UC BERKELEY

CENTER FOR LONG-TERM CYBERSECURITY

CLTC WHITE PAPER SERIES

Economics of Cyber Policies for Critical Care

MODELS FOR IMPROVING THE RESILIENCE OF THE HEALTHCARE SECTOR

ADEN KLEIN

This report was published as part of the
Center for Long-Term Cybersecurity's 2025 Public Interest
Cybersecurity Research Call for Papers and was presented in June at the
2025 Cyber Civil Defense Summit.

CLTC WHITE PAPER SERIES

Economics of Cyber Policies for Critical Care

MODELS FOR IMPROVING THE RESILIENCE OF THE HEALTHCARE SECTOR

ADEN KLEIN
Premier Inc.

August 2025

CLTC
Center for Long-Term Cybersecurity
UC Berkeley

Contents

Executive Summary

Cybersecurity insurance has become a key component of resilience for the healthcare sector, yet lower-resourced hospitals face gaps in coverage, and caps (i.e., maximum limits) on losses leave the entire sector vulnerable to catastrophic, large-scale cyberattacks. As federal and state lawmakers consider how to better secure hospitals and critical medical services against cyber threats and malicious actors, they have an opportunity to shape policies that would close cyber insurance gaps and bolster the overall cyber maturity of the healthcare sector. However, existing research has not yet established the most effective policy models to close gaps in coverage or fully examined whether cyber insurance actually drives improvement in overall cyber maturity in hospitals.

This paper examines a range of issues related to cyber insurance coverage in U.S. health systems, including whether premiums and loss caps vary based on hospital size and resource level; whether insurance coverage has driven cyber investment and maturity in hospitals; and the cost and efficacy of cyber insurance policies often proposed by industry and policymakers. The author, an employee of healthcare supply-chain company Premier Inc., surveyed ten U.S. health systems representing 116 hospitals and hundreds of clinics and facilities on a standard set of questions, including whether they had cyber insurance coverage, how much they pay in annual premiums, and whether their hospitals had adopted any of a set of cyber best practices in order to obtain coverage. To incentivize responses, hospitals were allowed to remain anonymous, but the survey did contain questions about details such as number of beds, in which states they are located, and special classifications, such as whether they are a rural or critical access hospital.

Survey responses indicated that small and rural hospitals pay the highest cyber insurance premiums per bed by a significant margin. Data also validated the hypothesis that typical loss caps could cover the average cyberattack but are well below the costs of a sector-wide incident. Finally, survey results indicated that most health systems have adopted best practices or invested in better cyber hygiene in order to obtain cyber insurance.

Based on these findings, policymakers should consider using a cyber insurance backstop — a mechanism through which the federal government limits insured losses above a certain threshold — to incentivize increased up-front cyber investment by health systems while simultaneously building resilience against large-scale cyber disruptions. Models of two commonly

proposed backstops — federally subsidized coverage for uninsured hospitals and an extension of terrorism insurance covering catastrophic cyberattacks — reveal challenges with cost-effectiveness and limited ability to actually close market gaps in coverage. However, a pooled insurance program paired with a government backstop would incentivize large health systems to participate in the pool and bolster sector resilience while also bringing down premiums and making coverage more accessible for small hospitals. Furthermore, requiring participants to adopt best cybersecurity practices could be an effective tool for elevating cyber maturity across the healthcare sector. Additionally, such a program would make cyber insurance more affordable, freeing up capital for health systems and hospitals to invest in cybersecurity.

Introduction

Cyber insurance has become a common element of cybersecurity resilience in the healthcare sector; however, market gaps exist for lower-resourced hospitals, and caps on losses leave the entire sector vulnerable to catastrophic, large-scale cyberattacks. Policymakers can address these gaps through backstop programs (i.e., policy mechanisms through which government limits insured losses above a certain threshold) while helping hospitals shift capital from high insurance premiums to investments in prevention and mitigation. This paper examines the healthcare financial and cybersecurity landscape, provides an analysis of survey data on cyber insurance costs and caps, and explores models of cyber insurance backstop policies to help inform policymakers and build resilience in the healthcare sector.

Literature Review

The cybersecurity challenges facing the healthcare sector are immense. Hospitals face unique pressures, both technical and financial, that inform how they invest in cybersecurity mitigation and resilience. The cybersecurity insurance market is similarly complex. This literature review highlights the necessary context for any policy discussion of cybersecurity insurance policy for healthcare, establishing the challenges that further research and data analysis must address.

HEALTHCARE CYBERSECURITY LANDSCAPE

Healthcare faces a complex cybersecurity threat environment that is rife with misconceptions. Cybersecurity policymaking is critical to ensuring continued access to medical services and essential care in American communities, but policy solutions require an evidence-driven understanding of the cybersecurity threats and realities facing the healthcare sector. Cyber risk is not uniform across hospitals and health systems: community health centers, small and rural hospitals, and critical access hospitals face different challenges than do large or multi-state systems.

Cybersecurity is a pressing threat to hospital operations, patient health data, and, most importantly, patient lives. Since 2018, downtime from ransomware attacks has cost U.S. healthcare organizations an average of $1.9 million per day.[1] Healthcare also leads all other sectors in average cost of a data breach, at $9.77 million.[2] Between July 1, 2024 and July 1, 2025, healthcare providers reported 349 hacks compromising the health information of 500 or more individuals to the U.S. Department of Health and Human Services (HHS).[3] Additionally, 92 percent of healthcare organizations experienced at least one cyberattack between April 2023 and April 2024.[4]

These numbers, albeit generalized to describe cyber threats against all healthcare organizations, illustrate the scope of the cyber threat facing hospitals. Incidents are frequent, costly, and nearly impossible to completely prevent.[5] This challenge arises in part from

1 Paul Bischoff, "Ransomware Attacks on U.S. Healthcare Organizations Cost $20.8Bn," *Comparitech*, December 18, 2024.
2 Cost of a data breach 2024, *IBM*, July 2024.
3 U.S. Department of Health and Human Services Office for Civil Rights Breach Portal. "Notice to the Secretary of HHS Breach of Unsecured Protected Health Information."
4 Ponemon Institute. *The 2024 Study on Cyber Insecurity in Healthcare: The Cost and Impact on Patient Safety and Care*, 2024.
5 Reed Abelson and Margot Sanger-Katz. "4 Things You Need to Know About Health Care Cyberattacks." *New York Times*, March 30, 2024.

healthcare organizations' reliance on third-party connected devices and technologies, which leads to a large number of potentially vulnerable endpoints in hospital networks.[6] Healthcare's large volume of sensitive data and unique vulnerability to disruption also make the sector an attractive target to cyber criminals and geopolitical adversaries.[7]

CONSEQUENCES OF DISRUPTION

Disruptions of operations in a healthcare setting can be particularly harmful. A 2024 survey by the Ponemon Institute found that the healthcare sector reported direct patient harms as a result of cyberattacks: 66% of respondents reported patient care disruptions, 57% observed poor patient outcomes, 50% saw medical complications, and 23% reported an increased mortality rate following cyber incidents.[8] The critical role that hospital IT systems play in operations and delivery of care has even led to industry and government operational guidance about ensuring patient safety in the event of a cyberattack.[9]

ECONOMICS OF CYBERSECURITY

Investing in cybersecurity often requires overcoming the reticence of executives asked to devote resources to reducing — but not eliminating — the likelihood of a catastrophic event. Given budgetary pressures, leaders may be reluctant to make the upfront investment needed to minimize potential costs of a cyber incident, particularly when even organizations with well-resourced cybersecurity programs frequently suffer cyberattacks.

One complicating factor in the economics of cybersecurity is the double-hatting of compliance and risk management roles, particularly in healthcare. Frequently, cybersecurity is considered a function of legal and compliance, rather than an operational risk with business continuity implications. This status quo has long placed cybersecurity and privacy together under the compliance umbrella. However, for healthcare organizations particularly, cybersecurity must be considered an operational and patient safety function.

6 John Riggi. "Third-Party Cyber Risk Impacts the Health Care Sector the Most. Here's How to Prepare." *AHA*, August 5, 2024.
7 Department of Health and Human Services. *Healthcare Sector Cybersecurity: Introduction to the Strategy of the U.S. Department of Health and Human Services*, December 2023.
8 Ponemon Institute. *The 2024 Study on Cyber Insecurity in Healthcare: The Cost and Impact on Patient Safety and Care*, 2024.
9 Barbara Pelletreau et al., "Cybersecurity and How to Maintain Patient Safety," *PSNet*. Agency for Healthcare Research and Quality, U.S. Department of Health and Human Services, March 27, 2024.

Hospitals operate on notoriously tight margins. In 2022, the median operating margin for U.S. hospitals was a loss of 3.8%, with an average operating margin of a 13.5% loss.[10] Furthermore, the median operating margin for America's smallest hospitals — those with 25 or fewer beds, which are often located in rural areas — was a loss of 6.1%.[11] In light of these margins, as well as limited cash on hand, hospitals often struggle to allocate money to cybersecurity.

The scope of challenges facing rural and resource-constrained hospitals is especially pronounced. Such hospitals typically serve a disproportionate number of elderly and low-income patients with chronic conditions who are either unable to pay in full for their treatments or rely on low-reimbursement federal programs. They also frequently face both medical and technical workforce shortages and rely on older and less secure technologies, making them vulnerable to digital threats.[12, 13, 14]

A 2025 report by Microsoft found that over 62 percent of rural hospitals face challenges implementing basic email security, multifactor authentication, and network segmentation.[15] Just 43 percent had a timely or regular patching process.[16] Rural hospitals would have to spend between $30,000–$40,000 to mitigate basic cybersecurity risks, for a total cost of $70 million to $75 million across all 2,100 rural hospitals in the U.S.[17] This is a relatively small sum for state and federal lawmakers relative to the value these hospitals provide to their communities, but the costs are often a steep investment for hospitals making difficult decisions about how to keep their doors open.

These gaps in cyber maturity and resource limitations leave many hospitals, particularly rural and under-resourced hospitals, vulnerable to cyberattacks. Low levels of cyber maturity, high operating costs, unreimbursed patient costs, and limited cybersecurity budgets (often trailing comparable critical infrastructure sectors) make the average hospital highly vulnerable to cyberattacks.[18, 19, 20, 21] Furthermore, the high-stakes nature of hospitals' services — where

10 Definitive Healthcare. "A Look at Hospital Operating Margins in the United States." Definitive Healthcare, March 18, 2024.
11 Ibid.
12 Ken Williams. "National Rural Health Association — NRHA: NRHA." National Rural Health Association, April 24, 2025.
13 Health Sector Coordinating Council Cybersecurity Working Group, "On the Edge: Cybersecurity Health of America's Resource-Constrained Health Providers," May 2025.
14 American Hospital Association, "Statement," May 17, 2023.
15 Erin Burchfield, Rachel Clark, and Laura Kreofsky. Rep. *The Rural Hospital Cybersecurity Landscape*. Microsoft, March 3, 2025.
16 Ibid.
17 Ibid.
18 Kroll, "The State of Cyber Defense," 2024.
19 HIMSS, "2024 HIMSS Healthcare Cybersecurity Survey," 2025.
20 American Hospital Association, "The Cost of Caring: Challenges Facing America's Hospitals in 2025," April 2025.
21 IANS and Artico Search, "Compensation and Budget for CISOs in Healthcare: 2025 Benchmark Report," 2025.

downtime can be measured in patient outcomes and mortality, as well as in dollars — makes hospitals a tempting target for ransomware attackers. If hospitals are incapable of restoring operations on their own, they may feel additional pressure to consider ransom payments to quickly recover patient care.

ECONOMICS OF CYBERSECURITY INSURANCE

In response to these challenges, hospitals often turn to cyber insurance as a way to accommodate and account for outsized cyber risk. Rather than risk a catastrophic lump-sum expense that could cripple operations, hospitals pay a predictable annual premium. At the most basic level, actuarially fair insurance is calculated so that the premium payment equals the expected value of a payout. In other words, the actuarially fair premium for one payment period (often a year) is the probability of a cyberattack multiplied by the expected payout.

$$\textbf{Premium} = \textbf{p(event)} \times \textbf{payout(event)}$$ [22]

While insurance premiums seldom match the actuarially fair value, the underlying economics reveal some valuable insights into how insurance interacts with policy and behavior.

A fixed premium limits downside risk for hospitals, as it allows them to budget a fixed expenditure in each payment period. Given the high cost of healthcare cyber incidents, insurance has emerged as a point of emphasis for hospitals seeking to mitigate unpredictable catastrophic losses, such as those resulting from high-cost disasters, including cyberattacks. With cyber incidents affecting 9 out of 10 U.S. hospitals, consideration has shifted to preparing to respond when, not if, disruptions occur.

However, the increased probability of expensive payouts has led to an increase in cyber insurance premiums. The 2024 National Association of Insurance Commissioners report highlighted a steady increase in the number of claims as well as claim severity throughout 2022 and 2023.[23] The Global Insurance Market Index, compiled by insurance company Marsh McLennan, showed corresponding increases in the price of cyber insurance into 2023, followed by a slight cooling

22 Autor, David. "Lecture Note 17: The Market for Risk." 14.03/14.003, *Microeconomic Theory and Public Policy*, Fall 2016. Lecture.

23 National Association of Insurance Commissioners. Memorandum to Members and Interested Regulators of the Property and Casualty Insurance (C) Committee and Innovation Cybersecurity and Technology (H) Committee. "Report on the Cyber Insurance Market," October 15, 2024.

into 2024 as insurance markets became saturated.[24] This may indicate increased maturity, as the market became better at accounting for cyber risk, therefore reducing fluctuation in rates.

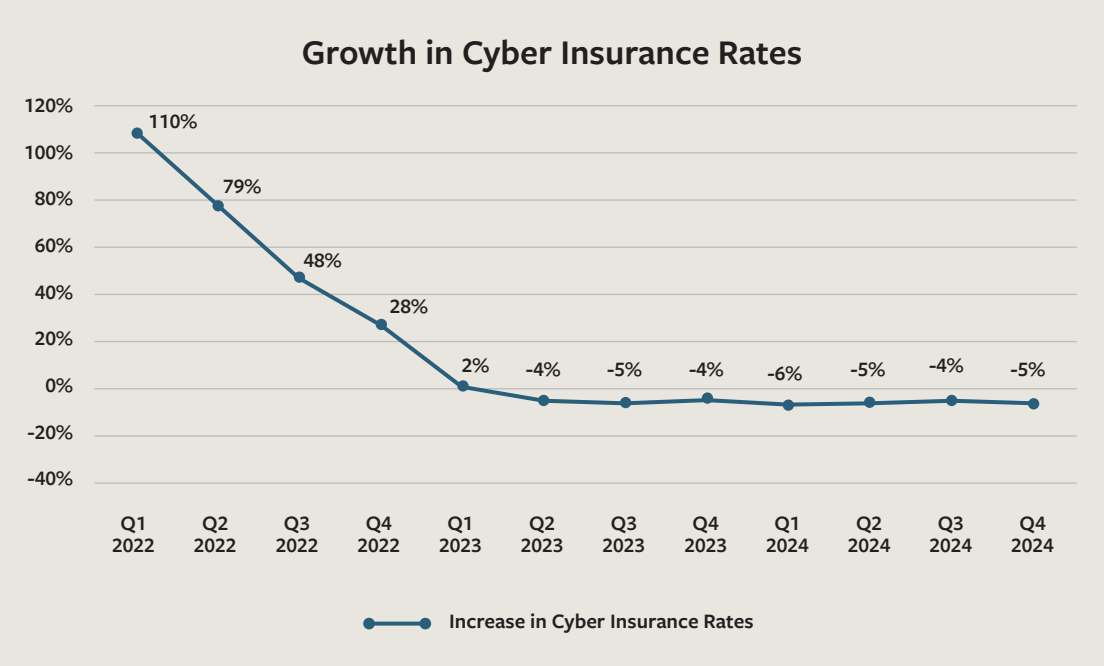


Figure 1: Quarterly data from the Marsh McLennan Global Insurance Market Index reveals a leveling-off in cyber insurance premium growth as the market has matured.

The mechanics of any form of insurance also raises the specter of first-party moral hazard, a situation where an insurance holder feels they are protected and so is less likely to take adequate steps to prevent the insured damages.[25] The economic rationale behind this behavior suggests that the insurance holder has already paid to insure losses and would, therefore, be less incentivized to take on additional expenses to mitigate the risk of the insured event.

However, the nature of cyber risk, particularly in healthcare, minimizes the distortion or externality caused by first-party moral hazard. The damaging effects of a cyber incident extend beyond typical insured losses. Publicly-traded companies lost an average of 7.5% of stock value following data breaches, representing a mean market cap loss of $5.4 billion; healthcare companies underperformed the NASDAQ by 10.6% in the six months following disclosure of a data

24 "Global Insurance Market Index 2025." Marsh McLennan.

25 Pauly, Mark V. "The Economics of Moral Hazard: Comment." *The American Economic Review* 58, no. 3 (1968): 531–37. http://www.jstor.org/stable/1813785.

breach.[26, 27] Furthermore, supply-chain ripple effects can cause up to 26 times the loss for a company in a multi-party breach as compared to single-party breaches.[28] The reputational and operational costs of a cyber incident drastically reduce any moral hazard that cyber insurance might introduce, as plans cannot remedy the reputational damage of a breach. For healthcare, where cyberattacks can put patient safety at risk while introducing immense operational disruption, the incentives to avoid a breach further counteract first-party moral hazard introduced by cyber insurance.

In practice, the cyber insurance industry has taken measures to mitigate moral hazard. Multiple studies have highlighted how cyber insurers require baseline cybersecurity measures to be in place before offering coverage, or they may offer discounted rates for organizations with enhanced cybersecurity postures, largely counteracting any first-party moral hazard that may have been introduced.[29, 30, 31]

26 Keman Huang et al., "The Devastating Business Impacts of a Cyber Breach." *Harvard Business Review*, May 4, 2023.

27 Bischoff, Paul. "How Data Breaches Affect Stock Market Share Prices." Comparitech, June 5, 2024.

28 "A Multi-Party Data Breach Creates 26x the Financial Damage of Single-Party Breach." Help Net Security, September 23, 2021.

29 Jamie MacColl, Jason R C Nurse, and James Sullivan. Publication. *Cyber Insurance and the Cyber Security Challenge*. Royal United Services Institute, June 2021.

30 Daniel W. Woods and Tyler Moore. "Does Insurance Have a Future in Governing Cybersecurity?" *IEEE Security & Privacy*, 2020.

31 Prysock, Mark. Comment Letter to Federal Insurance Office. "Comment Letter on Potential Federal Insurance Response to Catastrophic Cyber Incidents." *Regulations.Gov*, November 14, 2022.

Methodology

To collect evidence on the cost, limitations, and behavior change associated with cyber insurance coverage, the author issued a survey to hospitals and health systems with advocacy, technology, or supply chain relationships with Premier Inc., a technology-driven healthcare improvement company. The survey was distributed through Premier's weekly Washington, D.C. advocacy newsletter, as well as through mailing lists affiliated with member hospital technology committees and working groups. Responses were solicited over a six-week period between late April and early June 2025.

Respondents were asked whether their organizations had cybersecurity insurance; what their annual premiums and coverage caps are, if applicable; and whether they had implemented any of a number of cyber best practices in order to obtain or reduce the cost of cyber insurance. Respondents were also asked questions about their health systems' size (i.e., number of beds), special status (e.g., rural, critical access, etc.), and states in which they operate.

This survey faced a number of limitations. Response rate and selection bias may have affected results, and a longer-term study with a broader base of respondents could lead to additional insights. While respondents were geographically representative and included health systems of various sizes, responses were also limited to health systems with some form of relationship with Premier Inc.

RESULTS & KEY FINDINGS

Key findings include the following, which will be further discussed and contextualized in subsequent sections:

1. All respondents had cybersecurity insurance.
2. Respondents reported annual premiums ranging from $75,000 to $3.2 million, with an average premium of $676 per bed.
3. The average premium per bed was $818 for health systems with fewer than 1000 beds, $369 for systems with 1000 to 2000 beds, and $645 for systems with over 2000 beds. This reinforces anecdotal evidence in the literature that smaller systems pay higher relative premiums for cyber insurance.

4. Caps on insured losses were below $40 million for 80% of respondents. With an average cyberattack carrying a cost approaching $10 million, this indicates that most systems are insured against an average data breach, but not against any more significant or long-lasting incident.
5. Eight of ten respondents reported implementing one or more cybersecurity best practices, with most respondents increasing cybersecurity budgets, hiring or elevating cybersecurity personnel, or implementing best-practice cybersecurity standards and controls.

Analysis and Discussion

HEALTHCARE CYBER INSURANCE LANDSCAPE

Premier Inc.'s survey data provides further insight into how much healthcare facilities pay for cyber insurance, potential gaps in coverage, and the potential for cyber insurance to be a lever for cybersecurity behavior change.

All survey respondents did have some form of cyber insurance. Annual premiums ranged from $75,000 to $3.2M, with an average premium of $676 per bed across all respondents. However, smaller health systems paid a markedly higher premium per bed than medium or large health systems.

NUMBER OF BEDS	AVE PREMIUM PER BED
1–1000	
1001–2000	
2000+	

Figure 2: Each bed represents $200 in per-bed premium costs[32]

The breakdown of insurance caps among respondents provides useful insight into the ability of normal cyber insurance to cover losses from a catastrophic event. Respondents reported on coverage caps ranging from $10M to $100M, but these figures did not directly correlate to the per-bed premium paid by each system.

While there were a few larger systems with a higher cap on insured losses, the majority of systems had coverage that would insure only $10M to $40M in losses. Taken alongside IBM's estimated average cost of $9.77M for a data breach in the healthcare sector, the magnitude of losses illustrates just how vulnerable many systems are to a cyberattack by a sophisticated cybercriminal ransomware gang or state-backed actor.

32 Premier Inc. Survey Data

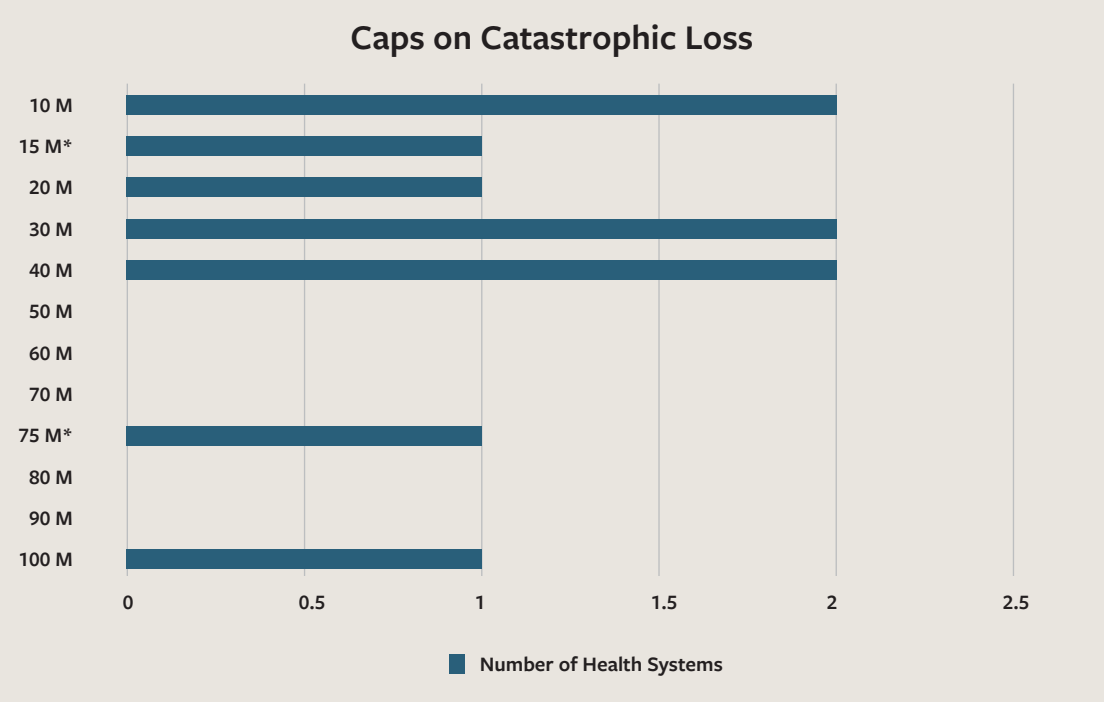


Figure 3: Caps on catastrophic losses cover the costs of average cyberattacks, but not large-scale incidents.[33]

A subset of respondents had cyber insurance plans with explicit exclusions for cyberattacks by state-backed actors. Two of the largest health systems surveyed indicated that their plans contained carve-outs that would limit coverage in the event that a nation-state targeted one of their hospitals. Two other respondents were unsure whether their plan covered state-backed actors, while the remaining systems had provisions that would cover all cyber incidents.

GAPS IN COMMERCIAL CYBER INSURANCE

The cyber threat facing hospitals today is partially driven by sophisticated geopolitical adversaries who are intent on disrupting critical infrastructure or funding criminal enterprises.[34, 35] This creates a coverage paradox: insurers must be able to accommodate the risk profile of the healthcare sector, while hospitals must be able to afford coverage. As the previous section highlighted, cyber insurance can be a useful vehicle to raise the overall cybersecurity profile of the healthcare sector — but market forces and rising costs often make

33 Ibid.
34 Office of the Director of National Intelligence. *Annual Threat Assessment of the U.S. Intelligence Community*, March 2025.
35 Health-ISAC. *2025 Health Sector Cyber Threat Landscape*, February 2025.

insurance less accessible. In 2017, research found that only 30% of healthcare organizations had cyber insurance, a share that reached 78% by 2022.[36, 37]

This leaves three key gaps in the insurance market, each of which complicates the use of cyber insurance as a tool to raise preparedness and resilience in the sector.

1. **The uninsured and uninsurable gap exists for hospitals that are either unable or unwilling to purchase or access cyber insurance, thus assuming all the risk for a significant cyber incident.** As insurers raise requirements and premiums for coverage, hospitals with the lowest levels of preparedness and the tightest margins face the highest cost of coverage, leaving some of America's most critical providers exposed. As the sophistication, frequency, and cost of cyber incidents continue to rise, this gap is poised to grow.

2. **The exclusions gap is a growing challenge that has directly resulted from the evolving threat landscape facing healthcare systems.** With an increase in disruptive cyberattacks undertaken by state-backed adversaries and sophisticated criminal enterprises, there is a growing question of whether traditional commercial cyber insurance plans can — and should — exclude these incidents. This presents a catch-22: either these attacks on critical infrastructure are included, subsequently increasing premiums due to higher potential costs, or they are excluded, leaving hospitals unprotected against the costliest incidents.

3. **The catastrophic loss gap is an ever-present reality of insurance.** There is typically a cap on the costs that an insurance plan will cover following a cyber incident. Yet cyberattacks and data breaches in the healthcare industry are among the most expensive of any sector, and attacks intended to disrupt critical infrastructure are particularly devastating. Loss caps exist to protect insurers from upside risk, and they play an important role in keeping the costs of cyber insurance accessible; however, in practice, the limits on coverage leave America's hospitals on their own in defending themselves against cascading or catastrophic supply chain attacks.

An additional consideration further complicates this paradigm: hospitals operate in a zero-fail environment, where extended downtime has consequences for patients, not just the bottom

36 Soumitra Bhuyan et al. "Transforming Healthcare Cybersecurity from Reactive to Proactive: Current Status and Future Recommendations." *Journal of Medical Systems*, April 02, 2020.

37 Puja Mahendru. "The State of Ransomware in Healthcare in 2022." Sophos, June 01, 2022.

line. This introduces the government as a vested stakeholder, as there is a significant positive externality associated with having more secure and resilient hospitals.

Given this landscape, it is up to policymakers to consider the value and tradeoffs of closing the three gaps in healthcare cybersecurity insurance: the uninsured or uninsurable gap, the exclusions gap, and the catastrophic loss gap.

POLICY OBJECTIVES

State and federal governments have a vested stake in keeping hospitals operational, including by ensuring they can defend their networks against sophisticated threats. Policymakers considering how to achieve this goal can focus on supplementing the risk management tools commercially available, namely cyber insurance, by closing the three gaps identified above. However, as policymakers consider how to protect America's critical healthcare infrastructure, it is crucial to determine which cyber incidents will be covered, what market incentives would be created by the policy program, and what potential factors (e.g., cybersecurity improvements over time that mitigate breach costs) could discount the overall cost of the policy.

Given the gaps in the commercial market, a cyber insurance backstop should be designed to make coverage more accessible for high-risk or under-resourced health systems, cover incidents that could be considered an attack on critical infrastructure, and assume risk beyond catastrophic loss caps to keep hospitals operational in the event of a major cyber incident.

INCENTIVIZING UP-FRONT CYBER INVESTMENT

Cybersecurity risk-sharing — whether across the private sector or through public-private cooperation — makes the healthcare sector stronger. It also offers another lever to raise the general level of cybersecurity preparedness and resilience in the sector without the use of heavy-handed penalties. Given the gaps in coverage, funding, and cyber maturity across the healthcare sector, punitive policy mechanisms — such as Medicare Conditions of Participation — penalize hospitals that are least able to move up the cyber maturity curve, particularly small, rural, or critical access hospitals.

By establishing a baseline set of cybersecurity best practices that hospitals must implement in order to participate in federal cyber insurance backstop programs, the government and

the cyber insurance sector can reduce the probability of minor cyber incidents — therefore reducing costs to the system — while also strengthening resilience in the face of sophisticated nation-state threats.

In order to avoid moral hazard and drive a sector-wide improvement in cyber maturity, it should be assumed that participation in or eligibility for federal funding and support — including cyber insurance backstops — would require healthcare organizations to make a good-faith effort to meet cybersecurity best practices, as defined in statute or regulation. In this manner, public programs would move healthcare along the cyber maturity curve, improving cybersecurity across the sector by shifting dollars from insurance premiums to baseline cyber best practices.

This is a plausible goal, and one that anecdotal evidence suggests may be achieved by using cyber insurance as a mechanism to encourage improved cyber hygiene. In Premier's survey, eight health systems reported that they had changed their cybersecurity practices to obtain cyber insurance coverage or lower premiums, with another reporting that it had already implemented all required best practices and only one claiming that it had made no changes to its cyber hygiene practices.

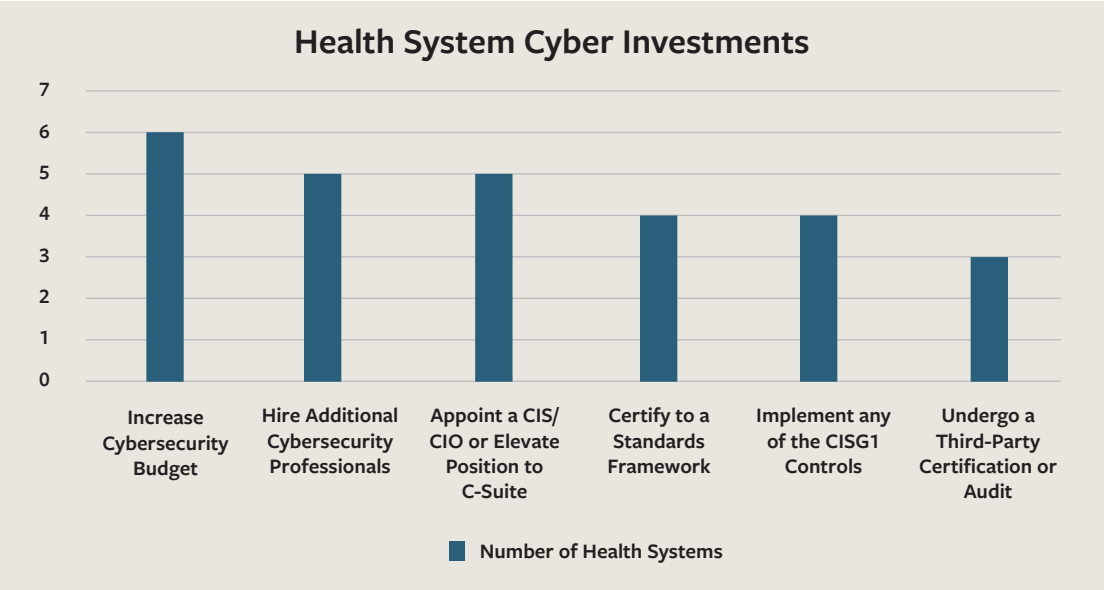


Figure 4: Most of the health systems responding to the survey indicated that they had incorporated cyber best practices to obtain cyber insurance.[38]

38 Premier Inc. Survey Data

Only two of the health systems surveyed did not attribute improved cybersecurity practices to the process of obtaining cyber insurance. As this chart illustrates, those systems that did make additional investments did so across multiple key areas, including obtaining certification to a standards framework, undertaking a third-party audit, hiring cybersecurity professionals, and increasing their cybersecurity budgets. Requiring hospitals to take such measures to be eligible to participate in federal programs could have a significant impact on the overall cybersecurity posture of the healthcare sector.

Government-backed cyber insurance policies will inevitably incur budgetary costs, but any evaluation of those costs should incorporate savings from up-front cyber preparedness and prevention. For reference, a recent Microsoft report found that rural hospitals would need to spend an average of $40,000 each to satisfy basic cyber hygiene best practices, with a total investment of $75M necessary to address gaps across all rural hospitals.[39] The return on these investments across the entire healthcare sector could be significant.

It is reasonable to expect that lower cyber insurance premiums may free additional capital for up-front investments in cyber hygiene, or that regulatory requirements for eligibility for any federal insurance program may require such investments. This could drive savings by reducing either the total cost or the overall probability of a cyberattack for healthcare organizations making these investments.

As shown in Figure 5, a $40,000 investment per hospital across quartiles of the 2100 rural hospitals demonstrates the relatively large potential sector-wide savings from even a 5% decrease in the probability or cost of a cyberattack for any percentage of rural hospitals. In other words, any federal program that mitigated the cost of an average cyber incident — even by as little as 5% — would drive significant savings over the initial investment amount. When evaluating the costs and benefits of potential cybersecurity programs to bolster the most resource-constrained hospitals, it is important to consider potential savings driven by up-front investment.

39 Erin Burchfield, Rachel Clark, and Laura Kreofsky. Rep. *The Rural Hospital Cybersecurity Landscape*. Microsoft, March 3, 2025.

Decrease in Expected Cost of Incident	0%	25%	50%	75%	100%
25%	0	$ 1,261,312,500	$ 2,522,625,000	$ 3,783,937,500	$ 5,045,250,000
20%	0	$ 1,004,850,000	$ 2,009,700,000	$ 3,014,550,000	$ 4,019,400,000
15%	0	$ 748,387,500	$ 1,496,775,000	$ 2,245,162,500	$ 2,993,550,000
10%	0	$ 491,925,000	$ 983,850,000	$ 1,475,775,000	$ 1,967,700,000
5%	0	$ 235,462,500	$ 470,925,000	$ 706,387,500	$ 941,850,000

Percentage of Rural Hospitals Adopting Improvements

Figure 5: At a cost of $40,000 to implement basic cybersecurity practices (as calculated by Microsoft), improvements across quartiles of America's 2100 rural hospitals would drive sector-wide savings on cybersecurity incident response.

If cyber insurers — or federal programs — were to publicly offer discounts on premiums or fees for hospitals taking specific actions to lower the potential cost of an incident, it would pass along savings to the hospital, the insurer, and potentially the federal government in the form of reduced recovery expenses and lower claim values.

Economic Models to Expand Coverage and Improve Cybersecurity Posture

Given the gaps in cyber insurance for healthcare identified in the literature and validated in this survey, there is significant motivation for policymakers to consider a government-backed program to bolster financial resilience in the healthcare sector. This paper presents evidence that up-front investment drives long-term savings in cybersecurity programs, and that hospitals are willing to make such up-front investments in order to secure eligibility for risk-transfer insurance programs.

Taken together, this evidence presents cyber insurance as a compelling mechanism for policymakers to both incentivize desired cybersecurity behaviors and secure the delivery of healthcare for communities.

Below, we evaluate the costs of frequently proposed models for cyber insurance. These models appear regularly in literature and policy discussion, but their actual cost — and their effectiveness in closing gaps in the private insurance market — have not been thoroughly examined.

1. FLOOD INSURANCE MODEL

One model that could help close coverage gaps in cyber insurance for healthcare would be a program similar to the National Flood Insurance Program (NFIP), where the government is an insurer of last resort. Through the NFIP, the government provides flood insurance to homes on floodplains or other high-risk areas that are uninsurable in the private market. Carrying the analogy to a potential cyber insurance backstop, this model would see the government provide subsidized coverage to hospitals that are unable to secure affordable private-market cyber insurance.

However, this program would require a massive expenditure from the federal government for health systems most likely to suffer a cyberattack. Even if coverage was conditioned on a baseline level of cyber hygiene, it is debatable whether this would meaningfully drive down the number of cyberattacks — or the total cost to the sector.

Assuming a structure similar to the NFIP — with actuarially fair full-risk rates for some subset of healthcare organizations, and subsidized rates for others incapable of affording full-risk (with an intention to shift a higher percentage of plan holders to the fair rate over time) — it is possible to model the expected cost for such a program.

Some baseline assumptions used for this model include an estimate that the likelihood of a cyber incident is 0.5 (meaning 50% of organizations experience a material hack in a given year — a low-end value from cybersecurity literature), that the average cost of a healthcare cyberattack is $9.77M (based on data from IBM), and that roughly 78% of hospitals already have cyber insurance and would be unlikely to move to an insurer of last resort if they could get a better rate elsewhere (based on estimates from Sophos).

The model for a subsidized cyber insurance rate begins at 10% of actuarially fair premiums (meaning eligible participants pay only 10% of market rate for cyber insurance coverage), comparable to the rate used by the National Flood Insurance Program. The model also phases out discounts until participants pay full, actuarially fair premiums by the end of a 10-year period, as is the stated intent of the NFIP. This assumes that the federal government would include a phase out and that the hospitals receiving a subsidized rate would be able to elevate their cybersecurity posture to afford an actuarially fair rate by the end of the program's lifetime.

With an insured mix containing 25% of participants paying an actuarially fair rate, the Net Present Value (NPV) of 10 years of modeled expenditures would be approximately $15.9B at a 10% discount rate. In other words, if the federal government subsidizes cyber insurance for 75% of uninsured hospitals, the price tag for the program would be immense.

Year	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8	Year 9	Year 10
Total Cost	$ 6,545,900,000	$ 6,545,900,000	$ 6,545,900,000	$ 6,545,900,000	$ 6,545,900,000	$ 6,545,900,000	$ 6,545,900,000	$ 6,545,900,000	$ 6,545,900,000	$ 6,545,900,000
Total Premium	$ 2,127,417,500	$ 2,618,360,000	$ 3,109,302,500	$ 3,600,245,000	$ 4,091,187,500	$ 4,582,130,000	$ 5,073,072,500	$ 5,564,015,000	$ 6,054,957,500	$ 6,545,900,000
Deficit	$ 4,418,482,500	$ 3,927,540,000	$ 3,436,597,500	$ 2,945,655,000	$ 2,454,712,500	$ 1,963,770,000	$ 1,472,827,500	$ 981,885,000	$ 490,942,500	$ -

With an insured mix containing 50% of participants paying an actuarially fair rate, the NPV of 10 years of modeled expenditures would be approximately $10.6B at a 10% discount rate.

Year	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8	Year 9	Year 10
Total Cost	$ 6,545,900,000	$ 6,545,900,000	$ 6,545,900,000	$ 6,545,900,000	$ 6,545,900,000	$ 6,545,900,000	$ 6,545,900,000	$ 6,545,900,000	$ 6,545,900,000	$ 6,545,900,000
Total Premium	$ 3,600,245,000	$ 3,927,540,000	$ 4,254,835,000	$ 4,582,130,000	$ 4,909,425,000	$ 5,236,720,000	$ 5,564,015,000	$ 5,891,310,000	$ 6,218,605,000	$ 6,545,900,000
Deficit	$ 2,945,655,000	$ 2,618,360,000	$ 2,291,065,000	$ 1,963,770,000	$ 1,636,475,000	$ 1,309,180,000	$ 981,885,000	$ 654,590,000	$ 327,295,000	$ -

With an insured mix containing 75% of participants paying an actuarially fair rate, the NPV of 10 years of modeled expenditures would be approximately $5.3B at a 10% discount rate.

Year	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8	Year 9	Year 10
Total Cost	$ 6,545,900,000	$ 6,545,900,000	$ 6,545,900,000	$ 6,545,900,000	$ 6,545,900,000	$ 6,545,900,000	$ 6,545,900,000	$ 6,545,900,000	$ 6,545,900,000	$ 6,545,900,000
Total Premium	$ 5,073,072,500	$ 5,236,720,000	$ 5,400,367,500	$ 5,564,015,000	$ 5,727,662,500	$ 5,891,310,000	$ 6,054,957,500	$ 6,218,605,000	$ 6,382,252,500	$ 6,545,900,000
Deficit	$ 1,472,827,500	$ 1,309,180,000	$ 1,145,532,500	$ 981,885,000	$ 818,237,500	$ 654,590,000	$ 490,942,500	$ 327,295,000	$ 163,647,500	$ -

This model — under any set of assumptions — would likely end up costing the federal government a substantial amount, as it is both in theory and practice simply subsidizing cyber insurance for those unable to privately obtain it at a reasonable rate.

It is also important to note that the likelihood of a cyber incident for this population of hospitals, including a large number of rural or critical access hospitals with a weaker security posture, is likely to be far higher than 0.5. As discussed in the background section, some reports indicate that over 90% of hospitals experience a cyberattack in a given year.

To emphasize the range of potential costs to the government under this model, the sensitivity analysis in Figure 6 illustrates the difference between net costs and net premiums in Year 1 of the program for a range of different incident likelihoods and insured mixes. Given a higher estimated likelihood of a cyber incident and a higher share of subsidized premiums, the cost in a given year balloons — as would be expected.

To place this model in context, it is important to understand that a flood insurance model for cybersecurity insurance in healthcare, even one intended to phase out the number of hospitals receiving a subsidized rate, would be a direct expenditure of taxpayer dollars. It is highly unlikely that this type of program would ever become law, but the model is illustrative of why prioritizing 100% cyber insurance coverage may not be the best designing principle for a federal backstop.

Incident Probability	25%	50%	75%
90%	$2,782,007,500.00	$5,564,015,000.00	$8,346,022,500.00
75%	$2,291,065,000.00	$4,582,130,000.00	$6,873,195,000.00
66%	$1,996,499,500.00	$3,992,999,000.00	$5,989,498,500.00
50%	$1,472,827,500.00	$2,945,655,000.00	$4,418,482,500.00
33%	$916,426,000.00	$1,832,852,000.00	$2,749,278,000.00
25%	$654,590,000.00	$1,309,180,000.00	$1,963,770,000.00

Percent of Insured with Subsidized Premiums

Figure 6: A sensitivity analysis depicting how cybersecurity incident probability represents immense upside risk for a cyber insurance backstop modeled on the NFIP: the higher the percentage of program participants receiving a subsidized rate in a given year, the more risk the government would assume.

While this model would help to close the uninsured/uninsurable gap, it does not address the catastrophic loss gap. While there can be reasonable debate over the value of subsidizing cyber insurance for healthcare critical infrastructure, particularly coupled with policies to elevate cyber maturity and phase out subsidies over time, advocates for this model are addressing only part of the challenge facing the sector.

2. TERRORISM INSURANCE MODEL

The most frequently discussed mechanism for making cyber insurance more accessible to hospitals is an expansion of the Terrorism Risk Insurance Program (TRIP) to include cyber insurance, an idea that has surfaced in academic literature, public comments, and Congressional legislative debates.

The model provides a public and private loss-sharing mechanism that covers acts of terrorism, as certified by the Secretary of the Treasury, resulting in over $200 million in insured losses. Once insured losses exceed $200 million, individual insurers must cover an amount equal to 20% of their prior year premiums — a figure that will vary by insurer size. After the deductible is met, the federal government will pay 80% of insurer losses up to $100 billion in aggregate losses. This model serves a dual purpose: it protects the private insurance market and insured entities from catastrophic loss while also limiting potential insurer payouts for malicious attacks, thereby keeping coverage relatively more affordable and accessible.

In its present form, TRIP does not include stand-alone cyber insurance. Despite legislative and legal debate, not to mention a policy purpose closely aligned with the challenge facing healthcare organizations today, definitions of "acts of terror" have generally been interpreted to exclude coverage for critical infrastructure — including healthcare — that frequently comes under attack by state-backed actors.

When TRIP comes up for renewal in 2027, Congress could consider extending the provision to include cyber insurance for critical infrastructure. In order to model the cost of this program for the healthcare sector specifically, it is necessary to first determine what incidents could be eligible under existing statutes and how they would be defined.

Current statute requires that the cyber incident be qualified as an act of terror. Using legislative discussion from the 118th Congress, it is possible to create a general approximation of the criteria that might be used to make such a designation. The Senate Intelligence Committee,

in its version of the FY25 Intelligence Authorization Act, included language to designate a list of ransomware organizations as hostile foreign actors and establish a process to designate certain nations as state sponsors of ransomware.[40] Given challenges with maintaining a list of leading ransomware groups, which frequently dissolve and reform under new names, it is preferable to use the state sponsor approach to determine whether a cyberattack is an act of terror. The 2025 Annual Threat Assessment of the U.S. Intelligence Community specifically lists China, Russia, Iran, and North Korea as cyber adversaries, so this model assumes that incidents attributable to organizations affiliated with these states would be eligible to be declared acts of terror.[41]

A review of the largest cyberattacks in healthcare over the past decade reveals that very few reached the aggregate cost or state attribution thresholds to be eligible for TRIP.

Incident	Responsible Actor	Year	Cost
Change Healthcare	ALPHV-BlackCat — Russia	2024	~$3.09B
Ascension Health	Black Basta - Russia	2024	~$1.3B
Texas Tech Health Sciences Center	Interlock — N/A	2024	~$2M
McLaren	INC Ransom — N/A	2024	~$100M
Acadian Ambulance Service	Daixan Team — N/A	2024	$7M ransom requested
McLaren	ALPHV-BlackCat — Russia	2023	Unreported
HCA Healthcare	Unknown	2023	Unreported
PJ&A	Unknown	2023	~$12.8M
Regal Medical Group	Unknown	2023	Unreported
Tampa General Hospital	Snatch/Nokoyawa Groups — N/A	2023	Unreported, but $6.8M settlement
CommonSpirit	Unknown	2022	~$160M
University Medical Center Southern Nevada	REvil — Russia	2021	~$12M Ransom
UVM Medical Center	Individual — Financially Motivated	2020	~$65M
LabCorp	Unknown	2019	$24M
Anthem	China	2015	~$260M
Premera Blue Cross	China — alleged	2015	$84M in settlements alone
Community Health Systems	China	2014	$75-150M

Figure 7: Data compiled by author illustrating the largest cyber incidents by cost affecting healthcare over the past decade. See Annex 1 for attribution and citations.

Even extending the net to the largest cyberattacks in the U.S. back to 2008, roughly half would likely have been excluded from TRIP under assumed criteria — either for lack of dollar damages or lack of state attribution.

40 Intelligence Authorization Act for Fiscal Year 2025, S.4443, 118th Cong. (2024).

41 Office of the Director of National Intelligence. *Annual Threat Assessment of the U.S. Intelligence Community*, March 2025.

Incident	Responsible Actor	Year	Cost
NVIDIA	Lapsus$ - Non-State	2022	Unknown
Colonial Pipeline	DarkSide — Russia	2021	~$4.4M Ransom + losses
Microsoft Exchange Server	Hafnium — China	2021	Unknown
SolarWinds	APT29 — Russia	2020	~$90B Insured Losses
Capital One	Non-State	2019	~$300M
Equifax	China	2017	~$1.38B
NotPetya	Russia	2017	~$10B
WannaCry	Lazarus — North Korea	2017	~$4B
Yahoo	Russia	2013-2014	~$470M
Target	Unknown	2013	~$252M
Sony/PlayStation	Non-State	2011	$171M
Heartland Payment Systems	Non-State	2008	~$200M

Figure 8: Data compiled by author illustrating the largest cyber incidents by cost in the U.S. since 2008. See Annex 1 for attribution and citations.

More incidents may be eligible if an expansion of TRIP included a way to designate non-state ransomware as an act of terror, but the real intent — and value — of the terrorism insurance model would be to protect U.S. critical infrastructure in the case of a malicious supply chain attack with sector-wide effects and possible spillover to interdependent sectors.

Extending TRIP to cover stand-alone cyber insurance would provide assurance that a large-scale cyberattack on the U.S. healthcare sector would not lead to a failure of the cyber insurance market or to unrecoverable losses for health systems. The U.S. government would be expected to intervene or provide support in the event of a catastrophic cyberattack by a foreign power — but no established mechanism to aid in cyberattack recovery exists today. Much as the supplemental appropriations process necessary after large natural disasters can delay essential aid and recovery efforts, the lack of a clear cyber backstop poses a clear and present threat to healthcare and other critical infrastructure sectors. It is reasonable to argue that TRIP was initially designed to provide just such a mechanism to backstop catastrophic attacks on U.S. industries.

While limiting catastrophic loss from cyberattacks is a legitimate policy objective, it is also clear that this program would not meaningfully close the undercoverage gap that exists for small and rural hospitals, as the total cost threshold would seldom be met by cyberattacks on individual small hospitals, assuming those hospitals are even insured in the first place.

Over the past decade, eligible healthcare cyber incidents — those perpetuated by state-backed groups and totaling over $200M in damages — would have cost TRIP approximately $1.8B, which the Treasury secretary would be authorized to recoup from insurers through surcharges

on insurance plans. This cost is almost entirely attributable to cyberattacks on Ascension and Change Healthcare in 2024.

This model is constructed using the same eligibility criteria and backstop calculations described in the previous section, with an aggregate premiums value obtained from the 2024 NAIC report. Eligible events are drawn from the healthcare cyberattacks table from the past decade, with only those events included that were attributable to a state-backed group and totaled over $200M in reported losses. Per TRIP statutory methodology, the private sector is responsible for $200M, as well as the value of 20% of aggregate cyber insurance premiums. Federal costs are obtained by taking 80% of the total cost less the private-sector share. A Net Present Value calculation for the 10-year period from 2015 to 2024 assumes a conservative 10% discount rate, arriving at a total NPV of $1.8B in federal expenditures.

Year	1	2	3	4	5	6	7	8	9	10
Expenditures	$ 260,000,000.00	0	0	0	0	0	0	0	0	$ 4,390,000,000.00
Federal Cost	$ -	0	0	0	0	0	0	0	0	$ 2,222,000,000.00

While this model would help to address the market-destroying aftermath of a catastrophic state-backed cyberattack by closing the catastrophic loss gap — and, to a certain extent, the exclusions gap — it would have only incidental effects on the uninsured/uninsurable gap. Although the average healthcare cyberattack costs $9.77M, incidents with an aggregate cost exceeding $200M are few and far between — and do not usually result from cyberattacks on small or rural hospitals.

3. PUBLIC-PRIVATE POOLED INSURANCE MODEL

Another option has recently emerged as a viable mechanism to close some of the coverage and catastrophic loss gaps in the cyber insurance market: insurance pools. A 2025 report from Pool Re outlined a handful of potential models for such pools, as well as an argument for the role that a catastrophic loss backstop would serve in a cyber-dependent global economy.[42]

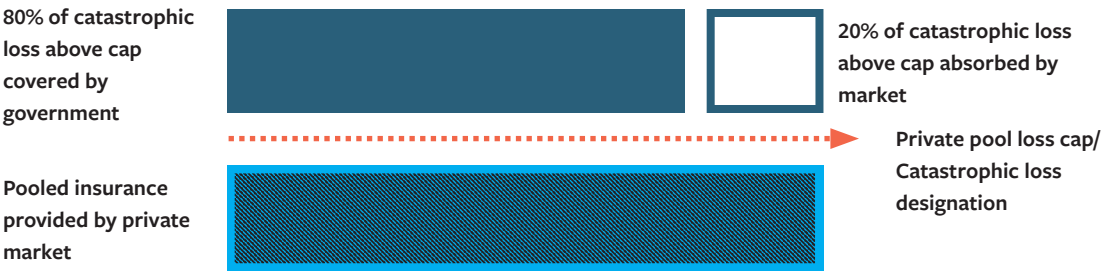
The pooled insurance model is a market-driven mechanism that does not require up-front government investment and aims to reduce premiums for high-risk hospitals that are lower on the cyber maturity curve. Such a model could help to close the uninsured gap, but only with an

42 Oliver Brew and Brian Lewis. "Cyber Risk Pools and Public Private Partnerships: Time to Dive In?" Lockton Reinsurance, 2024.

appropriate incentive structure for large, cyber-secure hospitals to participate. Pooled insurance assesses population risk and redistributes some of the cost of insuring high-risk entities to low-risk entities. This would require larger health systems with more robust cybersecurity hygiene and better risk profiles to pay higher premiums to absorb the risk from more vulnerable hospitals.

One potential incentive — which could also address the catastrophic loss and exemption gaps — is a federal catastrophic loss backstop, similar to the TRIP program. By limiting participation in the backstop to participants in pooled insurance plans, the federal government could create an incentive for the best-resourced health systems that are most likely to experience a catastrophic loss to pay an additional premium — essentially raising their loss cap. Catastrophic loss reimbursement through a pooled plan would also incentivize insurers to set premiums at accessible levels to expand pool participation.

Under this model, a pooled rate would cover cyber losses up to a certain catastrophic loss cap, after which the federal government would provide a backstop equal to 80% of losses up to an established limit. This would essentially create a TRIP-style backstop that is only available to healthcare organizations participating in the pool, exchanging insurance against catastrophic loss for participation in a model that would make cyber insurance available to less well-resourced hospitals.



This model, properly tuned, could achieve many of the coverage objectives of a flood insurance or subsidized insurance model without anywhere near the same level of government expenditure. It would also help to close the catastrophic loss gap and establish a clear mechanism for funding and response in the event of a large-scale cyberattack on U.S. healthcare infrastructure. Furthermore, such a program's cost would not exceed that of TRIP and could ultimately drive savings across the cyber insurance landscape.

Policy Implications

Policymakers should consider three key conclusions from the results of this analysis:

1. A cyber insurance backstop should prioritize closing coverage gaps for lower-resourced hospitals and providing insurance in the event of catastrophic supply-chain or sector-wide cyberattacks.

2. Eligibility for cyber insurance drives investments in cybersecurity maturity. By requiring such investments and the implementation of baseline cybersecurity controls as a condition of eligibility for a federal backstop or resilience program, policymakers can drive overall improvements in cybersecurity in the healthcare sector.

3. Policymakers should consider models, such as a pooled insurance model with a federal backstop, that align incentives for poorly resourced hospitals and large health systems.

Conclusion

Hospitals face a challenging cybersecurity landscape: up-front investment is costly, particularly for lower-resourced hospitals, while gaps in the cyber insurance market leave many hospitals exposed to losses following cyberattacks by sophisticated threats. Where hospitals are able to get cyber insurance coverage, small hospitals pay significantly higher premiums per bed than larger hospitals. Generally, caps on losses also fail to provide full coverage for a large-scale cyberattack. However, cyber insurance coverage has provided a mechanism to drive hospital investments in better cyber hygiene and controls. Ultimately, policymakers can ensure that healthcare providers find collaborative advantages in the face of a rising tide of cyber threats — but only if incentives are realigned to free up budget dollars for up-front investment and reward risk-sharing models that make resilience more affordable.

About the Author

Aden Klein is a Legislative and Policy Analyst in Premier's Washington, D.C. office, where he contributes to Premier's advocacy work on technology policy issues. He leads Premier's cybersecurity advocacy portfolio and handles issues across privacy, data, and AI policy. Aden is a recent graduate of Duke University and an alumnus of Duke's Technology Policy Lab, where he contributed to cybersecurity and privacy research and advocacy. He has also spent time working in state and federal politics, as well as consulted with the OECD on semiconductor supply chain development.

Acknowledgments

I would like to thank Premier Inc.'s advocacy team for their input and insights during the drafting of this paper — particularly Soumi Saha and Mason Ingram. A heartfelt thanks also to Ben Schwering, Premier's CIO, for expert insights.

I would also like to thank Jen Ellis and Davis Hake for providing background information on the cyber insurance and ransomware landscape.

Finally, I am deeply grateful for the direction and support of the Center for Long-Term Cybersecurity team during the drafting of this paper, particularly Shannon Pierson and Chuck Kapelke.

References

Abelson, Reed, and Margot Sanger-Katz. "4 Things You Need to Know About Health Care Cyberattacks." *New York Times*, March 30, 2024, sec. A. https://www.nytimes.com/2024/03/29/health/cyber-attack-unitedhealth-hospital-patients.html.

American Hospital Association, "The Cost of Caring: Challenges Facing America's Hospitals in 2025," April 2025. https://www.aha.org/system/files/media/file/2025/04/The-Cost-of-Caring-April-2025.pdf.

American Hospital Association, "Statement of the American Hospital Association for the Committee on Finance Subcommittee on Health Care of the U.S. Senate 'Improving Health Care Access in Rural Communities: Obstacles and Opportunities'," May 17, 2023. https://www.aha.org/system/files/media/file/2023/05/aha-statement-to-senate-finance-committee-subcommittee-on-health-on-improving-rural-health-care-access-5-17-2023.pdf.

Autor, David. "Lecture Note 17: The Market for Risk." *14.03/14.003, Microeconomic Theory and Public Policy, Fall 2016*. Lecture, n.d. https://ocw.mit.edu/courses/14-03-microeconomic-theory-and-public-policy-fall-2016/52fb22da4549f122296baafbf35a512d_MIT14_03F16_lec17.pdf.

Bhuyan, Soumitra Sudip, Umar Y Kabir, Jessica M. Escareno, Kenya Ector, Sandeep Palakodeti, David Wyant, Sajeesh Kumar, et al. "Transforming Healthcare Cybersecurity from Reactive to Proactive: Current Status and Future Recommendations." *Journal of Medical Systems* 44, no. 5 (April 2, 2020). https://doi.org/10.1007/s10916-019-1507-y.

Bischoff, Paul. "How Data Breaches Affect Stock Market Share Prices." Comparitech, June 5, 2024. https://www.comparitech.com/blog/information-security/data-breach-share-price-analysis/.

Bischoff, Paul. "Ransomware Attacks on U.S. Healthcare Organizations Cost $20.8Bn." Comparitech, December 18, 2024. https://www.comparitech.com/studies/ransomware-studies/ransomware-attacks-hospitals-data/.

Burchfield, Erin, Rachel Clark, and Laura Kreofsky. Rep. *The Rural Hospital Cybersecurity Landscape*. Microsoft, March 3, 2025. https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/TSI-Rural-Hospital-Cybersecurity-Landscape-Report-2025.pdf.

Brew, Oliver, and Brian Lewis. "Cyber Risk Pools and Public Private Partnerships: Time to Dive In?" Lockton Reinsurance, 2024. https://downloads.ctfassets.net/zr7mmeciv2ps/54J7FoRCbaWGhGrxmWbxxI/3328b4e72cf925e06a92ad32fb25fcc9/CyberRiskPoolsReportfeb25.pdf.

Cost of a data breach 2024, *IBM*, July 2024. https://www.ibm.com/reports/data-breach.

Definitive Healthcare. "A Look at Hospital Operating Margins in the United States." Definitive Healthcare, March 18, 2024. https://www.definitivehc.com/resources/healthcare-insights/hospital-operating-margins-united-states.

Department of Health and Human Services. *Healthcare Sector Cybersecurity: Introduction to the Strategy of the U.S. Department of Health and Human Services*, December 2023. https://aspr.hhs.gov/cyber/Documents/Health-Care-Sector-Cybersecurity-Dec2023-508.pdf.

"Global Insurance Market Index 2025." Marsh McLennan. Accessed May 27, 2025. https://www.marsh.com/en/services/international-placement-services/insights/global-insurance-market-index.html.

Health-ISAC. *2025 Health Sector Cyber Threat Landscape*, February 2025. https://health-isac.org/wp-content/uploads/Health-ISAC_2025-Annual-Threat-Report.pdf.

Health Sector Coordinating Council Cybersecurity Working Group, "On the Edge: Cybersecurity Health of America's Resource-Constrained Health Providers," May 2025. https://healthsectorcouncil.org/wp-content/uploads/2025/05/On-the-Edge-RESOURCE-CONSTRAINED-HEALTHCARE-CYBERSECURITY.pdf.

HIMSS, "2024 HIMSS Healthcare Cybersecurity Survey," 2025. https://cdn.sanity.io/files/sq08bpt9/production/4f1c1968050411b8bf9335a187301881f9153b9f.pdf.

Huang, Keman, Xiaoqing Wang, William Wei, and Stuart Madnick. "The Devastating Business Impacts of a Cyber Breach." Harvard Business Review, May 4, 2023. https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach.

IANS and Artico Search, "Compensation and Budget for CISOs in Healthcare: 2025 Benchmark Report," 2025. https://sf-cdn.iansresearch.com/sitefinity/docs/default-source/reports/2025-healthcare-comp-and-budget-report.pdf?sfvrsn=89991025_1.

Intelligence Authorization Act for Fiscal Year 2025, S.4443, 118th Cong. (2024).

Kroll, "The State of Cyber Defense," 2024. https://media-cdn.kroll.com/jssmedia/kroll/pdfs/publications/state-cyber-defense-healthcare-report.pdf.

MacColl, Jamie, Jason R C Nurse, and James Sullivan. Publication. *Cyber Insurance and the Cyber Security Challenge*. Royal United Services Institute, June 2021. https://static.rusi.org/247-op-cyber-insurance-fwv.pdf.

Mahendru, Puja. "The State of Ransomware in Healthcare in 2022." Sophos, June 01, 2022. https://news.sophos.com/en-us/2022/06/01/the-state-of-ransomware-in-healthcare-2022/.

"A Multi-Party Data Breach Creates 26x the Financial Damage of Single-Party Breach." Help Net Security, September 23, 2021. https://www.helpnetsecurity.com/2021/09/27/multi-party-data-breach/.

National Association of Insurance Commissioners. Memorandum to Members and Interested Regulators of the Property and Casualty Insurance (C) Committee and Innovation

Cybersecurity and Technology (H) Committee. "Report on the Cyber Insurance Market," October 15, 2024.

Office of the Director of National Intelligence. *Annual Threat Assessment of the U.S. Intelligence Community*, March 2025. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf.

Pauly, Mark V. "The Economics of Moral Hazard: Comment." *The American Economic Review* 58, no. 3 (1968): 531–37. http://www.jstor.org/stable/1813785.

Pelletreau, Barbara, John Riggi, Bryan Gale, and Sarah Mossburg, "Cybersecurity and How to Maintain Patient Safety," *PSNet*. Agency for Healthcare Research and Quality, US Department of Health and Human Services, March 27, 2024. https://psnet.ahrq.gov/perspective/cybersecurity-and-how-maintain-patient-safety.

Ponemon Institute. *The 2024 Study on Cyber Insecurity in Healthcare: The Cost and Impact on Patient Safety and Care*, 2024.

Prysock, Mark. Comment Letter to Federal Insurance Office. "Comment Letter on Potential Federal Insurance Response to Catastrophic Cyber Incidents." *Regulations.Gov*, November 14, 2022. https://www.regulations.gov/comment/TREAS-DO-2022-0019-0018.

Riggi, John. "Third-Party Cyber Risk Impacts the Health Care Sector the Most. Here's How to Prepare." *AHA*, August 5, 2024. https://www.aha.org/news/aha-cyber-intel/2024-08-05-third-party-cyber-risk-impacts-health-care-sector-most-heres-how-prepare.

U.S. Department of Health and Human Services Office for Civil Rights Breach Portal. "Notice to the Secretary of HHS Breach of Unsecured Protected Health Information." U.S. Department of Health & Human Services – Office for Civil Rights. Accessed May 27, 2025. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

Williams, Ken. "National Rural Health Association – NRHA: NRHA." National Rural Health Association, April 24, 2025. https://www.ruralhealth.us/blogs/2025/04/strengthening-cybersecurity-for-patient-care-and-data-protection.

Woods, Daniel W., and Tyler Moore. "Does Insurance Have a Future in Governing Cybersecurity?" *IEEE Security & Privacy* 18, no. 1 (2020): 21–27. https://doi.org/10.1109/msec.2019.2935702.


CLTC
Center for Long-Term
Cybersecurity
UC Berkeley