strong Passwords:** Use unique, complex passwords and consider using a password manager. Or Eliminate passwords altogether.
- **Software Updates:** Keep your software, apps, web browsers, and operating systems up-to-date to patch vulnerabilities.
- **Be Cautious with Links:** Think before clicking on suspicious links or attachments.
- **Multi-Factor Authentication (MFA):** Enable MFA for accounts, especially those with sensitive information.
- **Secure Your Devices:** Encrypt devices and secure your router.
- **User Access Control:** Restrict user access to sensitive information and systems.
- **Malware Protection:** Install and maintain anti-malware software.
- **Firewalls:** Use firewalls to protect your network from unauthorized access.
- **Secure Configuration:** Ensure web server and application server configurations are secure.
- **Security Update Management:** Regularly update security software and systems.
- **Train Staff:** Educate staff about cybersecurity risks and best practices.

Questions

MarshMcLennan Agency

Your future is limitless.℠

MarshMMAMidwest.com

MarshMcLennan Agency

A business of Marsh McLennan

TOP WORK PLACES USA