

What your Board wants you to know: Managing your Management Liability Risk & Insurance

HFMA Heartland Chapter – 10/21/2022



The Balancing Act: Understanding Management Liability Risk

Risk

What is your Organization's Risk Profile?

Who Decides?

Who are the Stakeholders?

Cost of Risk

What do you spend in pre-risk mitigation?

What do you spend in litigation?

What do you spend in Insurance costs?

Vendor costs?

Insurance

What are you buying?
How are you buying it?

What is your Broker expertise?

Do you understand what you are buying?

Have you tested it?

What does your Board expect you to know?

- Every Board expects, and should mandate, a working knowledge (NOT understanding) of the following:
 - Organizational Risk
 - Organizational Risk Tolerance
 - Total Cost of Risk
 - Confidence in Broker skillset
 - Critical Uninsured exposures
 - Frictional Costs (vendors, time, staffing)
 - Program purchased
 - Engagement in risk (meaning how often is it reviewed, tested and vetted)

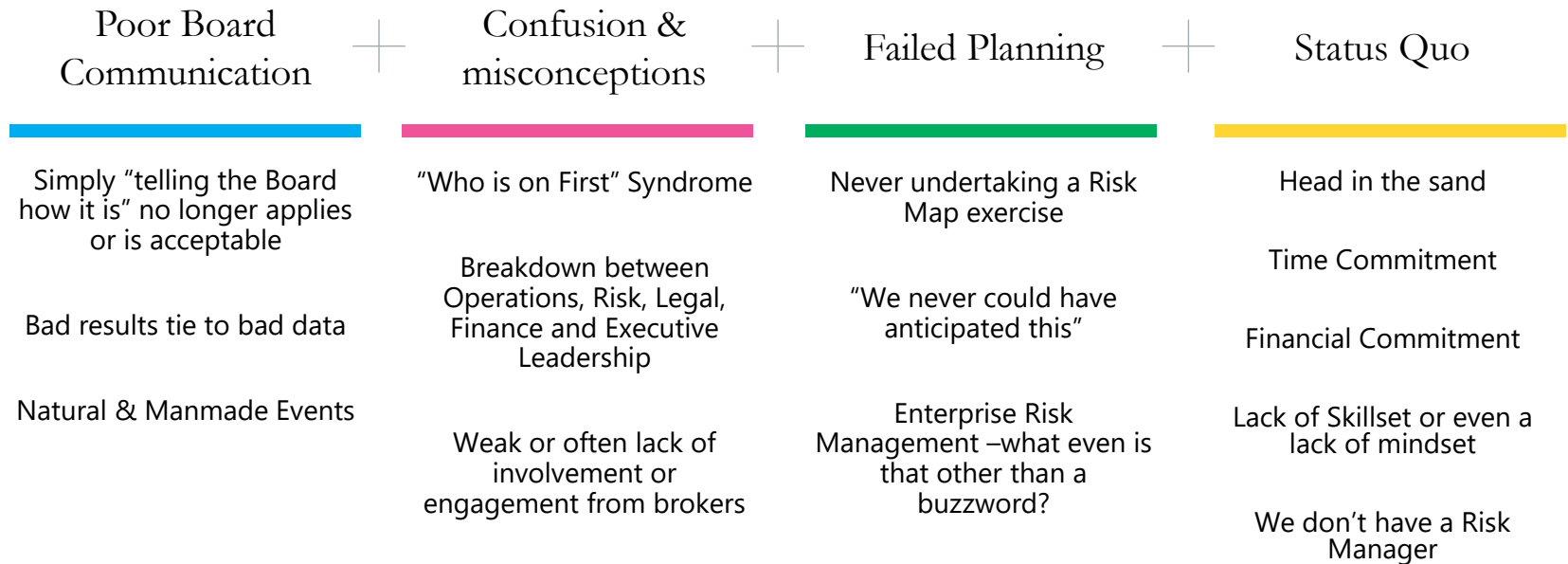




Why are they doing this?

- Cyber attacks and Ransomware events
- Public company experience
- Opportunity – Years of businesses being warned with little to no action towards risk or security
- COVID-19
- Complacency is no longer acceptable at the Board level
- ESG: stands for **Environmental, Social, and Governance**. Investors, Customers & Employees are increasingly applying these non-financial factors as part of their analysis process to identify material risks and growth opportunities
- Accountability
- Push by Auditors

How does this happen?



Understanding your Risk: Tips

- Determine your stakeholders
- Plan a Blue-Sky Session
- Look at your publicly traded competitors
- Survey your departments, practices
- Assign ownership
- Engage your broker
- Implement and empower a committee or team with accountable, actionable items



SAMPLE / Determine Stakeholders

CFO	Work on budget forecasting. Prepare Boards & CEO of the current market trend. Report to the Board the current market trends & concerns. Look to approve emergency funding for MFA or EDTR implementation. Look at expanding staffing of IT / Risk / CISO positions short and long term.
CISO	Fully own and understand Unique Record Counts. Assess exposures that can be fully taken off-line. Work with IT and Risk on best practices. Understand any Healthcare Provider (Hospitals, Clinic, Managed Care Employee Benefit Plan) cross-exposures as they are higher risk classes as well
Legal	Fresh review of contract wording –what can you push to vendors? Review of open matters –close what you can close. Secure confidence in reporting process / procedure. Hold and own the Incident Response Plan (IRP) ownership.
Risk	Review Incident Response Plans (can no longer be IT only plans). Work with vendors for best practices, engagement with Underwriters –set calls. Set extensive pre-renewal strategies. ENFORCE DEADLINES for submissions. Understand and embrace Best-Practices & Carrier/Lockton provided Loss Prevention Services.
IT	Assess MFA and EDTR positions. Look at Security Operation Center (SOC) staffing and get it to 24/7/365 active (passive is no longer acceptable). Identify and engage Stakeholders. Seek emergency budget approval for critical initiatives (present to CFO). Take active roll in on your Incident Response Plan.....integration if not already done so. Scrutinize renewal apps / submission.

SAMPLE: Blue Sky



- Natural Events: Tornado, Fire, Flood
- Manmade Events: Pandemic, Active Shooter, Ransomware
- Employee: Training, Harassment, Discrimination
- Competition
- Social Footprint
 - Employee communications
 - Twitter/FB/Forums
 - Community / Civic Involvement
- Terrorism / Social Unrest
- Fleet issues / Drive safety
- Patient Safety
- Government Oversight
- Vendor Relationships
- Market pressures
- Supply Chain
- Wrongful Death / "7 Deadlies"
- Loss of key Customer
- Loss or Executive Leadership
- Ability to recruit / retain / hire
- ESG Footprint
- Shareholder and Stakeholder engagement
- Employee safety
- Employee Satisfaction

SAMPLE: Competition



All publicly traded companies must annually disclose their top 10 risk factors in their SEC filing known as the 10K

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

Form 10-K

(Mark One)

ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934
For the fiscal year ended December 31, 2021

Or

TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934
For the transition period from _____ to _____
Commission File Number 1-11239

HCA Healthcare, Inc.
(Exact Name of Registrant as Specified in its Charter)

Summary Risk Factors

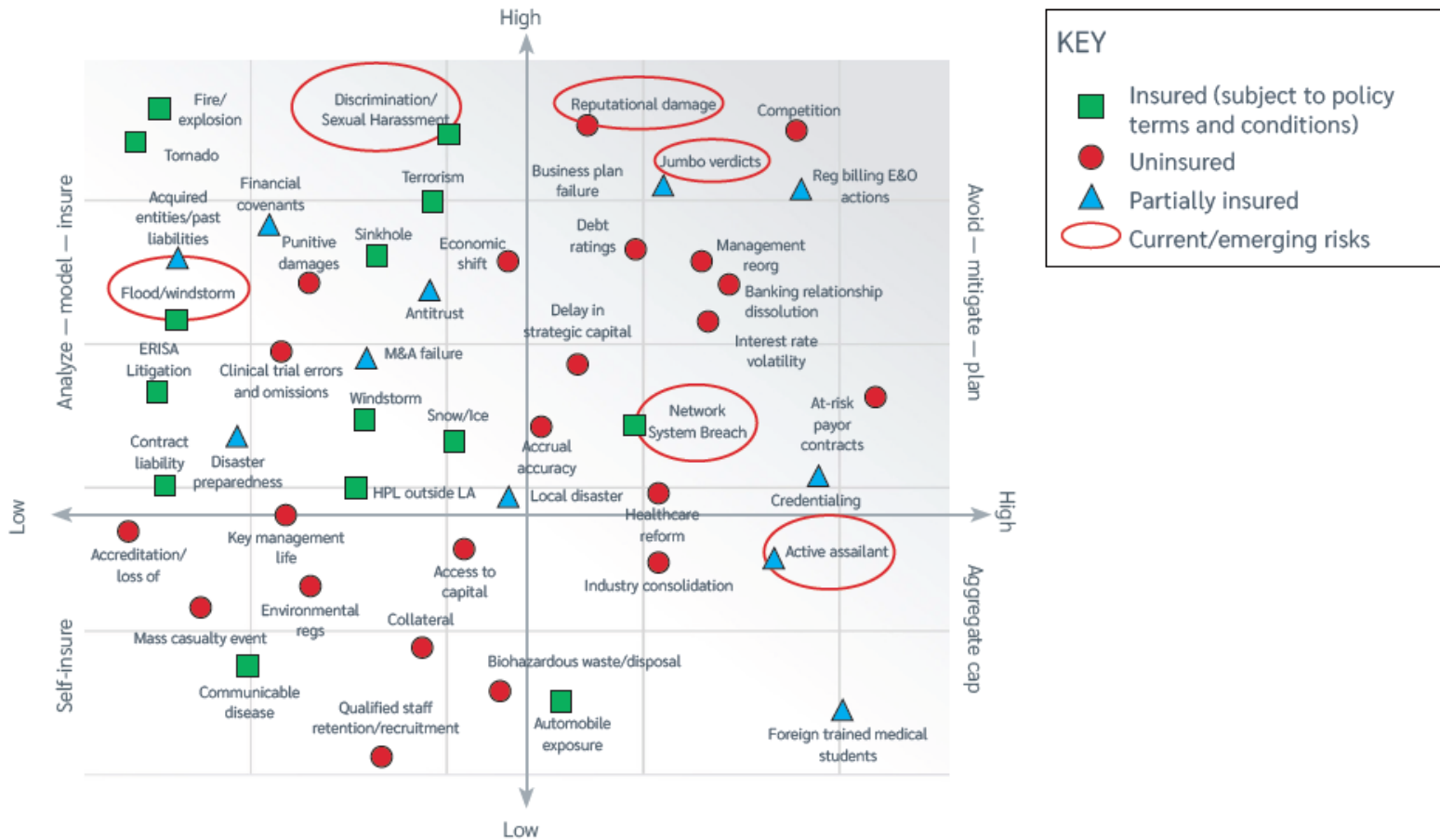
You should carefully read and consider the risk factors set forth under Item 1A, "Risk Factors," as well as all other information contained in this annual report on Form 10-K. Additional risks and uncertainties not presently known to us or that we currently deem immaterial may also affect us. If any of these risks occur, our business, financial position, results of operations, cash flows or prospects could be materially, adversely affected. Our business is subject to the following principal risks and uncertainties:

Risks related to the COVID-19 pandemic and other potential pandemics:

- The COVID-19 pandemic is significantly affecting our operations and could affect our business and financial condition. Our liquidity could also be negatively impacted by the COVID-19 pandemic, particularly if the U.S. economy remains unstable for a significant amount of time.

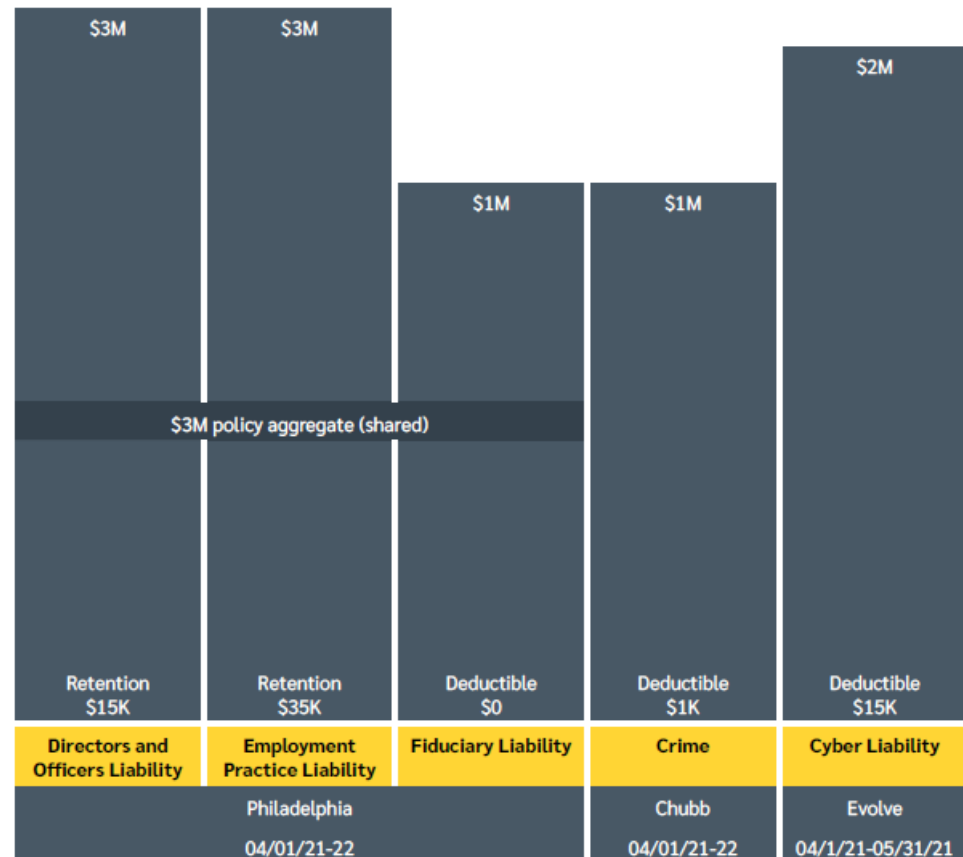
SAMPLE – RISK Map

SAMPLE RISK MAP



***SAMPLE:** Program Visualization*

If your Broker does not prepare a visualization graphic for you – ask them to do so. It will assist in your understanding of your program



SAMPLE - Readiness

Incident response planning – PRACTICE!

This is a business exercise, not a technical exercise.

1	2	3	4
Do not communicate over business email during an incident.	Who are the key department representatives that will be on the response team? <ul style="list-style-type: none">• Legal• HR• Technical• Finance• Etc.	Who do you contact at your insurance company?	Who do you contact at your broker?



***SAMPLE** -Incident response*

- Insurance
- Privacy counsel
- Forensic IT firms
- Threat actor negotiations
- Payment
 - Cryptocurrency – good and bad
 - OFAC
 - Trust in the threat group “keeping their word”
- Recovery
- Fallout

SAMPLE -Cyber Market Update – Q3 2022

CURRENT DYNAMICS

Recent Conditions – Ransomware losses drove the turbulence experienced in the cyber insurance market over the past 18+ months.

Current State – Major volatility is gradually stabilizing across the macro cyber market

- ✓ However, non-standard/counterintuitive results are common on individual renewals given the complexity/immaturity of the cyber product

Challenging Industries – Cyber carrier risk selection/high-hazard class avoidance is causing increased challenges in the following industries

- ✓ Technology
- ✓ Healthcare
- ✓ Public Entities
- *Cyber broker industry specialization enables superior risk transfer/management/mitigation outcomes*

Cyber Carrier Focus – Systemic Risk and Privacy Regulation

- ✓ This is due to the potential severity, aggregation, and rapidly evolving nature of these risks/exposures

Underwriting Requirements – Minimum security standards still must be evidenced to maintain coverage efficacy and secure renewal capacity

- ✓ Security requirements are a moving target given the evolving threat landscape and new attack vectors being exploited

KEY FACTORS

Actuarial Modeling



- + Cyber criminals and technology dependence create ever-changing exposures which inherently make pricing/modeling cyber insurance products elusive
- + Scope of coverage offerings must be narrowed (Cyber-As-A-Peril)

Underwriting Capacity



- + Carriers continue to extensively monitor capacity deployment across their books of business. Aggregation events (actual & potential) are driving this focus.
- + While \$10M capacity deployments have resurfaced, most clients will see maximum capacity of \$5M deployed by underwriters.

Rate Environment



- + Compounding rates and inflationary pressures are impacting cyber rate increases from a macro perspective
- + We anticipate the cyber rate environment to be fluid in the 2nd half of 2022

Coverage



- + Privacy regulatory coverage offerings/triggers are being reevaluated by carriers
- + Due to aggregation concerns, Dependent Business Interruption sublimits are becoming more common.

Retention Levels








- + Quantifiable cyber events typically result in severe losses – Carriers are setting retention levels relative to this problem
- + In general, we anticipate retention amounts to increase

***SAMPLE** - Closer look at the cyber market changes*

CAPACITY (LIMITS)	PREMIUM	APPLICATIONS	RETENTIONS AND COINSURANCE
<ul style="list-style-type: none">• Market capacity has decreased by over 135M.• Major markets have reduced their maximum lines from 50M to 25M and are regularly only offering a maximum of 10M.• Limited carriers willing to write new business.• Many London syndicates are no longer willing or able to write new business.	<ul style="list-style-type: none">• Increases of 20%-50% have become the bare minimum, even without any loss history.• It is not uncommon to see increases of 100%-150% or more with no significant changes in exposure.• Excess underwriters are no longer willing to offer 70%-80% ILF's further pushing increases on programs.• Expect further increases if there is recent loss history or less than fully mature IT security controls, even without a carrier payout.	<ul style="list-style-type: none">• Supplemental applications are required for ransomware, operational technology and biometrics.• Certain carriers have created scoring tools informed by application responses to be used to indicate coverage and rate quotes. One missing control, could cause changes in coverage or desire for the insurer to renew coverage.	<ul style="list-style-type: none">• Carriers are increasing minimum retentions and waiting periods.• SIRs are increasing with some markets requiring increases up to 500% or imposing minimums of \$250K-\$1M on all cyber business.• Some markets require co-insurance and a sublimit for certain coverages, including ransomware and contingent business interruption.

5 Key points to know about each line of Management Liability Insurance

Directors & Officers Liability

				
<p>Who is Covered?</p> <ul style="list-style-type: none">• Past, Present and Future Directors & Officers?• Functional Equivalents• Employees?• International Executives?• What about non-bylaw appointed officers? (HR, CISO, IT, CMO etc.)	<p>Antitrust Coverage?</p> <ul style="list-style-type: none">• Does the policy cover claims brought by competitors or the government asserting violations of trade?• If so, what is the coverage limit / deductible?• Is there co-insurance?• What does the defense arrangement look like under this coverage extensions?	<p>Regulatory</p> <ul style="list-style-type: none">• Does the policy cover claims brought by the government or agencies asserting violations of statute?• If so, what is the coverage limit / deductible?• Is there co-insurance?• What does the defense arrangement look like under this coverage extensions?	<p>Allocation</p> <ul style="list-style-type: none">• How does the policy respond to claims when some matters are excluded under the policy and yet coverage for covered matters remains intact?	<p>Policy Wording</p> <ul style="list-style-type: none">• Is the policy built around “Duty to Defend” wording – meaning the Carrier has the right and obligation to defend all actions• Is the policy Reimbursement – meaning you as the policy holder have the obligation to secure defense

Employment Practices Liability



Who is Covered?

- How is Employee defined?
- Are Directors & Officers Included?
- What about Independent Contractors?



Third Party Coverage?

- Does the policy cover claims brought by patients, customers, vendors or guests who allege your employees harassed or discriminated against them?



Defense

- Does the Insurance Company or your Company have the obligation to defend an action?
- Who gets to select the law firm to defend you?
- What is the rate cap?



Settlement

- Does the policy have a "Hammer Clause" – a provision that allows the Carrier to **force** a settlement?
- Is consent required to settle a matter



Vendors

- Does your policy include vendor or loss prevention services at no cost or low cost?
- Does the carrier provide any training services?

Fiduciary Liability



Who is Covered?

- How is Employee defined?
- Are Directors & Officers Included?
- What about Independent Contractors?



Is coverage ERISA only?

- The policy should extend to defend ALL employee benefits you secure –NOT just ERISA based plans



Defense

- Does the Insurance Company or your Company have the obligation to defend an action?
- Who gets to select the law firm to defend you?
- What is the rate cap?



Settlement






- Does the policy have a “Hammer Clause” – a provision that allows the Carrier to **force** a settlement?
- Is consent required to settle a matter








Fines & Penalties

- Are fines covered?
- Are penalties covered?
- What about Voluntary Reporting?
- What is the position on Punitive Damages?
- What about coverage for Excessive Fee cases?

Managed Care E&O Liability

				
<p>Credentialing</p> <ul style="list-style-type: none">• Are you doing this in house or via a vendor?• NOTE: If in-house this is not covered under D&O or PL coverage.	<p>Utilization Review</p> <ul style="list-style-type: none">• Are you doing this in house or via a vendor?• NOTE: If in-house this is not covered under D&O or PL coverage.	<p>Peer Review</p> <ul style="list-style-type: none">• Are you doing this in house or via a vendor?• NOTE: If in-house this is not covered under D&O or PL coverage.	<p>Health Management</p> <ul style="list-style-type: none">• Are you doing this in house or via a vendor? Do you sell your data to third parties or engage in third party wellness vendors?• NOTE: If in-house this is not covered under D&O or PL coverage.	<p>Third Party Liability</p> <ul style="list-style-type: none">• What are you contractually able to move from your Organization, onto a third-party vendor or platform?

Billing E&O Liability

				
<p>Billing Services</p> <ul style="list-style-type: none">• Are you doing this in house or via a vendor? • NOTE: If in-house this is not covered under D&O or PL coverage.	<p>Coding Services</p> <ul style="list-style-type: none">• Are you doing this in house or via a vendor? • NOTE: If in-house this is not covered under D&O or PL coverage.	<p>Payor Mix</p> <ul style="list-style-type: none">• Is your payor mix heavy on CMS? What type of CHIP or Military Services (TriCare) are your rendering?	<p>Audit Practices</p> <ul style="list-style-type: none">• Are you doing this in house or via a vendor? • NOTE: If in-house this is not covered under D&O or PL coverage.	<p>Audit Exposures</p> <ul style="list-style-type: none">• Recovery Asset Contractor (RAC) Audits –Medicare and Medicaid• Zone Program Integrity Contractors (ZPICs) Audits –Medicare driven• False Claim Act (FCA) allegations• Pharmacy Services Exposures• Commercial Payor Exposures

Questions & Answers?



Independence changes everything.



UNCOMMONLY INDEPENDENT