CFO PERSPECTIVE SERIES

Cyber Insurance in Healthcare: What Your Policy Actually Covers

(And What It Doesn't)

A CFO's Perspective on Risk Transfer, Coverage Gaps, and Insurability

CloudWave

When I first started spending more time on cyber insurance as part of my role, I approached it the same way most of us do: as a straightforward risk transfer mechanism.

We pay a premium. We get coverage. If something goes wrong, the policy helps absorb the financial impact.

That's how it works in theory.

In practice, cyber insurance in healthcare has become much more complicated—and much less forgiving—over the last few years. Premiums are rising, underwriting is tightening, and what's actually covered is often narrower than many of us assume.

The result is a growing blind spot for CFOs: we believe we've transferred risk that we're still largely carrying.

Joe Badziong
CHIEF FINANCIAL OFFICER

CloudWave partners with rural and mid-size healthcare systems to deliver cloud and cybersecurity solutions built for the operational realities you face every day.

COVERAGE LOOKS BROAD, UNTIL YOU NEED IT

On paper, most cyber policies appear comprehensive. They typically include some combination of:

- Incident response costs
- Legal and regulatory support
- Patient notification and credit monitoring
- Business interruption
- Ransomware payments

That can create a false sense of security.

But when you start looking more closely, especially in the context of a real event, the limitations become clearer.

Coverage is often conditional. Business interruption may only apply after a waiting period. Ransom payments may require insurer approval and strict documentation. Regulatory fines may be partially covered, disputed, or excluded depending on jurisdiction.

And in many cases, the largest financial impacts don't fall neatly into covered categories at all.

THE GAPS THAT MATTER MOST

There are three areas where I consistently see disconnects between expectation and reality.

1. Operational downtime

This is often the largest financial impact of a cyber event, and also the most misunderstood from an insurance standpoint.

Policies may cover business interruption, but coverage is typically tied to very specific definitions of "system failure" and may exclude certain types of operational disruption. Even when it applies, it rarely captures the full economic impact, especially in healthcare, where downtime affects not just revenue but patient flow, care delivery, and downstream operations.

From a finance perspective, this is not a small gap.

2. Reputational and patient impact

While some policies may include limited public relations or reputation management coverage, there is generally no meaningful insurance coverage for long-term loss of patient trust, patient acquisition challenges, or brand erosion.

Those effects show up gradually—in volume, mix, and growth—not as a clean line item tied to an incident. But they are real, and they compound over time.

This is one of the areas where the financial model and the insurance model diverge the most.

3. Coverage exclusions and conditions

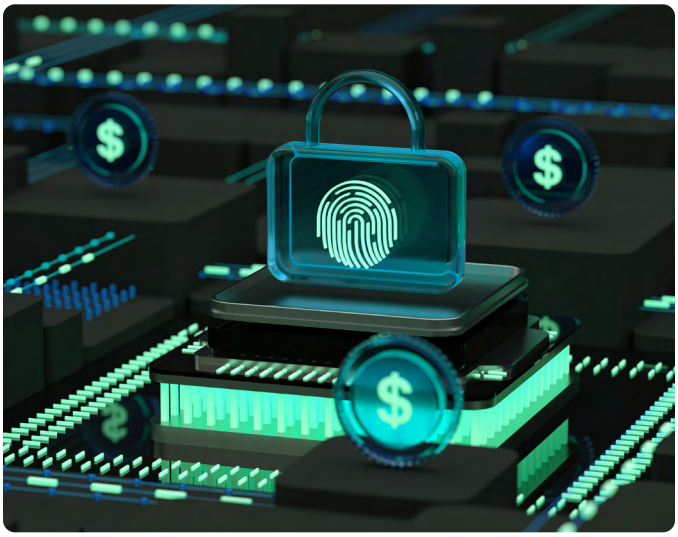
Cyber policies have become significantly more prescriptive.

Common requirements now include:

- Multi-factor authentication across critical systems
- Endpoint detection and response capabilities
- Documented incident response plans
- Regular security assessments

If those controls are not in place, or cannot be demonstrated at the time of a claim, coverage may be reduced, disputed, or, in some circumstances, denied if required controls cannot be demonstrated.

That's not always fully appreciated when policies are purchased or renewed.



While some policies may include limited public relations or reputation management coverage, there is generally no meaningful insurance coverage for long-term loss of patient trust, patient acquisition challenges, or brand erosion.

PREMIUMS ARE RISING, AND SO IS SCRUTINY

Most CFOs I speak with have seen meaningful premium increases over the past few renewal cycles. That's not surprising given the claims environment.

What has changed more significantly is how policies are underwritten.

Insurers are no longer evaluating organizations based solely on size, revenue, or historical claims. They are assessing cybersecurity maturity in a much more direct way.

Applications have become more detailed. Questionnaires go deeper into controls and practices. In some cases, external scans or third-party risk assessments are part of the underwriting process.

In effect, insurers are making their own judgment about your risk posture and pricing accordingly.

CYBERSECURITY MATURITY NOW IMPACTS INSURABILITY

This is the shift that I think matters most.

Cyber insurance used to be something you could obtain first and then improve your security posture over time. Increasingly, that order has reversed.

Today, your ability to secure favorable coverage, and in some cases, to secure coverage at all, is directly tied to your cybersecurity maturity.

That includes:

- How quickly you can detect and respond to threats
- How well you can contain an incident
- How effectively you can recover operations

From a financial standpoint, this creates a tighter linkage between security investment and insurance outcomes than we've historically modeled.

It's not just about reducing risk. It's about maintaining access to risk transfer.

HOW I THINK ABOUT THIS AS A CFO

I no longer think of cyber insurance as a primary risk mitigation strategy.

I think of it as one layer in a broader financial approach to cyber risk, alongside:

- Prevention (reducing the likelihood of an event)
- Detection and response (limiting the impact)
- Recovery (shortening the duration of disruption)

Insurance plays an important role, but it does not replace any of those elements, and it is increasingly dependent on them.

When I evaluate our position, I focus on three questions:

1. What portion of our true financial exposure is actually covered?
2. What assumptions are we making about coverage that may not hold in a real event?
3. How does our current security posture affect both our premiums and our ability to recover costs?

Those questions often reveal coverage and preparedness gaps quickly.

Today, your ability to secure favorable coverage, and in some cases, to secure coverage at all, is directly tied to your cybersecurity maturity.

A MORE PRACTICAL VIEW OF RISK TRANSFER

The takeaway for me has been fairly straightforward.

Cyber insurance is still valuable. But it works best when it is aligned with a realistic understanding of:

- What it covers
- What it doesn't
- And what it requires from us as an organization

The organizations that are navigating this well are not treating insurance as a safety net. They're treating it as part of a coordinated strategy, one that connects financial planning, operational resilience, and cybersecurity maturity.

That's a different mindset than most of us had even a few years ago.

But it's where the market has moved.

CLOSING THOUGHT

As CFOs, we are used to evaluating risk transfer mechanisms with a critical eye, whether it's liability coverage, property insurance, or contractual risk.

Cyber insurance deserves the same level of scrutiny.

Because in this case, the difference between what we think is covered and what actually is can be measured in millions.

Questions to Ask Before Your Next Renewal

1. What exclusions create the largest uninsured exposures?
2. What controls are required to maintain coverage?
3. How is business interruption defined?
4. Does the policy cover third-party service provider outages?
5. What evidence would be required during a claim?

CloudWave can help. We work with healthcare finance and technology leaders to review cyber risks, identify and remediate gaps, and ensure compliance. Contact us at customersfirst@gocloudwave.com.

CONTACT US →

DISCLOSURE

CloudWave provides healthcare-focused cloud and cybersecurity solutions to rural and mid-size health systems. Views expressed reflect the author's professional experience and perspective.